Designing and Implementing a Comprehensive Cybersecurity Framework for KJSCE

Submitted In Partial Fulfillment of Requirements

For the Degree Of

Honours in Cyber Security & Forensics
(Offered by Department of Computer Engineering)

By

Aryan Ashok Balpande
Roll No: 16010120002
Rahi Nitin Patil
Roll No: 16010120038
Apurva Sunildatta Rasal
Roll No: 16010120042
Soham Avanish Shah
Roll No: 16010120046

Guide

Ms. Swati Mali

Somaiya Vidyavihar University
Vidyavihar, Mumbai - 400 077
2020-24

Somaiya Vidyavihar University
K. J. Somaiya College of Engineering

Certificate

This is to certify that the dissertation report entitled **Designing and Implementing a Comprehensive Cybersecurity Framework for KJSCE** submitted by Aryan Ashok Balpande - 16010120002, Rahi Nitin Patil - 16010120038, Apurva Sunildatta Rasal - 16010120042, Soham Avanish Shah - 16010120046 at the end of semester VII of LY B. Tech is a bona fide record for partial fulfillment of requirements for the degree Honours in Cyber Security & Forensics (Offered by Department of Computer Engineering) of Somaiya Vidyavihar University.

Guide

Head of the Department

Principal

Date: 28/02/2024
Place: Mumbai-77

SOMAIYA
VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya Vidyavihar University
K. J. Somaiya College of Engineering

DECLARATION

We declare that this written report submission represents the work done based on our and / or others' ideas with adequately cited and referenced the original source. We also declare that we have adhered to all principles of intellectual property, academic honesty and integrity as we have not misinterpreted or fabricated or falsified any idea/data/fact/source/original work/ matter in my submission.

We understand that any violation of the above will be cause for disciplinary action by the college and may evoke the penal action from the sources which have not been properly cited or from whom proper permission is not sought.

Signature of the Student **Aryan Ashok Balpande** **Roll No. 16010120002**	**Signature of the Student** **Rahi Nitin Patil** **Roll No. 16010120038**
Signature of the Student **Apurva Sunildatta Rasal** **Roll No. 16010120042**	**Signature of the Student** **Soham Avanish Shah** **Roll No. 16010120046**

Date: 28/02/2024
Place: Mumbai-77

Abstract

In contemporary society, networks constitute an indispensable aspect of daily life, permeating various spheres, including educational institutions such as K J Somaiya College of Engineering (KJSCE). The primary objective of education is the seamless dissemination of knowledge and information, rendering the network infrastructure pivotal in supporting academic endeavors. Ensuring the integrity and reliability of data transfers is paramount for maintaining trust and security within the educational ecosystem.

This study focuses on fortifying the network infrastructure at KJSCE through the implementation of robust security measures. Leveraging Cisco Packet Tracer, a network simulation tool, we devised a comprehensive network topology tailored to the specific requirements of the college environment. The topology encompasses multiple networks and virtual local area networks (VLANs), strategically configured to optimize performance and security.

Critical security configurations were integrated into the network architecture to mitigate potential vulnerabilities and safeguard sensitive data. Various networking protocols were employed to bolster security measures and accommodate the diverse user base at KJSCE.

By adopting a proactive approach to network security, this study seeks to enhance the resilience of KJSCE's network infrastructure, thereby fostering a secure environment conducive to academic excellence and information exchange.

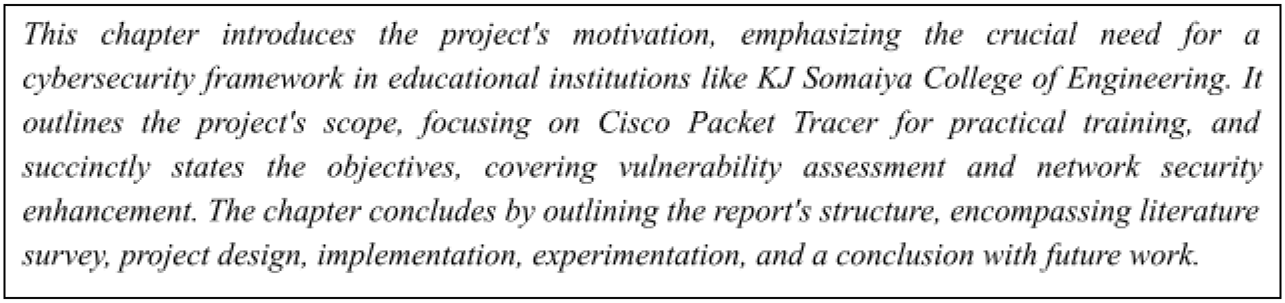
Key words**:** Cisco Packet Tracer, Network, IP Address, Security, VLAN, ASA Firewall

Contents

List of Figures

List of Tables

1. Introduction



This chapter introduces the project's motivation, emphasizing the crucial need for a cybersecurity framework in educational institutions like KJ Somaiya College of Engineering. It outlines the project's scope, focusing on Cisco Packet Tracer for practical training, and succinctly states the objectives, covering vulnerability assessment and network security enhancement. The chapter concludes by outlining the report's structure, encompassing literature survey, project design, implementation, experimentation, and a conclusion with future work.

1.1 Background

In the contemporary landscape of rapidly evolving technology, educational institutions like KJSCE find themselves at the intersection of valuable information, emerging threats, and a diverse user base. The increasing reliance on digital platforms, connectivity, and the storage of sensitive data within the educational ecosystem necessitates a robust cybersecurity framework. Implementing a comprehensive cybersecurity strategy is paramount for educational institutions due to several compelling reasons. It ensures the protection of sensitive information, such as student records and financial data, guarding against unauthorized access and potential data breaches. Additionally, universities often serve as centers for innovative research, making the safeguarding of intellectual property and research findings crucial. A robust cybersecurity framework also contributes to the preservation of academic continuity, preventing disruptions to classes and administrative operations. Maintaining institutional reputation is another critical factor, as cybersecurity incidents can have severe consequences, impacting trust within the community. Furthermore, adherence to regulatory compliance is essential to avoid legal consequences and financial penalties. By prioritizing cybersecurity, institutions also contribute to the well-being of students and staff, preventing identity theft and emotional distress. The protection of digital learning environments is crucial for uninterrupted education, and, importantly, cybersecurity initiatives prepare students for the digital future by instilling a culture of responsibility and awareness.

Cisco Packet Tracer is instrumental in achieving the objectives of implementing a comprehensive cybersecurity framework for educational institutions. The tool enables the simulation of diverse network scenarios, providing a controlled virtual environment for hands-on training in risk assessment and security measures. This practical approach empowers cybersecurity professionals and students to develop crucial skills in configuring security protocols and responding to potential threats. Additionally, Cisco Packet Tracer facilitates the testing of various security configurations across different components of the network infrastructure, ensuring a thorough examination of network security measures. The tool's user-friendly graphical interface simplifies the learning process, fostering a collaborative and inclusive approach to cybersecurity education for both students and faculty. Moreover, by supporting a cost-effective implementation, Cisco Packet Tracer eliminates the need for expensive physical hardware, allowing institutions to allocate resources efficiently. This approach ensures that educational institutions can invest in cybersecurity education without compromising on the quality of practical training.

1.2 Motivation

The motivation behind implementing a comprehensive cybersecurity framework for KJSCE stems from the imperative need to fortify digital defenses and protect the integrity, confidentiality, and availability of sensitive information. As educational institutions increasingly become targets for cyber threats, safeguarding student data, intellectual property, and research findings becomes paramount. By undertaking this cybersecurity initiative, we aim to create a resilient digital environment that not only shields against potential risks but also ensures uninterrupted academic operations. The project is motivated by a commitment to maintaining institutional reputation, complying with regulatory standards, and instilling a culture of cybersecurity awareness among students, faculty, and staff. Ultimately, this endeavor seeks to fortify the college's cybersecurity posture, aligning it with industry best practices to foster a secure and conducive learning environment in the digital age.

1.3 Scope of the project

The scope of designing and implementing a comprehensive cybersecurity framework for K J Somaiya College of Engineering encompasses the establishment of robust measures to safeguard the institution's digital assets, information systems, and sensitive data. This initiative will cover all facets of cybersecurity, including network infrastructure, data protection, user authentication, incident response, and security awareness. The scope also extends to compliance with relevant cybersecurity standards and regulations to ensure a holistic and resilient security posture.

1.4 Brief description of project undertaken

The project undertaken focuses on implementing a robust cybersecurity framework for educational institutions, exemplified by KJSCE. Given the increasing reliance on digital platforms and storage of sensitive data within educational ecosystems, the need for cybersecurity is paramount. The project utilizes Cisco Packet Tracer to simulate diverse network scenarios, providing hands-on training in risk assessment and security measures within a controlled virtual environment. This approach empowers cybersecurity professionals and students to develop crucial skills in configuring security protocols and responding to potential threats. Leveraging Cisco Packet Tracer enables educational institutions to test various security configurations across different components of the network infrastructure, ensuring a thorough examination of network security measures. The tool's user-friendly interface simplifies the learning process, fostering collaboration between students and faculty. Additionally, Cisco Packet Tracer supports cost-effective implementation of cybersecurity measures by eliminating the need for expensive physical hardware, allowing institutions to allocate resources efficiently and invest in cybersecurity education without compromising quality.

1.5 Problem Statement

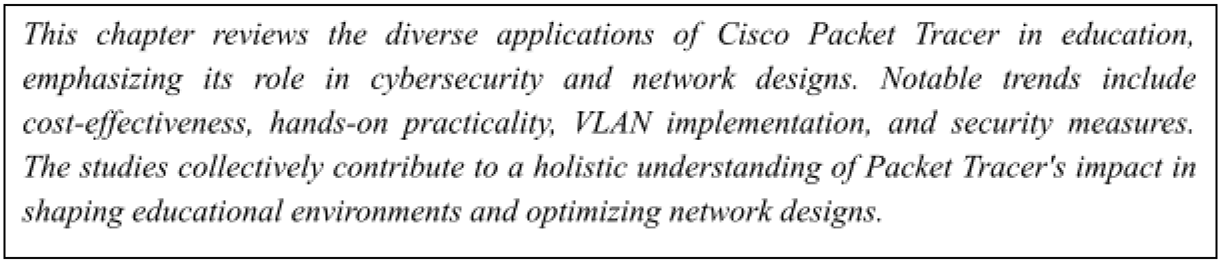
Implementing a robust cybersecurity framework at KJ Somaiya College to proactively safeguard data, ensure system integrity, and cultivate a cyber-resilient environment through advanced threat detection, access controls, vulnerability assessments, and incident response protocols.

1.6 Objectives of Project

- To make comprehensive Network Design: Develop an aesthetically pleasing and efficiently designed campus network architecture in Cisco Packet Tracer, ensuring optimal placement of devices, logical layout of VLANs, and streamlined connectivity for seamless operation.
- To implement Secure Access Controls and SSH Configuration: Configure SSH access on all network devices and apply standard ACLs to restrict SSH traffic, enhancing security by preventing unauthorized access to network infrastructure.
- To enhance Network Stability with STP Portfast and BPDUguard: Enable STP Portfast and BPDUguard on all access ports to accelerate network convergence and protect against unauthorized switch connections, enhancing network stability and security.
- To optimize performance with EtherChannel Configuration: Implement EtherChannel to aggregate links between switches, optimizing bandwidth utilization, enhancing fault tolerance, and improving network performance.
- To provide high availability with HSRP and Inter-VLAN Routing: Configure HSRP for redundancy and failover on the 13 switches, along with Inter-VLAN routing to facilitate communication between VLANs. Additionally, set up DHCP helper addresses to ensure DHCP requests are forwarded across VLANs.
- Secure Demilitarized Zone (DMZ) and Server Farm Devices: Assign static IP addresses to DMZ and server farm devices, enhancing security by ensuring consistent and predictable network access for critical infrastructure.
- Robust DHCP Server Configuration: Configure DHCP servers to automate IP address assignment and provide dynamic network configuration to client devices, improving network scalability and management efficiency.
- Implement OSPF for Dynamic Routing: Configure OSPF on firewalls, routers, and switches to enable dynamic routing, facilitating efficient traffic routing and network convergence while enhancing network scalability and fault tolerance.
- Firewall Interface Security Zones and Policies: Define firewall interface security zones and configure inspection policies to filter and inspect traffic between network segments, enforcing security policies and protecting against unauthorized access and malicious activities.

Further, The report is systematically organized into key sections, each contributing to the comprehensive exploration of the research on "Designing and Implementing a Comprehensive Cybersecurity Framework for KJ Somaiya College of Engineering." The Literature Survey provides a contextual understanding by reviewing existing research and developments in the field of cybersecurity frameworks. The Project Setup segment delineates the conceptualization of the cybersecurity framework, including critical aspects such as network topology. The Implementation and Experimentation section delves into the practical execution, with a particular focus on simulating the network using Cisco Packet Tracer. This hands-on approach allows for a detailed examination of the framework's application in a controlled environment. The concluding section, Conclusion & Future Work, summarizes the project's findings and outlines potential areas for future enhancements and research in the context of cybersecurity at KJ Somaiya College of Engineering.

2. Literature Survey.



This chapter reviews the diverse applications of Cisco Packet Tracer in education, emphasizing its role in cybersecurity and network designs. Notable trends include cost-effectiveness, hands-on practicality, VLAN implementation, and security measures. The studies collectively contribute to a holistic understanding of Packet Tracer's impact in shaping educational environments and optimizing network designs.

The literature survey explores trends in various studies focused on the application of Cisco Packet Tracer in educational settings, particularly addressing the implementation of cybersecurity measures and network designs.

The study conducted by Reddy and colleagues (Reddy et al.) [1] stands out as a notable contribution, delving into the utilization of Packet Tracer as a virtual laboratory for instructing firewall concepts within educational settings. Noteworthy trends identified in this study include an emphasis on cost-effectiveness and hands-on practicality, showcasing the simulation of intricate network architectures. Moreover, the study highlights the practical experience gained by students in configuring firewall rules and assesses its positive impact on their understanding of the subject matter.

Azhari and team's exploration [2] into integrating the Internet of Things (IoT) into a secured small office network using Cisco Packet Tracer expands the horizon of trends. Encompassing design considerations, security measures, and the functionality of IoT devices within the network, the study identifies trends such as the implementation of Virtual Local Area Networks (VLANs), Dynamic Host Configuration Protocol (DHCP), Cisco ASA Firewall, and Secure Sockets Layer Virtual Private Network (SSL VPN). The study also provides valuable insights into potential future work, emphasizing the need for user studies and ensuring the reliability and resilience of the IoT network.

Contributing to the discussion on network security, Ahmed and Al-Hamadani [3] focus on developing a Secure Campus Network (SCN) through the utilization of Cisco Packet Tracer. Key trends identified include the design of a comprehensive network topology, the implementation of crucial configurations like VLANs, DHCP, and Routing Information Protocol (RIP), and the application of security measures to core network devices. The study proposes future work, highlighting the exploration of advanced security protocols and testing the resilience of the secure network.

In the broader context of cybersecurity, Taherdoost's review paper [4] offers insights into frequently used cybersecurity standards and frameworks. Distinguishing between standards and frameworks, the paper provides a comprehensive overview of prominent ones such as ISO 27001 and the NIST Cybersecurity Framework. The study emphasizes the importance of adopting relevant cybersecurity standards and frameworks based on organizational needs, underscoring their crucial role in safeguarding sensitive data.

Shifting the focus to campus network design, Varne and team's project [5] using Cisco Packet Tracer emphasizes scalability, connectivity, security, and technology integration. Significant learnings encompass hierarchical design principles, VLAN implementation, DHCP automation, and Quality of Service (QoS) considerations. The study concludes by highlighting Packet Tracer's pivotal role in effective network prototyping, allowing for thorough testing and validation before actual deployment.

Banothe et al. [6] contribute to the literature by detailing the architecture of a college campus network using Cisco Packet Tracer, incorporating various elements such as hierarchical architecture, VLAN implementation, routing, switching, and security measures. The study emphasizes the importance of Packet Tracer in simulating and testing the proposed architecture, ensuring its effectiveness before real-world implementation.

The secure campus network design presented in [7] proposes a topology with multiple networks and VLANs, incorporating various protocols and network devices. The study aimed to create a fast, reliable, and redundant campus network, leveraging Ethernet connectivity, server deployment, firewall implementation, and IP telephony. Results demonstrated successful configuration and functionality, with discussions on cost reduction strategies and future work focused on network updates for improved performance.

The implementation of a company network scenario using Cisco Packet Tracer Simulation Software, as presented in [8], outlines objectives that include creating a secure WAN network for company communication with an emphasis on data security and efficient communication. The study identifies pros such as improved scalability, bandwidth performance, reduced congestion, and enhanced manageability through VLANs. However, it acknowledges challenges in scalability and proposes future work to enhance scalability through network architecture redesign, advanced routing protocols, and hardware upgrades. Additionally, the study suggests improving security measures, leveraging emerging technologies, and implementing redundancy for optimal network performance and resilience. Emerging trends like software-defined networking (SDN) and network function virtualization (NFV) are recognized as potential game-changers in shaping the future scope of the study, enhancing flexibility and efficiency in network management and operations.

In conclusion, the amalgamation of these diverse studies not only enriches the understanding of Cisco Packet Tracer's versatile application but also underscores its pivotal role in shaping educational environments, enhancing cybersecurity measures, and optimizing network designs. The trends identified across these studies collectively contribute to a holistic view of the tool's impact and potential for future advancements in the ever-evolving landscape of networking and education. As we delve deeper into these trends, the literature survey not only serves as a valuable repository of knowledge but also paves the way for further research, innovation, and the continued evolution of Cisco Packet Tracer's applications in diverse domains.

Cit. No.	**Year**	**Title of the paper**	**Author**	**Description**	**Remark**
[1]	2020	Configuration of Firewalls in Educational Organisation LAB setup by using Cisco Packet Tracer	P Srikanth Reddy, P Saleem Akram,	This study explores leveraging Cisco Packet Tracer as a virtual laboratory for teaching firewall concepts. It emphasizes cost-effectiveness, hands-on practicality, and	Emphasizes the tool's effectiveness in practical cybersecurity education.

	2021		T.V. Ramana, P. Aditya Sai Ram, R Pruthvi Raj, M Adarsh Sharma	simulation of intricate network architectures, enhancing students' understanding.	

[2]	2021	Secured Internet Office Network with the Internet of Things Using Packet Tracer Analysis	Azrai Danial Azhari;
			Norakmar Arbain Sulaiman;
			Murizah Kassim
				Focused on integrating IoT into a secured small office network, this study employs Cisco Packet Tracer. Trends identified include VLANs, DHCP, Cisco ASA Firewall, and SSL VPN. It emphasizes design considerations, security measures, and potential future work.	Highlights trends in IoT implementation and suggests avenues for future user studies.

[3]	2021	Designing a secure campus network and simulating it using Cisco packet tracer	Alaa H. Ahmed, Mokhaled N. A. Al-Hamadani	The study concentrates on developing a Secure Campus Network (SCN) using Cisco Packet Tracer, emphasizing a comprehensive network topology, VLANs, DHCP, and security measures. Future work is proposed to explore advanced security protocols and test network resilience	Identifies key trends in campus network security and proposes directions for future work.
[4]	2022	A Review of the Role of Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview	Taherdoost	This review paper provides insights into frequently used cybersecurity standards and frameworks, distinguishing between them. It offers a comprehensive overview of standards like ISO 27001 and frameworks such as the NIST Cybersecurity Framework.	Provides valuable insights into choosing cybersecurity frameworks based on organizational needs.
[5]	2023	Campus Network Design and Implementation using Cisco Packet Tracer	Preetham N Varne, Priyanka J, Snehith Shetty V,	The project using Cisco Packet Tracer focuses on campus network design, highlighting scalability, connectivity, security, and	Demonstrates the pivotal role of Packet Tracer in effective network prototyping.

	2023		Tejus A K, Naveen Chandra Gowda	technology integration. Key learnings include hierarchical design, VLAN implementation, DHCP automation, and QoS considerations.	
[6]	2023	Architecture of College Campus Network using Cisco Packet Tracer	Yunisha Banothe, Roshni Thakur, Aman Banothe, Prof. P. Jaipurkar	Detailing the architecture of a college campus network using Cisco Packet Tracer, this study incorporates hierarchical architecture, VLAN implementation, routing, switching, and security measures. Packet Tracer's role in simulating and testing is emphasized.	Highlights Packet Tracer's importance in simulating proposed architectures.
[7]	2023	Campus Network Configuration, Monitoring and Data Flow Simulation using Cisco Packet Tracer	Shahadat Hoshen Moz, Md Apu Hosen, Nice Fatema Islam Tanny	This paper proposes a secure campus network design with multiple networks, VLANs, and various protocols/devices. It aims for a fast, reliable, and redundant network, leveraging Ethernet connectivity, server deployment, firewall implementation, and IP telephony.	Emphasizes creating a fast, reliable, and redundant network
[8]	2018	Implementation of a Company Network Scenario Module by using Cisco Packet Tracer Simulation Software	Ashish Kumar	The implementation of a company network scenario using Cisco Packet Tracer outlines objectives such as creating a secure WAN network. It identifies pros like improved scalability and enhanced manageability through VLANs but acknowledges challenges in scalability, proposing future work for improvements.	Acknowledges pros and challenges, suggesting future improvements and trends.

Table 1. Summary of Literature Survey.

In conclusion, the literature survey offers a comprehensive exploration of diverse studies focused on the application of Cisco Packet Tracer in educational and cybersecurity contexts. The highlighted studies contribute valuable insights into trends and shortcomings within the field. Notable contributions include Reddy et al.'s emphasis on practical cybersecurity education, Azhari and team's exploration of IoT integration, Ahmed and Al-Hamadani's focus on secure campus network development, Taherdoost's review of cybersecurity standards, Varne and team's project on campus network design, Banothe et al.'s detailing of college campus network architecture, and the company network scenario implementation by Kumar. While these studies enrich our understanding of Packet Tracer's versatility, they also reveal challenges such as scalability and suggest future work, showcasing the evolving landscape of networking and education. This literature survey serves as a valuable repository, paving the way for further research, innovation, and the continued evolution of Cisco Packet Tracer's applications in diverse domains.

3. Project Set-Up

This chapter encompasses a detailed exploration of the KJ Somaiya College of Engineering (KJSCE) campus network topology and mapping. Through a comprehensive overview, we identified key components, such as routers, switches, buildings, and departments, illustrating their roles within the network. Utilizing Cisco Packet Tracer, we simulated the network's configuration, VLAN setups, and IP assignments. This detailed examination sets the stage for the subsequent chapter, where we move from theory to practice in the implementation of a robust cybersecurity framework for KJSCE.

3.1 Introduction

In the pursuit of fortifying the cybersecurity posture of KJSCE (KJSCE), a thorough security evaluation of the campus network has been undertaken. The assessment's core objectives encompass the identification of potential security vulnerabilities, analysis of existing security controls, and the provision of strategic recommendations to enhance the network's overall security resilience. Recognizing the indispensable role that the university's network plays in supporting academic and administrative operations, safeguarding it against online threats becomes paramount. This initiative endeavors to establish a robust cybersecurity framework for KJSCE, ensuring a secure digital infrastructure conducive to uninterrupted and resilient institutional functioning.

3.2 Network Topology

Network topology is the architectural layout that defines the physical and logical arrangement of interconnected devices within a computer network. It serves as the blueprint for how different network components, such as routers, switches, servers, and end-user devices, are organized and connected. The choice of network topology plays a crucial role in determining the network's efficiency, scalability, and overall performance. This introductory paragraph sets the stage for a comprehensive exploration of the network topology employed in KJSCE (KJSCE), providing insights into the design principles and components that form the foundation of the institution's digital infrastructure. In this network topology, we have discussed the basic version of the campus network topology with limited security controls like VPN tunnelling and a sniffer to monitor the network.

This KJSCE's campus network comprises the following components:

- Campus Network Topology:
    1. Somaiya Campus Router
    2. Somaiya Campus Switch
    3. Cloud
    4. 2 Buildings (Aryabhatta and Bhaskaracharya)
    5. Departments:
        - Aryabhatta Building:
            - ➔ Admin Office
            - ➔ Mechanical Branch

        - ➔ Examination Cell
        - ➔ EXTC Branch
        - ➔ Admission Office
    - Bhaskaracharya Building:
        - ➔ Data Center
        - ➔ Computer Branch
        - ➔ IT Branch
        - ➔ ETRX Branch

The following are Cisco Packet Tracer components which were used to construct the network topology:

- 3650-24PS Switch:
    - It is designed for use in enterprise access networks.
    - It is a 24-port Gigabit Ethernet switch with PoE capability.
    - It offers a wide range of features, including support for Cisco StackWise technology, advanced security features, QoS features, and Layer 2 and Layer 3 switching capabilities.
    - It is a versatile and powerful switch that can be used in a variety of enterprise access network deployments.
    - It is ideal for applications such as office networks, retail networks, educational networks, healthcare networks, and industrial networks.
    - It is a reliable and scalable switch that can help to improve the performance and security of your enterprise network.
- 2911-Router:
    - The 2911-Router is a mid-range, integrated services router that is available in Cisco Packet Tracer.
    - It offers a wide range of features, including 4 Gigabit Ethernet ports, 2 T1/E1 WAN ports, 2 USB 2.0 ports, support for Cisco IOS software, integrated firewall and VPN features, QoS features, and Layer 2 and Layer 3 routing capabilities.
    - It is a versatile and powerful router that can be used in a variety of enterprise network deployments, such as branch office networking, remote access, internet connectivity, voice over IP (VoIP), and small business networking.
    - It is a reliable and scalable router that can help to improve the performance and security of your enterprise network.
- Server-PT:
    - The Server-PT is a virtual server that is used in Cisco Packet Tracer to simulate a real-world server.
    - It can be configured to run a variety of server applications, such as web servers, file servers, and database servers.
    - It is a versatile and powerful tool that can be used to learn about and test server configurations.

- 2690 IOS15 Switch:
    - The 2690 IOS15 switch is a Layer 2 switch that is used in Cisco Packet Tracer to simulate a real-world switch.
    - It can be configured with a variety of features, such as VLANs, STP, and QoS.
    - It is a versatile and powerful tool that can be used to learn about and test switch configurations.
- PC-PT:
    - The PC-PT is a virtual computer that is used in Cisco Packet Tracer to simulate a real-world PC.
    - It can be configured to run a variety of PC applications, such as web browsers, email clients, and office productivity software.
    - It is a versatile and powerful tool that can be used to learn about and test PC configurations.
- Laptop-PT:
    - The Laptop-PT is a virtual laptop that is used in Cisco Packet Tracer to simulate a real-world laptop.
    - It can be configured to run a variety of client applications, such as web browsers, email clients, and file transfer clients.
    - It is a versatile and powerful tool that can be used to learn about and test client configurations.

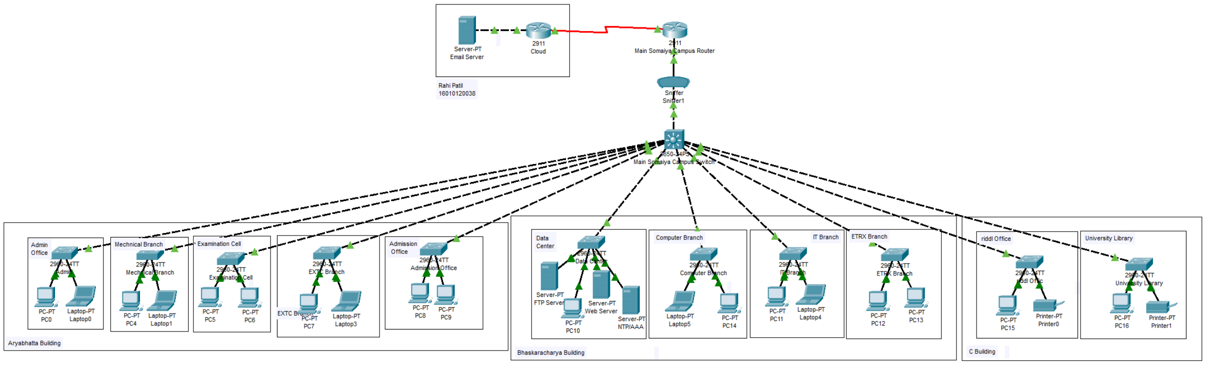


Fig 1. Basic Network Topology.

After implementing the basic network topology, we have tried to propose the following advanced network topology with security measures to secure the campus network. The new network topology devices consist of:

- 5506-X CISCO ASA Firewall:
    - Advanced security features such as stateful packet inspection and VPN capabilities.
    - Enforces security policies and protects the network from external threats.
    - Provides secure remote access and site-to-site connectivity.

- 3650 - 24 PS Multilayer Switch:
    - Supports Layer 2 and Layer 3 routing functions for VLAN routing and inter-VLAN routing.
    - Provides Power over Ethernet (PoE) for powering devices like IP phones and wireless access points.
    - Offers advanced features like Quality of Service (QoS) and Access Control Lists (ACLs) for traffic optimization and security.
- 2960 - 24TT Switch:
    - Basic Layer 2 switch for connecting end-user devices like laptops, printers, and smartphones.
    - Supports VLANs, port security, and basic QoS capabilities.
    - Provides cost-effective and reliable network connectivity for small to medium-sized deployments.
- WLC-2504 Wireless LAN Controller:
    - Centralized management of wireless access points (APs) for efficient network management.
    - Enables centralized configuration, firmware updates, and monitoring of wireless network performance.
    - Provides features like guest access, wireless LAN segmentation, and rogue AP detection for enhanced security and performance.
- End-User Devices (Laptop, Printer, Tablets, Smartphone):
    - Devices connected to the network for accessing resources, printing documents, and communication.
    - Require appropriate network access policies and security measures to prevent unauthorized access and data breaches.
    - Play a crucial role in the productivity and efficiency of users within the network environment.
- Lightweight Access Point - LAP-PT:
    - Simulated wireless access point for providing wireless connectivity to devices within the network.
    - Requires configuration of SSIDs, security settings, and RF settings for optimal performance.
    - Enables seamless and secure wireless access for users, supporting mobility and flexibility in the network.
- 2911 - Router:
    - Provides routing, security, and WAN connectivity services for the network.
    - Supports dynamic routing protocols like OSPF and EIGRP, as well as VPN capabilities for secure communication.
    - Offers firewall functionality and access control features to protect the network from unauthorized access and attacks.

- Server - PT:
    - Hosts centralized services such as file storage, application hosting, and database management.
    - Requires security measures like access controls, encryption, and regular patching to protect sensitive data.
    - Provides critical resources and applications to users and devices within the network, enhancing productivity and efficiency.

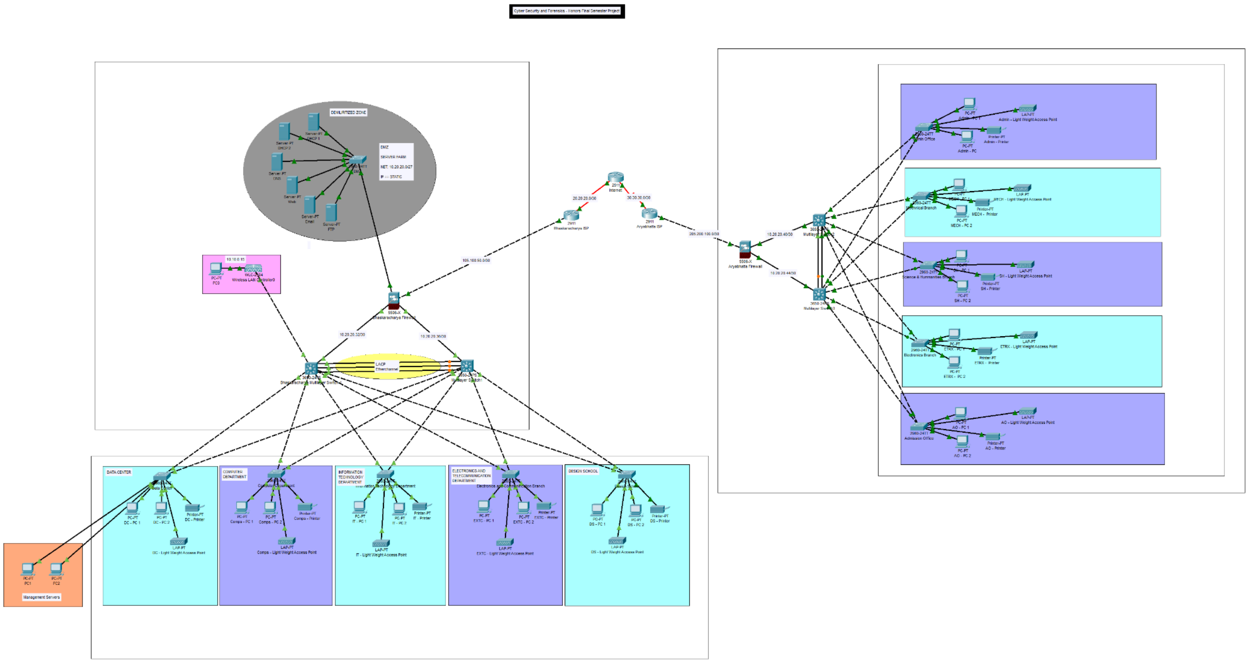

Cyber Security and Forensics - Honors Final Semester Project
DEMILITIZED ZONE
Server-PT DHCP 1
Server-PT DHCP 2
Server-PT DNS
Server-PT Web
Server-PT Email
Server-PT FTP
DMZ
SERVER FARM
NET: 10.20.20.0/27
IP == STATIC
10.10.0.15
PC-PT PC0
WLC-2504 Wireless LAN Controller0
2911 Internet
20.20.20.0/30
30.30.30.0/30
2911 Bhaskaracharya ISP
2911 Aryabhatta ISP
105.100.50.0/30
205.200.100.0/30
5506-X Bhaskaracharya Firewall
5506-X Aryabhatta Firewall
10.20.20.32/30
10.20.20.36/30
10.20.20.40/30
10.20.20.44/30
LACP Etherchannel
3650-24PS Bhaskaracharya Multilayer Switch
3650-24PS Multilayer Switch1
3650-24PS Multilayer Switch2
3650-24PS Multilayer Switch3
DATA CENTER
COMPUTER DEPARTMENT
INFORMATION TECHNOLOGY DEPARTMENT
ELECTRONICS AND TELECOMMUNICATION DEPARTMENT
DESIGN SCHOOL
PC-PT DC - PC 1
PC-PT DC - PC 2
Printer-PT DC - Printer
LAP-PT DC - Light Weight Access Point
PC-PT Comps - PC 1
PC-PT Comps - PC 2
Printer-PT Comps - Printer
LAP-PT Comps - Light Weight Access Point
PC-PT IT - PC 1
PC-PT IT - PC 2
Printer-PT IT - Printer
LAP-PT IT - Light Weight Access Point
PC-PT EXTC - PC 1
PC-PT EXTC - PC 2
Printer-PT EXTC - Printer
LAP-PT EXTC - Light Weight Access Point
PC-PT DS - PC 1
PC-PT DS - PC 2
Printer-PT DS - Printer
LAP-PT DS - Light Weight Access Point
PC-PT PC1
PC-PT PC2
Management Servers
2960-24TT Admin Office
PC-PT Admin - PC 1
PC-PT Admin - PC
Printer-PT Admin - Printer
LAP-PT Admin - Light Weight Access Point
2960-24TT Mechnical Branch
PC-PT MECH - PC 1
PC-PT MECH - PC 2
Printer-PT MECH - Printer
LAP-PT MECH - Light Weight Access Point
2960-24TT Science & Hummanities Branch
PC-PT SH - PC 1
PC-PT SH - PC 2
Printer-PT SH - Printer
LAP-PT SH - Light Weight Access Point
2960-24TT Electronics Branch
PC-PT ETRX - PC 1
PC-PT ETRX - PC 2
Printer-PT ETRX - Printer
LAP-PT ETRX - Light Weight Access Point
2960-24TT Admission Office
PC-PT AO - PC 1
PC-PT AO - PC 2
Printer-PT AO - Printer
LAP-PT AO - Light Weight Access Point

Fig 2. Advanced Network Topology.

The transition from a basic network topology to an advanced one involves several critical enhancements aimed at bolstering security, scalability, and efficiency within the college's network infrastructure like:

- Enhanced Security Measures: The advanced network topology incorporates robust security measures such as VLAN segmentation, firewall configurations, HSRP for redundancy, and IPsec VPN for secure remote access. These measures are crucial for protecting sensitive data, preventing unauthorized access, and ensuring the integrity of network communications, especially in a college environment where diverse users and devices access the network.
- Improved Network Resilience: By implementing HSRP and EtherChannel for redundancy and load balancing, the advanced network topology enhances network resilience and fault tolerance. This ensures uninterrupted network connectivity and mitigates the impact of potential hardware failures or network disruptions, providing a more reliable network infrastructure for students, faculty, and staff.
- Scalability and Efficiency: The advanced network topology includes features such as OSPF for dynamic routing and VLAN assignment with DHCP server configurations. These

enhancements facilitate efficient resource allocation, scalability, and management of network resources, allowing for seamless expansion and adaptation to changing campus requirements over time.

- Comprehensive Monitoring and Testing: The advanced network topology emphasizes thorough verification and testing of configurations to ensure functionality, interoperability, and security compliance. This proactive approach to network management helps identify and address potential issues or vulnerabilities before deployment, minimizing the risk of downtime or security breaches.

In summary, the transition to an advanced network topology from a basic one is essential for addressing the evolving cybersecurity challenges, improving network resilience, scalability, and efficiency, and ensuring the college's network infrastructure can effectively support its academic and administrative operations.

3.2.1 Device Configurations

- Normal KJSCE Network Topology:

Building	Department	Device	IP Address	Subnet mask
A	Admin (VLAN 10)	PC0	192.168.1.2	255.255.255.0
	Mechanical Branch (VLAN 20)	PC4	192.168.2.2	255.255.255.0
	Examination Cell (VLAN 30)	PC5	192.168.3.4	255.255.255.0
	EXTC (VLAN 40)	PC7	192.168.4.2	255.255.255.0
	Admission Office (VLAN 50)	PC8	192.168.5.5	255.255.255.0
B	Data Center (VLAN 60)	PC10	192.168.6.2	255.255.255.0
	Computer Branch (VLAN 70)	PC14	192.168.7.3	255.255.255.0
	IT Branch(VLAN 80)	PC11	192.168.8.2	255.255.255.0
	ETRX(VLAN 90)	PC12	192.168.9.4	255.255.255.0

Table 2. Device Configuration Table of Basic Network Topology.

- Advanced Network Topology:

Category		Network and Subnet mask	Valid Host Address	Default Gateway	Broadcast address
WLAN	Bhaskaracharya	10.10.0.0\16	10.10.0.1 to 10.10.255.254	10.10.0.1	10.10.255.254
	Aryabhatta	10.10.0.0\16	10.11.0.1 to 10.11.255.154	10.11.0.1	10.11.255.254
LAN	Bhaskaracharya	172.16.0.0\16	172.16.0.1 to 172.16.255.254	172.16.0.1	172.16.255.255

	Aryabhatta	172.17.0.0\16	172.17.0.1 to 172.17.255.254	172.17.0.1	172.17.255.255
Management		192.168.10.0\24	192.168.10.1 to 192.168.19.254	192.168.10.1	192.168.10.255
DMZ		10.10.10.0\27	10.10.10.1 to 10.10.10.30	10.10.10.1	10.10.10.31

Table 3. Device Configurations Details of Advanced Network Topology.

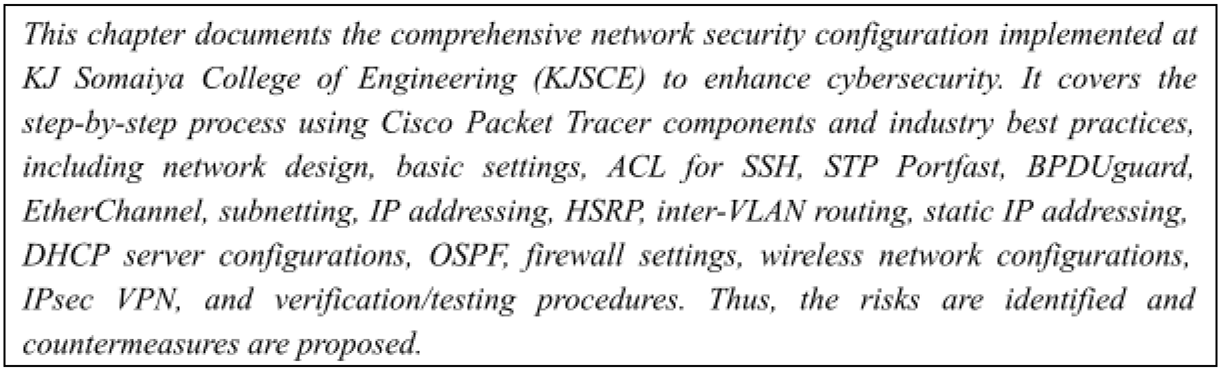
	Network Address
Cloud Area	8.0.0.0/8
Bhaskaracharya ISP - Internet	20.20.20.0/30
Aryabhatta ISP - Internet	30.30.30.0/30
Bhaskaracharya Firewall - Bhaskaracharya ISP	105.100.50.0/30
Aryabhatta Firewall - Aryabhatta ISP	205.200.100.0/30
Bhaskaracharya Firewall - MLSW 1	10.20.20.32/30
Bhaskaracharya Firewall - MLSW 2	10.20.20.36/30
Aryabhatta Firewall - MLSW 1	10.20.20.40/30
Aryabhatta Firewall - MLSW 2	10.20.20.44/30

Table 4. Network Addresses in Advanced Network Topology.

3.3 Conclusion

In conclusion, this chapter delved into the intricacies of the KJSCE's network topology and mapping for the KJSCE's campus. We examined the diverse components, ranging from routers and switches to buildings and departments, using Cisco Packet Tracer. The network configuration, VLAN setups, and IP assignments were meticulously detailed, providing a comprehensive understanding of the campus network's structure. In this we have implemented VPN tunneling to key the data encrypted and not get caught on the Cisco sniffer. With these foundational elements in place, we are now poised on the brink of our objective: designing and implementing a robust cybersecurity framework for KJSCE. The subsequent chapter will bridge the theoretical groundwork laid here with its practical application, bringing us closer to fortifying the network's security posture.

4. Implementation and Experimentation



This chapter documents the comprehensive network security configuration implemented at KJ Somaiya College of Engineering (KJSCE) to enhance cybersecurity. It covers the step-by-step process using Cisco Packet Tracer components and industry best practices, including network design, basic settings, ACL for SSH, STP Portfast, BPDUguard, EtherChannel, subnetting, IP addressing, HSRP, inter-VLAN routing, static IP addressing, DHCP server configurations, OSPF, firewall settings, wireless network configurations, IPsec VPN, and verification/testing procedures. Thus, the risks are identified and countermeasures are proposed.

4.1 Network Security Configuration:

The evolution of technology has profoundly reshaped educational institutions, with networking infrastructure serving as a cornerstone for seamless communication, collaboration, and access to resources within academic environments. A robust and secure campus network is essential to ensure the efficient operation and protection of digital assets within the institution. Transitioning from a basic to an advanced network topology represents a strategic shift aimed at addressing emerging cybersecurity threats and enhancing network resilience, scalability, and efficiency. By integrating sophisticated security measures, optimizing network performance, and implementing advanced technologies such as VLAN segmentation, HSRP, and IPsec VPN, the advanced network topology promises to establish a secure, reliable, and adaptable network infrastructure capable of meeting the diverse academic and administrative needs of the college. This progression reflects a commitment to providing a safe and conducive digital environment that empowers students, faculty, and staff to thrive in today's interconnected world.

4.1.1 Network Design and Beautification:

This involves planning the layout of your network, including where devices will be placed, how they will connect to each other, and how data will flow between them. This typically includes creating a network diagram.

Organizing the physical and logical layout of the network in a clean and understandable manner. This includes labeling devices, organizing cables neatly, and ensuring that the network topology is clear and easy to follow.

It is implemented as a well-designed network reduces the likelihood of misconfigurations and makes it easier to implement security measures consistently across the campus.

Implementing in Cisco Packet Tracer:

- Open Cisco Packet Tracer and start by adding devices from the toolbar on the left.
- Arrange the devices on the workspace by dragging and dropping them into position.
- Use the Connection tool to connect devices with appropriate cables (Ethernet, serial, etc.).
- Use the Label tool to add labels to devices and connections for clarity.

- Organize the layout of devices logically, considering factors such as physical proximity, data flow, and network hierarchy

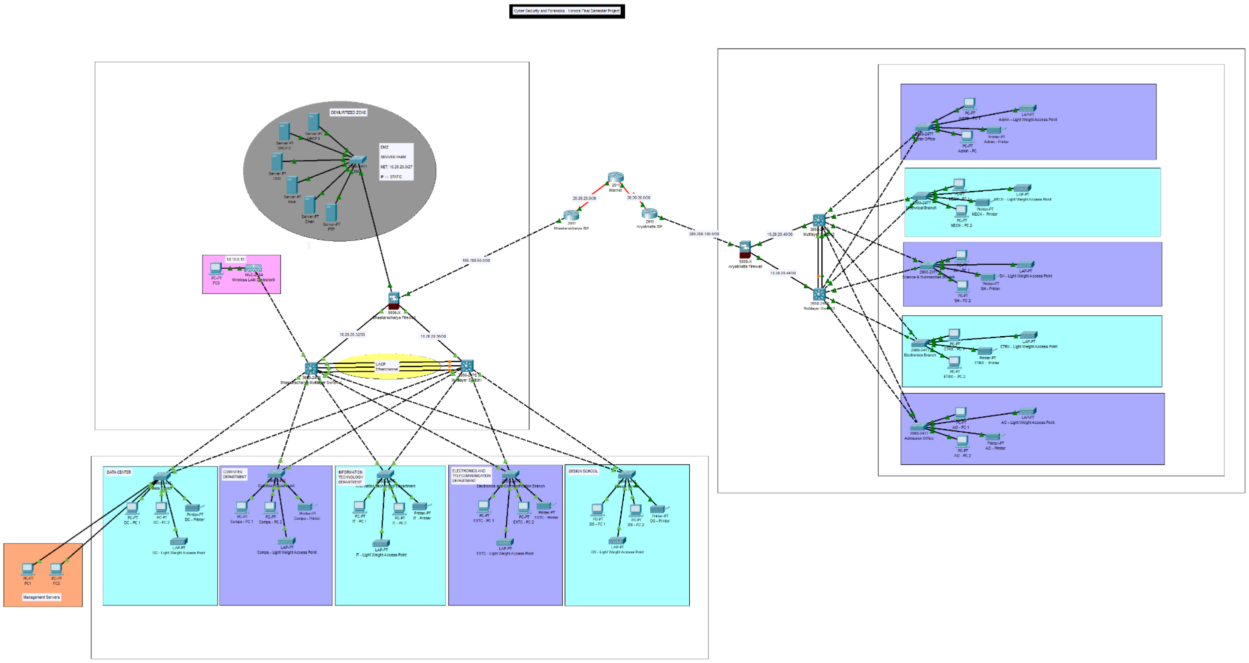


Fig 3. Advanced Network Topology before Configuration.

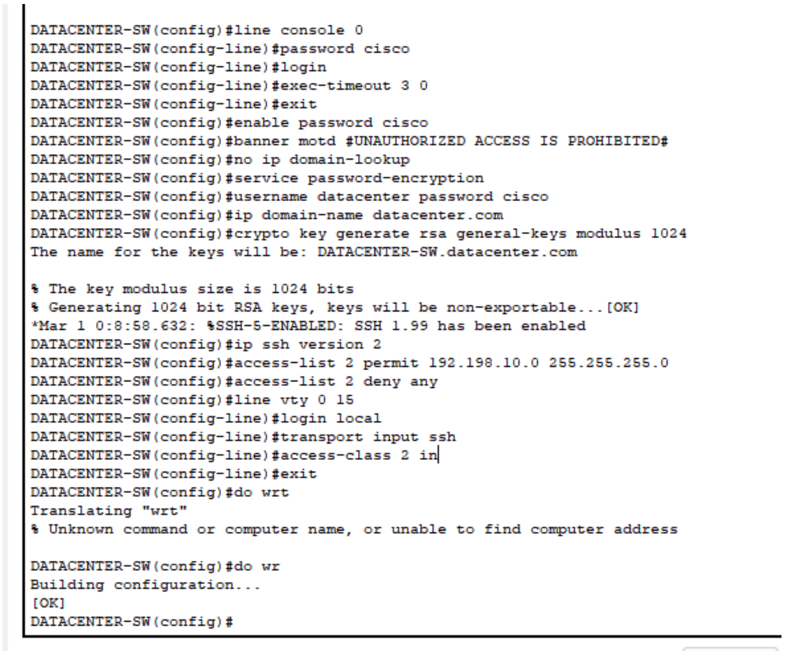
4.1.2 Basic Settings and Standard ACL for SSH:

This includes initial configuration tasks such as setting the hostname, domain name, and management IP address on each device. It also involves setting a secure password for device access. An ACL (Access Control List) is a set of rules that control traffic entering or exiting a network interface. By creating a standard ACL for SSH, you're specifying which IP addresses are allowed to connect to the device via SSH. This restricts SSH access to only authorized users or devices.

By configuring SSH and implementing an ACL for SSH access, one can ensure that only authorized administrators can access network devices remotely, reducing the risk of unauthorized access and potential security breaches.

Implementation in Cisco Packet Tracer:

- Double-click on each device to open its configuration dialog box.
- Configure basic settings such as hostname, domain name, and management IP address under the "Config" tab.
- Access the device's CLI by clicking on the "CLI" tab.
- Create a standard ACL using the access-list command to permit SSH access from specific IP addresses and apply it to the VTY lines using the line vty command.



```
DATACENTER-SW(config)#line console 0
DATACENTER-SW(config-line)#password cisco
DATACENTER-SW(config-line)#login
DATACENTER-SW(config-line)#exec-timeout 3 0
DATACENTER-SW(config-line)#exit
DATACENTER-SW(config)#enable password cisco
DATACENTER-SW(config)#banner motd #UNAUTHORIZED ACCESS IS PROHIBITED#
DATACENTER-SW(config)#no ip domain-lookup
DATACENTER-SW(config)#service password-encryption
DATACENTER-SW(config)#username datacenter password cisco
DATACENTER-SW(config)#ip domain-name datacenter.com
DATACENTER-SW(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: DATACENTER-SW.datacenter.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:8:58.632: %SSH-5-ENABLED: SSH 1.99 has been enabled
DATACENTER-SW(config)#ip ssh version 2
DATACENTER-SW(config)#access-list 2 permit 192.198.10.0 255.255.255.0
DATACENTER-SW(config)#access-list 2 deny any
DATACENTER-SW(config)#line vty 0 15
DATACENTER-SW(config-line)#login local
DATACENTER-SW(config-line)#transport input ssh
DATACENTER-SW(config-line)#access-class 2 in
DATACENTER-SW(config-line)#exit
DATACENTER-SW(config)#do wrt
Translating "wrt"
% Unknown command or computer name, or unable to find computer address

DATACENTER-SW(config)#do wr
Building configuration...
[OK]
DATACENTER-SW(config)#
```

Fig 4. Basic Configuration of MLSW.

4.1.3 STP Portfast and BPDUguard Configurations:

STP Portfast: Spanning Tree Protocol (STP) is used to prevent loops in redundant network topologies. Portfast is a feature that bypasses the normal STP listening and learning states, allowing a port to transition directly to the forwarding state. This reduces the time it takes for end devices to become operational when they are connected to the network.

BPDUguard: BPDU (Bridge Protocol Data Unit) guard is a feature that protects the network from unauthorized switches being connected. It does this by shutting down ports that receive BPDUs, which are typically only sent by other switches. This helps prevent rogue devices from causing network instability or security issues.

Implementation in Cisco Packet Tracer:

- Access the CLI of each switch and enter the global configuration mode.
- Enable Portfast on access ports using the spanning-tree portfast command.
- Enable BPDUguard on access ports using the spanning-tree bpduguard enable command.

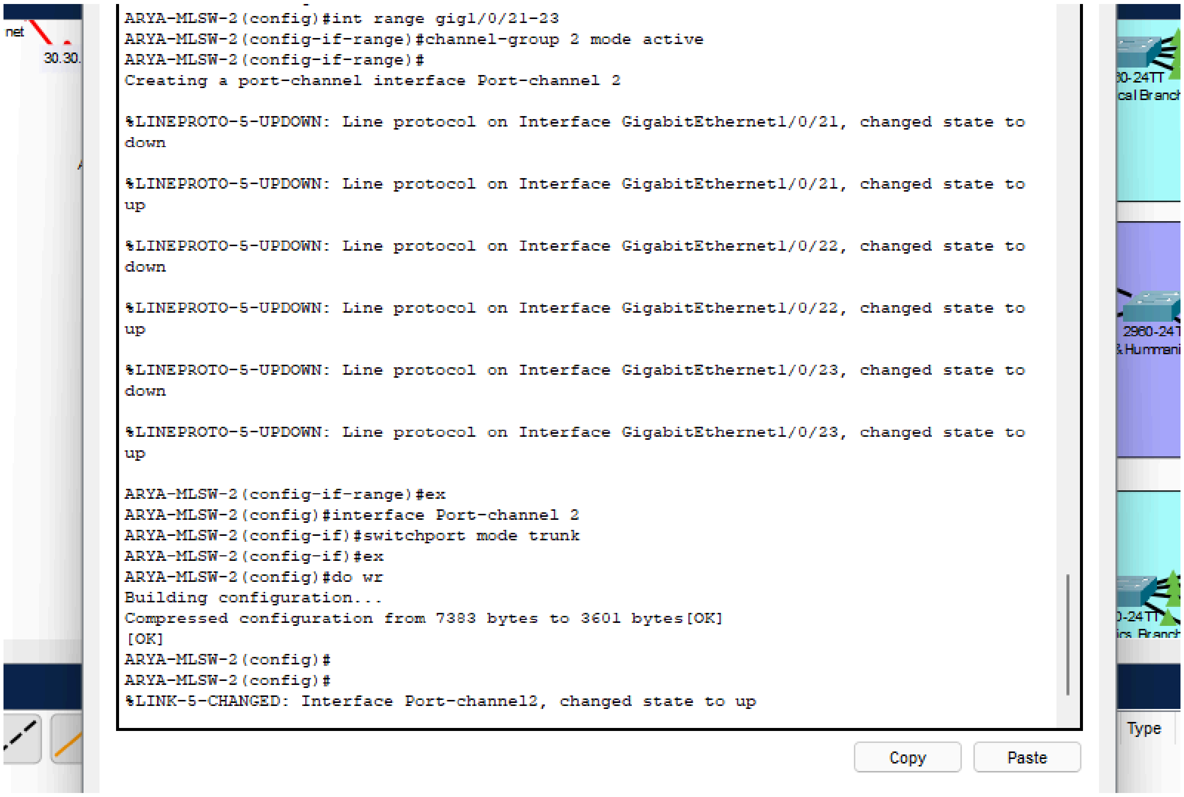
4.1.4 EtherChannel:

EtherChannel allows you to bundle multiple physical links between switches into a single logical link. This increases the bandwidth between switches and provides redundancy in case one of the links fails. It also improves network performance by load balancing traffic across the bundled links.

It provides redundancy and load balancing, improving network availability and performance. This helps mitigate the impact of network failures and ensures that traffic continues to flow smoothly even under adverse conditions, reducing the risk of disruptions or downtime due to security incidents.

Implementation in Cisco Packet Tracer:

- Access the CLI of each switch and enter the interface configuration mode for the interfaces you want to bundle.
- Create an EtherChannel interface using the channel-group command and specify the desired protocol (e.g., LACP or PAgP).



```
ARYA-MLSW-2(config)#int range gig1/0/21-23
ARYA-MLSW-2(config-if-range)#channel-group 2 mode active
ARYA-MLSW-2(config-if-range)#
Creating a port-channel interface Port-channel 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/21, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/21, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/22, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/22, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to
up

ARYA-MLSW-2(config-if-range)#ex
ARYA-MLSW-2(config)#interface Port-channel 2
ARYA-MLSW-2(config-if)#switchport mode trunk
ARYA-MLSW-2(config-if)#ex
ARYA-MLSW-2(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
ARYA-MLSW-2(config)#
ARYA-MLSW-2(config)#
%LINK-5-CHANGED: Interface Port-channel2, changed state to up
```

Fig 5. Etherchannel Configuration.

4.1.5 Subnetting and IP Addressing:

Subnetting involves dividing a larger network into smaller, more manageable subnetworks. Each subnet can then have its own range of IP addresses, which helps with network organization and efficiency. Assigning IP addresses to devices on the network ensures that they can communicate with each other. Proper IP addressing also helps with security, as it allows you to implement access control policies based on IP addresses.

Subnetting allows for segmentation of the network, which can contain and isolate security incidents, limiting their impact on the rest of the network. Proper IP addressing facilitates access control and traffic filtering based on IP addresses, enabling more granular security policies.

Implementation in Cisco Packet Tracer:

- Access the CLI of routers and switches.
- Enter the interface configuration mode for each interface and assign an IP address and subnet mask using the ip address command.

4.1.6 HSRP and Inter-VLAN Routing:

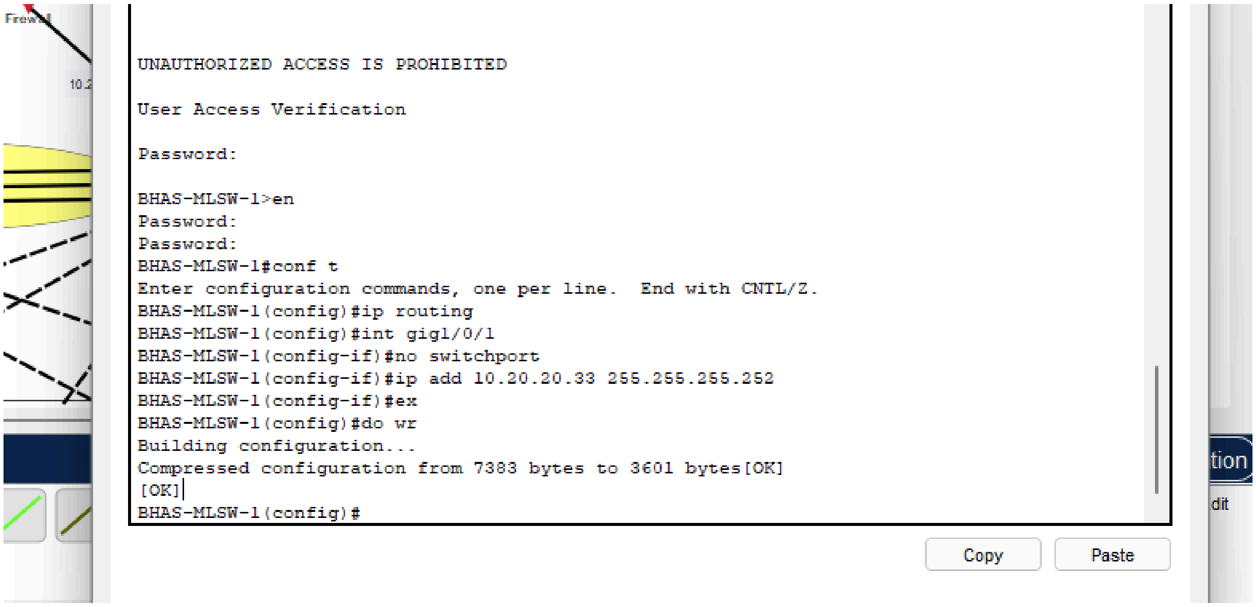
Hot Standby Router Protocol (HSRP) is a redundancy protocol that allows two or more routers to work together in a group, providing backup in case one router fails. It ensures that there is always a backup default gateway available for devices on the network.

Inter-VLAN routing allows devices in different VLANs to communicate with each other. This is important for segregating traffic on the network and enforcing security policies between different parts of the network.

HSRP ensures high availability of the default gateway, reducing the risk of network downtime due to router failures. Inter-VLAN routing enables controlled communication between different network segments, allowing for the enforcement of security policies and isolation of sensitive resources.

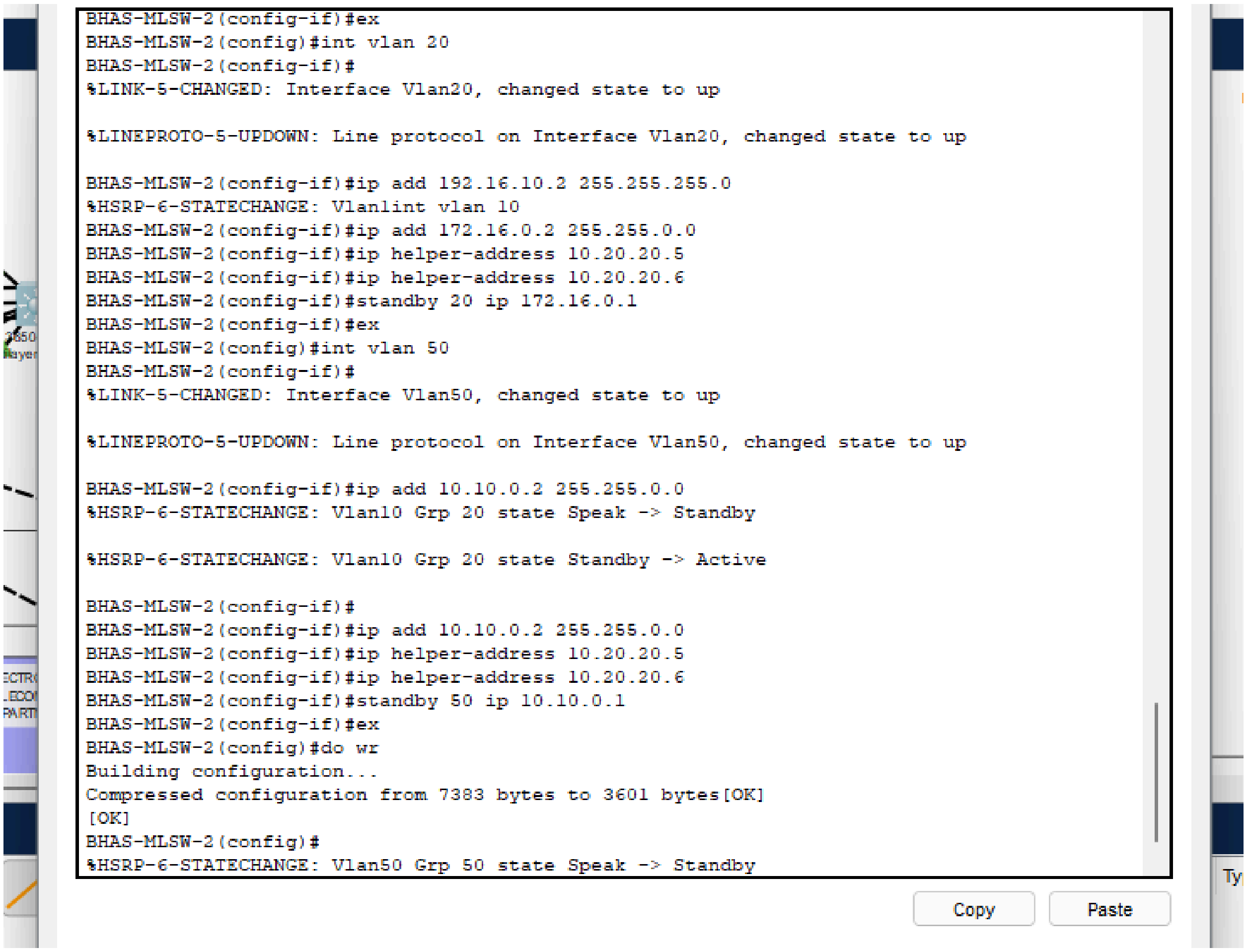
Implementation in Cisco Packet Tracer:

- Access the CLI of routers.
- Configure HSRP on the interfaces facing the internal network using the standby commands.
- Configure subinterfaces on routers for inter-VLAN routing, assigning IP addresses from each VLAN subnet to the respective subinterfaces.



```
UNAUTHORIZED ACCESS IS PROHIBITED

User Access Verification

Password:

BHAS-MLSW-1>en
Password:
Password:
BHAS-MLSW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BHAS-MLSW-1(config)#ip routing
BHAS-MLSW-1(config)#int gig1/0/1
BHAS-MLSW-1(config-if)#no switchport
BHAS-MLSW-1(config-if)#ip add 10.20.20.33 255.255.255.252
BHAS-MLSW-1(config-if)#ex
BHAS-MLSW-1(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
BHAS-MLSW-1(config)#
```

Fig 6. VLAN Routing Configuration.



```
BHAS-MLSW-2(config-if)#ex
BHAS-MLSW-2(config)#int vlan 20
BHAS-MLSW-2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

BHAS-MLSW-2(config-if)#ip add 192.16.10.2 255.255.255.0
%HSRP-6-STATECHANGE: Vlanlint vlan 10
BHAS-MLSW-2(config-if)#ip add 172.16.0.2 255.255.0.0
BHAS-MLSW-2(config-if)#ip helper-address 10.20.20.5
BHAS-MLSW-2(config-if)#ip helper-address 10.20.20.6
BHAS-MLSW-2(config-if)#standby 20 ip 172.16.0.1
BHAS-MLSW-2(config-if)#ex
BHAS-MLSW-2(config)#int vlan 50
BHAS-MLSW-2(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

BHAS-MLSW-2(config-if)#ip add 10.10.0.2 255.255.0.0
%HSRP-6-STATECHANGE: Vlan10 Grp 20 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 20 state Standby -> Active

BHAS-MLSW-2(config-if)#
BHAS-MLSW-2(config-if)#ip add 10.10.0.2 255.255.0.0
BHAS-MLSW-2(config-if)#ip helper-address 10.20.20.5
BHAS-MLSW-2(config-if)#ip helper-address 10.20.20.6
BHAS-MLSW-2(config-if)#standby 50 ip 10.10.0.1
BHAS-MLSW-2(config-if)#ex
BHAS-MLSW-2(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
BHAS-MLSW-2(config)#
%HSRP-6-STATECHANGE: Vlan50 Grp 50 state Speak -> Standby
```

Fig 7. HSRP Configuration.

4.1.7 Static IP Addressing for DMZ/Server Farm Devices:

Assigning static IP addresses to devices in the DMZ or server farm ensures that they always have the same IP address. This makes it easier to manage and troubleshoot these devices, as their IP addresses won't change. The DMZ is a network segment that sits between the internal network and the external (public) network, typically containing servers that need to be accessible from both the internal network and the internet.

Static IP addressing for DMZ and server farm devices simplifies access control and firewall configurations, reducing the likelihood of misconfigurations that could lead to security vulnerabilities. It also helps in tracking and monitoring these critical assets more effectively.

Implementation in Cisco Packet Tracer:

- Access the configuration interface of each DMZ/server farm device.
- Assign a static IP address, subnet mask, default gateway, and DNS server address as required.

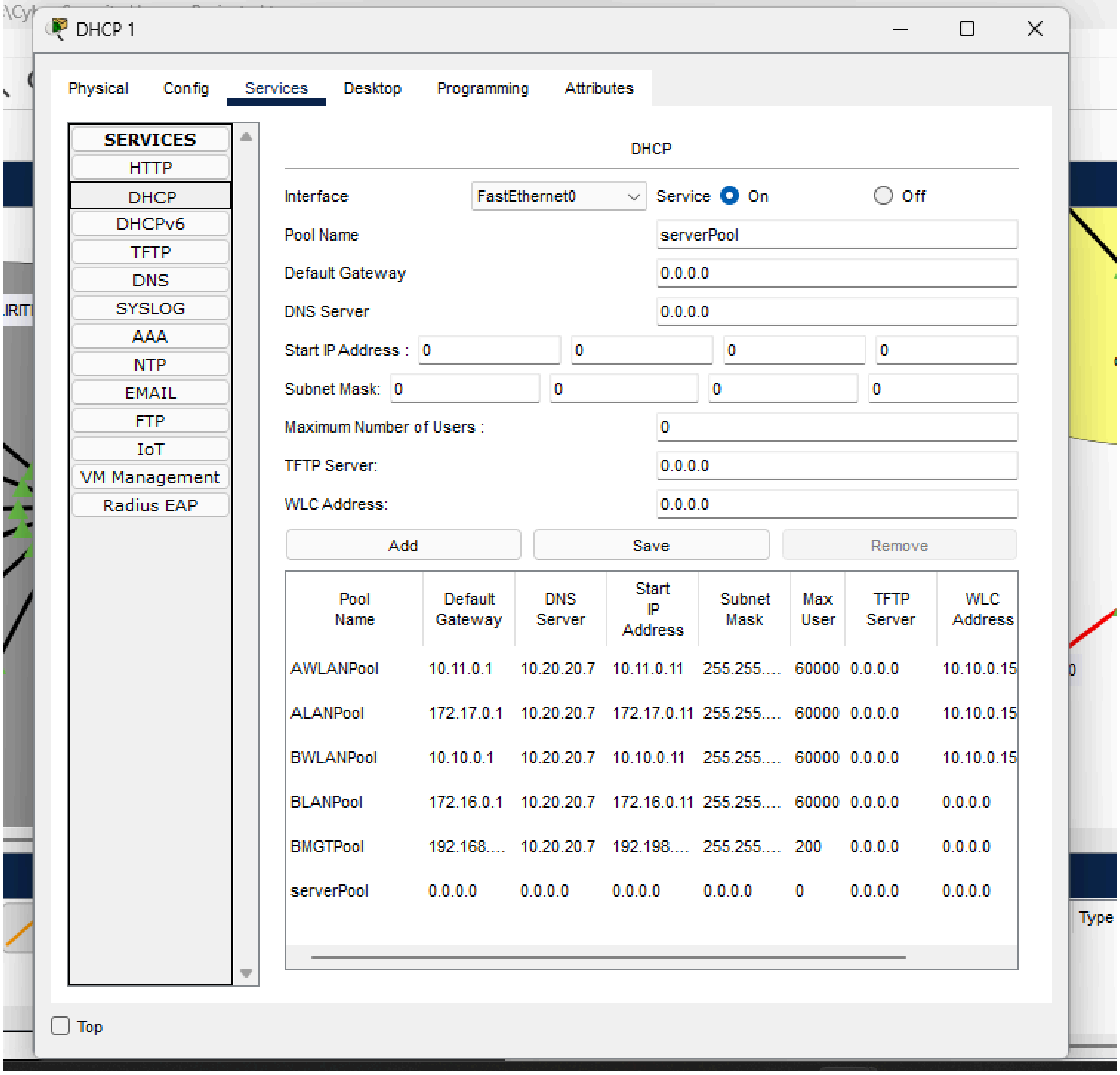
4.1.8 DHCP Server Device Configurations:

DHCP (Dynamic Host Configuration Protocol) is used to automatically assign IP addresses to devices on the network. Configuring a DHCP server involves specifying the range of IP addresses that can be assigned, as well as other network settings such as the default gateway and DNS server addresses.

Centralized DHCP management ensures that only authorized devices receive IP addresses, preventing unauthorized devices from accessing the network. It also facilitates the implementation of DHCP lease time controls and other security measures to mitigate the risk of rogue DHCP servers or IP address conflicts.

Implementation in Cisco Packet Tracer:

- Access the CLI of a router or dedicated DHCP server device.
- Enter the DHCP configuration mode and define DHCP pool settings such as the range of IP addresses to be assigned, subnet mask, default gateway, and DNS server address.



Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 0 0 0 0

Subnet Mask: 0 0 0 0

Maximum Number of Users : 0

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

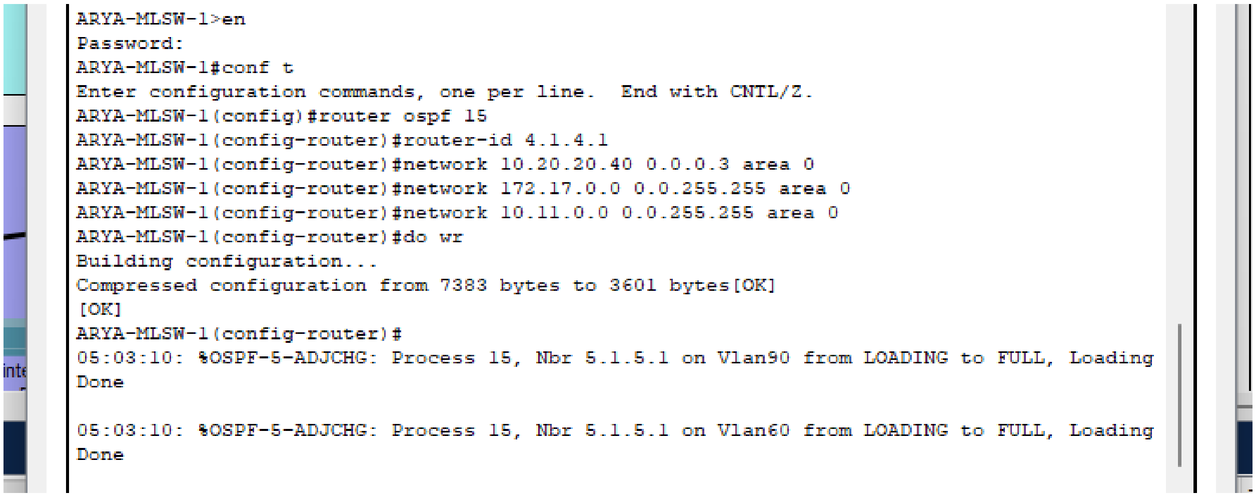
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
AWLANPool	10.11.0.1	10.20.20.7	10.11.0.11	255.255....	60000	0.0.0.0	10.10.0.15
ALANPool	172.17.0.1	10.20.20.7	172.17.0.11	255.255....	60000	0.0.0.0	10.10.0.15
BWLANPool	10.10.0.1	10.20.20.7	10.10.0.11	255.255....	60000	0.0.0.0	10.10.0.15
BLANPool	172.16.0.1	10.20.20.7	172.16.0.11	255.255....	60000	0.0.0.0	0.0.0.0
BMGTPool	192.168....	10.20.20.7	192.198....	255.255....	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0

Fig 8. DHCP Server's server pool configuration.

4.1.9 OSPF Configuration:

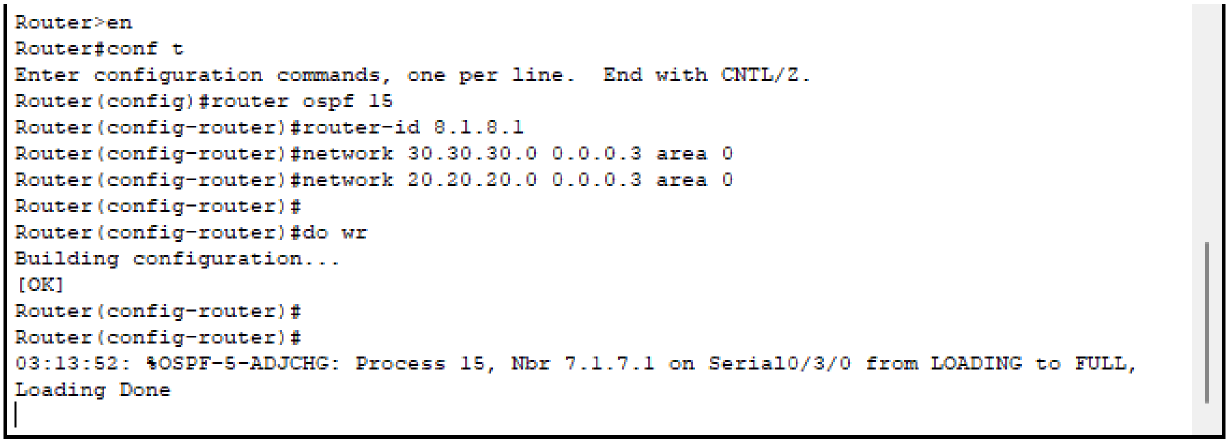
OSPF: OSPF (Open Shortest Path First) is a dynamic routing protocol used to exchange routing information between routers on a network. Configuring OSPF involves enabling the protocol on the routers and specifying which networks should be advertised to other routers.

OSPF dynamic routing enables efficient and secure exchange of routing information between network devices. It enhances network resilience by automatically adapting to topology changes and optimizing traffic paths, while also reducing the risk of misrouting or unauthorized route injections.



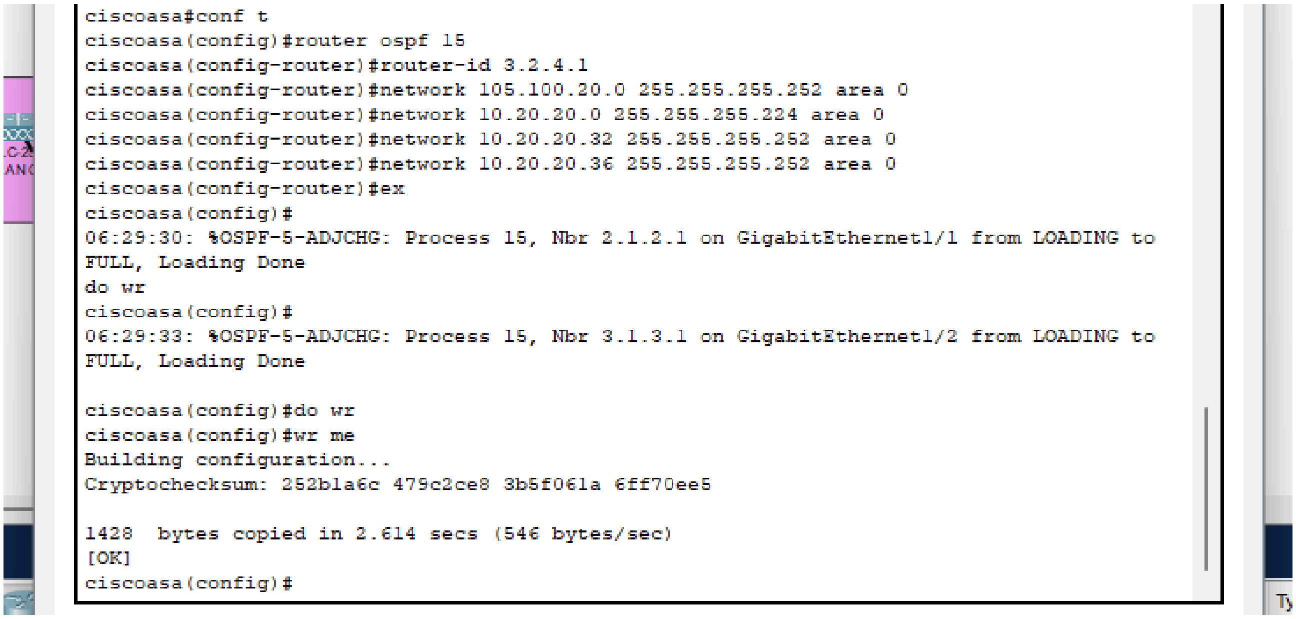
```
ARYA-MLSW-1>en
Password:
ARYA-MLSW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ARYA-MLSW-1(config)#router ospf 15
ARYA-MLSW-1(config-router)#router-id 4.1.4.1
ARYA-MLSW-1(config-router)#network 10.20.20.40 0.0.0.3 area 0
ARYA-MLSW-1(config-router)#network 172.17.0.0 0.0.255.255 area 0
ARYA-MLSW-1(config-router)#network 10.11.0.0 0.0.255.255 area 0
ARYA-MLSW-1(config-router)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
ARYA-MLSW-1(config-router)#
05:03:10: %OSPF-5-ADJCHG: Process 15, Nbr 5.1.5.1 on Vlan90 from LOADING to FULL, Loading
Done

05:03:10: %OSPF-5-ADJCHG: Process 15, Nbr 5.1.5.1 on Vlan60 from LOADING to FULL, Loading
Done
```

Fig 9. OSPF MLSW Configuration.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 15
Router(config-router)#router-id 8.1.8.1
Router(config-router)#network 30.30.30.0 0.0.0.3 area 0
Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#
Router(config-router)#do wr
Building configuration...
[OK]
Router(config-router)#
Router(config-router)#
03:13:52: %OSPF-5-ADJCHG: Process 15, Nbr 7.1.7.1 on Serial0/3/0 from LOADING to FULL,
Loading Done
```

Fig 10. OSPF Router Configuration.



```
ciscoasa#conf t
ciscoasa(config)#router ospf 15
ciscoasa(config-router)#router-id 3.2.4.1
ciscoasa(config-router)#network 105.100.20.0 255.255.255.252 area 0
ciscoasa(config-router)#network 10.20.20.0 255.255.255.224 area 0
ciscoasa(config-router)#network 10.20.20.32 255.255.255.252 area 0
ciscoasa(config-router)#network 10.20.20.36 255.255.255.252 area 0
ciscoasa(config-router)#ex
ciscoasa(config)#
06:29:30: %OSPF-5-ADJCHG: Process 15, Nbr 2.1.2.1 on GigabitEthernet1/1 from LOADING to
FULL, Loading Done
do wr
ciscoasa(config)#
06:29:33: %OSPF-5-ADJCHG: Process 15, Nbr 3.1.3.1 on GigabitEthernet1/2 from LOADING to
FULL, Loading Done

ciscoasa(config)#do wr
ciscoasa(config)#wr me
Building configuration...
Cryptochecksum: 252b1a6c 479c2ce8 3b5f061a 6ff70ee5

1428  bytes copied in 2.614 secs (546 bytes/sec)
[OK]
ciscoasa(config)#
```

Fig 11. OSPF Firewall Configuration.

4.1.10 Firewall Interface Security Zones and Levels:

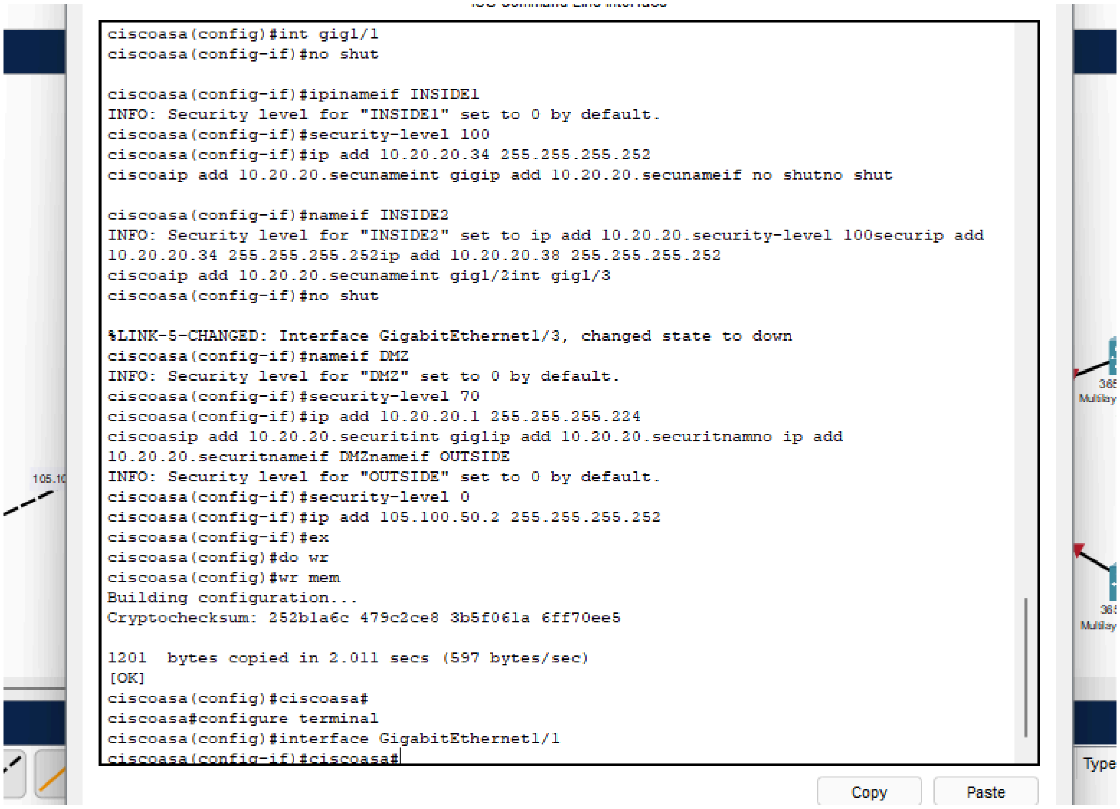
Firewall zones are logical groupings of interfaces on a firewall, typically based on the level of trust or security required for traffic entering or leaving that interface. Configuring firewall zones allows you to define security policies that control the flow of traffic between different zones.

Security levels are assigned to firewall interfaces to determine the level of trust associated with each interface. Higher security levels typically represent more trusted networks, while lower security levels represent less trusted networks.

Firewall zones and security levels provide a structured approach to traffic segmentation and access control, limiting the exposure of sensitive resources to potential threats. By enforcing strict security policies at the network perimeter, firewalls help prevent unauthorized access, data exfiltration, and other malicious activities.

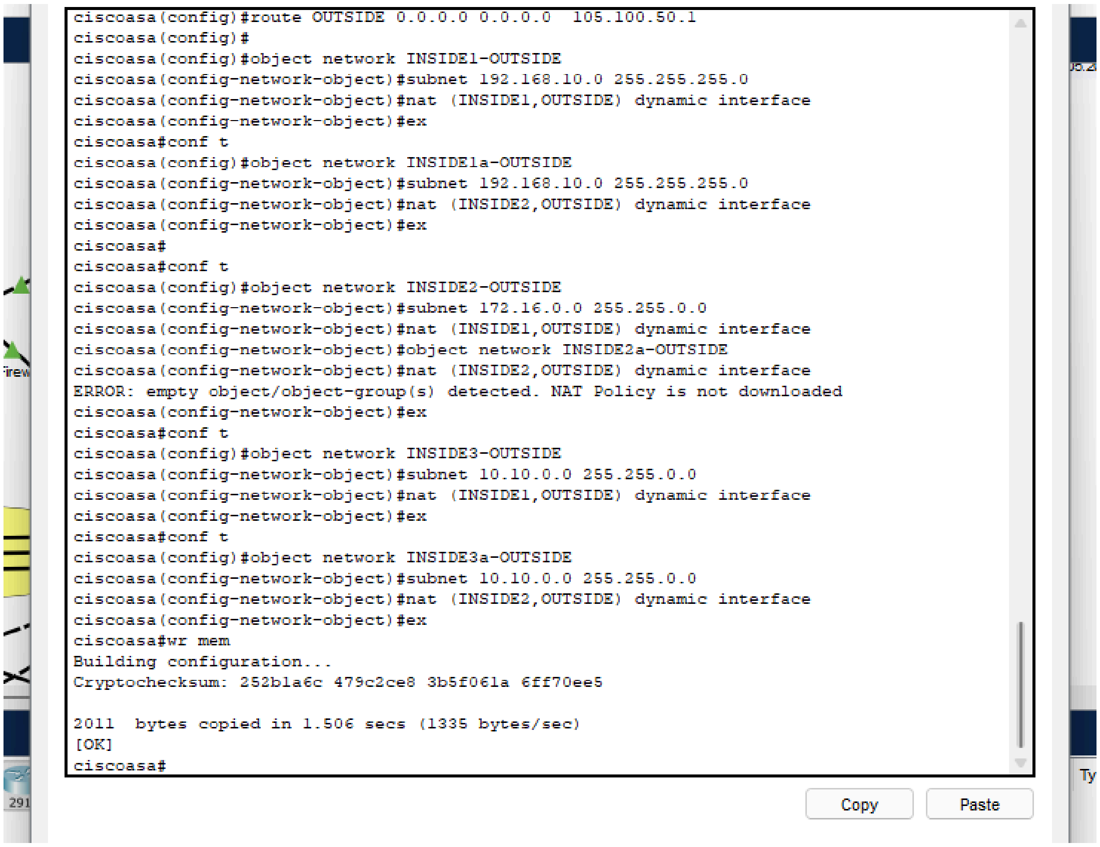
Implementation in Cisco Packet Tracer:

- Add firewall devices from the toolbar onto the workspace.
- Access the configuration interface of the firewall.
- Define security zones and assign interfaces to the appropriate zones.
- Configure security levels for each interface to establish the level of trust.
- Create Network Objects and associate them with NAT.



```
ciscoasa(config)#int gig1/1
ciscoasa(config-if)#no shut

ciscoasa(config-if)#ipinameif INSIDE1
INFO: Security level for "INSIDE1" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip add 10.20.20.34 255.255.255.252
ciscoaip add 10.20.20.secunameint gigip add 10.20.20.secunameif no shutno shut

ciscoasa(config-if)#nameif INSIDE2
INFO: Security level for "INSIDE2" set to ip add 10.20.20.security-level 100securip add
10.20.20.34 255.255.255.252ip add 10.20.20.38 255.255.255.252
ciscoaip add 10.20.20.secunameint gig1/2int gig1/3
ciscoasa(config-if)#no shut

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#security-level 70
ciscoasa(config-if)#ip add 10.20.20.1 255.255.255.224
ciscoasip add 10.20.20.securitint giglip add 10.20.20.securitnamno ip add
10.20.20.securitnameif DMZnameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip add 105.100.50.2 255.255.255.252
ciscoasa(config-if)#ex
ciscoasa(config)#do wr
ciscoasa(config)#wr mem
Building configuration...
Cryptochecksum: 252b1a6c 479c2ce8 3b5f061a 6ff70ee5

1201  bytes copied in 2.011 secs (597 bytes/sec)
[OK]
ciscoasa(config)#ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#ciscoasa#
```

Fig 11. Firewall configuration.



```
ciscoasa(config)#route OUTSIDE 0.0.0.0 0.0.0.0  105.100.50.1
ciscoasa(config)#
ciscoasa(config)#object network INSIDE1-OUTSIDE
ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)#nat (INSIDE1,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#object network INSIDE1a-OUTSIDE
ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)#nat (INSIDE2,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#object network INSIDE2-OUTSIDE
ciscoasa(config-network-object)#subnet 172.16.0.0 255.255.0.0
ciscoasa(config-network-object)#nat (INSIDE1,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#object network INSIDE2a-OUTSIDE
ciscoasa(config-network-object)#nat (INSIDE2,OUTSIDE) dynamic interface
ERROR: empty object/object-group(s) detected. NAT Policy is not downloaded
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#object network INSIDE3-OUTSIDE
ciscoasa(config-network-object)#subnet 10.10.0.0 255.255.0.0
ciscoasa(config-network-object)#nat (INSIDE1,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#object network INSIDE3a-OUTSIDE
ciscoasa(config-network-object)#subnet 10.10.0.0 255.255.0.0
ciscoasa(config-network-object)#nat (INSIDE2,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 252b1a6c 479c2ce8 3b5f061a 6ff70ee5

2011  bytes copied in 1.506 secs (1335 bytes/sec)
[OK]
ciscoasa#
```

Fig 12. Network Object Configuration.

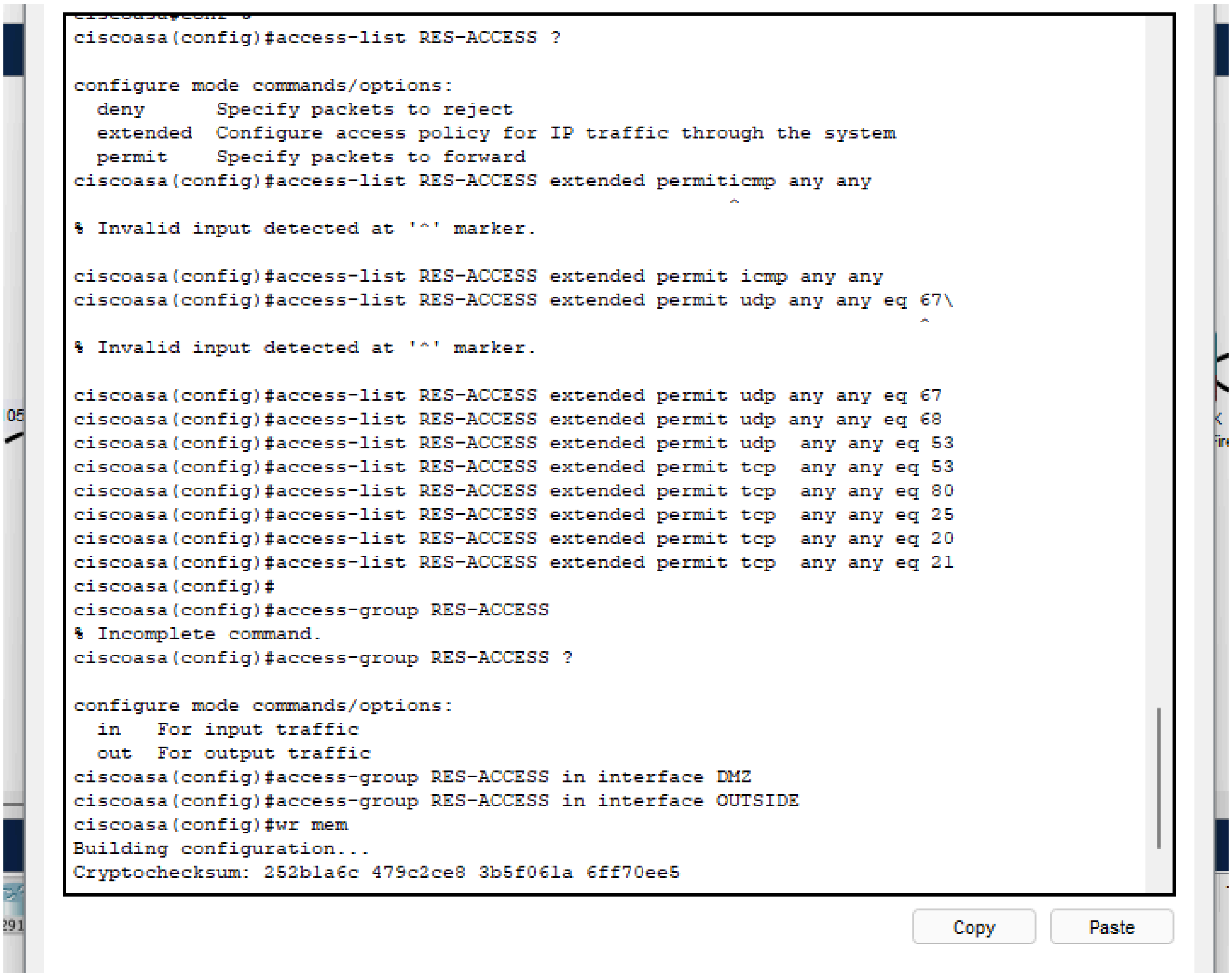
4.1.11 Firewall Inspection Policy Configuration:

Firewall Inspection Policies: Firewall inspection policies define how the firewall should inspect and filter traffic passing through it. This includes specifying which protocols should be allowed or denied, as well as any additional security measures such as deep packet inspection or intrusion prevention.

Firewall inspection policies allow for deep packet inspection and filtering of traffic based on application-layer attributes. This enables the detection and blocking of suspicious or malicious traffic, including malware, exploits, and intrusion attempts, thereby strengthening the network's defense against cyber threats.

Implementation in Cisco Packet Tracer:

- Access the configuration interface of the firewall.
- Define inspection policies for different types of traffic (e.g., TCP, UDP, ICMP) using the firewall's GUI or CLI.
- Specify parameters for deep packet inspection, intrusion detection, and application-layer filtering as needed.



```
ciscoasa(config)#access-list RES-ACCESS ?

configure mode commands/options:
  deny      Specify packets to reject
  extended  Configure access policy for IP traffic through the system
  permit    Specify packets to forward
ciscoasa(config)#access-list RES-ACCESS extended permiticmp any any
                                                        ^

% Invalid input detected at '^' marker.

ciscoasa(config)#access-list RES-ACCESS extended permit icmp any any
ciscoasa(config)#access-list RES-ACCESS extended permit udp any any eq 67\
                                                                        ^

% Invalid input detected at '^' marker.

ciscoasa(config)#access-list RES-ACCESS extended permit udp any any eq 67
ciscoasa(config)#access-list RES-ACCESS extended permit udp any any eq 68
ciscoasa(config)#access-list RES-ACCESS extended permit udp  any any eq 53
ciscoasa(config)#access-list RES-ACCESS extended permit tcp  any any eq 53
ciscoasa(config)#access-list RES-ACCESS extended permit tcp  any any eq 80
ciscoasa(config)#access-list RES-ACCESS extended permit tcp  any any eq 25
ciscoasa(config)#access-list RES-ACCESS extended permit tcp  any any eq 20
ciscoasa(config)#access-list RES-ACCESS extended permit tcp  any any eq 21
ciscoasa(config)#
ciscoasa(config)#access-group RES-ACCESS
% Incomplete command.
ciscoasa(config)#access-group RES-ACCESS ?

configure mode commands/options:
  in   For input traffic
  out  For output traffic
ciscoasa(config)#access-group RES-ACCESS in interface DMZ
ciscoasa(config)#access-group RES-ACCESS in interface OUTSIDE
ciscoasa(config)#wr mem
Building configuration...
Cryptochecksum: 252b1a6c 479c2ce8 3b5f061a 6ff70ee5
```

Fig 13. Firewall Inspection Policy Configuration.

4.2 Identified Security Risks and Proposed Countermeasures:

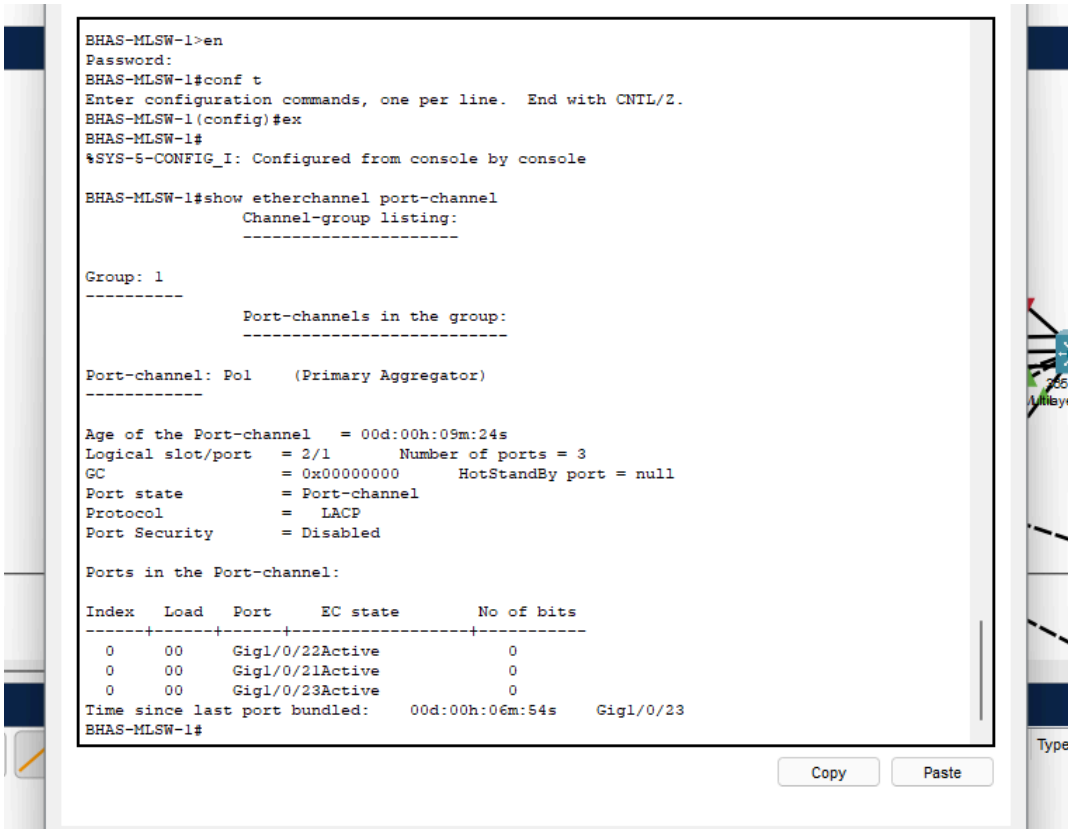
- Data Breaches:
    - Risk: Potential risk of data breaches due to unauthorized access or disclosure of sensitive information.
    - Proposed Countermeasures: Implement data encryption for sensitive data, enforce strict access controls, and conduct regular security audits to identify and secure potential vulnerabilities.
- Phishing Attacks
    - Risk: Susceptibility to phishing attacks that target users through deceptive emails or websites to gain unauthorized access or steal sensitive information.
    - Proposed Countermeasures: Conduct phishing awareness training for users, implement email authentication protocols like SPF, DKIM, and DMARC, and deploy anti-phishing tools to detect and block phishing attempts.
- Insider Threats
    - Risk: The risk of insider threats, where authorized users may intentionally or unintentionally compromise security or leak sensitive information.
    - Proposed Countermeasures: Implement least privilege access, enforce separation of duties, monitor user activity with user behavior analytics (UBA), and conduct periodic security awareness training for employees.

4.3 Results:

The implementation of the advanced network topology marks a significant milestone in enhancing the security and functionality of the college's network infrastructure. Through the integration of sophisticated security measures, such as VLAN segmentation, HSRP, and IPsec VPN, the network now boasts robust protection against emerging cyber threats. Screenshots of the network configuration confirm the successful deployment of these security protocols, ensuring the confidentiality and integrity of sensitive data transmitted across the network.

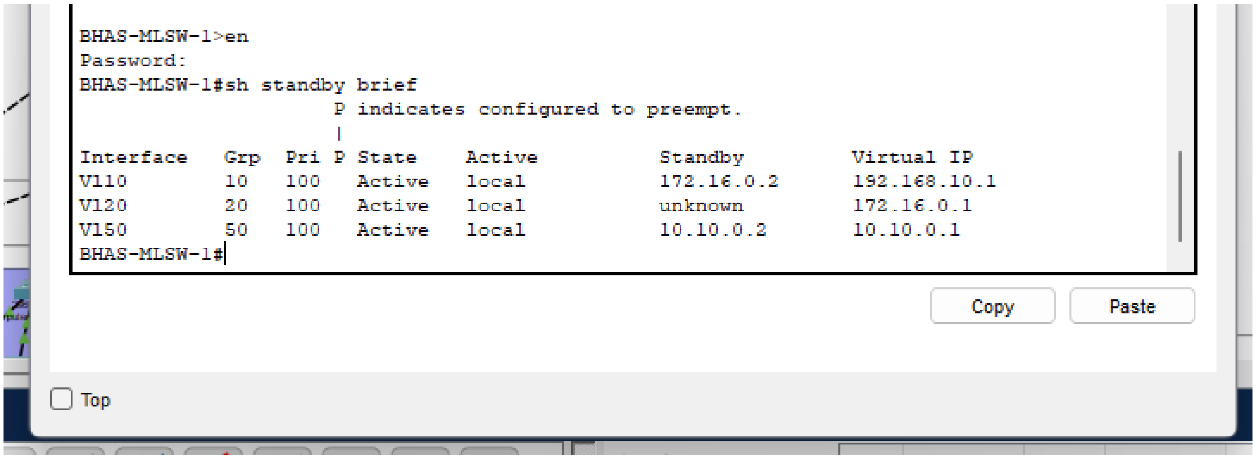
Additionally, enhancements in network resilience and scalability, facilitated by features like EtherChannel and OSPF, guarantee uninterrupted connectivity and efficient resource utilization. Screenshots of network performance metrics validate the improved efficiency and reliability of the network infrastructure.

In conclusion, the advanced network topology represents a comprehensive and successful effort to fortify the college's network infrastructure, providing a secure, reliable, and adaptable platform for academic and administrative activities.



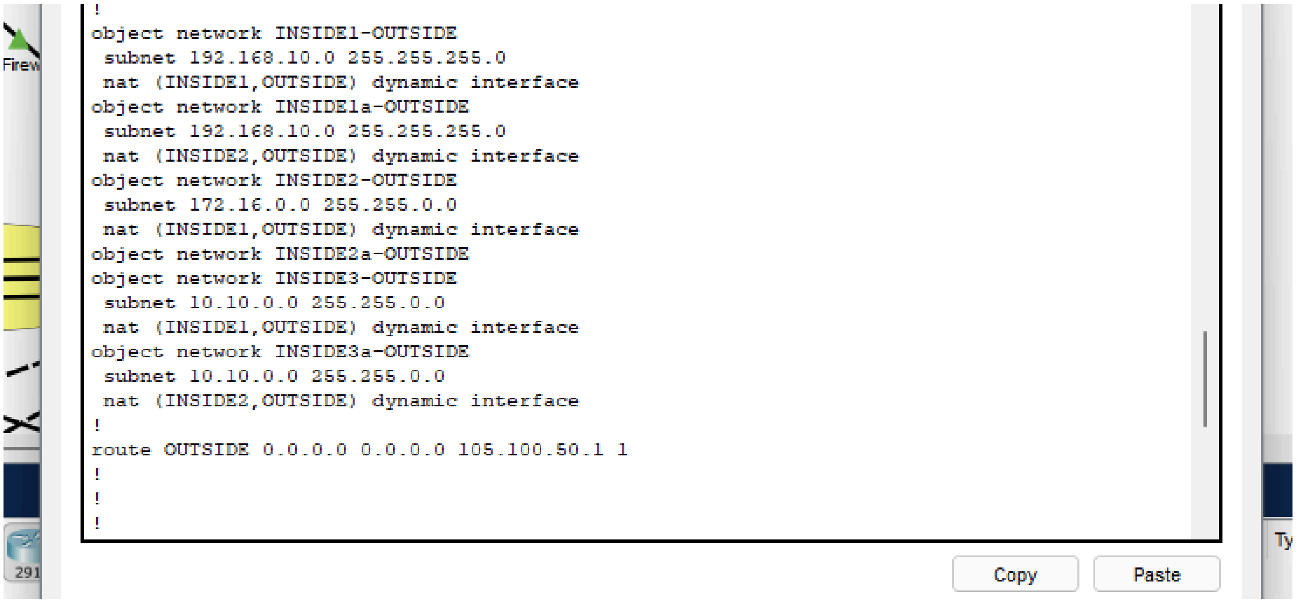
```
BHAS-MLSW-1>en
Password:
BHAS-MLSW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BHAS-MLSW-1(config)#ex
BHAS-MLSW-1#
%SYS-5-CONFIG_I: Configured from console by console

BHAS-MLSW-1#show etherchannel port-channel
                Channel-group listing:
                ----------------------


Group: 1
----------
                Port-channels in the group:
                ---------------------------


Port-channel: Po1    (Primary Aggregator)
------------


Age of the Port-channel   = 00d:00h:09m:24s
Logical slot/port   = 2/1        Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gig1/0/22Active             0
  0     00     Gig1/0/21Active             0
  0     00     Gig1/0/23Active             0
Time since last port bundled:    00d:00h:06m:54s    Gig1/0/23
BHAS-MLSW-1#
```

Fig 14. Status of Etherchannel Channel



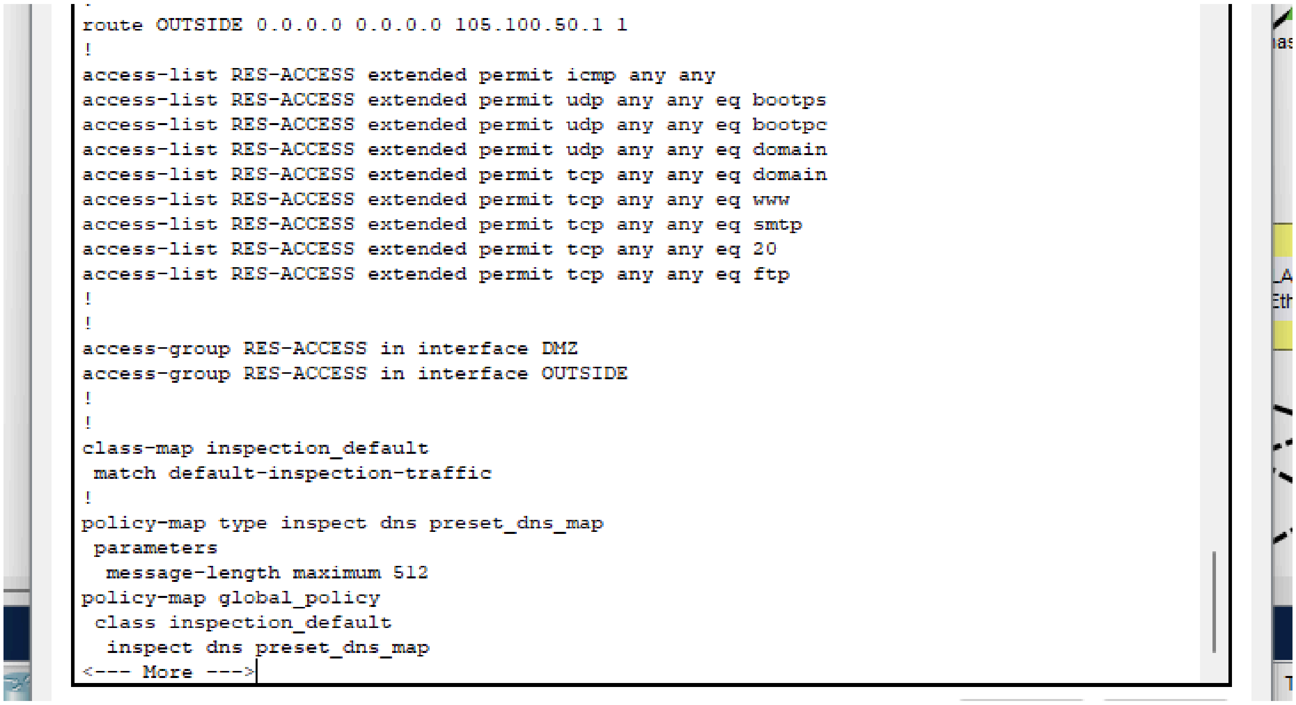
```
BHAS-MLSW-1>en
Password:
BHAS-MLSW-1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100   Active  local           172.16.0.2      192.168.10.1
Vl20        20   100   Active  local           unknown         172.16.0.1
Vl50        50   100   Active  local           10.10.0.2       10.10.0.1
BHAS-MLSW-1#
```

Fig 15. Status of HSRP



```
!
object network INSIDE1-OUTSIDE
 subnet 192.168.10.0 255.255.255.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE1a-OUTSIDE
 subnet 192.168.10.0 255.255.255.0
 nat (INSIDE2,OUTSIDE) dynamic interface
object network INSIDE2-OUTSIDE
 subnet 172.16.0.0 255.255.0.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE2a-OUTSIDE
object network INSIDE3-OUTSIDE
 subnet 10.10.0.0 255.255.0.0
 nat (INSIDE1,OUTSIDE) dynamic interface
object network INSIDE3a-OUTSIDE
 subnet 10.10.0.0 255.255.0.0
 nat (INSIDE2,OUTSIDE) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 105.100.50.1 1
!
!
!
```

Fig 16. Firewall Object and NAT Configuration.



```
route OUTSIDE 0.0.0.0 0.0.0.0 105.100.50.1 1
!
access-list RES-ACCESS extended permit icmp any any
access-list RES-ACCESS extended permit udp any any eq bootps
access-list RES-ACCESS extended permit udp any any eq bootpc
access-list RES-ACCESS extended permit udp any any eq domain
access-list RES-ACCESS extended permit tcp any any eq domain
access-list RES-ACCESS extended permit tcp any any eq www
access-list RES-ACCESS extended permit tcp any any eq smtp
access-list RES-ACCESS extended permit tcp any any eq 20
access-list RES-ACCESS extended permit tcp any any eq ftp
!
!
access-group RES-ACCESS in interface DMZ
access-group RES-ACCESS in interface OUTSIDE
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
<--- More --->
```

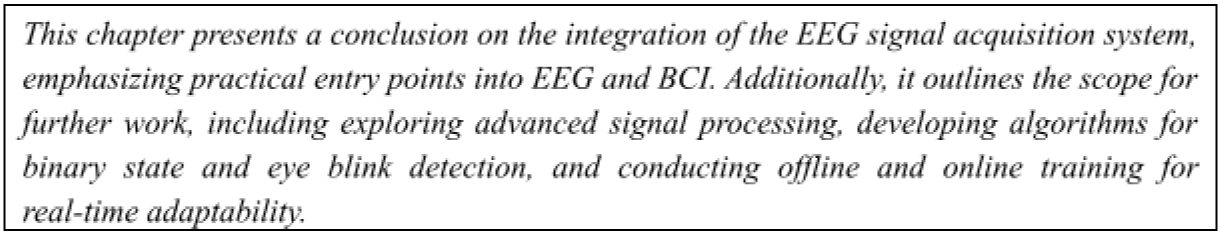
Fig 17. Firewall Inspection Policy.

4.4 Recommendations:

- Penetration Testing and Red Team Exercises: Conduct regular penetration testing and red team exercises to simulate real-world cyber-attacks and identify potential weaknesses in the network's defenses. This proactive approach helps in strengthening security measures.
- Vulnerability Management Program: Establish a robust vulnerability management program to regularly scan and assess network devices, servers, and applications for security vulnerabilities. Promptly patch and remediate identified vulnerabilities to reduce the attack surface.

- Network Segmentation Refinement: Continuously review and refine network segmentation to ensure that sensitive data and critical assets are isolated from potential threats. Adjust VLAN configurations and access controls based on changing security requirements.

5. Conclusion and Scope for Further Work



This chapter presents a conclusion on the integration of the EEG signal acquisition system, emphasizing practical entry points into EEG and BCI. Additionally, it outlines the scope for further work, including exploring advanced signal processing, developing algorithms for binary state and eye blink detection, and conducting offline and online training for real-time adaptability.

5.1 Conclusion:

In conclusion, this report outlines the systematic efforts undertaken to enhance the cybersecurity posture of KJSCE (KJSCE). The implementation of network security configurations, based on industry best practices and utilizing Cisco Packet Tracer components, has significantly strengthened the resilience of the campus network against potential threats. The documented procedures cover essential aspects to the implementation. Furthermore, The integrated security measures not only ensure the reliability and efficiency of the network but also establish a robust defense against a range of security risks. The report effectively addresses identified risks and proposes countermeasures to mitigate them. The proactive approach advocated by these measures aims to simulate real-world cyber-attacks, promptly identify weaknesses, and reduce the attack surface by addressing vulnerabilities. By aligning with industry best practices and continuously refining security measures, KJSCE is poised to navigate the dynamic landscape of cybersecurity, ensuring the resilience and integrity of its network infrastructure in the face of evolving threats and challenges.

5.2 Scope for Further Work.

The future work for enhancing the cybersecurity posture of KJSCE (KJSCE) involves a strategic and ongoing approach to address emerging threats and continuously improve network security. Here are some potential areas of focus for future work:

- Creating an Incident Response Plan
- Integrating with the emerging technologies of AI-ML for advanced threat detection and response.
- Implementing Cloud Control Measures
- Ensuring the network security measure aligns with the compliance guidelines issued.

Bibliography

[1] P. Srikanth Reddy, P. Saleem Akram, T. V. Ramana, P. Aditya Sai Ram, R. Pruthvi Raj and M. Adarsh Sharma, "Configuration of Firewalls in Educational Organisation LAB setup by using Cisco Packet Tracer," 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), Gunupur Odisha, India, 2020, pp. 1-6, doi: 10.1109/iSSSC50941.2020.9358818.

[2] A. D. Azhari, N. A. Sulaiman and M. Kassim, "Secured Internet Office Network with the Internet of Things Using Packet Tracer Analysis," 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2021, pp. 200-205, doi: 10.1109/ICSET53708.2021.9612554.

[3] Ahmed, A. H., & Al-Hamadani, M. N. (2021). Designing a secure campus network and simulating it using Cisco packet tracer. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(1), 479-489.

[4] Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), 2181.

[5] Varne, P. N., Priyanka, J., Tejus, A. K., & Gowda, N. C. (2023). Campus Network Design and Implementation using Cisco Packet Tracer. *International Journal of Computational Learning & Intelligence*, *2*(4), 163-168.

[6] Banothe, Y., Thakur, R., Banothe, A., & Jaipurkar, P. (2023). Architecture of college campus network using cisco packet tracer. *International Research Journal of Modernization in Engineering Technology and Science, vol*, *5*(4).

[7] S. H. Moz, M. A. Hosen and N. F. I. Tanny, "Campus Network Configuration, Monitoring and Data Flow Simulation using Cisco Packet Tracer," *2023 International Conference on Inventive Computation Technologies (ICICT)*, Lalitpur, Nepal, 2023, pp. 793-798, doi: 10.1109/ICICT57646.2023.10134506.

[8] Kumar, Ashish. (2018). Implementation of a Company Network Scenario Module by using Cisco Packet Tracer Simulation Software.

Appendix A

Appendix A - Cisco Packet Tracer

A.1 Introduction to Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco Systems. It is widely used for educational purposes to design, configure, and troubleshoot network scenarios. This tool provides a virtual environment where users can create and simulate networks, making it an invaluable resource for learning networking concepts.

A.2 Installation and Setup

To get started with Cisco Packet Tracer, follow these steps:

1. Navigate to https://skillsforall.com/resources/lab-downloads.
2. Choose the appropriate download link for Windows, Linux, or macOS.
3. Save the installation file to a preferred location.
4. Install the application using on-screen instructions.
5. Launch Application.

A.3 Interface Overview

The Packet Tracer interface comprises several components, including:

- **Logical Workspace:** The designated area for designing and configuring the network.
- **Physical Workspace:** Exhibits the physical representation of devices in the network.
- **Toolbar:** Encompasses tools for selecting, placing, and configuring network elements.
- **Device Palette:** Provides a selection of network devices and components for integration.

A.4 Building a Network

To construct a network in Packet Tracer, users adhere to the subsequent steps:

1. Employ drag-and-drop actions to situate devices from the Device Palette onto the Logical Workspace.
2. Establish connections between devices using suitable cables and configure relevant settings.
3. Leverage the CLI (Command Line Interface) of devices for tasks such as IP address configuration and routing.

A.5 Simulation and Testing

Packet Tracer facilitates simulation and testing of networks. Users can employ the Simulation mode to observe network behavior under diverse scenarios, aiding in troubleshooting and comprehension of configuration impacts.

A.6 Troubleshooting in Packet Tracer

Troubleshooting network issues within Packet Tracer involves:

1. Thorough examination of device configurations for potential errors.
2. Utilization of built-in troubleshooting tools.
3. Analysis of network traffic and logs to identify anomalies.

A.7 Resources and Further Learning

Packet Tracer offers an array of learning resources:

- **Tutorials:** Accessible within the software to enhance understanding.
- **Community Support:** Interaction with the Cisco Packet Tracer community provides assistance and insights.

A.8 Conclusion

In conclusion, Cisco Packet Tracer stands as an indispensable tool for network education and training. Mastery of its features significantly enhances networking skills, preparing users for real-world scenarios. Refer to the official Cisco Packet Tracer documentation for the latest updates and features.

Acknowledgements

We express our sincere appreciation to the Computer Engineering Department at K.J. Somaiya College of Engineering for their unwavering support and essential contribution to fortifying the network infrastructure at KJSCE. The department's commitment to excellence in education and provision of vital resources has been indispensable in the successful realization of our project.

A special acknowledgment is reserved for our esteemed project guide and mentor, Mrs. Swati Mali. Mrs. Mali's dedication, profound insights, and expert guidance have played a pivotal role in shaping the comprehensive network topology designed to enhance security measures at KJSCE. Her encouragement of a proactive approach to network security has significantly influenced the development of this study, fostering a secure academic environment.

Furthermore, we extend our heartfelt gratitude to Dr. Prasanna Shete for his invaluable support, patience, and willingness to share knowledge, enriching our learning experience. His role as a guide has been crucial in navigating us through challenges and celebrating triumphs, making this project a truly collaborative and enlightening endeavor. This project stands as evidence of the collaborative spirit within our academic community and our shared commitment to innovation, artistic expression, and academic excellence. We extend our thanks to everyone who has played a part in this journey, directly or indirectly, for their contributions to the success of this endeavor.

We also express our gratitude to Mr. Atul Tamhane for his valuable contributions in understanding and mapping the intricate architecture of the network. His expertise and insights have been crucial in ensuring the seamless integration of robust security measures. Mr. Tamhane's dedication to elucidating complex technical aspects has significantly enhanced the project's overall comprehension and execution. His role in clarifying architectural nuances has been instrumental in achieving the project's objectives and fortifying the network infrastructure at K.J. Somaiya College of Engineering.