Design and Implementation of a Secure Corporate Network System using Cisco Packet Tracer

Alishba Mumtaz[1], Maheen Siraj[2], Maria Munawwar[3], Nensi Batra[4]
Software Engineering Department, *NED University of Engineering and Technology*, Karachi, Pakistan
[1]alishbaamumtaz@gmail.com, [2]maheensiraj018@gmail.com, [3]mariakhan5028@gmail.com, [4]nensibatra1122@gmail.com

***Abstract*—In the modern digital era, ensuring robust security within corporate networks is critical to protect against both internal and external threats. This project proposes a comprehensive strategy to fortify network security by designing a segmented network architecture that strategically allocates servers and security zones. By dividing the network into external, internal, and demilitarized zones (DMZ), the project ensures enhanced protection for vital services. Critical infrastructure servers such as Active Directory (AD), DHCP, DNS, and Radius are securely housed within the internal zone. Conversely, services requiring external access, including FTP, web, email, applications, and NAS storage, are positioned in the DMZ, equipped for secure connectivity through firewalls. This systematic deployment not only secures sensitive components but also maintains network integrity and operational continuity. The project provides a detailed framework for organizations aiming to develop secure, resilient, and efficient network systems, addressing essential elements of network design, security posture, and overall functionality.**

***Keywords*—Network Security, Corporate Networks, Segmented Network Architecture, Security Zones, Demilitarized Zone (DMZ), Active Directory (AD), DHCP, DNS, Radius, Firewall, Secure Connectivity, Network Integrity, Network Design, Cisco Packet Tracer,**

I. Introduction

In today's dynamic business environment, the design and implementation of a secure and efficient network system are crucial for organizational success. Companies increasingly rely on digital infrastructure to support their operations, highlighting the need for robust, scalable, and secure network solutions. This project addresses these needs by proposing a comprehensive approach to network design that incorporates key elements of security and efficiency, leveraging the capabilities of Cisco Packet Tracer.

In developing this network infrastructure, our focus is on meeting the specific needs of a dynamic organization poised for growth. The targeted organization comprises a workforce of approximately 600 members spread across three floors, each housing two distinct departments (Robinson, 2021). This distributed setup necessitates a robust network design capable of supporting seamless communication and collaboration among departments and ensuring secure connectivity for all devices.

This report outlines a systematic framework developed for the creation and deployment of a resilient network infrastructure, rooted in fundamental network design principles. It details the essential configurations, including SSH setup, VLAN assignments, EtherChannel configuration, subnetting, and IP addressing. By focusing on these core components, the project ensures a strong foundation for the network's functionality and security.

Key features of this network design include the implementation of HSRP (Hot Standby Router Protocol) for gateway redundancy, Inter-VLAN routing for efficient communication between network segments, DHCP server configuration for dynamic IP address allocation, and OSPF (Open Shortest Path First) routing protocol for optimized data routing. These elements are meticulously configured to guarantee high availability, seamless communication, and efficient resource management within the network. [1] [2]

The project also integrates stringent firewall security measures, replacing traditional routers with Cisco ASA 5506 firewalls to create a zone-based security model. This model divides the network into distinct zones: the DMZ (Demilitarized Zone) for public-facing servers, the Inside Zone for internal users and sensitive resources, and the Outside Zone for external clients. This approach enhances the network's defense mechanisms, providing robust protection against potential threats. Similar to how the DMZ is utilized in the Korean government's Metaverse platform for maintaining strict access control and enhancing security in sensitive areas [3], the implementation of the Cisco ASA 5506 firewalls ensures that different segments of the corporate network are securely isolated and protected.

Additionally, the network design includes wireless configurations using lightweight access points managed by a Wireless LAN Controller. This change enhances the network's flexibility and manageability, allowing for seamless connectivity of wireless devices such as laptops, smartphones, and tablets. Similar to the deployment of intelligent surfaces in advanced wireless networks to optimize performance and flexibility [4], the use of Wireless LAN Controllers ensures robust and adaptable wireless network management. The implementation phase involves deploying critical hardware components, including ISP routers, firewalls, multilayer switches, and departmental switches. Each component is configured to ensure optimal performance and reliability. Devices such as PCs, printers, VoIP phones, and wireless devices are integrated into the network, with specific configurations to ensure their proper functioning. Rigorous verification and testing procedures are conducted to validate the reliability and effectiveness of the network design. These procedures ensure that the network meets the high standards required for modern organizational operations,

providing a secure, efficient, and scalable solution. This report offers a comprehensive framework for organizations aiming to establish secure and efficient network systems. By addressing critical aspects of network design, security, and functionality, it serves as a valuable resource for network administrators and IT professionals seeking to enhance their network infrastructure.

II. Literature Review

This section reviews the literature on network security, segmented network architecture, DMZ implementation, protection of critical infrastructure, and the use of Cisco Packet Tracer for network simulations.

A. Network Security

In order to protect data availability, confidentiality, and integrity, network security is a crucial component of business network design. It includes safeguards against online attacks and guarantees safe data transfer. [5]

To show the applicability of network security measures in a controlled setting, Krishanu Kundu et al. (2023) investigated the simulation of Local Area Networks (LAN) using Cisco Packet Tracer. The significance of IP packet switching and data flow demonstration for network design and troubleshooting was emphasized by their study. [6]

Exsyal Syahputra et al. (2023) also used Cisco Packet Tracer to create an Internet of Things-based home security system. Their study showed how security measures in smart home environments can be improved by using network simulation tools. [7]

Additionally, the use of Cisco Packet Tracer for smart room automation was covered by Bharat Ratnala et al. (2023), with an emphasis on the integration of IoT devices and enhancing efficiency and safety in office settings. In creating safe and effective automation systems, network simulations play a crucial roleBuilding Smart Room Using Cisco Packet Tracer Simulator, as this research demonstrated. [8]

Table I highlights the studies that simulate network security measures using Cisco Packet Tracer as a tool.

TABLE I
Key Aspects of Network Security Simulation

Aspect	Description	Reference
IP Packet Switching	Demonstrates data flow between network nodes, enhancing understanding of packet transmission and network behavior.	Kundu et al. (2023). Simulating a Local Area Network with Cisco Packet Tracer: A Comprehensive IP Packet Switching Network Demonstration.
Home Security Systems	Uses IoT and Cisco Packet Tracer to design and test automated home security measures.	Syahputra et al. (2023). Perancangan Model Simulasi Sistem Keamanan Rumah Berkonsep Internet of Things Berbasis Cisco Packet Tracer.
Smart Room Automation	Integrates IoT devices for automating office environments, improving safety and efficiency.	Ratnala et al. (2023). Designing Smart Room Using Cisco Packet Tracer Simulator.
Network Design and Troubleshooting	Provides a practical platform for planning and testing network configurations before physical implementation.	Kundu et al. (2023). Simulating a Local Area Network with Cisco Packet Tracer: A Comprehensive IP Packet Switching Network Demonstration.
IoT Integration	Improves automation and security in smart settings by simulating detailed networks.	Syahputra et al. (2023) Perancangan Model Simulasi Sistem Keamanan Rumah Berkonsep Internet of Things Berbasis Cisco Packet Tracer Ratnala et al. (2023) Designing Smart Room Using Cisco Packet Tracer Simulator

B. Segmented Network Architecture

To improve security and speed, a network can be divided into smaller, more controllable pieces using segmented network architecture. By separating distinct network components from one another, this method lowers the attack surface and slows the propagation of possible breaches. The ability to apply unique security measures suited to each segment is one of the main advantages of segmented network architecture. Sensitive information, for example, can be kept in extremely secure sections with limited access, while less important information can be kept in more easily accessible locations. This approach not only improves security but also optimizes network performance by cutting down on superfluous traffic and allocating resources more effectively. [9]

Campus network configuration and monitoring with Cisco Packet Tracer were studied by Shahadat Hoshen Moz et al. (2023). The study focused on how to establish a secure campus network using VLANs and security parameters. As a result of separating several departments or campus regions, segmentation can enhance network security by thwarting potential breaches and unauthorized access. Further, the study demonstrated the usefulness of utilizing Cisco Packet Tracer for network design simulation and testing prior to deployment, emphasizing the function of network monitoring in preserving the integrity and functionality of divided networks. [10]

Furthermore, in order to improve the students' comprehension of computer networks at SMK Ar Rahmah Bantul, Tikaridha Hardiani et al. (2023) investigated the usage of Cisco Packet Tracer in training sessions. With an emphasis on real-world VLAN implementations in a simulated scenario, the study showed how network segmentation enhances performance and security in educational environments. The understanding of network segmentation ideas and the students' ability to configure VLANs practically both significantly improved, according to the results. In the simulated settings, this improved comprehension resulted in more effective network security measure deployment and more efficient network performance. [11]

C. Demilitarized Zone (DMZ) Implementation

DMZs serve as a buffer zone between the internal network and outside threats, making them an essential part of network security architecture. It protects the internal network from direct exposure while hosting services that must be reachable from the outside world, such as web servers, email servers, and file transfer servers. By isolating these services in a DMZ, organizations can reduce the risk of attacks on their internal networks and enhance overall security. [12]

The deployment of DMZs in university networks was discussed by the authors in [13], who also demonstrated how this strategy may protect communication and data transfer across network segments. By limiting unauthorized access and isolating critical resources, their study proved how successful DMZs are in preserving network integrity and security. They observed data flows between the DMZ and other network segments and simulated different network topologies using Cisco Packet Tracer. The findings validated the DMZ's function in improving overall network security and performance, demonstrating a marked decline in unauthorized access attempts and more effective traffic management.

Additionally, M. I. Arifin and Antoni Zulius (2019) explored the design of a network security system for Universitas Bina Insan Lubuklinggau using DMZ techniques. They showed how DMZ installation may offer an extra degree of security for vital server resources by focusing on isolating server traffic from student and external network traffic. Incoming and outgoing data traffic is filtered by the security barrier they built using the DMZ, guaranteeing that only authorized data can pass through. The outcomes demonstrated how well DMZ filters data flow and improves network security. Their research revealed, in particular, a marked reduction in possible attack points and enhanced defense for the university's servers, which were kept apart from less secure student networks and outside dangers. [14]

D. Protecting Critical Infrastructure

Radius servers, DHCP, DNS, Active Directory (AD), and other servers and services necessary for day-to-day operations are examples of critical infrastructure in a business network. These elements need to be kept in a highly guarded internal network zone that is governed by strict security guidelines and regulations. Preserving sensitive data, avoiding unwanted access, and preserving operational continuity all depend on these components' security. [15]

Kavya Duvvuri et al. (2023) concentrated on integrating IoT devices, designing and implementing smart classrooms using Cisco Packet Tracer, and safeguarding internal network components. Their efforts made clear how crucial it is to safeguard vital infrastructure in order to maintain data security and operational continuity. The study showed that simulating network environments using Cisco Packet Tracer aided in identifying possible vulnerabilities and optimizing the security settings of crucial infrastructure components. [16]

Also, security of DHCP servers is crucial for critical infrastructure, as shown by the analysis of DHCP vulnerabilities, attacks, and countermeasures conducted by Abdulaziz Abdulghaffar et al. (2023). Their research uncovered typical flaws in the DHCP protocol, namely its vulnerability to several types of attacks and lack of authentication. To minimize these vulnerabilities and provide more secure and dependable DHCP operations within corporate networks, the authors offered solutions. [17]

For the purpose of assessing and ranking the criticality of different assets inside an organisation, the NISTIR 8179 Criticality Analysis Process Model offers an organised approach. This methodology is useful for determining which components are most important and need to be secured tightly. Organisations may more effectively spend resources to defend their most important infrastructure by using the NISTIR 8179 framework, which guarantees that the most essential systems are protected from possible attacks. This is consistent with research by Duvvuri et al. (2023) and Balais et al. (2023), which highlight how crucial it is to safeguard internal network components in order to preserve data security and operational continuity.

In Table II, we highlighted the critical infrastructure security elements.

TABLE II
CRITICAL INFRASTRUCTURE SECURITY ELEMENTS

Security Element	**Key Measures and Benefits**	**Reference**
Active Directory (AD)	Implementing security measures to protect AD, ensuring secure authentication and access control.	Duvvuri et al. (2023). Design and Implementation of Smart Classroom Using Cisco Packet Tracer
DHCP	Identifying and mitigating vulnerabilities in DHCP to prevent unauthorized access and attacks.	Abdulghaffar et al. (2023). An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures
DNS	Implementing robust security measures to protect DNS servers from attacks and ensure reliable domain name resolution.	Zebin et al. (2022) An Explainable AI-Based Intrusion Detection System for DNS Over HTTPS (DoH) Attacks [18]
Radius Servers	Ensuring secure authentication and authorization processes to protect against unauthorized access.	Saputra & Irwan (2020) Sistem Keamanan Pada Jaringan Wireless Menggunakan Protokol RADIUS [19]
Intrusion Detection (IDS)	Using machine learning techniques to detect and mitigate cyber threats to critical infrastructure.	Pinto et al. (2023) Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure [20]

E. Firewall Security

Maintaining the security of DMZs and segmented networks requires firewalls. They regulate the movement of data across various network zones, preventing illegal access and facilitating authorized correspondence. [21]

Özge Ersoy Cangir et al. (2023) configured firewalls and several security protocols to safeguard network integrity while implementing a faculty network system. Their research demonstrated how firewall configurations may be made in network simulations to improve security and prevent unwanted access. The outcomes showed a notable enhancement in the security posture of the network, indicating the significance of firewalls in safeguarding networks. [22]

Moreover, the use of dual DMZ firewall architecture in electrical systems to improve IT/OT cybersecurity was investigated by Agus Harya Maulana et al. in 2023. Dual DMZs, which divide IT and OT networks, dramatically lower high-severity threats and improve overall network security, according to their study. The outcomes proved how successful dual DMZs are at defending vital infrastructure from cyberattacks by reducing vulnerabilities and boosting resistance to them. [23]

III. Methodology

In the modern digital era, robust security within corporate networks is critical to protecting against internal and external threats. This project aims to fortify network security by designing and implementing a segmented network architecture. The focus is on transitioning from traditional networking systems to an advanced, secure, and efficient network using Cisco Packet Tracer. The current system comprises routers, basic switches, and limited security measures. This project introduces firewalls, VLANs, enhanced security protocols, and wireless access points to improve performance, redundancy, scalability, and availability. As emphasized by previous studies, achieving an environment that fosters productivity, security, and adaptability amidst rapid technological changes requires meticulous redesign and implementation. [24]

A. Existing System and Proposed Changes

The existing traditional network infrastructure includes routers connected to Internet Service Providers (ISPs) and basic switches for departmental connectivity. However, this system lacks comprehensive security zones and advanced configurations necessary for modern enterprise operations. Key changes proposed include replacing routers with firewalls to establish secure connectivity, introducing lightweight wireless access points managed by a centralized Wireless LAN Controller (WLC), and segregating the network into distinct zones: external, internal, and demilitarized (DMZ). Critical infrastructure servers such as DHCP, DNS, and Radius will be securely housed within the internal zone, while services requiring external access like FTP, web, email, applications, and NAS storage will be positioned in the DMZ. This systematic deployment not only secures sensitive components but also maintains network integrity and operational continuity.

The diagram above (Fig 1) illustrates the current traditional network infrastructure comprising routers connected to ISPs and basic switches for departmental connectivity. This setup forms the basis for proposed improvements aimed at enhancing security and operational efficiency.

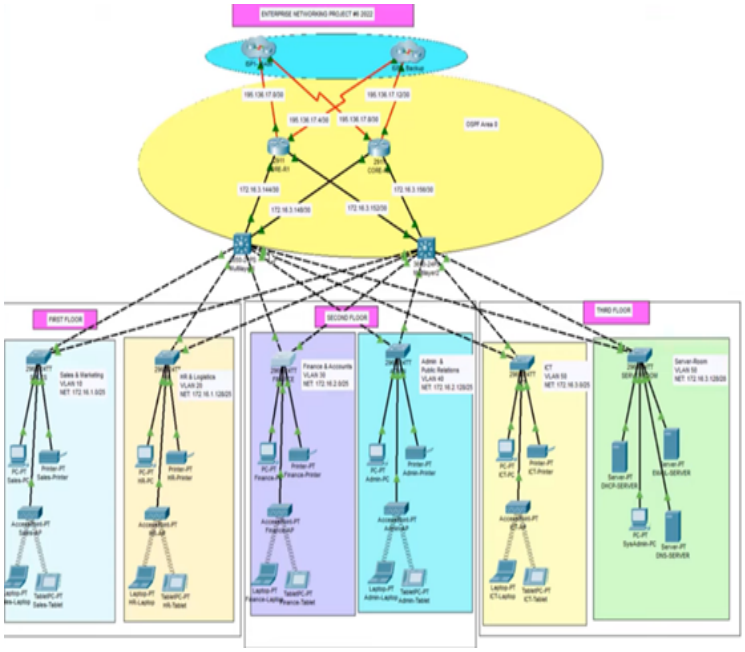

Fig. 1. Targeted Traditional network infrastructure

B. Addressing Network Gaps

To address the gaps in the existing network, a comprehensive redesign and implementation plan will be executed, targeting an organization with a workforce of approximately 600 staff members. The new design will include hierarchical models for redundancy, VLAN assignments, EtherChannel configuration, DHCP and DNS setup [25], and firewall security zones. These measures will collectively enhance network resilience, security, and efficiency. To identify and protect critical infrastructure servers, the NIST Criticality Analysis Process Model (CAPM) was utilized, providing a comprehensive framework for assessing and categorizing the importance of various network components based on their role and impact on organizational operations. The CAPM aligns with organizational project design and implementation processes, and it supports comprehensive risk management approaches, integrating with various risk management standards and guidelines [26]. The methodology involved the following steps:

*1) **Identification of Assets**:* All network assets, including servers, applications, and services, were cataloged to compile a detailed inventory. This process outlined the function of each asset and its importance to the organization's operations.

*2) **Criticality Assessment**:* Using the Critical Asset Protection Model (CAPM) framework, each asset underwent a criticality assessment. Factors such as its role in organizational processes, potential impact of disruptions, and sensitivity of processed information were evaluated. This assessment included analyzing operational impact, information sensitivity, and dependency within the network infrastructure

*3) **Classification and Prioritization**:* Assets were classified based on criticality assessment into different levels of importance. Critical infrastructure servers such as Active Directory

(AD), DHCP, DNS, and Radius servers were identified for their fundamental roles in network authentication, address management, name resolution, and access control.

*4) **Strategic Placement**:* Critical infrastructure servers were strategically placed within the internal zone of the network architecture. This zone features enhanced security measures, including restricted access controls and robust firewall protections, to safeguard these vital servers from internal and external threats.

*5) **Implementation of Security Zones**:* The network was segmented into three primary security zones: the Internal Zone, the Demilitarized Zone (DMZ), and the External Zone. Each zone serves distinct purposes in securing and segregating network traffic and services, ensuring secure external connectivity while protecting internal resources.

By following the NIST CAPM, a methodical and rigorous approach to identifying and protecting critical network components was ensured. This structured methodology not only secured sensitive components but also maintained network integrity and operational continuity, providing a robust framework for developing secure, resilient, and efficient network systems.

C. Implementation Steps

1) Phase 1: Basic Network Design and Beautification:

The implementation of the network design began with the initial setup, where two Cisco 2911 routers were designated as ISPs. Two Cisco ASA 5506 firewalls were deployed for enhanced security, and two multilayer Cisco 3650 switches were installed for core networking. Six Cisco 2960 switches were allocated for departmental connectivity, with two switches per floor. The server room configuration represented the internal server zone. Automatic connection types were utilized to connect ISPs to firewalls and subsequently to switches. Three cable connections were established between the two multilayer switches. Host devices, both wired (PC, printer, VoIP phones) and wireless (laptop, smartphone, tablet), were added along with lightweight access points managed by the WLC. VoIP phones and lightweight access points were powered and configured appropriately. The DMZ zone was set up by adding a basic Cisco switch, connecting five servers to the switch, and subsequently connecting the switch to the firewall. Acknowledgment of a single point of failure in the DMZ setup was made, considering potential issues with switch, cable, or firewall failure. For global client connectivity, a Cisco 2911 router was added, connected to a switch with two PCs representing clients in different countries. These devices were clustered and configured as a cloud network.

The figure (Fig 2) above illustrates the complete network infrastructure as implemented by the end of this phase. It shows the connections between ISPs, firewalls, core switches, departmental switches, and host devices, as well as the segregation of internal, DMZ, and external zones.

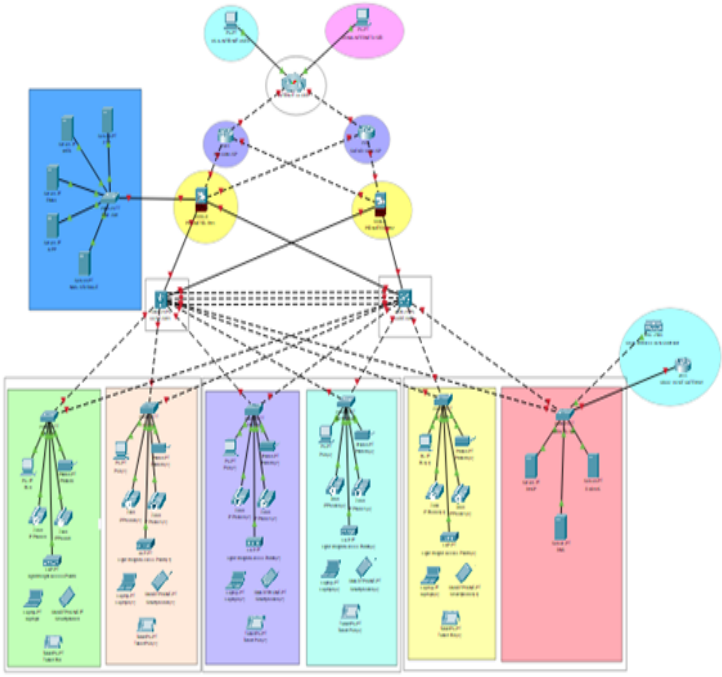

Fig. 2. Basic Network Infrastructure

2) Phase 2: Network Configuration and SSH Access Control:

The configuration of each switch began with basic settings using the CLI. Hostnames, console passwords, enable passwords, and banners were set. IP domain-lookup was disabled, and password encryption was enabled.

SSH was configured with commands to establish secure remote access. It is used for secure remote access, file transfer, and tunneling application protocols [27]. A username and password were set for remote users, and SSH version 2 was enabled. The VTY interface was configured for SSH access, and an access control list (ACL) was created to permit SSH access from the management network and deny others.

Multilayer switches were powered on by connecting the AC supply, and basic and SSH settings were applied similarly to regular switches, ensuring secure and efficient operations.

3) Phase 3: VLAN, Access, and Trunk Configuration:

In Phase 3 of the network implementation, the primary focus was on configuring VLAN assignments and ensuring the proper setup of access and trunk points across all departmental switches.

Configuration of Departmental Switches The configuration process for departmental switches involved setting up Virtual Local Area Networks (VLANs) to logically segment network traffic based on organizational needs. VLANs such as Management (MGT), LAN, WLAN, VoIP, and Blackhole were established to facilitate different types of network communication and security policies. Trunk interfaces were configured

to enable the passage of multiple VLANs between switches, ensuring efficient data transmission and network scalability.

Device-Specific Configurations Devices within each department, including printers, PCs, and VoIP phones, were configured to operate within their designated VLANs. This setup ensures that each device type operates securely and efficiently within the network environment. For instance, printers and PCs were assigned to the LAN VLAN for general data communication, while VoIP phones were configured with both an access VLAN and a dedicated voice VLAN to prioritize voice traffic.

Deployment of Lightweight Access Points (LWAP) Lightweight Access Points (LWAPs) were strategically deployed across the network to provide wireless connectivity. Each LWAP was integrated into the WLAN VLAN to support wireless LAN services. This configuration ensures seamless connectivity for mobile devices and enhances network accessibility within the organization.

Blackhole VLAN Configuration Interfaces that were not actively used or required for specific operational purposes were assigned to the Blackhole VLAN. This VLAN serves as a security measure to restrict access and mitigate potential threats from unauthorized network access attempts.

Configuration of Remaining Departmental Switches Following the initial setup on the primary departmental switch, similar VLAN assignments and access/trunk configurations were replicated across all remaining departmental switches. This approach ensures uniformity in network configuration and facilitates consistent network performance and security measures across the organization.

Configuration of Server Department Switch The server department switch was configured to support critical server infrastructure within the internal network zone. VLANs such as Inside-Servers and WLAN were allocated to servers and wireless LAN controllers, respectively, to segregate and manage network traffic effectively. Trunk ports enable data transmission across multiple VLANs, enhancing flexibility and scalability by allowing devices on different VLANs to communicate directly, bypassing the need for a router [28].

Configuration of Multilayer Switches Multilayer switches played a crucial role in managing VLAN traffic between departmental switches and other network segments. During configuration, trunk interfaces on multilayer switches (GigabitEthernet1/0/3-8) were initially set up to facilitate the passage of multiple VLANs. An error was encountered initially due to the need to explicitly set the trunk encapsulation mode to dot1q before configuring the trunk interfaces. This adjustment resolved configuration errors and ensured seamless VLAN communication, enhancing network flexibility and scalability for future organizational needs and technological advancements.

STP Portfast and BPDUguard Configuration STP Portfast and BPDUguard configurations were methodically applied to enhance device connectivity and network robustness. Beginning with the internal server switch (excluding trunk interface fa0/7), ports fa0/3-6 and fa0/8-24 were configured. This initiative aimed to minimize reconnection delays, ensuring swift restoration of critical network services. For department switches, spanning ports fa0/3-24, consistent STP Portfast and BPDUguard settings were implemented. This approach extended rapid port activation and improved network stability across departmental areas, optimizing device connectivity and reducing downtime. Similarly, the DMZ zone switch was configured across ports fa0/1-24, reinforcing service reliability and security within the demilitarized zone. By enforcing STP Portfast and BPDUguard protocols, network resilience was enhanced, mitigating disruptions and unauthorized access attempts.

In Phase 3, these configurations enhanced network responsiveness and reliability, aligning with effective network management practices.

4) Phase 4: EtherChannel Configuration:

EtherChannel was implemented to aggregate multiple physical links into a single logical channel, enhancing network performance and bandwidth utilization. Specifically, LACP (Link Aggregation Control Protocol) was utilized to dynamically manage and balance traffic across the bundled links. If a single active link becomes unavailable, the traffic is distributed evenly across the remaining operational active links [29]. Three physical links between the multilayer switches (interfaces gig1/1/9-11) were consolidated into a single EtherChannel. This configuration maximized throughput and provided fault tolerance, crucial for ensuring reliable inter-switch communication and data transmission. By activating the EtherChannel in active mode, traffic distribution across the links was optimized, promoting efficient utilization of available bandwidth. The Port-channel interface was configured with trunking capabilities, enabling seamless VLAN traffic across the aggregated links. To maintain consistent trunking operation, the trunk encapsulation was standardized to dot1q. This ensured compatibility and interoperability across the interconnected switches, supporting reliable and scalable network operations. The implementation of EtherChannel effectively enhanced network resilience, performance, and scalability by aggregating bandwidth and optimizing traffic distribution across interconnected switches.

5) Phase 5: Subnetting and IP Addressing:

In this phase, we selected IP address ranges based on standard private IP address allocations, adhering to industry guidelines such as RFC 1918 [30]. This approach ensures efficient network segmentation and management, providing ample address space for each network segment. The chosen ranges facilitate effective traffic management and enhance overall network security, aligning with best practices in network design.

We used the IP address ranges 197.200.100.0/30 and 197.200.100.4/30 for ISP2-FWL1 and ISP2-FWL2. Comments were added for each of these IP addresses to clearly show the IP addresses assigned to each device (Fig 3).

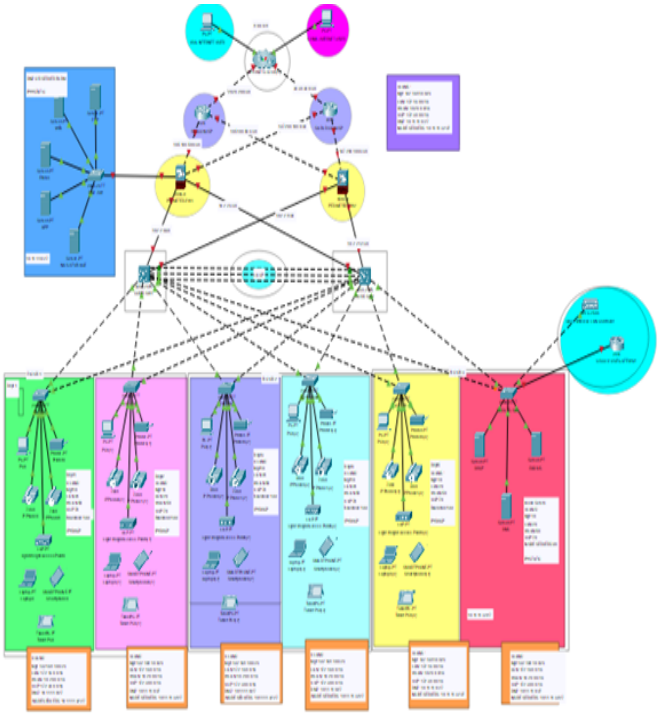

Fig. 3. IP Addresses visible thorough comments

The initial step involved enabling routing on the multilayer switch. Following this, specific interfaces on the core switches, namely gigabit1/0/2 and gigabit1/0/4 on core switches SW-1 and SW-2, were configured with appropriate IP addresses. For Multilayer Switch 1, interface gig1/0/1 was assigned the IP address 10.2.2.1 with a subnet mask of 255.255.255.252, and interface gig1/0/2 was assigned the IP address 10.2.2.5 with the same subnet mask. Similarly, for Multilayer Switch 2, interface gig1/0/1 was assigned the IP address 10.2.2.9 with a subnet mask of 255.255.255.252, and interface gig1/0/2 was assigned the IP address 10.2.2.13 with the same subnet mask.

Next, the cloud was unclustered to allow for IP addressing using the GUI. Specific interfaces were selected as per the connection table, turned on, and assigned IP addresses along with their respective subnet masks. The same steps were repeated for the remaining two routers and the unclustered router.

Finally, the IP addresses and configurations were added to the two PCs representing internet users. This included setting the IP address, default gateway (the IP address of the router to which they are connected), and the DNS server.

This comprehensive approach to subnetting and IP addressing ensures efficient traffic management and enhances overall network security.

6) Phase 6: Implementing HSRP and Inter-VLAN Routing with IP DHCP Helper Addresses:

In this phase, we focus on configuring Hot Standby Router Protocol (HSRP), a Cisco-developed redundancy protocol that facilitates the backup of the next-hop IP device [31], and inter-VLAN routing on Layer 3 switches, along with setting up IP DHCP helper addresses. This ensures robust network redundancy and efficient communication between different VLANs.

IP Address Allocation and VLAN Configuration

We begin by assigning IP addresses to various interfaces based on the VLANs they belong to.Switches can also have broadcast traffic by means of VLANs, which offer an alternative to routers for broadcast containment [32].The IP addresses and VLAN configurations are carefully chosen to optimize network performance and security. All departments will connect to the Active Directory (AD) DHCP server,which serves as a common repository for data on networked items [33],located in the server department, except for the server farms, which will receive their IP addresses from the voice gateway.

Inter-VLAN Routing

Inter-VLAN routing is implemented to allow communication between different VLANs within the network. With Inter VLAN, users may log in to any network within the same set without having to change their IP address, which improves network performance [34]. This is achieved by configuring the Layer 3 switches to route traffic between VLANs. The VLANs we will focus on include:

- **Management Network (VLAN 10):** Ensures network management traffic is isolated and secure.
- **LAN (VLAN 20):** Facilitates internal network communication.
- **WLAN (VLAN 50):** Manages wireless network traffic.
- **Inside Servers (VLAN 90):** Secures internal server communication.

Configuring HSRP

HSRP is configured between the two multilayer switches to provide gateway redundancy.To enable multiple routers to be recognized as a single gateway IP address, the Hot Standby Router Protocol was created [35].This protocol allows for a standby router to take over if the active router fails, ensuring continuous network availability. We distribute the traffic load by configuring one switch to be the active router for VLANs 10 and 20 and the other switch for VLANs 50 and 90. This configuration allows each switch to act as both a standby and active router, optimizing traffic distribution and enhancing network resilience.

IP DHCP Helper Addresses

To facilitate dynamic IP address allocation, IP DHCP helper addresses are configured on the VLAN interfaces. These helper addresses point to the DHCP server, ensuring that devices within each VLAN can obtain IP addresses dynamically from the centralized DHCP server.

Practical Implementation

Layer 3 Switch Configuration: The Layer 3 switches are configured with the necessary VLANs, IP addresses, and HSRP settings. Each VLAN interface is assigned an IP address and a standby IP address for HSRP.

Traffic Distribution: VLAN traffic is distributed such that the first switch handles management and LAN traffic, while the second switch handles WLAN and inside server traffic. This ensures balanced load distribution and redundancy.

DHCP Helper Addresses: Each VLAN interface is configured with a DHCP helper address to forward DHCP requests to the DHCP server, enabling dynamic IP allocation across the network.

By implementing HSRP, inter-VLAN routing, and IP DHCP helper addresses, we ensure high availability, efficient traffic management, and seamless communication within the network. This setup provides a resilient and scalable network infrastructure capable of supporting the dynamic needs of modern organizational operations.

7) Phase 7: Static IP Address Assignment to DMZ / Server Farm Devices:

In this phase, we focus on assigning static IP addresses to the devices within the DMZ or server farm to enhance network stability and security. The process begins by accessing the DHCP server's desktop and navigating to the IP configuration settings. Here, we manually configure IP addresses for each server, including the web, FTP, email, application, and NAS storage servers, ensuring that they operate within the specified subnet (10.11.11.0/27). This static assignment not only simplifies network management but also reduces the risk of IP conflicts and unauthorized access. By ensuring each server has a fixed IP address, we improve the reliability and security of the network, making it easier to monitor and manage the server farm's connectivity and performance.

8) Phase 8: DHCP Server Device Configurations:

In this phase, the DHCP server configuration is focused on efficiently allocating IP addresses to various network segments, specifically the MGT, LAN, and WLAN pools. Distribution of host configurations to all devices is handled by the DHCP server [36]. To begin, navigate to the DHCP server in the server department and access the services tab. Within this tab, go to the DHCP section and initially set all fields to 0. This step ensures a clean configuration setup for the IP addresses to be assigned.

Next, proceed to create the necessary server pools for the different network segments. For this project, three distinct pools are required: one each for MGT (Management), LAN, and WLAN (Wireless Local Area Network). For each pool, enter the appropriate values for the default gateway, DNS server, start IP address, subnet mask, and the maximum number of users. These values ensure that each network segment receives the correct IP configurations, thereby maintaining network efficiency and connectivity [37].

The most critical pool to configure is the WLAN pool, as it will integrate with the Wireless LAN Controller. For this setup, assume the IP address of the Wireless LAN Controller is 10.20.0.10. Proper configuration of this pool is essential to ensure seamless wireless connectivity and management within the network.

By accurately setting up these DHCP server pools, the network can dynamically allocate IP addresses, ensuring efficient management and connectivity across all network segments. This phase is crucial for maintaining an organized and functional network infrastructure, adhering to industry standards and best practices in network management.

9) Phase 9: OSPF on Firewalls, Routers, and Switches:

In Phase 9, OSPF (Open Shortest Path First), a dynamic and layered protocol [38], will be implemented on routers and switches to facilitate dynamic routing within the network. This phase excludes configuration for firewalls.

Implementing OSPF on Multi-Layer Switch 1: Begin by identifying the networks connected to Multi-Layer Switch 1. OSPF, the most often employed intera-domain routing protocol [39], will advertise a total of 6 networks, including those configured for inter-VLAN routing and additional networks like gig1/0/1 and gig1/0/2.

Configuring OSPF on Multi-Layer Switch 2: Similar to Multi-Layer Switch 1, OSPF configuration on Multi-Layer Switch 2 involves advertising the connected networks to facilitate routing efficiency across the network.

OSPF Configuration on Routers: Each router connected to the network will also have OSPF configured. It's crucial to assign unique router IDs (router-id) to avoid conflicts within the OSPF domain. Network statements in OSPF configurations should reflect the IP addresses of the networks directly connected to each router. The performance of the network may be noticeably improved by such arrangements [40].

10) Phase 10: Firewall Interface Security Levels and Zones:

In Phase 10, we will configure firewall interface security levels and zones. A firewall must be positioned carefully such that all traffic transiting between the internal network and the external world goes through it in order for it to be effective [41]. The first firewall will have two inside zones, two outside zones, and one DMZ (Demilitarized Zone), while the second firewall will have two inside zones and two outside zones only. Each interface must have a unique name.

The security level for all inside zones will be set to 100, representing the highest level of trust. Outside zones will have a security level of 0, indicating the least trust. The DMZ, which has partial security, will have a security level greater than 0 and less than 100. Proper configuration of security levels and zones is essential for effective firewall management and network security [42].

For Firewall 1, the inside zones will have IP addresses and security levels configured accordingly. Similarly, the DMZ zone will have an IP address and a security level that ensures partial security. The outside zones will have IP addresses and the lowest security level.

For Firewall 2, the inside and outside zones will be configured similarly, with appropriate IP addresses and security levels. The inside zones will be set to the highest security level, and the outside zones will have the lowest security level.

By default, the firewall blocks any traffic flowing from a lower security level to a higher security level. Unauthorized access is prevented by firewalls [43]. This ensures that the most trusted areas of the network are protected from less trusted areas. Properly configuring these settings is crucial for maintaining network security and managing traffic effectively.

11) Phase 11: OSPF and Static Routes Configuration on Firewalls:

Phase 11 involves configuring OSPF and static routes on firewalls to enhance network routing capabilities. OSPF will be used to dynamically advertise directly connected networks, ensuring efficient routing updates across the network.

Each firewall will implement OSPF process ID 35 with unique router IDs (router-id) to prevent conflicts. Network statements will specify the IP networks participating in OSPF routing within Area 0.

Additionally, the configuration includes: Primary Static Routes: These routes define default gateway settings, directing traffic from any network or subnet to specified IP addresses without relying on dynamic routing protocols.

Backup Static Routes: Configured with lower administrative distances (AD), these routes act as failover mechanisms. If the primary interface fails, traffic reroutes through the backup route.

These configurations aim to enhance network reliability, efficiency, and resilience to network disruptions.

12) Phase 12: Firewall Inspection Policy Configurations:

Before configuring inspection policies on the firewall, it is essential to set up NAT (Network Address Translation) [44] and create object networks. This phase involves the configuration for the first firewall, addressing different network segments such as LAN, WLAN, and DMZ.

For the LAN segment on the first firewall, object networks are created for both primary and backup outside interfaces. The configurations involve defining subnets and setting up dynamic NAT interfaces for each inside-to-outside network. For the LAN, object networks are created with subnets 172.16.0.0/16 and NAT is configured to use dynamic interfaces for both INSIDE1 and INSIDE2 networks, mapping them to OUTSIDE1 and OUTSIDE2 interfaces.

Similarly, for the WLAN segment, object networks are created with subnets 10.20.0.0/16. NAT configurations use dynamic interfaces for INSIDE1 and INSIDE2 networks, mapping them to OUTSIDE1 and OUTSIDE2 interfaces, ensuring proper traffic flow and network address translation.

The DMZ segment receives its own NAT configurations. Object networks are created with subnets 10.11.11.0/27 and NAT is configured to use dynamic interfaces for the DMZ network, mapping it to both OUTSIDE1 and OUTSIDE2 interfaces.

After configuring NAT on the first firewall, the same configurations are applied to the second firewall. This can be done manually or by using the do sh start command to copy relevant NAT details. The configurations for the second firewall are similar to those for the first firewall, ensuring consistency across the network.

With NAT configurations in place, the focus shifts to implementing inspection policies to allow specific services through the firewall. Additional policies are set up for web traffic (TCP port 80) and DNS traffic (both TCP and UDP port 53). These policies ensure that essential services are accessible while maintaining network security.

The inspection policies are then appended to the relevant interfaces using access groups. This step ensures that the inspection rules are applied to traffic entering the DMZ, OUTSIDE1, and OUTSIDE2 interfaces. The configurations are saved, and the system is prepared for testing.

During testing, services enabled by the inspection policies are verified. For instance, DHCP functionality is tested by navigating to a computer in the second department and checking the DHCP radio button. Successful DHCP operation is confirmed, but an issue arises when testing ping functionality to the network. The ping test from the DMZ works, but further troubleshooting is required for other network segments.

To debug the issue, various show commands are used to check ARP entries, access lists, and interface statuses. For example, using show arp [45] provides ARP entries for different interfaces, while show access-list displays the access control list and hit counts. Show interface provides status information for each interface, including packet counts, errors, and configurations. This diagnostic information helps identify and resolve potential configuration issues, ensuring that the firewall operates as intended and provides the necessary security and connectivity for the network.

13) Phase 13: Wireless Network Configurations:

In Phase 13, the focus was on wireless network configurations. To start, we needed to add a PC directly or connect it to the management network. We connected it directly to the wireless LAN controller and, by navigating to the IP configurations tab, added the IP address of the wireless LAN controller, subnet mask, default gateway, and DNS server. We attempted to ping the address 10.20.0.10 to ensure the setup was working, but initially, it was not successful. However, after reconfiguration, it worked as expected. The next step involved navigating to the web browser option in the desktop tab of the PC to access the console/interface of the wireless LAN controller. Typing the IP address of the LAN controller into the URL section should display a Cisco interface, but this did not work in our case. Once successful, we created an admin account with the ID: Admin and Password: Cisco123. We then added the system name, IP address, subnet mask, and default gateway.

Following this, we created a Wi-Fi network for employees, named it ”employees,” and set the password as Cisco123. After clicking next and confirming the configurations, we

applied the settings and waited for the process to complete. We then attempted to ping the address 10.20.0.10 again using the command prompt. We accessed the web browser again and added https instead of http to the URL, which successfully displayed the login page for the LAN controller. After logging in with the admin credentials, we proceeded to create Wi-Fi networks for guests, employees, auditors, and corporates. This required synchronization with the access points placed in the five departments. By navigating to the wireless tab, we checked the IP addresses to which each lightweight access point was connected.

We created different WLANs by navigating to the WLAN tab and clicking "Create New." After entering the necessary information and enabling the network, we configured security settings by adding WPA2 policy and PSK, and then set the password to Cisco123. We saved these settings and modified the name of the "EMPLOYEES" network to "EMPLOYEES WIFI." We created two more networks, "CORPORATE WIFI" and "GUEST WIFI," following the same instructions, and saved the configurations. After saving the changes in the WLAN controller, we verified that the Wi-Fi names reflected correctly on each lightweight access point, although the IPs appeared different in our case. We then connected wireless devices in each department to the appropriate Wi-Fi networks:

- Dept 1: Laptop to "employees," tablet to "auditors," smartphone to "guest."
- Dept 2: Laptop to "employees," tablet to "corporate," smartphone to "auditors."
- Dept 3: Laptop to "guest," smartphone to "corporate," tablet to "employees."
- Dept 4: Laptop to "auditors," smartphone to "corporate," tablet to "guest."
- Dept 5: Laptop to "employees," smartphone to "corporate," tablet to "auditors."

Finally, we navigated to the IP configurations on all the devices and turned on DHCP. The IP addresses started appearing on each wireless device. We saved the file, closed it, and reopened it to ensure all configurations were correctly applied.

14) Phase 14: VOIP Configurations:

In Phase 14, we configured VOIP settings on the network device by first enabling configuration mode and accessing interface fa0/0. VoIP is a network-based communication protocol [46]. We activated the interface and established a sub interface specifically for VOIP, assigning it an IP address of 172.30.0.1 with a subnet mask of 255.255.0.0. DHCP services were then set up to manage IP addresses for VOIP devices, creating a DHCP pool on the 172.30.0.0 network with a default gateway set to 172.30.0.1. Option 150 was configured to specify the IP address for VOIP service. Telephony services were implemented next, defining maximum limits for phones and directory numbers, and assigning the IP source address with its associated port. Directory numbers were allocated from 401 to 410 for individual phones. Finally, configurations were saved using "do wr". Verification included restarting the packet file and successfully testing calls between department phones as per the instructional video's guidance.

IV. Comparative Analysis

This section provides a detailed comparison between the original network design and the modified network design. The analysis is divided into two parts: Qualitative Analysis and Quantitative Analysis. Each part highlights the key differences and improvements made in the modified network design.

A. Qualitative Analysis

The qualitative analysis focuses on the architectural and management aspects of the network. It evaluates how the modifications have enhanced the network's overall structure, security measures, management capabilities, and wireless network configurations. The detailed comparison is presented in Table III.

B. Quantitative Analysis

The quantitative analysis examines the metrics related to device count, segmentation, scalability, performance, security, and costs. This analysis provides a numerical comparison between the original and modified network designs, illustrating the improvements in terms of device utilization, redundancy, and overall efficiency. The detailed comparison is presented in Table IV.

V. Conclusion

This paper provides a detailed analysis of the steps taken to design and implement a robust network infrastructure. Key elements of the design include the use of VLANs for network segmentation, HSRP for gateway redundancy, and OSPF for optimized routing. The implementation of Cisco ASA 5506 firewalls ensures that different segments of the network are securely isolated, enhancing overall security. The configuration of lightweight access points managed by a Wireless LAN Controller improves network flexibility and manageability.

The enhancement of network topology through the strategic implementation of firewalls, DMZ zones, and outside zones significantly fortifies overall network security. By deploying firewalls, organizations can establish robust barriers that regulate incoming and outgoing traffic, ensuring only authorized access and protecting sensitive data from unauthorized intrusions. The incorporation of DMZ zones offers an additional layer of security by isolating publicly accessible services from the internal network, thereby reducing the risk of potential attacks on critical assets. Outside zones further strengthen the network's defense by providing an extra perimeter of security, creating a buffer zone that can detect and mitigate threats before they reach the core infrastructure.

These improvements in network topology not only enhance the protection of digital assets but also promote a more resilient and adaptive security posture. Organizations can better manage and monitor network traffic, quickly respond to potential threats, and maintain the integrity and confidentiality of their data.Future work could focus on continuous

TABLE III
QUALITATIVE ANALYSIS

Metric	Original Network	Modified Network
Architecture and Redundancy	The original network uses a hierarchical model with two routers and two multilayer switches. It connects to two ISPs for redundancy. Each department is separated by VLANs, with static IP addresses allocated to server room devices and dynamic IP addresses for other devices via dedicated DHCP servers.	The modified network replaces routers with firewalls, creating a segmented and more secure architecture. It introduces DMZ, Inside, and Outside zones, enhancing traffic management. Lightweight access points are used for wireless networks, improving network efficiency and manageability.
Security Measures	Basic security configurations including setting hostnames, console and enable passwords, disabling IP domain lookup, and using OSPF for dynamic routing and PAT for address translation.	Enhanced security with firewalls providing better traffic control between zones. NAT and ACLs configured on firewalls with stringent firewall inspection policies.
Network Management	SSH configured for secure remote access on routers and multilayer switches. Dedicated DHCP servers provide dynamic IP allocation.	VLANs, EtherChannel, OSPF, and inter-VLAN routing configured in detail. DHCP used for dynamic IP allocation and SSH configured for secure remote access to all network devices.
Wireless Network	Each department has a dedicated wireless network ensuring user connectivity.	Lightweight access points managed by a Wireless LAN Controller, enhancing wireless connectivity and network management.

TABLE IV
QUANTITATIVE ANALYSIS

Metric	Original Network	Modified Network
Device Count and Distribution	Two routers, two multilayer switches, and a standard number of access points.	Two firewalls replacing routers, two multilayer switches, and likely increased number of lightweight access points.
Segmentation and Zones	VLANs for each department, ensuring logical segmentation and efficient communication.	Enhanced segmentation with DMZ, Inside, and Outside zones, and continued use of VLANs for department segmentation.
Scalability and Redundancy	Adequate scalability with VLANs and a hierarchical model. Redundancy with multiple ISPs and multilayer switches.	Improved scalability with firewalls and lightweight access points, allowing easier expansion and management. Enhanced redundancy with firewalls and continued use of multiple ISPs and multilayer switches.
Performance Metrics	Processing power handled by two routers, standard load distribution.	Optimized device load with better traffic management through segmentation and firewalls.
Security and Compliance	Basic security with VLANs and routers, standard compliance.	Enhanced security with firewalls, improved segmentation and control, likely better compliance.
Device Utilization	Standard load distribution on routers and switches.	Optimized load with better segmentation and traffic management through firewalls.
Maintenance and Management	Moderately complex management with routers, switches, and VLANs. Maintenance as needed for routers and switches.	Potentially reduced complexity with centralized access point management and structured security zones. Streamlined maintenance with better device segmentation and enhanced security measures.
Cost Analysis	Standard costs for routers, switches, and access points.	Higher initial costs due to firewalls and advanced access points, but potential long-term savings with improved security and manageability.
Energy Consumption	Standard power usage for routers and switches.	Possibly higher power usage with firewalls and advanced access points, but overall efficiency likely improved.

monitoring and updating of network configurations to adapt to evolving technological and security challenges. This paper serves as a valuable resource for network administrators and IT professionals aiming to enhance their network infrastructure.

REFERENCES

[1] Ravikumar, C. V. et al. "Performance Analysis of HSRP in Provisioning Layer-3 Gateway Redundancy for Corporate Networks." Indian journal of science and technology 9 (2016): n. Pag.

[2] Pouriyeh, Seyedamin et al. "Secure Smart Communication Efficiency in Federated Learning: Achievements and Challenges." Applied Sciences (2022): n. pag.

[3] Choi, Sangsu et al. "Building Korean DMZ Metaverse Using a Web-Based Metaverse Platform." Applied Sciences (2022): n. pag.

[4] Wu, Qingqing et al. "Intelligent Surfaces Empowered Wireless Network: Recent Advances and The Road to 6G." ArXiv abs/2312.16918 (2023): n. pag.

[5] Abirami, A., and S. Palanikumar. "Proposed Security Models for Node-level and Network-level Aspects of Wireless Sensor Networks Using Machine Learning Techniques." Iraqi Journal of Science (2023): 6493-6508.

[6] Kundu, Krishanu et al. "Simulating a Local Area Network with Cisco Packet Tracer: A Comprehensive IP Packet Switching Network Demonstration." 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC) (2023): 247-252.

[7] Syahputra, Exsyal et al. "Perancangan Model Simulasi Sistem Keamanan Rumah Berkonsep Internet of Things Berbasis Cisco Packet Tracer." (2023).

[8] Ratnala, Bharat et al. "Designing Smart Room Using Cisco Packet Tracer Simulator." 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (2023): 183-188.

[9] Niedermaier, Matthew et al. “A Secure Network Scanner Architecture for Asset Management in Strongly Segmented ICS Networks.” International Conference on Information Systems Security and Privacy (2021).

[10] Moz, Shahadat Hoshen et al. “Campus Network Configuration, Monitoring and Data Flow Simulation using Cisco Packet Tracer.” 2023 International Conference on Inventive Computation Technologies (ICICT) (2023): 793-798.

[11] Hardiani, Tikaridha et al. “Pelatihan Jaringan Komputer Menggunakan Cisco Packet Tracer di SMK Ar Rahmah Bantul.” Dharma Raflesia : Jurnal Ilmiah Pengembangan dan Penerapan IPTEKS (2023): n. pag.

[12] BouSaba, Dr. Chafic and Guilford College. “Implementing a Demilitarized Zone Using Holistic Open Source Solution.” (2019).

[13] Valcourt, Scott A. ”Major Factors in Science DMZ Deployment at Small Institutions.” Proceedings of the Practice and Experience on Advanced Research Computing. 2018. 1-8.

[14] Arifin, Mt Ir. Syamsul and Antoni Zulius. “PERANCANGAN SISTEM KEAMANAN JARINGAN PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ).” Jusikom : Jurnal Sistem Komputer Musirawas (2019): n. pag.

[15] Balais, Maricel A. et al. “Wireless Network Infrastructure and Security Enhancement for St. Joseph School.” Proceedings of the 2023 4th Asia Service Sciences and Software Engineering Conference (2023): n. pag.

[16] Duvvuri, Kavya et al. “Design and Implementation of Smart Classroom Using Cisco Packet Tracer.” 2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS) (2023): 116-120.

[17] Abdulghaffar, Abdulaziz et al. “An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures.” 2023 Biennial Symposium on Communications (BSC) (2023): 119-124.

[18] Zebin, Tahmina et al. “An Explainable AI-Based Intrusion Detection System for DNS Over HTTPS (DoH) Attacks.” IEEE Transactions on Information Forensics and Security 17 (2022): 2339-2349.

[19] Saputra, Aldi Sigit and Dadan Irwan. “Sistem Keamanan Pada Jaringan Wireless Menggunakan Protokol RADIUS.” JUSS (Jurnal Sains dan Sistem Informasi) (2020): n. pag.

[20] Pinto, Andrea et al. “Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure.” Sensors (Basel, Switzerland) 23 (2023): n. pag.

[21] Patel, Hiral B. et al. “Approach of Data Security in Local Network Using Distributed Firewalls.” (2013).

[22] Ersoy Cangir, Özge, Mustafa Yıldırım, and Nurgül Bostan. ”Faculty network system implementation using Cisco packet tracer.” Journal of Computer & Electrical and Electronics Engineering Sciences 1.1 (2023): 20-24.

[23] Maulana, Agus Harya et al. “Analysis of the Demilitarized Zone Implementation in Java Madura Bali Electrical Systems to Increase the Level of IT/OT Cyber Security With the Dual DMZ Firewall Architecture Method.” 2023 International Conference on Smart Applications, Communications and Networking (SmartNets) (2023): 1-6.

[24] Varne, P. N., P. J. Shetty, V. T. A. K., and N. C. Gowda. ”Campus Network Design and Implementation using Cisco Packet Tracer.” Milestone Research Publications, vol. 02, no. 4, Oct. 2023. doi: 10.5281/zenodo.10254264. Accessed 23 June 2024. Available at: https://doi.org/10.5281/zenodo.10254264.

[25] Chatterjee, T. ”Configuration of DNS server with cryptographic algorithm for secure DNS and DHCP updates.” In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT’12), Coimbatore, India, 2012, pp. 1-7. doi: 10.1109/ICCCNT.2012.6395990.

[26] Paulsen, Celia, Jon M. Boyens, Nadya Bartol, and Kris Winkler. Criticality Analysis Process Model. National Institute of Standards and Technology, 9 Apr. 2018.

[27] Gasser, O., R. Holz, and G. Carle. ”A deeper understanding of SSH: Results from Internet-wide scans.” Technische Universität München, Faculty of Informatics, Chair for Network Architectures and Services. Accessed 23 June 2024. Available at: gasser@net.in.tum.de, holz@net.in.tum.de, carle@net.in.tum.de.

[28] ”Access and Trunk Ports.” GeeksforGeeks, 4 May 2023. Accessed 23 June 2024. Available at: www.geeksforgeeks.org/access-trunk-ports/.

[29] Hongye, Sun. ”What Is Link Aggregation Control Protocol (LACP)?” Huawei, 26 May 2022.

[30] Rekhter, Yakov, et al. ”Address Allocation for Private Internets.” RFC 1918, Internet Engineering Task Force, Feb. 1996, www.ietf.org/rfc/rfc1918.txt.

[31] Cisco Hot Standby Router Protocol (HSRP) Explained.” Study-CCNA, https://study-ccna.com/

[32] Mehdizadeha, Abbas, et al. ”Virtual Local Area Network (VLAN): Segmentation and Security.” The Third International Conference on Computing Technology and Information Management (ICCTIM2017). Vol. 78. 2017.

[33] Allen, Robbie, and Alistair Lowe-Norris. Active directory. ” O’Reilly Media, Inc.”, 2003.

[34] Ahmad, Iqbal. ”Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP.” Asian Journal of Applied Science and Technology 4.3 (2020): 37-44.

[35] YanHua, Zhang, and Ma WeiZhe. ”The design of cable television IP access network based on hot standby router protocol.” 2012 International Conference on Image Analysis and Signal Processing. IEEE, 2012.

[36] Pradana, Dio Aditya, and Ade Surya Budiman. ”The dhcp snooping and dhcp alert method in securing dhcp server from dhcp rogue attack.” IJID (International Journal on Informatics for Development) 10.1 (2021): 38-46.

[37] Szigeti, Tim, et al. End-To-End QoS Network Design: Quality of Service for Rich-Media and Cloud Networks. Pearson Education, 2014.

[38] Sidhu, Deepinder, et al. ”Open shortest path first (OSPF) routing protocol simulation.” ACM SIGCOMM Computer Communication Review 23.4 (1993): 53-62.

[39] Ghazala, Ahmed Abo, Ayman El-Sayed, and Mervat Mousa. ”A survey for open shortest path first weight setting (OSPFWS) problem.” 2008 International Conference on Information Security and Assurance (isa 2008). IEEE, 2008.

[40] Pióro, Michal, et al. ”On open shortest path first related network optimisation problems.” Performance evaluation 48.1-4 (2002): 201-223.

[41] Keromytis, Angelos D., and Vassilis Prevelakis. ”Designing firewalls: A survey.” Network Security: Current Status and Future Directions (2007): 33-49.

[42] Stouffer, Keith, Joe Falco, and Karen Scarfone. ”Guide to industrial control systems (ICS) security.” NIST special publication 800.82 (2011): 16-16.

[43] Hayajneh, Thaier, et al. ”Performance and information security evaluation with firewalls.” International Journal of Security and Its Applications 7.6 (2013): 355-372.

[44] Srisuresh, Pyda, and K. Egevang. ”Rfc3022: Traditional ip network address translator (traditional nat).” (2001).

[45] ”Show ARP.” Aruba Networks, www.arubanetworks.com. Accessed 7 July 2024.

[46] Shaw, Urjashee, and Bobby Sharma. ”A survey paper on voice over internet protocol (VOIP).” International Journal of Computer Applications 139.2 (2016): 16-22.