كـلية الشـرق الأوسـط
Middle East College

A PROJECT REPORT
ON
ENHANCING NATIONAL UNIVERSITY NETWORK SECURITY:
ATTACK SIMULATION AND CYBERSECUITY AWARENESS

By

Laila Tamer Mekhimar - 23F24083
Hamza Suleiman Aladawi - 23F24607
Sheikha Rashid Al Hinai - 23F24676
Taha Mohammed Al Balushi - 23F24590
Yamen Hamed Al Dhanki - 23S23781

Guided by

IBTISAM AL QARI

A project report submitted in partial fulfillment of the requirements

for the award of

Computer Engineering - Cybersecurity

Middle East College
Knowledge Oasis Muscat, Oman
JUNE, 2025

كلية الشرق الأوسط
Middle East College

A PROJECT REPORT

ON

ENHANCING NATIONAL UNIVERSITY NETWORK SECURITY: ATTACK SIMULATION AND CYBERSECUITY AWARENESS

By

Laila Tamer Mekhimar - 23F24083

Hamza Suleiman Aladawi - 23F24607

Sheikha Rashid Al Hinai - 23F24676

Taha Mohammed Al Balushi - 23F24590

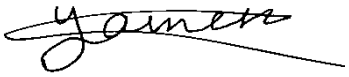
Yamen Hamed Al Dhanki - 23S23781

JUNE 2025

1. Declaration of Originality

We, Hamza Suleiman Aladawi, Laila Tamer Mekhimar, Sheikha Rashid Al Hinai, Taha Mohammed Al Balushi, and Yamen Hamed Al Dhanki, declare that the project title we chose and presented in the Project Initiation Report is an original idea conceived by us. To the best of my knowledge, this project has not been previously undertaken or completed within this college or any other institution. We affirm that the proposed work is unique and does not infringe upon the intellectual property or academic contributions of others. We are fully aware of the implications of replicating or infringing upon intellectual property, including potential disciplinary action, and acknowledge my responsibility to ensure the project is original and unique.

2. Signatures:

Name	Signature
Hamza Suleiman Aladawi	
Laila Tamer Mekhimar	
Sheikha Rashid Al Hinai	
Taha Mohammed Al Balushi	
Yamen Hamed Al Dhanki	

APPROVAL FORM

The project report entitled "Enhancing national university network security attack simulation and cybersecurity awareness" submitted by Laila Tamer Mekhimar - 23F24083, Hamza Suleiman Aladawi - 23F24607, Sheikha Rashid Al Hinai - 23F24676, Taha Mohammed Al Balushi - 23F24590, Yamen Hamed Al Dhanki - 23S23781 is approved in partial fulfillment of the requirements for diploma in Project 1 (PROJN 20001.1) – Computer Engineering - Cybersecurity.

Supervisor

Full name:

Department:

Date:

Signature:

Examiner Full name:

Department:

Date:

Signature:

ACKNOWLEDGEMENT

We would like to thank Middle East College, Oman, for providing us with both the knowledge and practical skills that made it possible to complete this project successfully. Our learning environment, supported by the regular help and advice from teachers, helped us build our technical skills and use them in real situations.

We would like to extend our gratitude to our academic mentor, Ms. Ibtisam AlQari, for constantly supporting us and keeping us motivated. We express our gratitude to Dr. Abdullah Abbasi for sharing his knowledge and insights throughout the whole research process. We would also like to thank Dr. Saleh Al Arimi from the National University of Science and Technology for agreeing to an interview. Because he shared insights from his real-world experiences, our work turned out to be more meaningful and practical. Because of their guidance, mentoring, and trust in us, we were able to complete this project with success.

ABSTRACT

Today, universities rely on advanced technology and online systems to handle their academic, administrative and research tasks. Because institutions depend on digital technology, they need stronger and more aware cybersecurity measures. Although cybersecurity is extremely important, universities find it difficult to prepare their students and staff with the hands-on knowledge and experiences they need to manage and prevent cyber threats. With technology developing rapidly, the usual ways of teaching cybersecurity in schools are not enough to prepare individuals for the real-world difficulties they might encounter.

To bridge this gap, we are setting up and running a Cybersecurity Awareness and Simulation Lab using Cisco Packet Tracer at the National University of Science and Technology (NU), Oman. Developing a cybersecurity lab helps the university fulfill its goals related to digital progress and quality education. The lab's purpose is to create a secure, orderly and interactive space for students and teachers to study cybersecurity through simulation exercises.

This project allows students to use Cisco Packet Tracer to learn in a way that copies what they would find in real networking settings. Building network topologies, configuring gadgets and observing several networking behaviors will be possible for both students and school staff. The hardware in this design consists of core routers, access switches, firewalls, segmentation via VLAN, plus important servers including DHCP, DNS and Web. A Web Server is included to host a Cybersecurity Awareness Webpage designed to explain best practices, policies and ways of maintaining network cleanliness through education, not with stories of threats or fears.

The main idea of the project is to help students learn and practice proper online habits using various experiences. Instead of focusing entirely on lectures, the simulation helps students and staff work with practical examples of security options like ACLs, managing IP addresses, and sorting network traffic. The features described are actual parts of the digital environment, designed to represent real-world infrastructure. Therefore, students become more confident in handling network issues, configuring them for security and keeping an eye on their systems.

The project leads to several significant achievements in the long run. It helps students get ready for work in fields such as ethical hacking, network administration, cybersecurity engineering and systems analysis by teaching them about real-world cybersecurity and networking. It also helps NU's own IT and security experts by giving them a secure platform to experiment with different policies, settings and find vulnerabilities risk-free. It also helps the whole community understand the need for security which prevents problems that could result from people not being aware.

The Cybersecurity Awareness and Simulation Lab serves as a good example of how colleges and universities can face modern challenges in the digital world. The addition of Cisco Packet Tracer, attention to hardware, real-time monitoring tools and educational content provides a well-rounded and modern approach to cybersecurity training. As a result, this project addresses today's issues at NU and supports future enhancement and responsiveness in the digital world of colleges and universities.

Table of Content

List of Figures

List of Tables

CHAPTER 1: OVERVIEW AND BACKGROUND

1.1 Overview of Project case / Business case

1.1.1. Background of the Organization

Established in 2018 the National University of Science & Technology (NU) stands as the premier educational institution for higher learning in Oman. The institution originated from the unification of the established research hubs Caledonian College of Engineering (CCE) and Oman Medical College (OMC). The university spreads its operations throughout different campuses where Bawshar in Muscat Campus serves as headquarters (National University of Science & Technology, 2022).

Students from more than 33 countries choose NU because it delivers an extensive portfolio of undergraduate and postgraduate educational programs. The institution delivers superior educational and research programs as well as innovative practices across engineering, medicine, pharmacy, applied technology, and maritime studies. Student readiness for digital-era challenges stands as a primary goal for the university through its commitment to developing modern technological and cybersecurity proficiencies.

Due to phishing email attacks and ransomware threats NU viewed network security enhancement as an immediate necessity. The solution to strengthen the defenses involved creating the NU Cybersecurity Awareness Lab in Cisco packet tracer network simulation tool to build an advanced network protection system. The laboratory provides students and staff with real-world cybersecurity simulations that enable them to acquire the necessary expertise for recognizing and addressing cyber threats professionally. NU uses practical training to build both specialized skills of its students and broader understanding of modern security dangers.

1.1.2. Background of the Topic

The digital revolution continues to expand cybersecurity threats which expose universities along with other organizations to multiple cyber-attack methods. The high level of targeting educational institutions occurs because they maintain extensive databases which store sensitive information about students and faculty members along with research data. Students along with staff members struggle to handle authentic cyber dangers because they do not have enough experience dealing with these threats. Modern security challenges surpass the capabilities that traditional classroom learning provides to students for preparation (Selvidge, 2024).

Realistic cybersecurity simulation labs enable students to gain hands-on experience through practicing attacks that happen in actual environments and developing defensive methods. Organizations face difficulties in managing the massive amount of data produced by networked devices because advanced cybersecurity training programs are essential according to (Ariganello, 2022). The educational programs teach learners the necessary capabilities to detect cyber dangers as well as establish methods to protect against them.

Digital platform reliance prompts universities to strengthen their cybersecurity systems to safeguard both operational continuity as well as protected data. The initiative develops a Cybersecurity Awareness and Attack Simulation Lab through the implementation of Cisco Packet Tracer for training purposes. The new lab provides students together with staff members with the opportunity to practice defending against phishing attacks, packet sniffing and Social Engineering attacks.

1.2 Preliminary Investigation

1.2.1. Defining the Problem

Higher education institutions face rising cybersecurity threats because their sensitive data makes them target for constant cyber-attacks. The National University must strengthen network security measures to protect vital operational student data and research information and administrative processing systems. The staff, along with students at present, receive insufficient training to properly detect and respond effectively to cyber threats. The university's network remains at high risk since it has encountered phishing Email attacks alongside ransomware attacks which demonstrate a pressing need for improved security protocols (Love Tech AI, 2024).

The key issues faced by the university include:

General Problems

- Educational institutions have become common targets for cyber-attacks due to the vast amount of sensitive data in universities.
- Many students and staff are not knowledgeable enough to notice or deal with cyber threats.
- Instructional weakness: Most organizations do not invest in structured cybersecurity education or protective measures.

Specific Problems

- There are few cybersecurity training courses for staff and students, so they are not getting the chance to practice in real world situations.
- Phishing, malware, packet sniffing and web cloning are some of the threats that can harm the university's connection.
- No Centralized training: There is no single platform for teaching cybersecurity practices.
- Outdated security measures: The present security system does not match the challenges of the modern threat environment.

1.2.2. Consequences of the Problem

Challenges related to cybersecurity at the university can result in serious situations such as data loss, failures in important systems and a lack of confidence in the institution. If staff receive poor training, roles in security and safety become more challenging, leaving the network at greater risk. A decrease in cybersecurity knowledge for students can negatively impact their chances of being prepared for jobs in digital companies (NIST, 2023).

Possible Effects:

- Confidential academic and personal information could get stolen or exposed.
- A cyber-attack could interrupt education, experiments and organizational activities.
- The college could experience setbacks in finances and its reputation.
- Those landing technical degrees may not understand cybersecurity well, making it hard for them to compete in the job market.

1.2.3. Introducing the Project

The proposed solution involves developing a Cybersecurity Awareness and Attack Simulation Lab for upgrading National University network through Cisco Packet Tracer to tackle existing challenges with website's awareness pages, the interactive dashboard and educational videos created on YouTube are valuable for students to learn from real cases. Because of this approach, Students and Staff can recognize the best ways to protect themselves in the digital world. The project creates network architecture by combining: Core, Distribution, and Access layers with security features that fit the university needs. This educational approach embedded into university classes enables students to build capabilities that defend against actual cyber threats in the real world.

1.2.4. Justification of Project

Multiple advantages emerge from this project because it enables both students and staff to develop fundamental attacking skills alongside threat understanding that strengthens their readiness against cybersecurity attacks. Enhancing the university's security infrastructure enhances both network safety and the capability to prevent threats. The curriculum enables students to build the necessary abilities required for employment as ethical hackers or network security engineers thus enhancing their employment potential within the field of cybersecurity. The training facility stays current by conducting regular updates to introduce fresh attack scenarios that help the university maintain preparedness against new security risks. Security skills taught to upcoming National University students will build their capabilities to perform well in an evolving field. The project enhances network performance through VLAN-based department segregation Access control list (ACL) implementation creates authorized communication between different network segments while establishing defined access rules. The integration of DHCP and DNS core network services will improve IP allocation and resource accessibility. Network safety includes also physically securing the ports by learning the devices MAC-addresses. Network segmentation through security measures combined with policy enforcement and well-trained staff implements defense strategies that follow industry standards and network security guidelines (Aleksic, 2022).

1.2.5. Project Benefits

The project benefits include:

- Helps students and staff gain hands-on experience with cyber threats by simulating real attacks.
- Supports employees in noticing, tackling and avoiding phishing, malware and ransomware issues.
- Supports students in advancing their careers by training them for jobs such as ethical hacking and networking security.
- Enhances the security of networks by using VLAN segmenting, Access Control Lists, port security and integrating with DHCP and DNS servers.
- Ensure the content stays fresh by providing updated situations to train on.

- Help establish cybersecurity culture among students and faculty similar to industry standards.

1.3. Project Scope Aims/Objectives

1.3.1. Impact of the project on people

This project ensures that academic staff, administrative personnel, students and network administrators can operate in a safer and more secure manner on the network. It prevents users from facing recent issues like packet sniffing, web cloning and malicious payload delivery. Data is protected from users on the network with VLAN segmentation, ACLs, port security and through using encrypted services. A cybersecurity website informs users about safe habits and phishing simulations give them training in spotting and avoiding common online dangers. Because SNMP works in real time, it helps network administrators address and prevent issues with user security and network performance (Stallings, 2016).

1.3.2. Features of System

- Three distinct layers – Core, Distribution and Access – help maintain scalability, manageability and performance in a network.
- By grouping departments in VLANs, it is possible to separate and safeguard sensitive information.
- Set up Access Control Lists (ACLs) to guard against unauthorized interaction between VLANs.
- With MAC address-based port security, only recognized devices can connect to the network.
- Setting up a DHCP server to provide IP addresses in an automated and dynamic manner.
- By integrating DNS, domain names are resolved and access to both internal and external resources become simple.
- Managers can use SNMP (Simple Network Management Protocol) to constantly review the state and performance of the network.

- Administrators can use SSH to securely access and manage the network through a remote connection.
- Blocking malicious traffic and preventing unauthorized connections from the outside using firewall rules and ACLs.
- Conducting phishing simulations during training to help users understand social engineering.
- An awareness site for cybersecurity offering instructions, safe behavior tips and login options.
- A display showing training results, how many staff are aware of risks and clear risk signs.
- Users produce and share awareness-raising YouTube videos that clarify technical setup processes.
- Offer simulation classes for students to learn about and deal with denial-of-service and spoofing attacks.
- By practicing packet sniffing and web cloning, you can see how frequent cyberattack tactics work.
- Lab environments are now adjusted to depict recent digital security challenges and boost learner readiness.
- Ensuring that current cybersecurity practices are implemented across the system to meet industry needs.

1.3.3. Software and Hardware Components

Table 1.1

Hardware Deployment Schedule

Hardware Component	Deployment Tasks
Router (Cisco 2911)	Install and configure routing functionalities
Core Switch (Cisco 2960)	Set up and connect VLANs across network infrastructure

Hardware Component	Deployment Tasks
Access Switches	Deploy switches and assign VLANs to ports
Access Points	Configure wireless access points for each VLAN
Servers (DHCP, DNS, Mail, Web)	Install, configure, and test core services
Workstations (PCs)	Connect and verify end-user devices

Table 1.2

Software Deployment Schedule

Software Component	Deployment Tasks
Packet Tracer	Install and configure network simulation tools
Microsoft Visio	Design diagrams showing how the physical network will be structured.
Power BI	Design dashboards for cybersecurity awareness and user feedback
Windows/Linux OS	Set up and configure operating systems for servers
Kali Linux OS	Conduct various simulated cyberattacks, including web cloning, sniffing and using reversed payloads.
DHCP Service	Configure IP address allocation for VLANs
DNS Service	Set up domain name resolution for internal resources
Email Service	Deploy and test internal email communication system
Web Server (HTTP)	Install and configure web server for awareness page
Wireshark	Capture packets and analyse the traffic on the network

Software Component	Deployment Tasks
SNMP Configuration	Set up real-time monitoring and receive event alerts through SNMP traps.
Port Security Configuration	Use MAC binding and port security to control access to switches.

1.3.4. Aim of the Project

The primary aim of this project is to set up a network that is secure, properly structured and logically separated to support improved security and better operation by allowing different departments to communicate through VLANs, ACLs and core service distribution and by providing continuous training to educate users on safer online habits and protect the network.

1.3.5. Objectives of the Project

The key objectives of this project are:

1. To strengthen security, handle network management easily and allow managed coordination between different university departments, use VLANs to separate the network, configure a router with one physical port for routing various VLANs and use Access Control Lists (ACLs) to block unauthorized attempts.
2. To ensure proper operation of services and networks, including DHCP, DNS, email and web services, while securing messages over the Internet with HTTPS, encryption and digital signatures using PGP and S/MIME and saving details of NAT logger.
3. To ensure that a network is well-protected against cyberattacks, by imitating web cloning, packet sniffing and paying back attacks with custom data, while blocking DHCP hijacking and preventing fake IP addresses using DHCP snooping and setting up port-level security.
4. To watch over, control and protect network equipment and connections, SNMP arranged traps that send alerts when there is a security issue, keep SNMP monitoring switched on for timely updates and use encrypted SSH to secure the management of remote devices.

5. To enhance knowledge and prepare employees for cyber risks, construct a security website, establish a dashboard that displays attack patterns that can teach students and staff how to stay secure and offer courses on avoiding online dangers.

1.4. Feasibility Study

1.4.1. Introduction

This project suggests creating a virtual cyber security lab at the National University of Oman using Cisco Packet Tracer, which look like the real university network. Virtual LANs will be used to divide departments, like the Information Technology Department and Engineering. Students and staff will have the opportunity to assess security rules and practice protecting their systems from several types of attacks using Cisco Packet Tracer.

The project will participate in achieving the following benefits:

- Train students and University IT personnel on the best practices on protecting networks and their machines.
- Provide a firsthand experience to show a demo on how attacks happen and how to avoid their impact.
- Honing cyber security information and awareness all over the university in various departments and sections.

The scope of this project includes:

- Build a network with VLANs for each department.
- Allow communication between VLANs using Router.
- Add services such as DHCP, DNS, Web (HTTP), and Email.
- Control traffic between departments by using ACLs.
- Simulate attacks and get to know about their impact.
- Create alerts when attacks happen.

In addition, the stakeholders for this project has been outlined in the following table:

Table 1.3

Stakeholders

Stakeholder	Role
Students	Learn and practice cyber security skills.
IT Department	Use lab for training unfamiliar staff.
Instructors	Add simulations to courses.
University Admin	Improve overall cyber security awareness.

1.4.2. Environmental Feasibility

- Oman's fast-developing 5G network allows for more advanced projects such as cybersecurity training labs. Students and staff at the National University can simulate cyberattacks and defenses by virtual machines, saving time and resources. This setup provides real cybersecurity Training needs without relying fully on physical equipment that uses a lot of energy.
- National University has the needed computer and network facilities; there is no requirement for new construction. Using virtual environments helps cut down on electronic waste, reduces the amount of electricity used and supports a greener way of learning. It follows current trends in sustainability and at the same time covers cybersecurity principles in practical and useful ways.

1.4.3. Economic Feasibility

Table 1.4

Estimated Cost Software

Item	Structure	Cost (USD)
Cisco Packet Tracer		0.0

Item	Structure	Cost (USD)
Canva		0.0
MS Word		0.0
MS PowerPoint		0.0
Power BI		0.0
Microsoft Visio		0.0
YouTube		0.0
Microsoft Teams		0.0

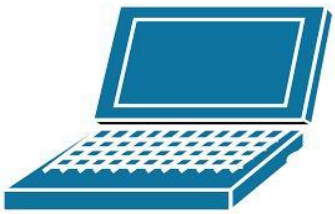
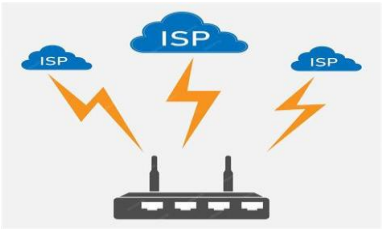
Item	Structure	Cost (USD)
Cap cut		0.0
Kali Linux		0.0
Google Docs		0.0
Wireshark		0.0
Total Cost		**0.0**

Table 1.5

Estimated Cost Hardware

Item	Count	Structure	Unit Price (USD)
Router (Cisco 2911)	2		850
Distribution Switch	2		1,500

Item	Count	Structure	Unit Price (USD)
Access Switch	8		1,500
Access Points	7		20
DHCPs Server	1		2,000
DNS Server	1		2,000
Mail Server	1		2,000
Web Server (HTTPS)	1		2,000
PC	14		1,000

Item	Count	Structure	Unit Price (USD)
Laptops	7		1,000
ISP	1		730
Total	**45**	**--**	**46,570**

Note the cost in OMR is 17,905.63, since the exchange rate for OMR is 0.380 OMR per USD.

This is a project you can use, it works well, and it saves money. The platform prepares students and staff by allowing them to interact with common cyber threats and witness how they harm systems.

The benefits of the Economic Feasibility include the following:

- Offers in-house cybersecurity education without the need to attend special workshops.
- Contributes to the completion of IT and cybersecurity degrees.
- Achieves savings around 5,000 OMR on external training every year.

1.4.4. Operational Feasibility

This section outlines the key details related to where the project will be implemented, who will be involved, and how long it will take. It highlights the main locations where the system will be used, identifies the people responsible for its execution, and presents the overall timeline to ensure smooth and effective implementation.

1.4.4.1. Location

- In university labs and cybersecurity classes.
- For training new IT support staff.
- In workshops for teachers and staff.
- Later, in online classes too.

1.4.4.2. People Needed

- Teachers or Lab assistants.
- Students Volunteers.
- Optional IT admin to support the rollout.

1.4.5. Timeline

The project will last 3 months, spanning from the month of march till the month of June, progressing through network design, VLAN configuration, security policy implementation, service deployment, attack simulations, and final testing. The project's phases will be closely tracked to guarantee that projects maintain their targets while staying within set time frames.

Total Duration: 3 Months (March 3 to June17, 2025)

Table 1.6

Total Duration

Task	Time
Research	1 week
VLAN Configuration	1 weeks
ACLs and Servers	1 weeks
Attack Simulation	3 weeks
Port Security & SSH	1 week
Final Testing	1 weeks
Documentation	4 weeks

Total	12 Weeks

1.4.6. Technical Knowledge

This section explains the technical knowledge required to understand and implement the project. It focuses on essential concepts in computer networking, including how devices are connected, how data travels through the network, and the specific functions of core components like routers, switches, and servers. It also introduces the use of a hierarchical network design to ensure efficient performance and scalability throughout the project.

1.4.6.1. Computer Networking

- Learn how PCs, routers, and switches are connected to build a network.
- Learn how data moves inside a network using IP addresses and subnets.
- Know the roles of core network components such as routers (for routing traffic), switches (for internal communication), and servers (for services like DHCP, DNS, Web, and Email).
- The project used a hierarchical design (Core, Distribution, Access layers) to ensure scalability, performance, and proper traffic flow.

1.4.6.2. Cybersecurity Threats

Learn about common types of cyber-attacks such as:

- Phishing Attacks: Simulated using Kali Linux and the Social Engineering Toolkit (SEToolkit). Fake login pages were created to collect test credentials and demonstrate how attackers trick users.
- Reverse Shell Attacks: Tested using Metasploit to simulate how attackers can gain remote control of a device through a payload. Packet Sniffing: Implemented using Wireshark to observe unencrypted traffic and understand data interception techniques.
- Packet Sniffing: Implemented using Wireshark to observe unencrypted traffic and understand data interception techniques.

1.4.6.3. Cyber Defense Techniques

- Understand and learn how to use Access Control Lists (ACLs) to allow or control and block who can access different parts of the network.
- Add security settings to routers and switches to keep important data safe.
- Learn how to detect and respond to unusual activities on the network.

1.4.6.4. Cisco Packet Tracer

- Use this tool to build virtual networks for practice and testing.
- Simulate attacks and test how to stop them in a safe virtual environment.
- Understand how to use simulation features for training.

1.4.6.5. Cisco Packet Configuration

- VLANS: To help separate traffic and improve security. Virtual LANs were created for each department like IT, HR, and Guests (Cisco, n.d. -a).
- Router Setup: The router was configured using “Router-on-a-Stick” method to connect all VLANs together and allow communication (Cisco, n.d. -b).
- SSH: SSH was used for safe and encrypted remote access to routers and switches (Cisco, n.d. -c).
- Port Security and DHCP Snooping: To stop unknown devices and protect against fake IP addresses these features were enabled on switches (Cisco, n.d. -d).
- NAT: To allow devices in the lab to access the internet by changing private IPs to public ones (Cisco, n.d. -e).
- TFTP: Configurations were saved to a TFTP server, so they can be restored if needed (Cisco, n.d. -f).
- SNMP: To monitor the network and collect information from devices (Cisco, n.d. -g).
- DHCP setup: Provide automatic IP addresses (Cisco, n.d. -h).
- Access Control Lists (ACLs): Specify which devices can talk to each other and prevent the ones that are not allowed (Cisco, n.d. -i).
- Testing tools: Use commands to check if the devices are connected correctly.

1.4.6.6. Ethical and Social Concerns

Every single data breach case and software we used was done only for educational purposes, not in a real live setting. Ethical rules were applied, making sure skillful activities stayed within the lesson plans.

- Education on privacy, unauthorized access and compliance with cybersecurity rules was given to every student.
- The lab encourages responsible online behavior, making sure students realize how cyberattacks can impact society and why ethics matter in their responses.
- More attention was given to improving defenders, rather than attackers, since this fits better with having strong character and a professional work principle.

1.5. Chapter Summary

Hackers are increasingly targeting educational institutions because of the sensitive information they handle. In the past, NU faced phishing and ransomware attacks, suggesting the importance of stronger network security and more awareness among users. Many students and staff are not familiar with hands-on practices needed to address and respond to developing threats. Therefore, the project builds the University network in Cisco Packet Tracer, a Cybersecurity Awareness, Attack Simulations Lab along with an interactive dashboard, website and educational videos created so learners can practice with real-life attack situations.

Key issues uncovered during the investigation were lack of training for cybersecurity, susceptibility to attacks and not having a central learning platform. The aim of this project is to overcome these issues by giving students, IT staff and faculty simulation training that will improve their abilities. A network solution uses VLANs to maintain separation for each department, ACLs to check and regulate what is sent over the network and DHCP and DNS to provide secure connectivity. After doing a feasibility study, it is confirmed that the project is reliable, affordable, manageable to run and ensures sustainability. The presence of virtual machines and existing university infrastructure, along with Oman's 5G technology, allows the lab to develop cybersecurity skills using a modern and environmentally friendly approach.

CHAPTER 2: PROJECT PLAN

2.1 Introduction

Project planning and control center on the schedule plan and risk management plan as key elements in this chapter. Any project needs these fundamental parts to run successfully towards its completion milestones. A proper schedule plan functions as a navigational guide that produces project-developing tasks alongside their deadlines and assignment expectations for each project segment. Project members follow the set goals and deadlines to achieve better coordination which leads to increased productivity. Schedule plans include communication planning as their crucial component because it maintains team clarity and reduces misunderstandings while it prevents conflicts between members. The project team enhances collaboration through transparency and accountability because they create defined rules for information distribution. This section presents a risk management plan that helps teams prepare for possible project-disrupting uncertainties. The contingency matrix functions as a strategic tool through which possible risks get identified and evaluated according to their potential occurrence followed by establishing proactive response plans. Through the structured risk method, the team becomes both informed about possible challenges and competent at executing effective solutions that reduce adverse results.

2.2 Scheduled Plan

A structured schedule plan is crucial for project management, helping everyone stay organized, reach deadlines and track progress. The structured timeline set up in our diploma project started on March 3, 2025, and ended on June 8, 2025, taking 70 working days. Every aspect of the plan was organized in chapters and each chapter had specific tasks, people responsible and a set time period. First, we looked at Project Forming and Initiation and then examined the main chapters in this order: Introduction, Planning, Requirement Gathering, Design, Development & Testing and finally Deployment & Conclusion. Group meetings, mentor reviews, a work breakdown structure, Gantt chart, system configuration, testing and a final presentation were clearly specified for each chapter.

The rules of the schedule provided realistic timing for activities and a structured setup for their execution. In addition, Friday and Saturday were days off for everyone, giving the team a reoccurring break from their work. Breaking the project into bits with WBS and Gantt charts helped visualize tasks and holding meetings with peers and mentors made sure everyone was on the same page and received on-time feedback. As a result of following this plan, we were able to manage our work systematically, divide tasks evenly and communicate well, making delays or mismanagement less likely. By following this timeline, we were able to deliver a project that was well-documented and fully functional.

Figure 2.2.1

Project Schedule By using Project Libre

	Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Diploma Project**	70 days?	**3/3/25 8:00 AM**	**6/8/25 4:00 PM**		
2	**Project Forming**	4 days	**3/3/25 8:00 AM**	**3/6/25 4:00 PM**		
3	Forming a Group	2 days	3/3/25 8:00 AM	3/4/25 4:00 PM		Laila Tamer
4	Project Initiation Report	2 days	3/5/25 8:00 AM	3/6/25 4:00 PM	3	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
5	**Chapter 1: Introduction**	9 days	**3/10/25 8:00 AM**	**3/20/25 4:00 PM**		
6	Background	1 day	3/10/25 8:00 AM	3/10/25 4:00 PM	4	Yamin Al-Dhanki
7	Group Meeting	1 day	3/11/25 8:00 AM	3/11/25 4:00 PM	6	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
8	Preliminary Investigation	2 days	3/12/25 8:00 AM	3/13/25 4:00 PM	7	Hamza Al-Adawi
9	Mentor Meeting	1 day	3/16/25 8:00 AM	3/16/25 4:00 PM	8	Yamin Al-Dhanki
10	Project Scope	2 days	3/17/25 8:00 AM	3/18/25 4:00 PM	9	Taha Al-Balushi
11	Feasibility Study	1 day	3/19/25 8:00 AM	3/19/25 4:00 PM	10	Laila Tamer
12	Summary	1 day	3/20/25 8:00 AM	3/20/25 4:00 PM	11	Sheikha Al-Hinai
13	**Chapter 2: Project Plan (17 days)**	17 days	**3/26/25 8:00 AM**	**4/17/25 4:00 PM**		
14	Introduction	1 day	3/26/25 8:00 AM	3/26/25 4:00 PM	12	Hamza Al-Adawi
15	Scheduled plan	3 days	3/27/25 8:00 AM	3/31/25 4:00 PM	14	Hamza Al-Adawi
16	Work Breakdown Structure (WBS)	3 days	4/1/25 8:00 AM	4/3/25 4:00 PM	15	Taha Al-Balushi
17	Group Meeting	1 day	4/6/25 8:00 AM	4/6/25 4:00 PM	16	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
18	Gantt Chart	1 day	4/7/25 8:00 AM	4/7/25 4:00 PM	17	Sheikha Al-Hinai
19	Risk Plan	3 days	4/8/25 8:00 AM	4/10/25 4:00 PM	18	Laila Tamer
20	Mentor Meeting	1 day	4/13/25 8:00 AM	4/13/25 4:00 PM	19	Taha Al-Balushi
21	Role of team members	1 day	4/15/25 8:00 AM	4/15/25 4:00 PM		Yamin Al-Dhanki
22	Team Communication Plan	1 day	4/16/25 8:00 AM	4/16/25 4:00 PM	21	Laila Tamer
23	Chapter Summary	1 day	4/17/25 8:00 AM	4/17/25 4:00 PM	22	Sheikha Al-Hinai

	Name	Duration	Start	Finish	Predecessors	Resource Names
24	**Chapter 3: Requirement Gathering ar**	15 days	**4/20/25 8:00 AM**	**5/8/25 4:00 PM**		
25	Introduction	1 day	4/20/25 8:00 AM	4/20/25 4:00 PM	23	Laila Tamer
26	Methodology Used (SDLC Model)	1 day	4/21/25 8:00 AM	4/21/25 4:00 PM	25	Laila Tamer
27	Tools of Data Gathering	3 days	4/22/25 8:00 AM	4/24/25 4:00 PM	26	Sheikha Al-Hinai
28	Group Meeting	1 day	4/25/25 8:00 AM	4/27/25 4:00 PM	27	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
29	Data Analysis	1 day	4/28/25 8:00 AM	4/28/25 4:00 PM	28	Hamza Al-Adawi
30	Technical Requirement	2 days	4/30/25 8:00 AM	5/1/25 4:00 PM	29	Taha Al-Balushi
31	Mentor Meeting	1 day	5/4/25 8:00 AM	5/4/25 4:00 PM	30	Sheikha Al-Hinai
32	Literature Review	2 days	5/5/25 8:00 AM	5/6/25 4:00 PM	31	Yamin Al-Dhanki
33	Summary	2 days	5/7/25 8:00 AM	5/8/25 4:00 PM	32	Taha Al-Balushi
34	**Chapter 4: Design (8 days)**	5 days?	**5/11/25 8:00 AM**	**5/15/25 4:00 PM**		
35	Introduction	1 day?	5/11/25 8:00 AM	5/11/25 4:00 PM	33	Yamin Al-Dhanki
36	Logical Network Design	1 day	5/12/25 8:00 AM	5/12/25 4:00 PM	35	Sheikha Al-Hinai
37	Group Meeting	1 day?	5/13/25 8:00 AM	5/13/25 4:00 PM	36	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
38	Physical Network Design	1 day	5/14/25 8:00 AM	5/14/25 4:00 PM	37	Hamza Al-Adawi
39	Summary	1 day?	5/15/25 8:00 AM	5/15/25 4:00 PM	38	Taha Al-Balushi
40	**Chapter 5: Development and Testing**	9.2 days?	**5/19/25 8:00 AM**	**6/1/25 9:36 AM**		
41	Introduction	1 day?	5/19/25 8:00 AM	5/19/25 4:00 PM	39	Laila Tamer
42	Network Metadata	1 day?	5/20/25 8:00 AM	5/20/25 4:00 PM	41	Laila Tamer
43	Networking Protocols & Security	1 day?	5/21/25 8:00 AM	5/21/25 4:00 PM	42	Yamin Al-Dhanki
44	Communication Protocols	1 day?	5/22/25 8:00 AM	5/22/25 4:00 PM	43	Taha Al-Balushi
45	System Configuration	2 days	5/25/25 8:00 AM	5/26/25 4:00 PM	44	Hamza Al-Adawi
46	Configuration Summary	1 day?	5/27/25 8:00 AM	5/27/25 4:00 PM	45	Hamza Al-Adawi

	Name	Duration	Start	Finish	Predeces...	Resource Names
47	Testing	0.2 days?	5/28/25 8:00 AM	5/28/25 9:36 AM	46	Laila Tamer;Hamza Al-Adawi;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
48	Mentor Meeting	1 day?	5/28/25 9:36 AM	5/29/25 9:36 AM	47	Taha Al-Balushi
49	Summary	1 day	5/29/25 9:36 AM	6/1/25 9:36 AM	48	Sheikha Al-Hinai
50	**Chapter 6: Deployment, Limitation and Conclusic**	6 days	**6/1/25 8:00 AM**	**6/8/25 4:00 PM**		
51	Introduction	1 day	6/1/25 9:36 AM	6/2/25 9:36 AM	49	Laila Tamer
52	Deployment	1 day	6/2/25 9:36 AM	6/3/25 9:36 AM	51	Yamin Al-Dhanki
53	Challenges / Limitations	1 day	6/3/25 9:36 AM	6/4/25 9:36 AM	52	Hamza Al-Adawi
54	Future Enhancement	1 day	6/4/25 9:36 AM	6/5/25 9:36 AM	53	Hamza Al-Adawi
55	Group Meeting	1 day	6/6/25 8:00 AM	6/8/25 4:00 PM	54	Hamza Al-Adawi;Laila Tamer;Sheikha Al-Hinai;Taha Al-Balushi;Yamin Al-Dhanki
56	Conclusion	1.25 days	6/1/25 8:00 AM	6/2/25 10:00 AM	48	Taha Al-Balushi
57	Reflection	1.375 days	6/2/25 10:00 AM	6/3/25 1:00 PM	56	Taha Al-Balushi;Hamza Al-Adawi;Yamin Al-Dhanki;Sheikha Al-Hinai;Laila Tamer
58	Mentor Meeting	1.125 days	6/3/25 3:00 PM	6/4/25 4:00 PM	57	Laila Tamer
59	Final Report Submission	2 days	6/5/25 8:00 AM	6/8/25 4:00 PM	58	Hamza Al-Adawi

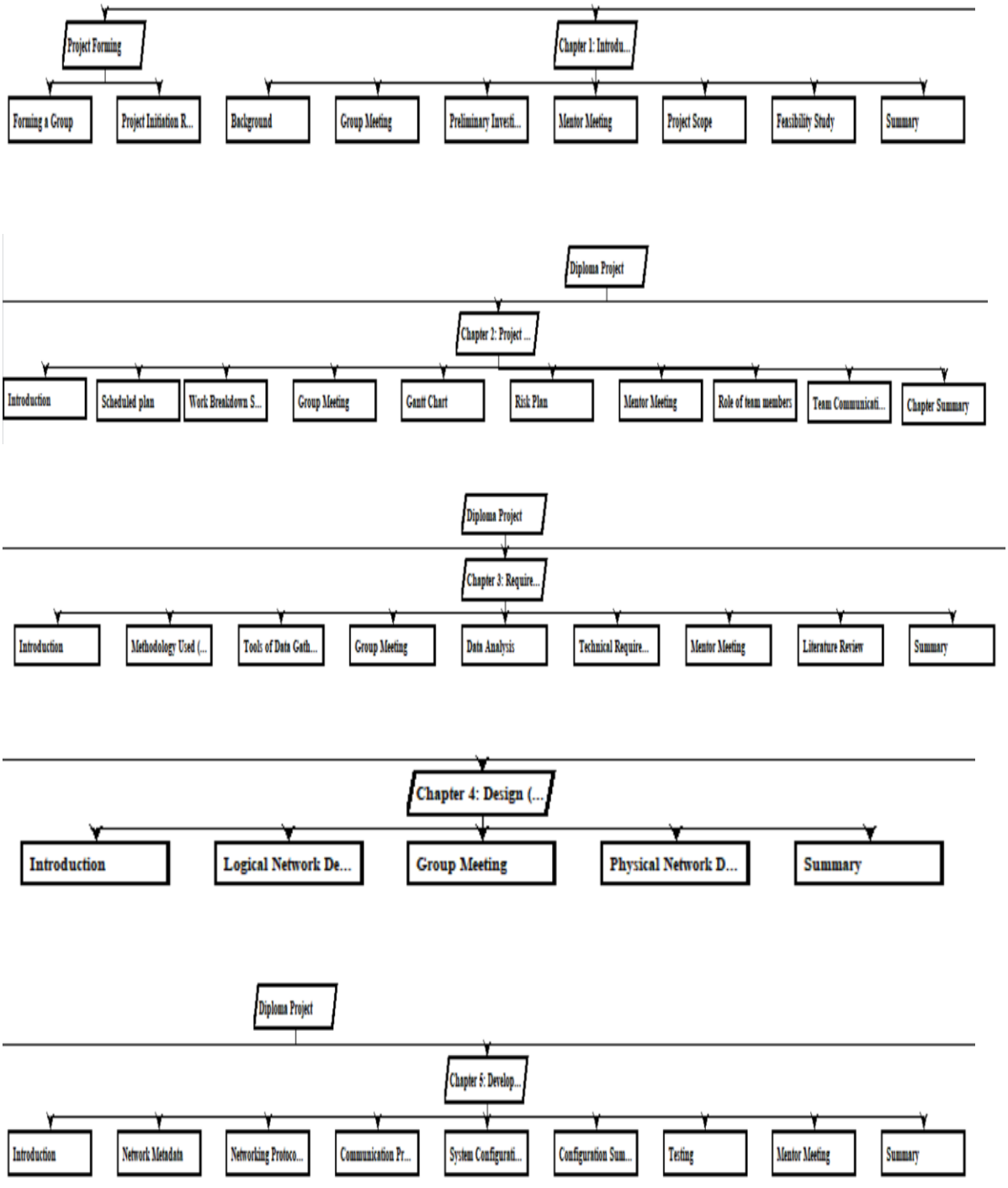
	Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Diploma Project**	70 days?	**3/3/25 8:00 AM**	**6/8/25 4:00 PM**		
2	**Project Forming**	4 days	**3/3/25 8:00 AM**	**3/6/25 4:00 PM**		
5	**Chapter 1: Introduction**	9 days	**3/10/25 8:00 AM**	**3/20/25 4:00 PM**		
13	**Chapter 2: Project Plan**	17 days	**3/26/25 8:00 AM**	**4/17/25 4:00 PM**		
24	**Chapter 3: Requirement Gathering and Analysis**	15 days	**4/20/25 8:00 AM**	**5/8/25 4:00 PM**		
34	**Chapter 4: Design**	5 days?	**5/11/25 8:00 AM**	**5/15/25 4:00 PM**		
40	**Chapter 5: Development and Testing**	9.2 days?	**5/19/25 8:00 AM**	**6/1/25 9:36 AM**		
50	**Chapter 6: Deployment, Limitation and Conclusion**	6 days	**6/1/25 8:00 AM**	**6/8/25 4:00 PM**		

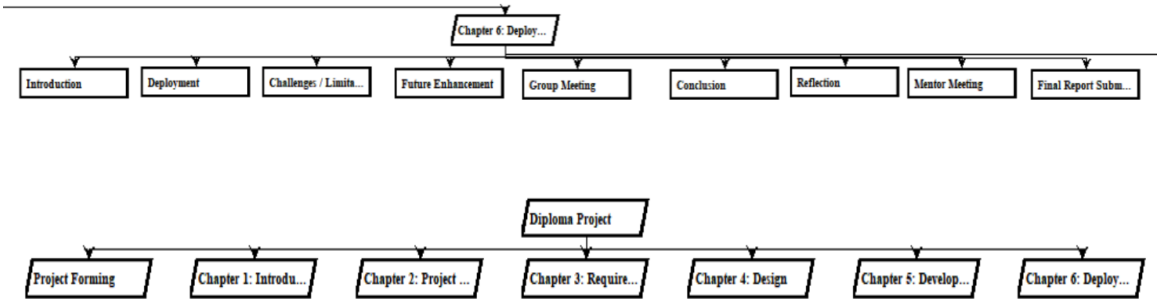
2.3 Work Breakdown Structure

A Work Breakdown Structure (WBS) provides a chart or diagram that breaks a narrow down the project into smaller parts. Starting from the main goal and dividing it into clear and simple steps, tasks, and sub-tasks. Each level gives more detail. By showing all the work in a clear, organized way, this will help the project team understand what work needs to be done, who will do it, and when. It is useful and crucial for everyone in the team and minimizes confusion during the project by planning, scheduling and tracking the progress of the project (ScienceDirect Topics, n.d.).

Figure 2.3.1

Work Breakdown Structure (WBS) in Project Libre



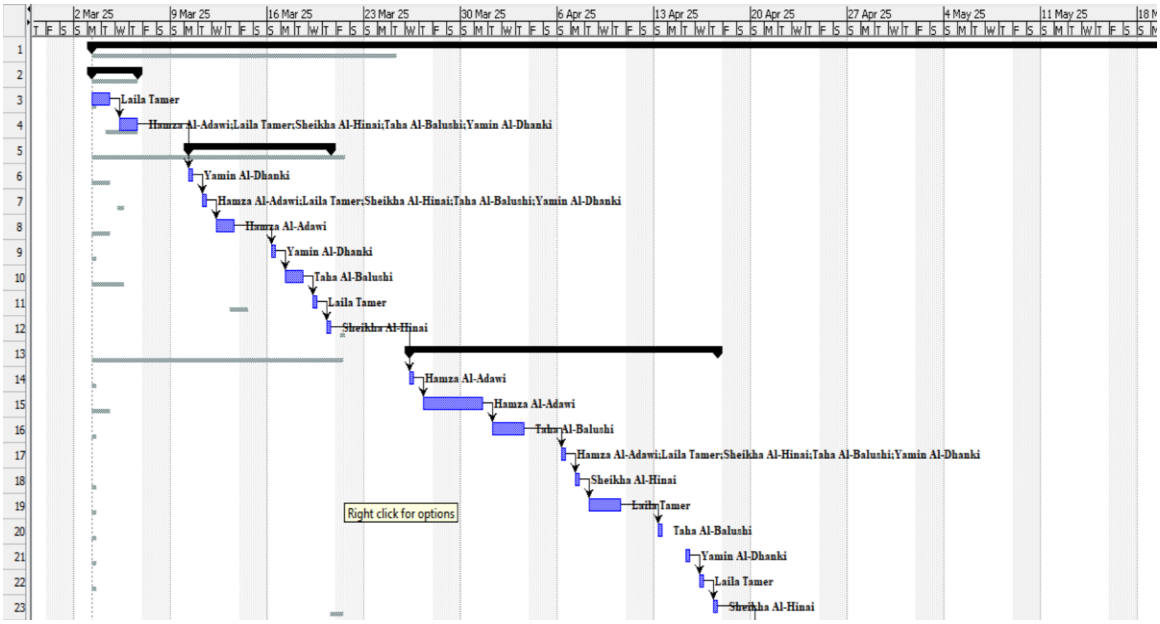


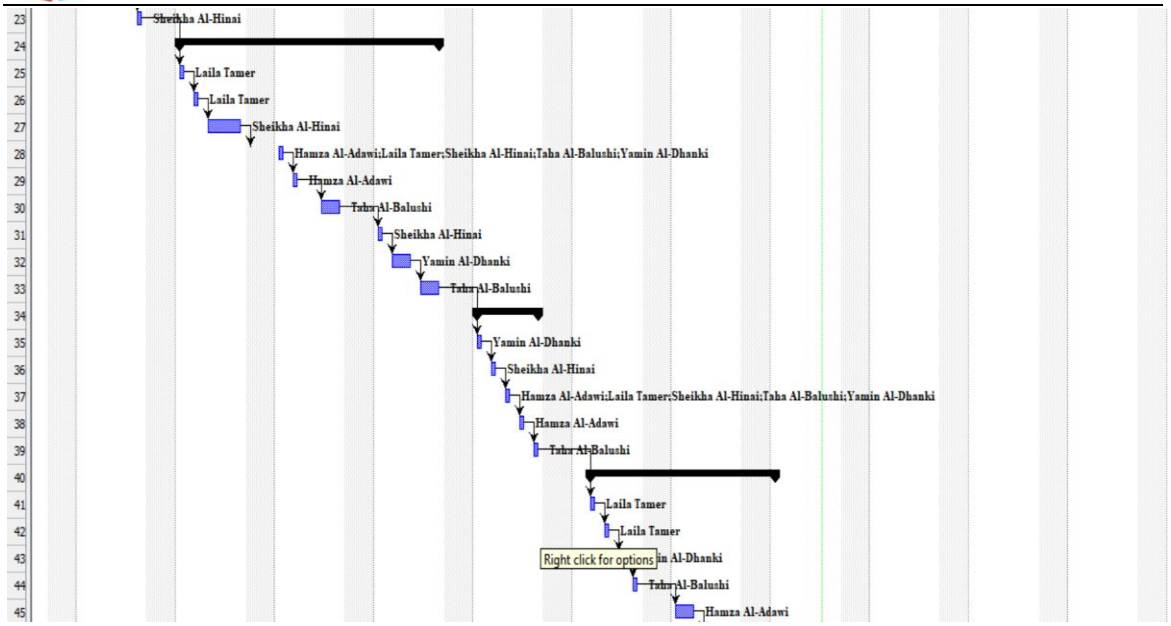
2.4 Gantt Chart

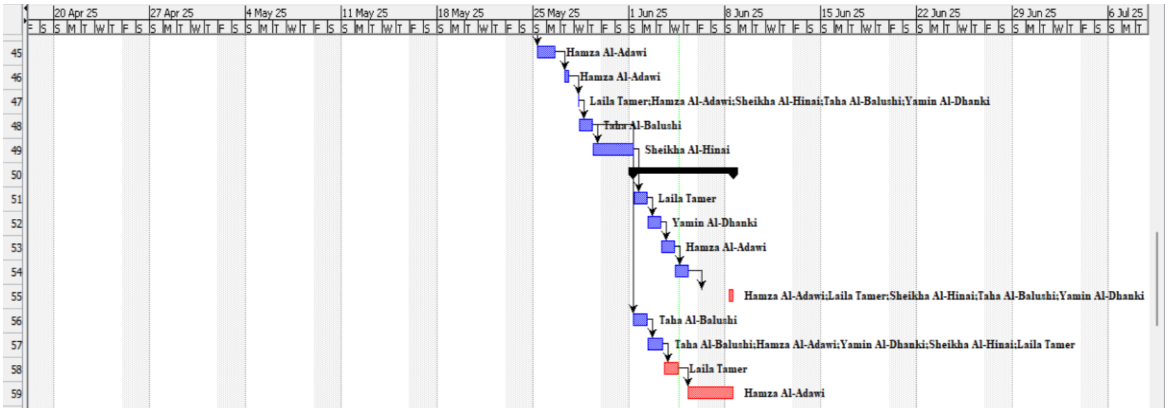
To manage a project properly one of the most important tools is a Gantt Chart, because it helps in planning, organizing, and managing the resources. It makes sure that the tasks are done within a specific time frame, budget, and scope these are important points to achieve any successful project. It also helps teams in visualizing the overall process and timelines, making it easier to monitor progress, assign responsibilities, and meet the project goals (Wadhwa, 2024).

Figure 2.4.1

Gannt chart by Project libre







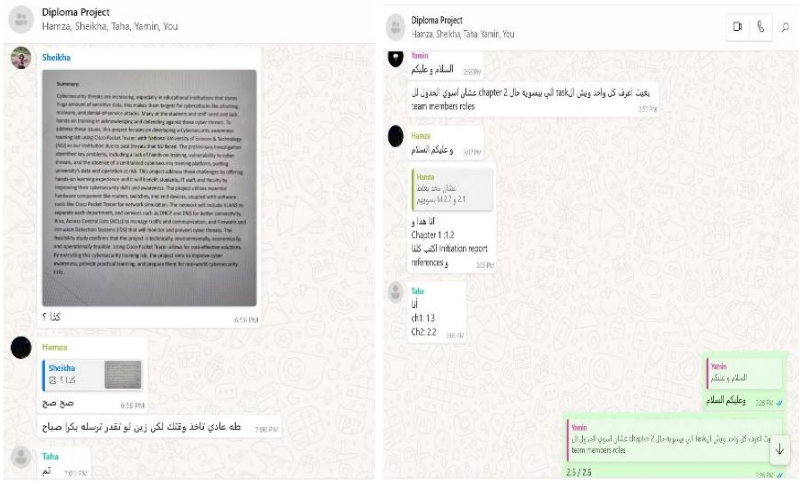
2.5 Team Communication

A communication plan is a simple document that explains how team members in a project will talk to each other and share important information. This involves identifying who sends the messages, who receives them, clarifying the topic or purpose of the communication, determining the timing and what tools they will use, such as WhatsApp, email, or meetings. These steps are crucial to help the team stay organized, avoid misunderstanding, and make sure everyone understands what they need to do (Haiilo, 2023).

In our group, we all contribute equally to writing the chapters of the project. Each chapter is assigned to a specific team leader, who is responsible for collecting the work of that chapter, checking and reviewing it with our supervisor and lecturer to ensure it meets all academic standards. This structure allows for an organized workflow where each member knows their responsibilities. For communication, we meet in person at the library, and we also communicate daily via platforms like WhatsApp or MS Teams. When needed, we book appointments with our supervisor and lecturer through SIS or by contacting them directly.

Figure 2.5.1

Screenshots of Whatsapp coversations



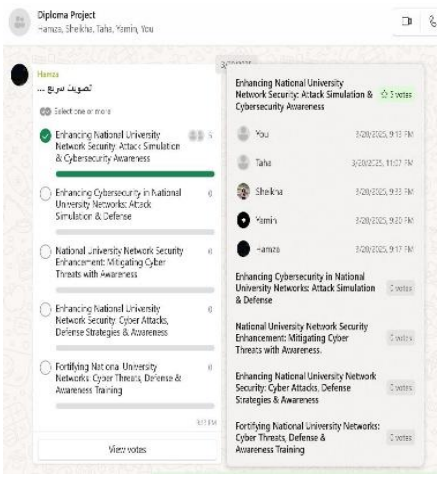
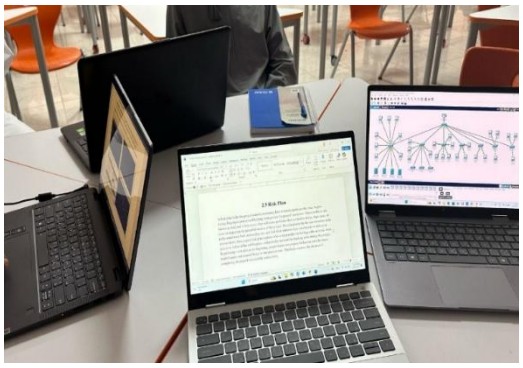


Figure 2.5.2

Pictures of Team meetings



2.6 Communication plan

Table 2.6.1

Communication Plan Table

DAY	VENUE	TIME	TYPE OF MEETING	NOTES
Saturday	Virtual (Microsoft teams)	4:00 pm - 4:30 pm	Video Call	Weekly Kick-off: Review previous week, set goals for the current week.
Monday	MEC Library	3:00 pm - 4:10 pm	Face-to-face	Mid-week Check-in: Discuss progress, assign roles, and address any immediate issues.
Daily	Team Chat (Microsoft Teams, WhatsApp)	During working hours	Online Chat	Asynchronous updates, quick questions, file sharing.
As Needed	Email	During working hours	Email	Formal communication, detailed reports, external communication.

2.7 Risk Plan

A Risk plan helps the project team by explaining how to handle problems that may happen during the project process and helping them protect the project's purposes. These problems are known as risks and if they occur, they will cause problems that can lead to delays, high costs, or have an impact on the potential success of the project. The risk plan helps the team to notice risks early, understand how serious they are, and find what solutions they need to take to reduce or prevent them. Also, a good risk plan explains who is responsible for dealing with each risk, what actions to follow if the risk happens, and provides methods for tracking risks during the project. By planning a risk plan at the beginning, project teams can prepare for known risks the know might happen and respond better to unexpected ones. This helps improve the chances of completing the project successfully and on time.

Table 2.7.2

Risk Plan

Risk	Category	Severity	Likelihood	Risk Rating	Treatment	Chance	Effect	Mitigation Plan
Wrong setup	Technological	4	3	12	Manage	Medium	Medium	Assess step-by-step and save commands
Low student interest	Social	3	3	9	Reduce	Medium	High	Show how it helps in real jobs
Time delays	Management	2	2	4	Manage	Low	Medium	Follow weekly checklist
One person knows everything	Knowledge-based	4	2	8	Avoid	Medium	High	Train more than one person and write guides

2.8 Role of team members

This project was built through the contributions of all team members. We made sure that the tasks were divided by each person's strengths and preferences to maintain efficiency in every step. This area summarizes each participant's part and what they contributed throughout the project.

Table 2.8.3

Role Of Team members

Chapters	Tasks	Done by
Chapter 1	1.1 Introduction/ Project Overview	Yamen Hamed Aldhanki
	1.2 Preliminary Investigation	Hamza Suleiman Aladawi
	1.3 Project scope	Taha Mohammed Al Balushi
	1.4 Feasibility study	Laila Tamer Mekhimar
	1.5 Summary	Sheikha Rashid Al Hinai
	Initiation report/References	Yamen Hamed Aldhanki Hamza Suleiman Aladawi Taha Mohammed Al Balushi Laila Tamer Mekhimar Sheikha Rashid AL Hinai
Chapter 2	2.1 Introduction	Hamza Suleiman Aladawi
	2.2 Scheduled Plan	Hamza Suleiman Aladawi
	2.3 Work Breakdown Structure (WBS)	Taha Mohammed Al Balushi
	2.4 Gantt Chart	Sheikha Rashid Al Hinai
	2.5 Team Communication	Laila Tamer Mekhimar
	2.6 Communication Plan	Hamza Suleiman Aladawi
	2.7 Risk Plan	Laila Tamer Mekhimar
	2.8 Role of Team Members	Yamen Hamed Aldhanki
	2.9 Chapter Summary	Laila Tamer Mekhimar

Chapter 3	3.1 Introduction	Laila Tamer Mekhimar
	3.2 Methodology	Laila Tamer Mekhimar
	3.3 Tools for Data Gathering	Sheikha Rashid Al Hinai
	3.4 Data Analysis and Findings	Hamza Suleiman Aladawi
	3.5 Technical Requirement	Taha Mohammed Al Balushi
	3.6 Literature Review	Yamen Hamed Aldhanki
	3.7 Summary	Taha Mohammed Al Balushi
Chapter 4	4.1 Introduction	Yamen Hamed Aldhanki
	4.2 Logical Design	Laila Tamer Mekhimar & Sheikha Rashid Al Hinai
	4.3 Physical Design	Taha Mohammed Al Balushi
	4.4 Summary	Taha Mohammed Al Balushi
Chapter 5	5.1 Introduction	Laila Tamer Mekhimar
	5.2 Network Metadata	Laila Tamer Mekhimar
	5.3 Networking protocols, Security and Topology	Yamen Hamed Aldhanki
	5.4 Communication Protocols and Secure Service	Taha Mohammed Al Balushi
	5.5 System Configuration	Hamza Suleiman Aladawi
	5.6 Configuration Summary	Hamza Suleiman Aladawi
	5.7 Chapter Summary	Sheikha Rashid Al Hinai
Chapter 6	6.1 Introduction	Laila Tamer Mekhimar
	6.2 Deployment	Laila Tamer Mekhimar
	6.3 Challenges / Limitations	Laila Tamer Mekhimar
	6.4 Future Improvements	Hamza Suleiman Aladawi
	6.5 Conclusion	Hamza Suleiman Aladawi
	6.6 Reflection	Laila Tamer Mekhimar
	References	Sheikha Rashid Al Hinai

2.9 Chapter Summary

Chapter 2 explains the key factors considered in planning how the diploma project would be organized and managed. The process starts by constructing a schedule that lists the jobs for each chapter, schedules their deadlines and informs everyone who is responsible over the course of 70 working days. With the help of a Work Breakdown Structure (WBS) and Gantt Charts, managing different parts of the project was easier and everyone understood their role well. Because of these tools, the team could track their progress, sort their tasks well, stick to deadlines and make sure everyone stayed in sync with set meetings and feedback.

Furthermore, the chapter makes clear that project success depends greatly on good communication and risk management. The plan specified that information would be exchanged among team members using WhatsApp, MS Teams and face-to-face conversations. It revealed possible issues in the project and outlined approaches to address them using a contingency table. Everyone was given duties that suited their abilities which made it possible for the project to be completed successfully by the full team.

CHAPTER 3: REQUIREMENT GATHERING AND ANALYSIS

3.1 Introduction

The chapter covers the research framework, tools for collecting data, what was needed to develop the Lab and the literature that informed the procedure. The purpose of this chapter is to provide a clear plan for the project's design, execution and evaluation. The first step is to introduce the SDLC, a method of breaking the project down into orderly stages for building the software part. Several SDLC models are examined such as Waterfall, Iterative, Prototyping, Time-boxing and Agile, to determine which fits a lively and hands-on cybersecurity environment best. Considering the requirements, the Agile approach was picked because it is flexible, has a feedback loop that never stops and closely matches the project needs.

Following this, the chapter details the process of surveying students and staff at the National University with questionnaires and interviewing cybersecurity experts. The purpose of using these tools was to check how knowledgeable users are about cybersecurity threats and what kinds of learning suit them best. Most learners picked hands-on, laboratory exercises for their preferred type of training and the big issues they worry most about are phishing, malware and using weak passwords. The findings led to the establishment of the training lab, supported by simulation tools, interactive dashboard and real cyber-attack cases. Furthermore, the chapter looks at the required hardware and software which are routers, switches, Packet Tracer, Kali Linux and Wireshark. They are applied in a practical setting to help students get ready for the issues they may face in the digital world. Following the main section, a literature review compares global experiences, available training plans and learning techniques, agreeing that practicing real-world skills is the most effective approach to security awareness. This chapter brings together academic ideas, technical practices and input from regular users, all in line with the national plan for strong digital security as seen in Oman Vision 2040.

3.2 Methodology

Software Development Life Cycle (SDLC) is a step-by-step process used by the software industry to design, develop and test software. This process aims to produce high quality and cost-effective software in order to meet the customer expectations and needs.

"A software development life cycle provides a structured framework that helps ensure consistency, completeness, and quality across the development process" (Hossain, 2023).

A typical Software Development Life Cycle consists of the following stages (Hossain, 2023).

3.2.1. Stages

3.2.1.1. Planning - What Are the Existing Problems?

In this crucial stage, we identify the project scope, objectives, and feasibility. This stage involves gathering requirements and conducting analysis to ensure the project is viable.

3.2.1.2. Analysis – What Do We Want?

Detailed requirements are gathered from stakeholders. This includes identifying the requirements that the software must meet. In this stage, we analyzed the need for our project and documented it properly.

3.2.1.3. Design – How It Should Look Like?

The framework of the system is designed. This incorporates high level concept (how the system will be structured) and detailed design (how individual components will function).

3.2.1.4. Development – Let's Create It

The development team writes the code for the product. Sometimes, multiple developers are needed to work on the code and in such case the coding tasks are divided between them. A developer leader has to review the final code to make sure there is consistency.

This phase often involves multiple iterations and collaboration among team members.

3.2.1.5. Testing – Is It the Exact One We Needed?

The software is tested to identify and resolve any bugs identified. There are different tupes of testing such as unit testing (usually done by the developer), integration testing, and black box testing. In well-organized companies, a dedicated testing team and environment will be provided to make sure that the highest level of product quality is delivered.

3.2.1.6. Deployment

Once testing stage is complete, the stakeholder will give a decision to go live and to deploy the product to the production environment.

3.2.1.7. Maintenance – Let's Make the Improvements

After the product is successfully deployed to production, the product will be moved to this phase and will be kept monitored by all stakeholder to provide enhancements, updates, or changes to make the product more robust.

To summarize, the SDLC is a thorough and well-defined approach to system development that ensures systems are delivered on time, within budget, and with high quality.

3.2.2. SDLC Models

There are six popular SDLC methodologies that we can use (Hossain, 2023).

The following are the most common models in the Software industry:

1. Waterfall Model
2. Prototyping
3. Iterative Model
4. Time boxing model
5. Agile process

3.2.2.1. Waterfall Model

The waterfall model was the most fundamental Software Development Life Cycle model. Winston Royce introduced it in 1970. It is quite easily understandable and applicable. Basically, in this, each phase must be finalized before the next phase commences. There is no overlap between phases. Therefore, it's another name is "linear-sequential life cycle model."

This model splits the whole project into many phases and no phase can begin unless the previous one is completed. Therefore, the output of one phase acts as the input of the next phase.

Advantages of the Waterfall model:

1. More accurate estimates of time and cost.
2. It is easier to plan and schedule resources.
3. Knowing what you are going to get at the end.
4. Transfers information well.
5. Easy to measure progress.

Disadvantages of using the Waterfall model:

1. Changes are costly and requires more time.
2. Customers are not involved till the end result is presented to them.
3. All or nothing (you have to wait till the end to get what you ask for).
4. Testing is done at the end (sometimes skipped if the project is behind).

3.2.2.2. Prototype Model

A prototype is a fundamental part of creating software. Prototyping allows us to examine the workflow and review the user interface as well as getting valuable feedback on how to improve it. In addition, the prototype is the optimal way to gather early feedback and helps all stakeholders to understand the requirement with the opportunity to give any comments or update them. The cost of change in this phase is low compared to change in other phases.

Advantages of Prototype models:

1. Requirement Understanding: It helps to clarify the requirements and collect user feedback, which contributes to customer satisfaction.
2. Enhanced User Participation: Users can participate in the prototyping early, leading to a system that better matches their business needs.

Disadvantages of Prototype model:

1. This model can be costly as the developer may need to spend too much time developing the prototype.
2. This methodology may increase the complexity of the system as the scope of the system may go beyond original plans.

When to use Prototype model:

On a case-to-case basis, software developing companies need to decide if prototyping will be helpful to a specific project or not. These are a few considerations and situations where prototyping is the best decision to implement:

1. When the requirements of the software are not precisely clear to the team.
2. When the demands of the software are unpredictable and change rapidly.
3. When there are software-intensive and complicated systems that need experimentation and the least risk.
4. Prototyping is recommended if the software or product requires a lot of communication and interactions between the stakeholders.

3.2.2.3. Iterative Model

An iterative model is a development approach that involves iterations of processes to gradually enhance a product or project. This model is commonly used in software development and project management, allowing teams to build, test, and revise their work in manageable segments rather than attempting to complete the entire project in one go.

Advantages of Iterative model:

1. Allows flexibility and adaptability to changing requirements.
2. Encourages stakeholder involvement and feedback throughout the process.
3. Helps in identifying and addressing issues early.

Disadvantages of Iterative model:

1. Scope Creep: This can happen if it's not managed in the right way, as continuous changes may extend the project timeline.
2. Effective communication and collaboration are needed among team members to ensure they are aligned and understand the requirements.

When to use iterative model:

Iterative models are valuable in environments where user feedback and adaptability are crucial for success, making them a popular choice in modern development practices.

3.2.2.4. Time boxing model

1. Timeboxing is a time management technique, which incorporates specifying a fixed time to an activity or task and completing it within that allocated timeframe, regardless of the outcome. Once the time is up, we stop working on that task, regardless of how far we've progressed. This method helps improve focus, reduce procrastination, and enhance productivity by creating a sense of urgency.
2. Timeboxing is a goal-based time management technique that was introduced by James Martin as part of agile software development.

Advantages of Time-boxing:

1. Increased Productivity: By creating a sense of urgency, you are more likely to stay focused and complete tasks more efficiently.
2. Reduced Procrastination: Knowing you only need to work on something for a set period can make starting less daunting.
3. Improved Time Management: Helps in planning your day better by giving you a clearer picture of how much time you can devote to various activities.
4. Enhanced Work-Life Balance: By setting boundaries on work tasks, you can ensure you make time for personal activities and relaxation.

Disadvantages of Time-boxing:

Risk of Rushed Work: Strict time constraints might lead to rushed or lower-quality work.
Pressure on Complex Tasks: For complex or high-stakes tasks, rigid timeboxing might not allow for adequate depth or exploration.

Conclusion, Timeboxing is a powerful time management strategy that brings structure and focus to your daily routine. By allocating dedicated timeboxes to tasks and activities, we can optimize productivity, manage time effectively, and achieve a balance between work life and personal life. Embrace the mindset methodology of timeboxing and unlock its potential to enhance efficiency, focus, and overall success.

3.2.2.5. Agile Process Model

Agile is a mindset which has to be adopted by all stakeholders. It's built on the pillars of understanding, collaboration, and staying flexible. This mindset will help the team to adapt to the changes that arise during the lifecycle. Projects which follow Agile methodology have a high rate of success.

There are many Software Development Methodologies available but Agile is one of the most popular in industry. It is because nothing is permanent in Agile until the project has delivered a solution that is good and sufficient to the needs of its users. *(Beck et al., 2001; Amin, 2019; Heusser, 2013; Fowler, n.d.)*

Some of the major principles are:

1. Early and iterative delivery of valuable software.
2. Flexibility in changing requirements.
3. Working collectively daily throughout the project.
4. Face-to-face conversation with team members.
5. Encouraging simplicity.

Agile outperforms traditional software development techniques. That's why this model is attracting more and more attention from businesses today.

Advantages of Agile model:

1. The ability to handle change gracefully without having project plans impacted under new requirements.
2. Adaptive approaches and teamwork focus on continuous improvement.
3. Agile flexible approach enables team members to work together with stakeholders during all phases of development, which encourages clients' feedback instead of waiting until the whole implementation is completed.

4. Agile projects involve multiple software members working together in small teams to quickly deliver the product.
5. Agile software development is based on iterative development cycles and everything starting from the requirements until building the product are based on the collaboration between self-organizing cross-functional teams.

Disadvantages of Agile model:

1. Lack of Predictability: Agile is an iterative nature that can make it difficult to predict project timelines, costs, and deliverables. This can be challenging for stakeholders who prefer fixed schedules and budgets.
2. Team Dependency: Agile relies on team collaboration and communication. If team members are not engaged or lack the necessary skills, the project can be impacted.
3. Scope Creep: The flexibility of Agile can lead to adding more requirements, where continuous changes and additions can make the original project not feasible.
4. Documentation Challenges: Agile pays more attention to working software than heavy documentation. Unfortunately, that can result in insufficient documentation for future references.

When to use Agile model:

1. Short to medium-term projects: Projects that are expected to last for a short period of time are well-suited for Agile, as the methodologies are designed for shorter, iterative delivery cycles.
2. Projects with a high degree of certainty: Projects where the requirements or deliverables are highly certain are well-suited by Agile, as the methodologies rely on a clear and well-defined set of requirements.
3. Flexible budget or timelines: Projects with flexible budget or timelines are well-suited for Agile, as the methodologies rely on flexibility and the ability to adapt to change.
4. Projects with clear goals or objectives: Projects with clear goals or objectives are well-suited for Agile, as the methodologies rely on a clear and well-defined set of objectives.

3.2.3. Choice of SDLC Methodology: Agile Model

A methodology is centered around a process which is enriched. Normally speaking, it is based upon knowledge and experience.

We may not assume that there is a standard methodology that suits a specific project, because every project is unique. Consequently, practitioners select a methodology that is the best fit for their project and then adapt it. Being able to adapt a methodology supposes having the same skills necessary to design a methodology from scratch. It requires an understanding of what to do, why, when, how, the prerequisites, limitations and alternatives. (Beck et al., 2001).

Justification for Choosing the Agile Model

1. Agile promotes incremental development, delivering functional software in short sprints (1-4 weeks). It also reduces the time between idea conception and product launch.
2. Unlike Waterfall, Agile allows teams to adjust to changing requirements even in later stages. In addition, Agile incorporates continuous testing, code reviews, and integration, leading to fewer bugs and higher stability.
3. Agile promotes cross-functional teamwork and regular sync-ups through daily stand-ups, sprint planning, and retrospectives. It prioritizes customer feedback, ensuring the final product meets user needs, which increases customer satisfaction by delivering working solutions in each sprint.

Agile methodology is not just a development approach; it's a mindset that fosters innovation, collaboration, and adaptability. It ensures that software projects meet user needs, deliver value faster, and maintain high quality while reducing risks and costs.

3.3 Data Gathering Tools

Selecting the right data gathering tools in research is very important for getting reliable and valid information. These tools are important for getting evidence-based information, and help researchers find patterns and come to a valid conclusion (Creswell & Creswell, 2017).

3.3.1. Methods of Data Gathering

- Questionnaire: It consists of a group of questions related to the subject being researched and it aims to collect information from a large group of people (Creswell & Creswell, 2017).
- Interviews: A direct method usually face to face conversations with the participants, allowing researchers to explore detailed perspectives and perceptions that might not be gaining using other gathering tools (Bryman, 2016).
- Focus Groups: It is a group discussion led by a facilitator. It is organized to collect multiple opinions, experiences, and perceptions from the participants on a particular topic (Creswell & Creswell, 2017).
- Observation: This involves watching and recording behaviors and events as they happen in a natural way in their original environment. Observation provides data especially when the study is related to actions, routines, and settings (Bryman, 2016).
- Document Analysis: It is the process of carefully reviewing documents that already exist such as policies, reports, articles, and books to get relevant and useful information (Creswell & Creswell, 2017).

These tools mentioned can be classified as quantitative or qualitative data:

- Quantitative: These include gathering tools like questionnaires and observations that give numerical data.
- Qualitative: These include gathering tools like interviews, focus groups, and document analysis that gives non-numerical data (Creswell & Creswell, 2017; Bryman, 2016).

3.3.2. Selecting data gathering tool for the project

Deciding which tool to use depends on a lot of factors like time management and resource availability and the type of information needed. Given that the project is on the Cybersecurity Awareness Training Lab and after careful consideration, it has been decided to use the Questionnaire as the primary data collecting tool.

The questionnaire involves collecting information from students and staff at the Middle East College. It was carefully designed by using Google Forms. It aimed at getting participants' view on current theoretical cybersecurity education and if they will be interested in participating with hands-on and practical training modules. And the questionnaire also investigates participants' overall awareness of cyber security threats and how they will keep their online environment safe.

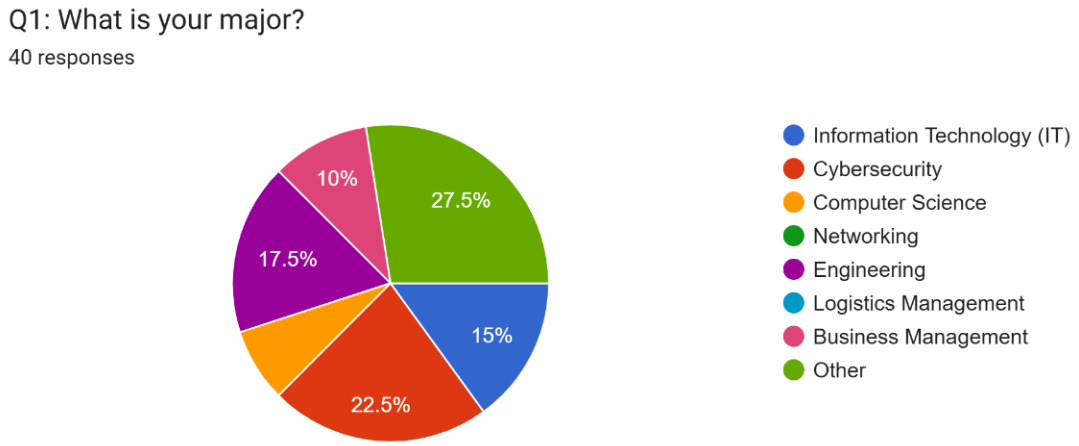
Additionally, an interview was also conducted with a cybersecurity expert to get more technical advice and professional recommendations, which helped in better understanding on how to shape and improve the project.

3.4 Data Analysis & Findings

This section reveals outcomes from a cybersecurity awareness questionnaire and interview that included students and Faculty members from Higher Education Institutions in Oman. The data delivers insights regarding participant academic backgrounds alongside their knowledge of prevalent cybersecurity threats and learning approaches while revealing their self-perceived understanding of cybersecurity fundamentals. The data examines present cybersecurity operations together with student evaluations of applied labs and their suggestions for practical teaching programs. The use of visual aids through charts and graphs show key responses and trends in the data. The study analyzes questionnaire data together with interview responses which resulted in a broad comprehension regarding Omani HEI students' cybersecurity awareness levels.

Figure 3.1

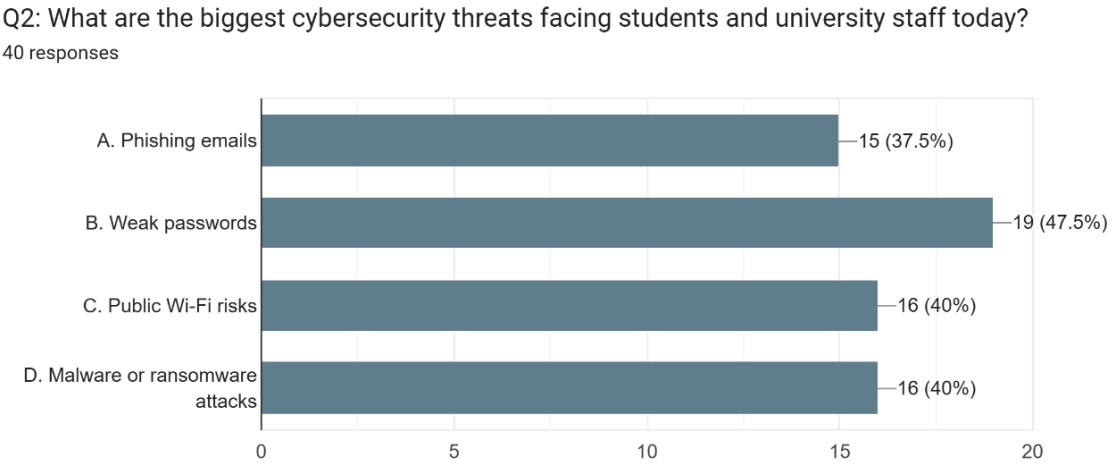
Majors of Participants



The chart shows that many survey participants are from technical educational programs as shown in the chart. There are two dominating major groups among respondents including Cybersecurity with 9 students (22.5%) while Information Technology (IT) maintains 6 students (15%). Our participant groups included Engineering (7 students making up 17.5%) and Business Management (4 students as 10%) as well as Computer Science (3 students representing 7.5%). The category of "Other" major occupied the position of eleven students (27.5%) out of the total sample.

Figure 3.2

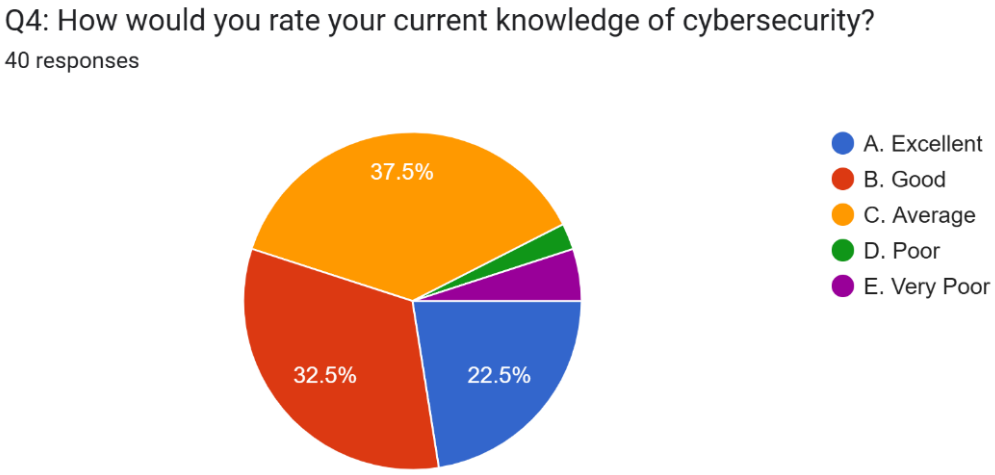
Common Cybersecurity Threats



This chart reveals what students consider as the main cyber threats they must address. Phishing emails stand out as a big threat according to students who numbered 15 among them (37.5% of the total respondents). Students identify weak passwords as the most concerning cyber danger (47.5% or 19 students). Malware or ransomware attacks (40% or 16 students). The risk factor related to public Wi-Fi access was understood by 16 students (40%) among the total respondents. The survey participants had the ability to choose multiple answers thus creating total percentages that exceeded one hundred.

Figure 3.3

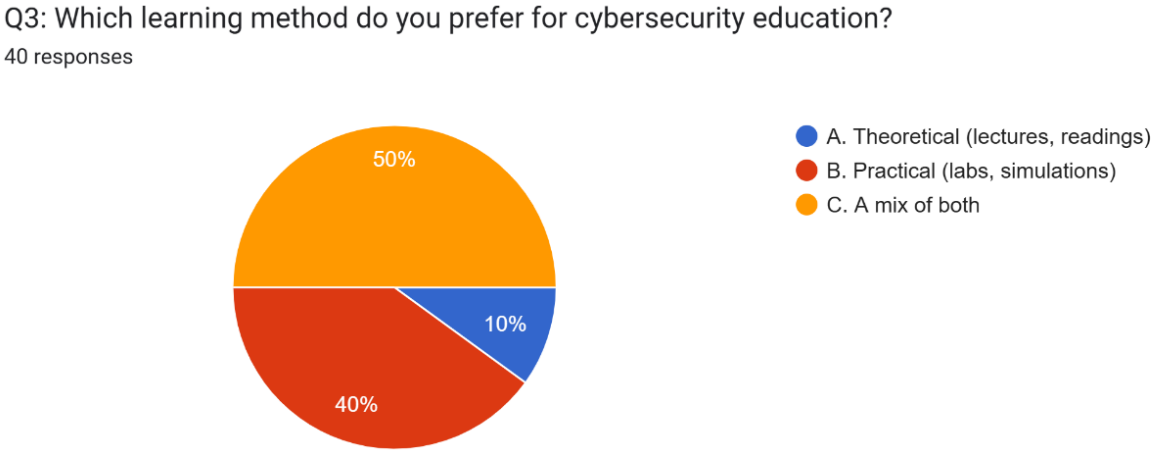
Preferred Cybersecurity Learning Methods



Most students prefer hands-on experience when it comes to learning. According to the data presented in the chart practical educational methods involving labs and simulations are preferred by 90% (36 students) of responders. Twenty students representing 50% of the total participants chose to blend learning with theoretical and practical content while sixteen students from 40% of the survey showed a preference for hands-on learning. Out of the contributors only four students selected theory-based learning methods which include lectures together with reading materials.

Figure 3.4

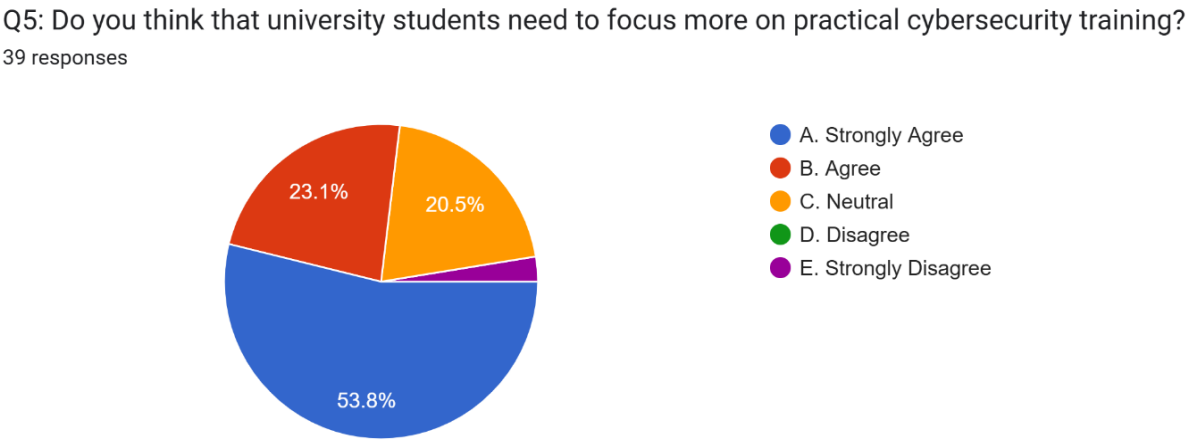
Self-Rated Cybersecurity Knowledge



Students typically evaluate their cybersecurity knowledge to fall at a middle level. Students who selected Average as their cybersecurity knowledge level made up the largest group at 37.5% or 15 out of 40 participants. Thirty-two and a half percent of students (13 among 40) considered their understanding as Good while another 22.5% (9 among 40) claimed to have Excellent skills. The ratings of two students and one student placed their knowledge in the Poor category while two other students placed theirs in the Very Poor category. Students generally understand cybersecurity basics, yet they recognize the need to enhance their knowledge further.

Figure 3.5

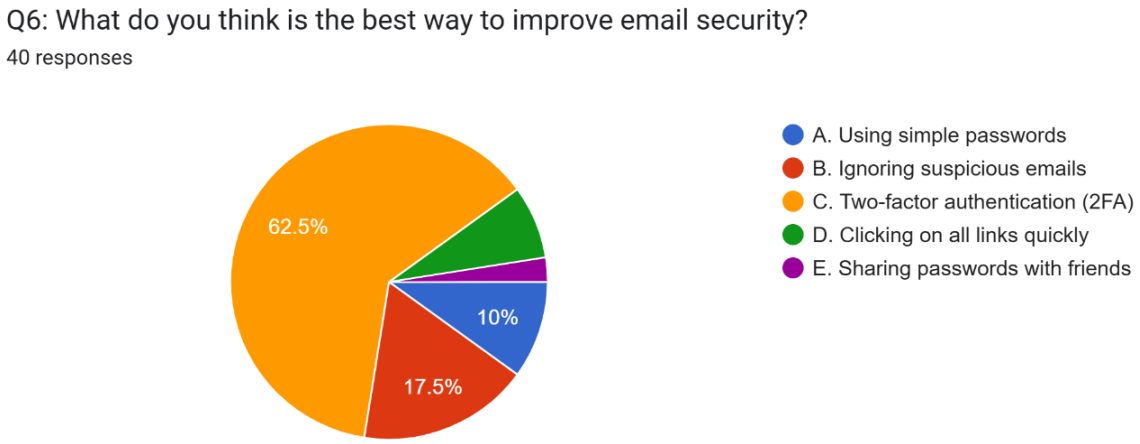
Importance of Hands-On Labs



Most students believe hands-on labs represent a crucial element for cybersecurity education as shown in this Chart. The data shows that hands-on labs receive full student understanding for cybersecurity education. The survey results indicated that hands-on labs carry great importance to students because 76.9%, or 30 students, declared their agreement to their value. The students displayed a 20.5% (8 students) neutral stance followed by 2.6% (1 student) who strongly disagreed. Most respondents expressed their preference for real-world laboratory experiences by giving the results depicted in this chart.

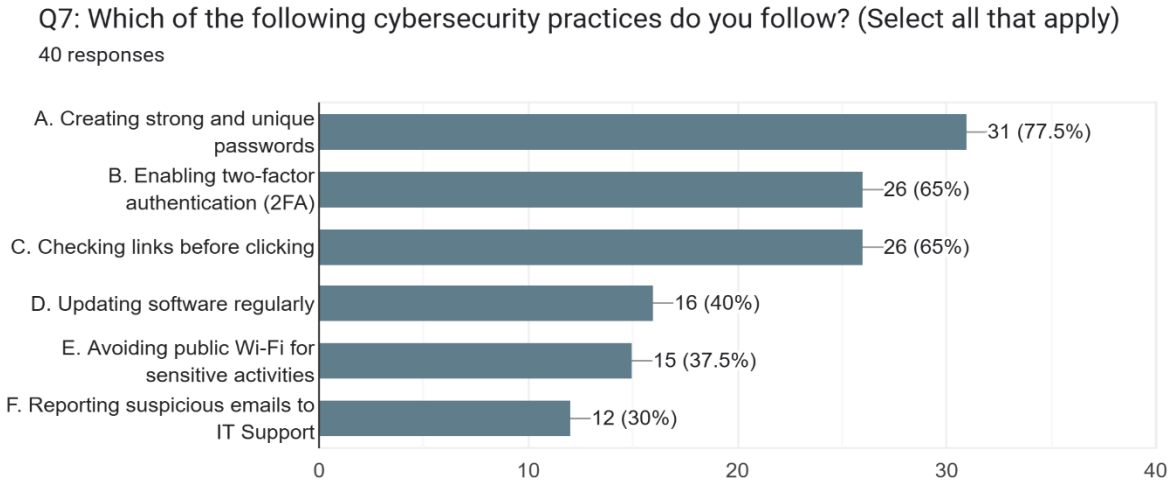
Figure 3.6

Best Ways to Secure Email Accounts



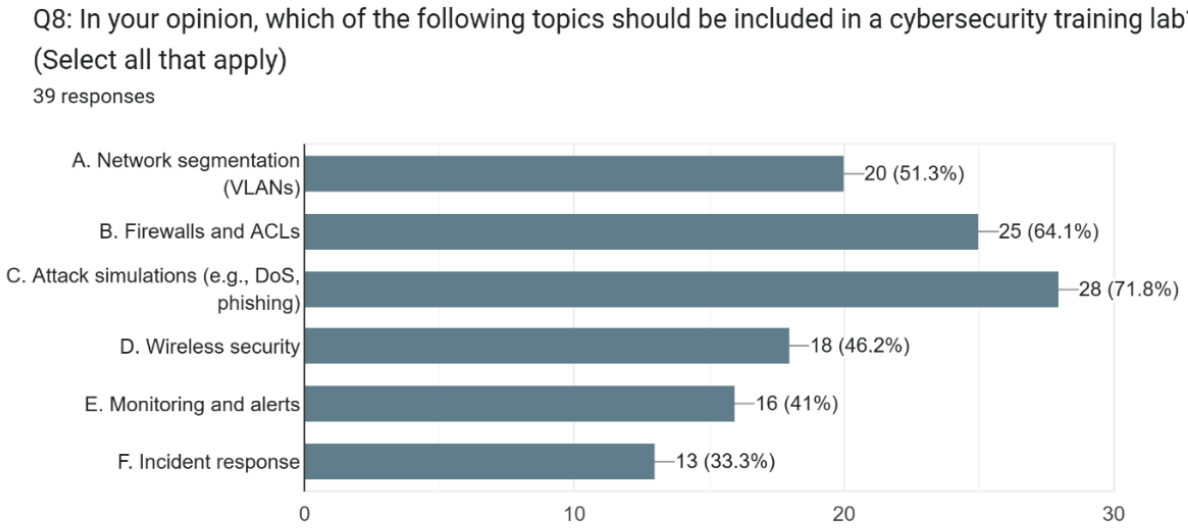
The students believe Two-Factor Authentication (2FA) provides the most secure approach to protect email accounts. Students favor two-factor authentication (2FA) as the most secure method to protect email accounts since 62.5% (25 students) selected it. The students who made these suggestions about addressing threats through ignorance of suspicious messages or use of basic passwords or rapid link clicks were in the minority (17.5% and 7 students and 10% and 4 students and 7.5% and 3 students respectively). One student among 40 respondents shared the practice of giving passwords to friends making it 2.5% of the total. This shows that most students understand the importance of 2FA, but some still follow risky habits.

Figure 3.3



The security practices of students are demonstrated through the chart above which reveals their behavior in Mail securing. Most students practice responsible actions to protect their digital security. According to the chart 77.5% of students (31 students) practice using strong passwords while 65% of students (26 students) have enabled 2FA security. Students routinely verify links prior to clicking (65 percent which amounts to 26 students). Data shows that a minority of students (16 students, 40%) fail to maintain software updates while 37.5% (15 students) choose not to perform sensitive tasks on public Wi-Fi networks. Only 30% of the students surveyed reported receiving suspicious emails suggesting organizations could enhance their performance in this area.

Figure 3.4



According to the chart above many of our participants believe attack simulations through DoS and phishing should form the core component of cybersecurity labs because 71.8% (28 students) indicated attack simulation as their preferred approach. Students demonstrate interest in two subjects the most: Firewalls and ACLs (64.1%, or 25 students) along with Network segmentation (VLANs) (51.3%, or 20 students). The voting results show Wireless security as a priority with 46.2% student interest followed by an Incident response with 33.3% student selection and Monitoring and alerts at 41%. Many students demonstrated their desire to engage in practical cybersecurity tasks dealing with real-life situations through their responses.

Figure 3.5

Q9: Do you believe hands-on labs are important for learning cybersecurity? Why or why not?

36 responses

Yes, hands-on labs are a vital part of cybersecurity education because they transform theoretical knowledge into practical skills. They allow learners to experience real-world scenarios, use professional tools, and develop critical thinking necessary to handle cyber threats effectively. Without hands-on practice, students may struggle to apply their knowledge in real situations, which limits their readiness for the cybersecurity field.

yes

yes, because it teaches the students real life examples and make them more aware

Yes, I think hands-on labs are very important for learning cybersecurity. Reading and studying are good, but practicing is better. When I do labs, I understand better and learn how to deal with real problems. It also makes me more confident.

All students responding through the open-ended question stated that practical lab work remains vital for learning cybersecurity. According to their view these practical labs benefit students by using theoretical concepts on actual operational environments. The students reported that laboratory practical strengthen their abilities to handle real security threats while developing a safe space for making mistakes. Student participants strongly back the conclusion that practical experience remains essential to master cybersecurity concepts.

3.4.1. Summary of Questionnaire findings

Results from the questionnaire show that students and faculty members working at Higher Education Institutions (HEIs) in Oman display rising knowledge about cybersecurity concerns. A key number of respondents belonged to technical areas including Cybersecurity alongside Information Technology and Engineering programs. Students and faculty members most experienced weak passwords as well as phishing emails and unsecured public Wi-Fi connections. Hands-on practical learning methods were preferred above abstract teaching methods according to 90% of research participants. The respondents indicated most of their cybersecurity knowledge fell into the “Average” or “Good” categories, yet they recognized the necessity for additional skill building. The security practiced most often involved maintaining secure passwords and activating Two-Factor Authentication (2FA) and performing careful link verification showing students had foundational security practices skills.

Participants stressed the importance of cybersecurity labs that demonstrate practical applications such as phishing simulations and Denial-of-Service (DoS) attacks coupled with firewall configuration and VLAN segmentation. The feedback collected demonstrates that students require scenario-based training that reflects current cyber security threats. Students through open-ended feedback recognized that practical labs create a perfect learning environment to bridge theory with practice because they allow controlled error-based learning. Research findings support earlier investigations which show that adding visual elements and interactive training elements using visual programming languages improves security training outcomes (Glas et al., 2023). Primary evidence shows that immersive learning focused on skills development stands crucial for enhancing cybersecurity competence development within Oman's higher education institution learner population.

3.4.2. Summary of interview

The interview gave expert information in support of our cybersecurity project in the National University HEI in Oman. The discussion highlighted the following in relation to network design: the need to implement port security, VLAN network segmentation, redundancy, Access Control Lists (ACLs) and future scalability. It was emphasized that isolating the cybersecurity lab by separate VLAN, firewalls, and, in some cases, VPNs is very important for protecting the campus network, as well as to ensure that students who work in the lab should be meticulously guided. It was also stressed that real world attacks are rampant today and are a real threat to digital world and therefore hands-on practice is called for. The project, which involves developing a website and a dashboard consisting of quizzes and video demonstrations to simulate attacks, was identified as an effective realistic solution.

It was suggested that cybersecurity labs should concentrate on social engineering attacks, malware analysis, ransomware defense and AI-based attacks. It was explained that cybersecurity awareness needs to get out of lectures, suggesting practical approaches like simulated phishing, interactive workshops and digital campaigns. The discussion affirmed that the project is strongly in line with Oman Vision 2040 goals, with it creating digital resilience, cultivating a knowledge-based economy, and training local cyber professionals. The interview was documented by use of online tool, Microsoft Teams (Microsoft Teams, n.d.). The direction provided confirms that the project is both technology-savvy and purposeful at the national level.

3.4.3. Summary of Findings

This study collected data via two methods. a questionnaire administered to students from different majors at Higher Education Institutions (HEIs) in Oman, and an interview of an expert with a faculty member National University (NU). Through the questionnaire students' cybersecurity awareness was evaluated against the backdrop of the disciplines such as Cybersecurity, Information Technology, Engineering, and Business. Although most participants were of technical background, gaps in the basic cybersecurity practice were evident. However, students considered weak passwords, phishing, malware, and the use of unsafe public Wi-Fi to be great threats. The majority of the participants liked the hands-on approach in terms of labs and simulations expressing clear understanding of the fact that practical practice is of significance for acquiring genuine cybersecurity skills.

Regardless of some awareness, the findings demonstrate that harmful online behaviors are still prevalent. Many students do not frequently update their software and do not use public Wi-Fi in processing sensitive tasks. Although most people are aware of the need for Two-Factor Authentication (2FA) and strong passwords, these results demonstrate that the vast proportion of the Oman's student community is ignorant of how dire digital attacks have become. Self –assessments put most students within an "Average" or "Good" knowledge level, but many acknowledged the need for additional training. This shows that though growth can be seen, the issue of cybersecurity education is still lacking attention to address current complex digital issues.

The expert interview further reinforced the depth aspects of the key network security measures to include, port security, VLAN segmentation, redundancy and Access Control Lists (ACLs). It was highlighted that cybersecurity labs must be made independent through VLANs, firewalls and in some cases VPNs to how to protect the main campus systems from being jeopardized. Although cyberattacks are becoming more common, scenario-based training is no longer optional but must be essential. The project approach – development of a website and dashboard with quizzes with attack simulation videos was validated as an effective technique to increase awareness as well as technical abilities.

From the findings of the questionnaire and the interviews, it is evident that Oman's universities must continue to invest in practical cybersecurity education. Real-life training, such as phishing simulations, how to configure firewalls as well as the use of network segmentation can work much better to prepare the students for dealing with present and future threats to cybersecurity. The outcomes also correlate highly with the goals of Oman Vision 2040 especially in promoting digital resilience and creating knowledge-based economy. The interview was recorded and transcribed with Microsoft Teams (Microsoft Teams, n.d.), accurate source material for this research.

3.5 Technical Requirements

Ensuring that a network is both reliable and secure requires integrating all necessary tools such as hardware, software and training users carefully. Working together, these elements allow systems to run smoothly, exchange data properly and be available all the time in organizational environments (Hayudini, 2021).

3.5.1. Hardware Requirements

Table 3.1

List of the Required Hardware

Hardware Component	**Deployment Tasks**
Router (Cisco 2911)	The deployment of network hardware involves the installation of the Cisco 2911 router followed by the activation of network routing functions throughout the system.
Core Switch (Cisco 2960)	The core switch (Cisco 2960) serves to connect and manage VLANs throughout the core infrastructure.
Access Switches	Access switches establish the VLAN configuration that delivers network access to end users.

Access Points	Wireless access points must be set up to provide specific VLAN server connections for DHCP, DNS, MAIL, and WEB functions.
Servers (DHCP, DNS, Mail, Web)	Installation and configuration of vital network services must be accomplished.
Workstations (PCs)	Devices connected through workstations obtain network authentication to access the system.

3.5.2. Software Requirements

Table 3.2

List of the Required software

Software Component	**Deployment Tasks**
Packet Tracer	Enables network designers to design and test different network plans in simulation which helps reduce the risk of deployment and confirms configurations are working properly before they are connected to hardware.
Windows/Linux OS	Ensures that DHCP, DNS, email and web servers can function properly by providing the necessary environment for them.
Kali Linux	Allows security analysts, students and anyone else to develop tools for hacking, testing systems and running attack simulations, while boosting their protection skills.
DHCP Service	Automatically gives IP addresses to devices in a VLAN, making it easier to manage networks, avoid configuration faults and ensure all devices stay connected.
DNS Service	Converts a domain name to an IP address for access on the network by users, so they do not have to remember numbers to get to the resources they need.

Email Service	Allows staff, students and administrators to exchange emails securely and in an organized way.
Web Server (HTTP)	Hosts educational materials, online tutorials and updates on cybersecurity issues to teach users how to avoid security risks.
Wireshark	Allows network administrators and students to investigate network traffic, spotting unauthorized actions, trying out security rules and studying live packet movements.
SNMP Configuration	Assures network administrators can always monitor devices to know their status, get performance updates, receive alerts and identify issues proactively.
Port Security Configuration	Allows access to switch ports just for approved devices, so chances of internal attacks and unauthorized connections are greatly reduced.
MS Visio	Assists in developing easy-to-read network diagrams and documentation, so planners can plan, report on and better understand their networks.
YouTube	Includes extra video-based cybersecurity lessons and examples to support learning and improve the effectiveness of the training.

3.5.3. Other Requirements

Student Knowledge Development

To ensure the technical implementation of the project, students must complete different learning modules and video tutorials to enhance their basic knowledge and skills in networking and cybersecurity. These include:

Table 3.3

List of the Required knowledge and skills

Learning Module / Tutorial	Description
Fundamentals of Computer Networking (Microsoft Learn)	Includes foundation networking knowledge, including network protocols, topology, device types, communication foundations (for instance, TCP/IP, DNS, ports), and how this applies to the Azure networking settings (Microsoft, 2018).
YouTube Tutorial: Networking Project Simulating Network Design Using Cisco Packet Tracer and Cybersecurity Attacks	A tutorial to instruct users on constructing and testing a corporate network using Cisco Packet Tracer. It also shows how to use Wireshark to conduct internet crimes such as making web clones, delivering payloads and sniffing for packets. Since the tutorial teaches about network architecture planning, router and switch setup, giving IP addresses and testing, it means it is suitable for learners who study by sight and for first-time users of cybersecurity attack simulations (Networking, 2021).
Packet Tracer Tutored Activity Course (NetCad)	With the use of Cisco Packet Tracer tools for simulation purposes, you will have practical activities on structured cabling, configuration network devices, manage wireless connections, monitor networks (CNA, 2023)
Introduction to Cybersecurity (Cisco Networking Academy)	A study of major cyber security concepts will enable students to know about digital threats and corporate security strategies. (CNA,n.d)

3.6 Literature review

3.6.1. Systematic review of current cybersecurity training methods:

The field of cyber security expands continuously because cyber-attacks lead to economic losses and operational setbacks and reputation decline of businesses. Based on user activities and their awareness of security protocols an organization will secure itself against cyber-attacks. Organizations need to create official training methods which operate as essential instruments for developing proper user conduct in this domain.

Different stakeholders disagree on specific methods that work best for teaching behavioral cyber security principles. The study performed a systematic review to analyze different training methods and their effects on cyber security behavior inside organizations. The research identified 16,771 relevant articles within Web of Science, ACM Digital Library, ProQuest, PubMed and PsycINFO databases. The researchers evaluated 142 studies after examining their titles abstracts and full texts.

The results showed that participants who received training showed better performance when it came to positive cybersecurity actions whether they learned through traditional methods or online. The application of games for training purposes emerged as one of the most frequently employed techniques. Most studies employed non-experimental methods while mostly using pretest-posttest designs. A significant percentage of studies in this analysis performed research beyond organizational settings because they contained small sample populations. The review also highlights additional insights regarding the structure, features, and evaluation of training interventions (Prümmer, van Steen, & van den Berg, 2023)

3.6.2. Navigating cybersecurity training: A comprehensive review:

Awareness training plays an important role in the vibrant interplay of cybersecurity, in reinforcing protection in cyber space. This survey covers a range of cybersecurity awareness training processes, evaluating the traditional approach, technology-based approach, and innovative approach. It assesses the principles, effectiveness, and limitations of every method, with a comparative analysis that points to the pros and cons of each. There are also emerging trends such as artificial intelligence and extended reality which are explored in the study alongside their prospective impact on cybersecurity training in the future. Also, it deals with implementation problems and offers solutions based on the insights gained from real-world case studies. The intention is to enhance the knowledge of the existing paradigm of cybersecurity awareness training, providing relevant dimensions for both practitioners and scholars (Qawasmeh, AlQahtani, & Khan, 2025).

3.6.3. Evaluation Strategies for Cybersecurity Training Methods: A Literature Review:

Cybersecurity researchers and professionals worldwide face continuous challenges due to human factors in their work. The ongoing efforts to resolve security breaches have not prevented major breaches that originate from user activities. Security and Awareness Training (SAT) presents a long-promoted solution to improve user cybersecurity behavior. Current SAT practices seem inadequate because attackers continue to capitalize on human vulnerabilities successfully. Several researchers reject user knowledge increase as an effective method and many existing SAT approaches remain insufficiently tested empirically. A structured review explores the assessment approaches of SAT in current academic writing in this paper. This research unites multiple evaluation methods that reveal their specific findings. Several different assessment methods serve SAT programs because each method provides specific information. The obtained findings provide useful guidance for researchers who study SAT design or evaluation techniques (Kävrestad & Nohlberg, 2021).

3.6.4. Game-based Cybersecurity Training for High School Students:

Purdue University Northwest used National Security Agency and National Science Foundation funding to run four GenCyber summer camps in 2016 and 2017 which taught high school students cybersecurity skills. Educational programs expanded middle-school and high-school student knowledge of cybersecurity through the implementation of hands-on laboratories featuring interactive cyber-defense games. In the Cyber Defense Tower Game students needed to safeguard servers through defensive choices while the game introduced progressively complex challenges. Students learned cybersecurity principles together with practical skills through interactive teaching methods that utilized immersive design elements. Survey results showed that game-based learning successfully attracted male students and had beneficial effects on multiple student types (Jin et al., 2018).

3.6.5. An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness Training Model (CATRAM). A Case Study in Canada:

The previously used security awareness programs by organizations proved ineffective in helping employees detect or defend against cyber incidents. The inability of current security programs to improve user behavior has resulted in sustained human errors known as the primary vulnerability in cybersecurity systems. CATRAM supplies specialized training content that supports specific needs of organizational groups with identified training objectives. Research concentrates on creating everlasting methods for establishing organizational security awareness. This research shows organizations should create innovative approaches for sustainable cybersecurity understanding development in upcoming studies (Sabillon et al., 2021).

3.6.6. Integrated framework for hands-on cybersecurity training: CyTrONE:

Merging practical education with cybersecurity training has become crucial because cyberattacks continue to become more frequent and complex. The current manual training environment setup proves too time-consuming and produces subpar systems that include multiple possible errors during both creation and application. The automated system of CyTrONE creates training material and deploys simulation platforms to handle these training problems. This study demonstrated that their framework created performance-based training systems specifically designed for operational security environments (Beuran et al., 2018).

3.6.7. Modeling effective cybersecurity training frameworks: A Delphi method-based study:

Organizations have universally implemented cybersecurity training programs yet increasing cyberattacks indicate current programs deliver insufficient results. Current training models found in the market exclude vital learning components involving both cognitive ability development and metacognitive skills together with learning preference mapping. A cybersecurity training framework has integrated automation training principles into the ADDIE model and personalized learning practices to create its framework. Critically evaluated by the Delphi method based on input from both academic and industrial experts, this framework was developed for validation. The validation of educational programs depends on two criteria: consensus evaluations combined with specialized solutions validation that should reflect individual learner requirements (Chowdhury et al., 2021).

a. Critical Review – Strengths and Weaknesses of the Previous Articles:

Strengths:

1. Diverse Methodologies: The examined articles depended on methods such as case studies, overview papers and tests, giving a broad overview of how cybersecurity training can be effective.

2. Focus on Practical Learning**:** Various works including (Domínguez et al., 2017; Beuran et al., 2018) highlight how important it is to educate students through practical experience which is relevant for today's cybersecurity schools.
3. Use of Modern Tools and Techniques: Studies such as Prümmer et al. (2023) and Chowdhury et al. (2021) introduced game-based learning, AI and automation into their teaching schemes, allowing them to be suitable for today's technology landscape.
4. Relevance to Target Groups: Different authors such as Jin et al. (2018), focused on high school students, whereas some others concentrated on employees or university students, sharing strategies suited for various learners.

Weaknesses:

1. Insufficient Long-Term Evaluation: Many research trials used little to no long-term checks to measure if learners still knew and practiced cybersecurity guidelines.
2. Limited Sample Sizes: Several studies that depended on game-based or case examples had groups of only few participants, so the results could not be applied widely.
3. Underdeveloped Frameworks: There were not enough specific instructions provided in some models which made it approaching them at a wider scale in schools and universities tough.

b. Link to Own Project – How These Studies Support and Relate to Your Project:

1. Emphasis on Hands-on Learning: Many studies highlight that strong cybersecurity training involves practical, hands-on learning over just reviewing theories. Like what Domínguez et al. (2017) and Beuran et al. (2018) proposed, we include labs, simulation attacks and real-life situations in our project.
2. Use of Interactive Tools: Interactive Tools: Like Jin et al. (2018), our dashboard has interactive quizzes and video explanations to make learning engagement for users.

3. Addressing Educational Gaps: Many research papers, including that by Prümmer et al. (2023), find that knowing about cybersecurity risks does not always help users learn necessary behaviors. Accordingly, our project teaches students safe online habits and allows them to experience safe internet actions.
4. Supporting Regional Goals: Our project indirectly supports national goals, as found in Oman Vision 2040, by organizing development programs for skilled local cybersecurity professionals.
5. Aligning Global Knowledge with Regional Educational Goals: Focusing on Oman's Higher Education: Since most research findings are from Western backgrounds, our project adapts their successes and applies them to Omani institutions.

3.7 Chapter Summary

This chapter presented the research methodology, data collection, analysis procedures, technical requirements, and literature support for the Cybersecurity Awareness Training Lab project. A qualitative comparison approach was adopted to explore popular Software Development Life Cycle (SDLC) models; like Waterfall, Prototyping, Iterative, Time-Boxing, and Agile. Having analyzed their structures, process flows, merits, and demerits, Agile model was selected because of its flexibility, focus on teamwork and appropriateness for dynamic and time-sensitive software development environments.

The chapter also explained the data collection methods adopted which included surveys and interviews. The questionnaire was developed to assess the cybersecurity knowledge, perceived dangers, students and faculty members' favored learning methods, and what they perceive as their knowledge level concerning cybersecurity in different Higher Education Institutions (HEIs) of Oman. The findings showed that weak passwords, phishing, and use of public Wi-Fi were considered the biggest concerns. Most of the participants were in favor of hands-on, practice-based learning instead of pure learning by theory approach. Majority rated their knowledge on cybersecurity to be "Average" or "Good" and indicated the need for enhanced practical aspects.

An expert interview highlighted the need for technological safeguards in network design, proposing such methods as VLAN segmentation, Access Control Lists (ACLs), port security and firewalls to isolate cybersecurity training locations and make the institutional networks safe. The expert approved the use of simulated real-world cyberattacks and interactive training modules, affirming that the policy of Oman Vision 2040 is into digital resilience and workforce readiness.

The chapter ended with a description of technical requirements for the implementation of the project, which included requirements for the project's requisite hardware, software, and student skill development modules. They gave weight to the pedagogical foundation of the project as the literature review left in evidence the function of hands-on, interactive, and scenario-based cybersecurity training in developing practical competencies and increasing awareness for students in educational settings.

CHAPTER 4: DESIGN

4.1. Introduction

Setting up a cybersecurity awareness training lab begins with designing the network architecture, which includes both logical and physical elements. These designs form the foundation of how the lab will work both in theory and in practice. A well-thought-out plan doesn't just explain how everything should function; it also creates an environment where students can try different security tasks, explore problems, and learn by doing.

The logical design focuses on the structure and the purpose of the network. It explains how data is supposed to move through the system, what users can access, and how servers are connected. It also outlines the security mechanisms in place, tools for content delivery, and how user accounts are organized. Basically, it’s about defining how each part of the network interacts and how information gets to the right people through safe, managed paths. The idea here is to keep everything secure and aligned with the learning goals, even if the lab is running in a cloud-based setup or using virtual machines (Lewis & Lewis, 2020). Logical design is like the blueprint before you even touch the hardware.

Then comes the physical design, which deals with the real devices you can see and touch or simulate, depending on the setup. This includes routers, switches, NICs, cables, computers, and physical servers. This part is usually done in a real lab or using simulation tools like Cisco Packet Tracer and Microsoft Visio (Microsoft, 2023; Cisco Systems, 2023). It also covers practical stuff like placing access points, figuring out where the power sources go, organizing cables so it’s not a mess, and splitting up the network into segments so it's safer and faster (Patnaik, 2024). A good physical design helps plan what hardware is needed and how it’s all going to be arranged and managed later (Tunc et al., 2015).

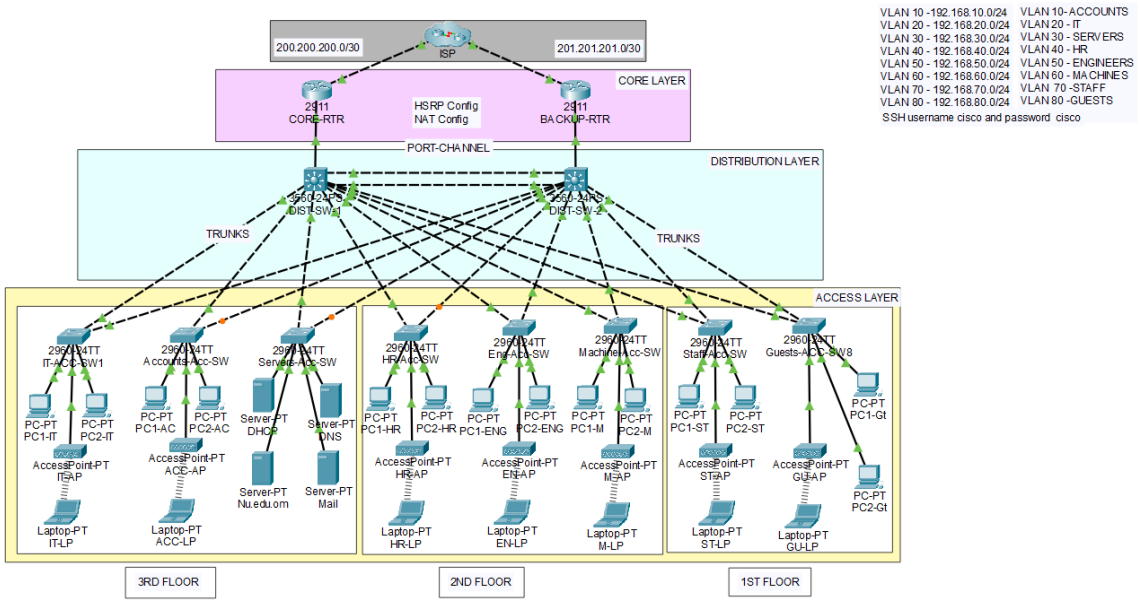
Overall, the success of a cybersecurity training lab really depends on how solid the planning is. Logical and physical design go together—they each play a different but important role. Logical design helps control data access and user behavior, while the physical design makes it all real and working. Together, they make sure students have a safe, hands-on space to practice and improve their cybersecurity skills.

4.2. Logical Network Design

Network designs can be divided into smaller pieces known as Virtual Local Area Networks (VLAN) to make it more structured and secure (Rouse, 2022). Each VLAN functions similarly to a single group or department, making management easier. It's also possible to create a backup plan so that another router will take over in the event of a router failure. That's the Hot Standby Router Protocol (HSRP), which also helps in determining who is allowed access to certain areas of the network, which is like granting keys to only the appropriate individuals network has been built so that changes can be made later without the need to complete restart. The logical network design of cybersecurity training lab features is:

Figure 4.2.1

Logical Design



4.2.1. VLANs and Departments

9 VLANs, each one is for one department in the college or company. Also, each VLAN has its own IP range, like its own zone.

VLAN ID	Department	IP Range
10	Accounts	192.168.10.0/24
20	IT	192.168.20.0/24
30	Servers	192.168.30.0/24
40	HR	192.168.40.0/24
50	Engineers	192.168.50.0/24
60	Machines	192.168.60.0/24
70	Staff	192.168.70.0/24
80	Guests	192.168.80.0/24
99	Management	192.168.99.0/24

Each VLAN is separated. So, the devices in one VLAN cannot reach others unless there is access.

4.2.2. Tree Topology in This Network Design

Tree topology is a hierarchical network structure that combines features of both star and bus topologies. It consists of 3 layers used to organize the network: core, distribution, and access. Each layer has a specific role, which improves performance, scalability, and ease of management (Shiksha, 2024).

This topology is suitable for large networks because:

- It allows scalable expansion without major redesign.
- It isolates faults, so issues in one section do not affect the entire network.
- It supports clear data paths, reducing network traffic.

4.2.3. IP Rules – How IPs assigned to Devices.

- Every device in each VLAN gets an IP from that VLAN's range.
- Each VLAN has a **gateway**, which helps it talk to other networks.

- We made sure IPs do not clash and every department has enough space for all its devices.

4.2.4. Routers and Backup (HSRP)

Two routers have been utilized. One is the primary, while the other is an aid, known as secondary.

If the primary router fails, the secondary (backup) router will automatically take over. This is an implementation of Hot Standby Router Protocol (HSRP), which is a CISCO proprietary technology protocol used to provide redundancy in a network (Cisco, n.d. -a). Only one router is the active router while others will be in standby state i.e., the standby router will be responsible for forwarding the traffic when the active router fails.

Using this protocol has the advantage of increasing the network's dependability (Cisco, 2023).

4.2.5. Layer 2 Switches and Trunk Ports

- Layer 2 switching (or Data Link layer switching) is the process of using devices' MAC addresses to decide where to forward frames. Switches and bridges are used for Layer 2 switching. They break up one large collision domain into multiple smaller ones (Cisco, n.d. -a).
- The switches used to connect computers and printers are called access switches. An access switch can be defined as a network device that connects end-user devices, such as computers and printers, to the broader network infrastructure, serving as the entry point for data communication.
- Each port in the switch is connected to just one VLAN.
- But when switches talk to each other or to the router, they use something called trunk ports, which can carry traffic for all VLANs. A trunk port is a type of network switch port that carries traffic from multiple VLANs at the same time. Unlike an access port, which only handles traffic for one VLAN, a trunk port can send data from several VLANs over a single connection. This helps streamline network communication (GeeksforGeeks, 2024).

- That way, all parts of the network can still connect without mixing up data.

4.2.6. VTP – Makes VLAN Setup Easy

Cisco has a proprietary protocol called VLAN Trunking Protocol (VTP), which is used to manage VLANs in a network. It enables the dissemination of VLAN information across all switches in a VTP domain, hence ensuring consistency and reducing the need for manual configuration on each switch. The VLAN Trunking Protocol (VTP) allows adding, deleting, and renaming VLANs, and these changes are automatically broadcast to all switches in the domain.

Therefore, one switch has been selected as the server, and others are clients so that when changes are made on the server, all other switches get updated automatically and that saves time (Cisco, 2025).

4.2.7. STP – No Network Loops

When we connect switches in multiple ways, we can create loops, which is not beneficial. Therefore, we use the Spanning Tree Protocol (STP) to protect Layer 2 broadcast domains from broadcast storms by placing certain links into standby mode to avoid loops. In standby mode, these links temporarily stop transferring user data. The Spanning Tree Protocol (STP) helps identify one primary (root) and one secondary switch (backup root) for each VLAN (Cisco, 2025).

A faster version called Rapid PVST has been implemented, allowing the network to recover quickly if something changes.

4.2.8. DHCP Snooping and Port Security

DHCP snooping was enabled on switches across all VLANs, to protect them from unauthorized network access and DHCP spoofing. On the switches, some specific ports were manually configured as trusted so they could allow DHCP traffic only from the real DHCP servers and blocking the fake ones (Cisco, n.d. -b). This doesn't allow unauthorized DHCP servers from giving incorrect IP addresses. Also, port security was applied to access ports. Using sticky MAC address binding allows the switch to remember the MAC addresses of real devices, and any attempt to connect unauthorized devices sets off security violations. By adding this configuration, it helps to limit physical access and reduces the risk of MAC flooding and spoofing attacks (Cisco, n.d. -k).

4.2.9. Access Control Lists (ACLs)

Access control was applied using extended ACLs to block traffic between different network segments. For example, an ACL named BLOCK-GUEST was applied to prevent users in VLAN 80 which is Guest VLAN from accessing internal networks such as HR, Admin, and IT. This makes sure that guest devices can browse the internet but are restricted and blocked from reaching sensitive data or internal services. This control strengthens internal security and simulates common enterprise access policies (Cisco, n.d. -c).

4.2.10. Secure Remote Access (SSH Configuration)

SSH (Secure Shell) allows routers and switches to be remotely managed in a secure way and was configured so that any connection would be encrypted and secure from unauthorized access. RSA keys were created to activate encrypted communication, and a local username and password were created on the router to allow only authorized administrators to securely log in. SSH replaced Telnet to make sure that remote management is encrypted and safe from eavesdropping or interception. It is important in environments like in educational institutions, where secure remote access is required (Cisco, n.d. -L).

4.2.11. Configuration Backups using TFTP

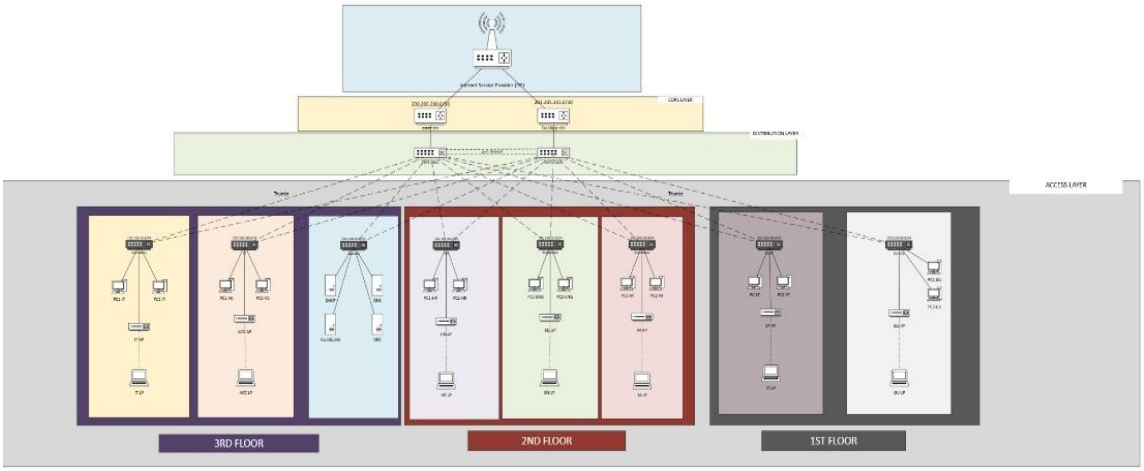
TFTP (Trivial File Transfer Protocol) server backs up router and switch configurations. This allows for easy recovery in case there are configuration errors or device failure. This process helps make sure that the latest device settings are always saved safely, which is important in a lab environment where students usually change configurations during their practice and performing experiments (Cisco, n.d. -e).

4.2.12. NAT Configuration

NAT (Network Address Translation) provides internet connectivity to internal users and was configured on the gateway router which is a router that connects the internal network to external networks like the internet. This makes it possible for many internal devices that use private IP addresses to share a single or limited number of public IPs when accessing the internet. This not only conserves public address space but also hides internal IP structures, which also helps protect the internal network from being directly exposed to the internet (Cisco, n.d. -O).

4.2.13. Management VLAN (VLAN 99)

A Management VLAN (VLAN 99) was created to separate network administration traffic from regular user traffic. This VLAN is only used to manage all the network devices like switches and routers. Management VLAN was given its own IP address range and configured with a DHCP helper address, so that it could still get IP addresses from the main DHCP server, even though they are on a different network. HSRP (Hot Standby Router Protocol) was also added within the management VLAN to make sure that if one gateway fails, another one is available to handle the traffic. Separating the management VLAN improves security and ensures better performance and organization of administrative functions (Cisco, n.d. -g).



4.2.14. SNMP Configuration

Simple Network Management Protocol (SNMP) was configured on the main network devices using a basic read-only community string. And this lets administrators keep track of key network statistics like device status, interface usage, uptime, and error rates. Because the string is read-only, admins can see data but cannot make any changes, this helps provide network security. SNMP support makes it easier to detect failures or unusual activity early, which is important in any network with goals of simulating real-world cybersecurity scenarios (Cisco, n.d. -h).

4.3. Physical Network Design

The physical design of devices and cables in a network determines how devices can communicate and achieve good performance. It affects how easily a network can handle the rise in traffic, remain secure, operate reliably and be fixed by skilled people. Planning the physical design helps data move smoothly, set up failover and suit business requirements (Stallings, 2020).

In today's enterprises, physical design involves more than cable connections; it ensures that digital activities are stable, safe and fast.

Figure 4.3.1

Physical network design

4.3.1. Tree Topology and Hierarchical Structure

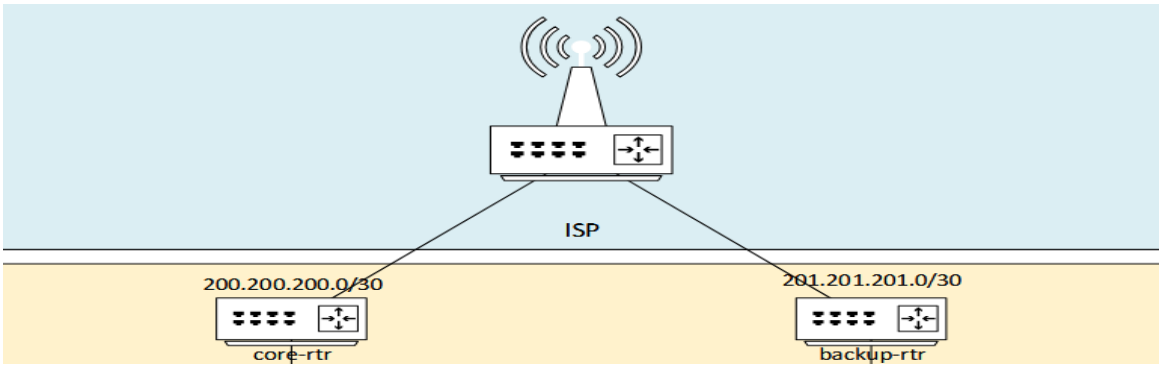
The figure above depicts a hierarchical network model divided into three layers: core, distribution, and access. This hierarchical approach is essential for network architecture since each layer serves a specific purpose. The core layer is responsible for rapid routing and external communication, while the distribution layer oversees inter-VLAN routing and departmental traffic. The access layer connects end-user devices to local equipment.

This layered architecture naturally resembles a tree structure, with connections branching downward from the core through distribution to access. This structure simplifies network management, improves traffic flow control, and enables economical scalability. Each department and device can be readily incorporated into the network without overwhelming a single point, ensuring both performance and reliability (GeeksforGeeks, 2024).

4.3.2. ISP Integration

Figure 4.3.2

ISP Integration

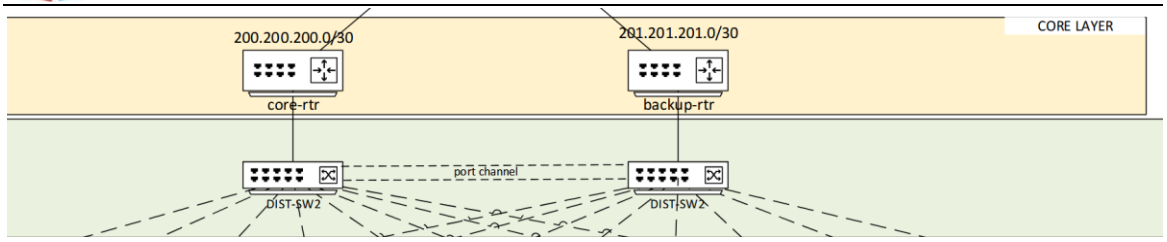


The figure above reflects the flow of communication between the network and an ISP through the main router and a backup router. By making the connection redundant, you can ensure that your internet keeps going when one connection fails. If one main router fails, a second router will keep the network up and running (Cisco Systems, n.d.).

4.3.3. Core Layer Design

Figure 4.3.3

Core Layer Design

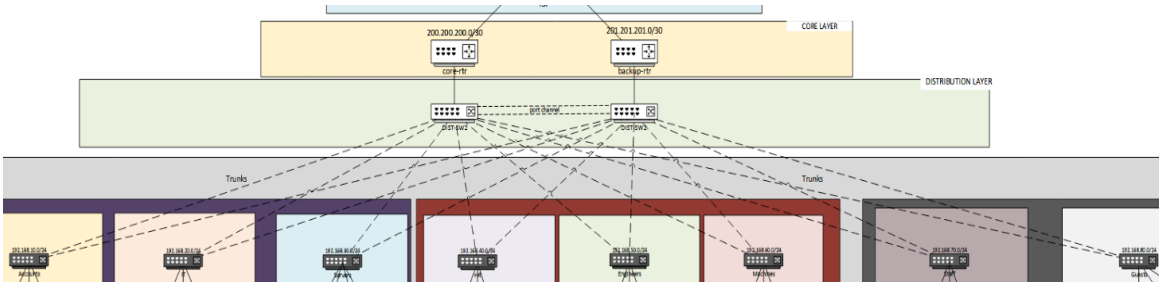


The main part of the network which includes the core router, central switches and backup router, is illustrated above in the figure. Trunks and port channels are used to link these items which gives them faulty tolerance and helps spread the workload. The core layer manages how data is transferred by route switching and via external connections using distribution switches (ManageEngine, n.d.).

4.3.4. Distribution Layer Configuration

Figure 4.3.4

Distribution Layer Configuration

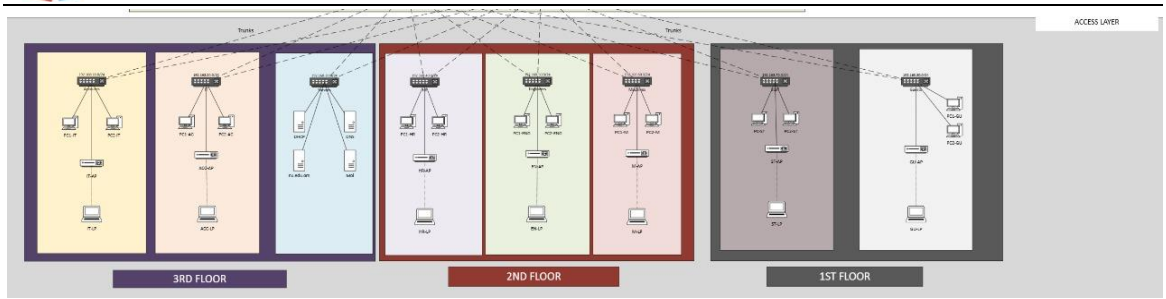


The figure above shows that the distribution layer uses two primary switches next to the core networks. They handle how traffic from different VLANs communicates and how it is managed between core and access network parts. There is a special VLAN set for each network department which ensures improved speed and security. All the building's access switches are wired to the distribution switches too. If one distribution device becomes unavailable, the other can still function, so systems keep working reliably.

4.3.5. Access Layer Overview

Figure 4.3.5

Access Layer Overview

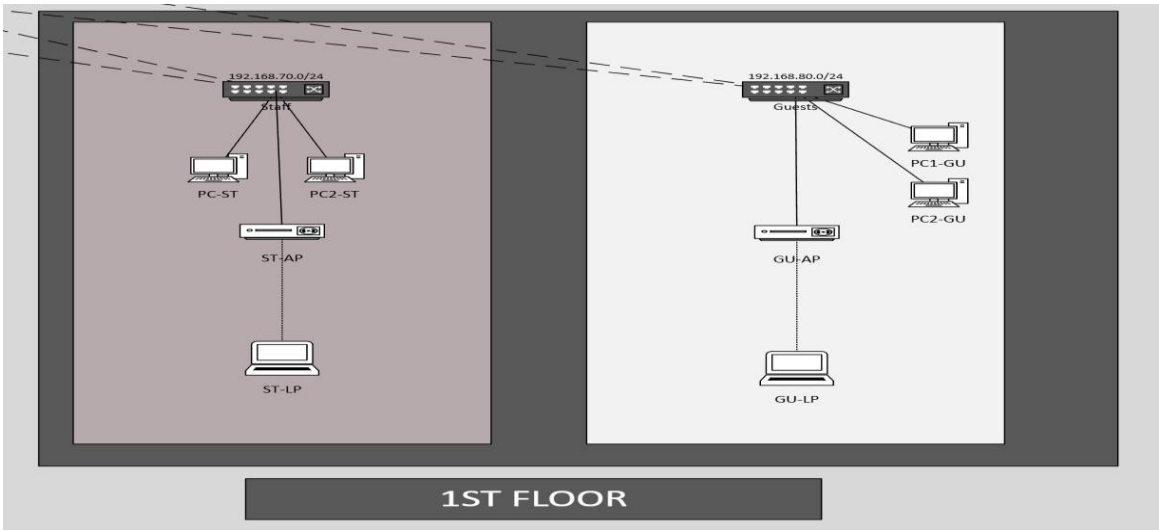


This figure above highlights that the access layer links all user devices, including desktops, laptops, printers and wireless access points. Individual access switches tie the network devices on each floor and trunk lines tie those devices to the distribution layer. Berufsschulen separate broadcast domains and secure access by joining each group into their own department-specific VLAN.

4.3.6. 1st Floor Access Device

Figure 4.3.6

1st Floor Access Device

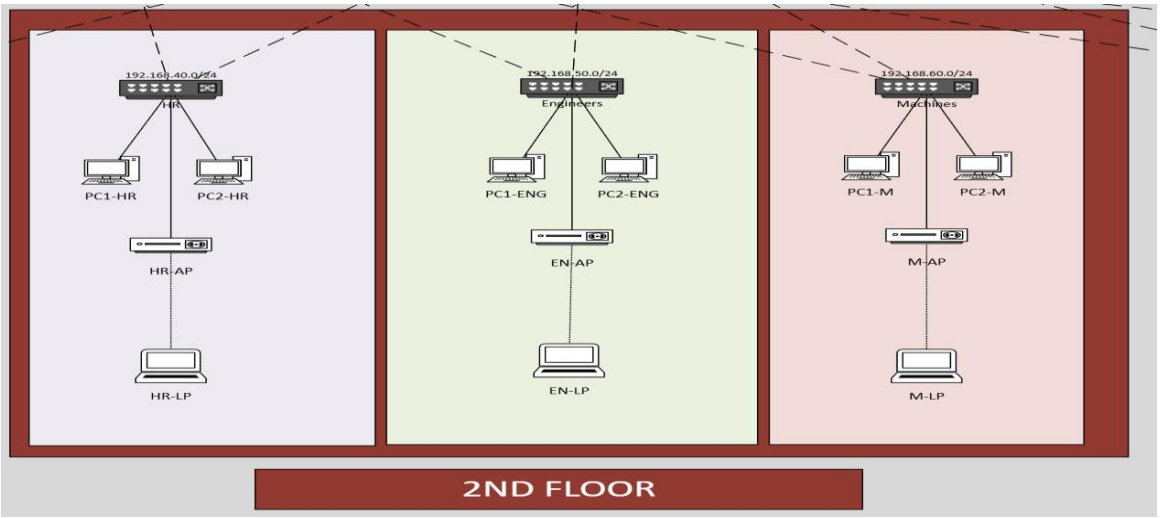


The figure (4.2.6) shows the area on the first floor that is designed for staff and guests' computers. Links between access switches are made with floor-level access switches and VLANs are applied to separate guest traffic from the internal network. The network makes it possible for both groups to smoothly connect without allowing accidental contact.

4.3.7. 2nd Floor Access Devices

Figure 4.3.7

2nd Floor Access Devices

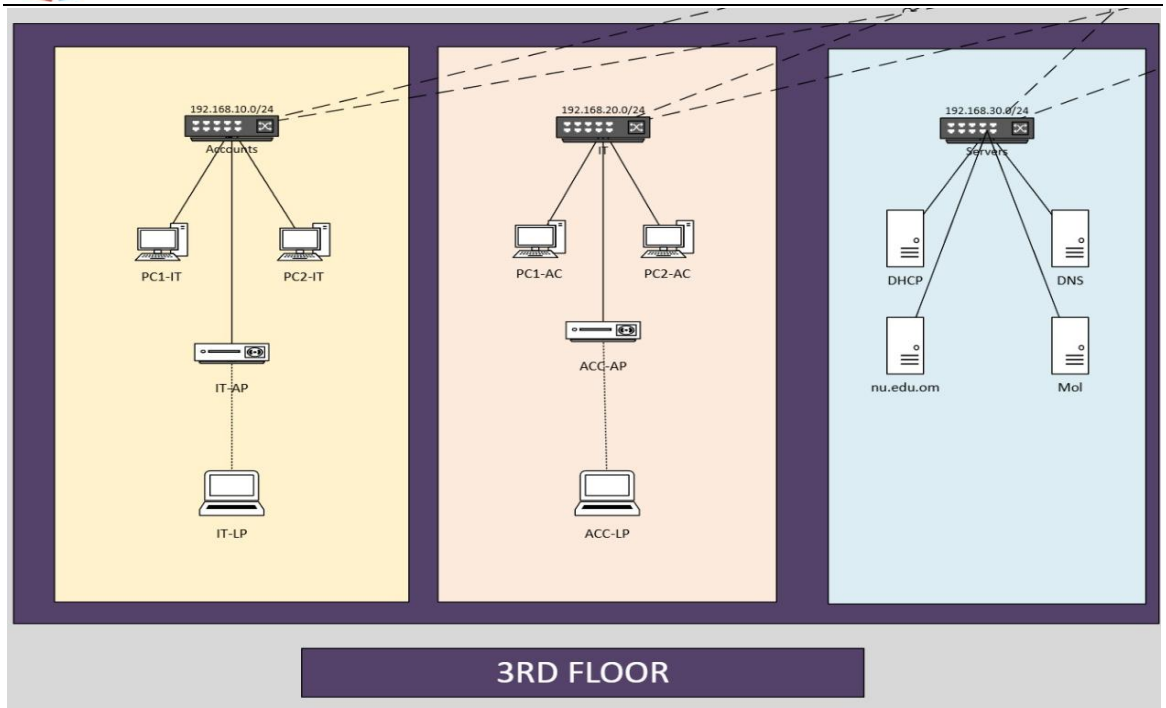


The 2nd floor is shown above, where the Human Resources, Engineering and Machines departments are located. By giving each department, a separate access switch and grouping VLANs, rules remain clear and there isn't any excess communication among different departments.

4.3.8. 3rd Floor Access Devices

Figure 4.3.8

3rd Floor Access Devices



As seen in the figure, the IT Department, Accounts Department and central Servers are all located on the 3rd floor. Devices are attached to special access switches that form their own VLANs. The Servers VLAN is crucial for separating DHCP, DNS and web hosting from the regular traffic, so security and availability are improved

4.4. Chapter Summary

Chapter 4 describes how a cybersecurity awareness training lab should be structured with special attention to both the logical and physical arrangements of the network. Because of these two qualities, the lab can run important functions and support easy learning interactions. The logical design lays out the path of data in the network, what each user can do and how servers, tools and accounts are linked. The goal is to sort the network into VLANs—such as one for IT, HR and another for Servers—to keep the data safe and well-arranged. If your network uses core, distribution and access layers, it can grow and be handled easily.

To make the network more secure and reliable, HSRP can act as a backup when a router goes down and ACLs, DHCP snooping and port security can prevent anyone who should not be there from accessing your traffic. The security of remote management relies on SSH, and all configuration backups are handled with TFTP. NAT makes sharing the internet safer for users on the network and the admin functions are isolated in VLAN 99 for better security. By using these elements, the labs become safe and realistically match the environments students will use at work.

Physical design implements the logical structure using genuine or virtual building tools such as Cisco Packet Tracer and Microsoft Visio. Its goal is to design a network layout that allows speed, withstands errors and ensures security. Under the hierarchical design, the key role is played by the core, followed by the distribution layer collecting data within and the access layer connecting users and their devices. Separating departments on the floor by both equipment and VLANs stops accidental access and makes the layout more orderly.

The most important message from this chapter is that thoughtful design of both logical and physical parts of the network play a big role in the success of the lab. Thanks to these tools, students have a good practice place to test, learn and practice their skills in a way they would use on the job.

CHAPTER 5: DEVELOPMENT AND EVALUATION

5.1. Introduction

This chapter illustrates how a systematic and secure network was created using Packet Tracer. To enhance learners' understanding of cybersecurity, the network is configured as a real system of a company. The primary focus is to implement fundamental networking theories, including VLANs, IP allocation, remote secure access, and control of traffic in a manner that optimally balances security and performance.

For ease of control and to increase protection from unauthorized access, the network is split into domains with departments using IP ranges controlled by metadata and VLANs. Each department has been assigned specific IP ranges. Use of DHCP snooping allows tracking of IP addresses and blocking of rogue servers. Access Control Lists are used to limit interdepartmental traffic in addition to restricting guest access to sensitive areas.

Through the utilization of port security, control over access via MAC addresses, SSH is used for safekeeping during remote access, strengthening security. Secure communication over email is provided using tools S/MIME and PGP in addition to websites that use HTTPS and SSL/TLS. SNMP serves as a network performance monitor.

The network diagram is provided to show the structure graphically. This example is useful for understanding how to design, secure, and manage a current network with modern industry standards.

5.2. Network Metadata

In our system, we rely on metadata to make network management simpler, more secure and help resolve issues. A dataset's metadata usually contains the elements:

- Every device in a VLAN and subnet is allocated its own IP address by the network. For example, machines used in Accounts are given IPs from the 192.168.10.0/24 subnet and those in IT are given addresses using the 192.168.20.0/24 subnet. It enables us to break up the system logically and makes handling the network much simpler.

- Grouping devices using VLAN Association means they are organized by what they do in various departments which improves network security. VLAN configurations are listed below:
    1. VLAN 10: Accounts (192.168.10.0/24)
    2. VLAN 20: IT (192.168.20.0/24)
    3. VLAN 30: Servers (192.168.30.0/24)
    4. VLAN 40: HR (192.168.40.0/24)
    5. VLAN 50: Engineers (192.168.50.0/24)
    6. VLAN 60: Machines (192.168.60.0/24)
    7. VLAN 70: Staff (192.168.70.0/24)
    8. VLAN 80: Guests (192.168.80.0/24)
    9. VLAN 99: Management (192.168.99.0/24)

As a result, information from each part of the network is separated, making illegal access and leaks unlikely.

- Port security in the network uses MAC address tracking to oversee and keep rules for connected devices. After issuing the switchport port-security mac-address sticky command, a switch will learn the MAC addresses of devices and remember them. Using this approach blocks unapproved devices and helps discover any dangers to the network (Cisco, n.d.--a).
- Remote Device Management: Using SSH protocol is still considered the primary way for secure user access. In order to secure network devices, SSH settings require providing usernames, passwords and encryption keys. Using Zero Trust, the system protects access as well as offers logs for review at a later point (Cisco, n.d.-b).
- DHCP Lease Information is Used for: DHCP snooping is configured across VLANs to note and control IP address leases. The DHCP snooping binding table records MAC addresses, the IP addresses next to them, how long the lease lasts, each VLAN involved and the name of the interface. The details are required to trace device activity and to stop other servers from distributing IP addresses (Cisco, n.d.-c).
- Access Control Lists (ACLs) act to manage the flow of traffic connecting various VLANs. As an illustration, the BLOCK-GUEST ACL prevents access of devices in VLAN 80 to the internal network and allows only traffic going to the internet. As a result, guests cannot affect how the network is managed.

- Users attach to the internet via their NAT networks, allowing their internal private IP addresses to be translated into its public IP. The table stores the inside IP, the onward IP to the Internet and the time the translation lasted. Looking at and analyzing these logs makes it feasible to follow outbound activity and find potential unusual behavior (Cisco, n.d.-d).

5.3. Networking Protocols, Security and Topology

We use a variety of protocols to ensure that communication between our nodes is flawless and secure.

Our network is built on the TCP/IP protocol suite which enables all devices to communicate end to end. TCP is responsible for successful data delivery and IP is responsible for identifying and sending the messages to the right location.

- With Dynamic Host Configuration Protocol (DHCP), you can automatically assign IP addresses simply, meaning less work for IT and better control of IP addresses.
- The Domain Name System (DNS) translates website addresses we can read into their corresponding IP codes.
- SSH is used to give secure, remote access to network devices through encryption (Cisco, n.d.-b).
- SNMP stands for Simple Network Management Protocol. SNMP keeps watch of network habits and helps organize the information needed for managing devices.

5.3.1. Access to Secure Communication

- We use various secure communication services in our network to protect the data we exchange.
- Even our private email systems are protected with Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) before any transfer. Only those people who want to see the email content can do so thanks to these protocols.

All Web services are operated securely by HTTPS and SSL/TLS encryption. It keeps hackers and unauthorized from accessing communication and services.

- MAC Address Tracking: The network employs port security mechanisms to monitor and restrict devices based on their MAC addresses. By enabling the switchport port-security mac-address sticky command, switches dynamically learn and retain the MAC addresses of connected devices. This approach prevents unauthorized devices from accessing the network and aids in identifying potential security threats (Cisco, n.d.-a).
- Access Methods and User Authentication: Secure Shell (SSH) is the primary protocol for remote device management. SSH configurations include specifying usernames, passwords, and encryption keys, ensuring that only authorized personnel can access network devices. This setup not only secures administrative access but also provides logs for auditing purposes (Cisco, n.d.b).
- DHCP Lease Information: Dynamic Host Configuration Protocol (DHCP) snooping is enabled across VLANs to monitor and record IP address assignments. The DHCP snooping binding table maintains records of MAC addresses, assigned IPs, lease durations, VLAN numbers, and interface details. This information is crucial for tracking device activity and preventing unauthorized DHCP servers from distributing IP addresses (Cisco, n.d.-c).
- Access Control Lists (ACLs): Access Control Lists are implemented to regulate traffic between VLANs. For example, the BLOCK-GUEST ACL restricts devices in VLAN 80 (Guests) from accessing internal VLANs, allowing only internet-bound traffic. This ensures that guest users cannot interfere with internal network operations.
- Network Address Translation (NAT) Logging: NAT configurations translate internal IP addresses to a public IP for internet access. The NAT translation table logs details such as the internal IP, translated public IP, and the duration of the translation. Monitoring these logs helps in tracking outbound connections and identifying potential anomalies (Cisco, n.d.-d).

5.3.2. Network Topology

Our network architecture follows a 3-layer hierarchical design, comprising core, distribution, and access layers. This structure enhances scalability, manageability, and fault tolerance.

- Core Layer: The core layer serves as the backbone, facilitating high-speed data transfer between distribution layers. It is designed for optimal performance and minimal latency.
- Distribution Layer: This layer aggregates data from the access layer and implements policies for routing, filtering, and Quality of Service (QoS). It also provides redundancy and load balancing.
- Access Layer: The access layer connects end-user devices to the network. It manages device access, enforces security policies, and provides necessary services like DHCP and VLAN assignments.

5.4. Communication Protocols and Secure Services

Our network leverages a suite of protocols to ensure reliable and secure communication.

- Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP is the foundational protocol suite for our network, facilitating end-to-end communication. TCP ensures reliable data transmission, while IP handles addressing and routing.
- Dynamic Host Configuration Protocol (DHCP): DHCP automates IP address assignment, reducing administrative overhead and ensuring efficient IP management.
- Domain Name System (DNS): DNS resolves human-readable domain names to IP addresses, enabling seamless access to network resources.
- Secure Shell (SSH): SSH provides encrypted remote access to network devices, ensuring secure management and configuration (Cisco, n.d.-b).
- Simple Network Management Protocol (SNMP): SNMP monitors network performance and facilitates management by collecting and organizing information about managed devices.

Secure Communication Services

To safeguard data integrity and confidentiality, our network incorporates several secure communication services.

- Private Email Communication: We utilize encrypted email protocols, such as Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP), to protect email content and attachments. These protocols ensure that only intended recipients can access the email content.
- Secure Websites (HTTPS): All web-based services operate over HTTPS, employing SSL/TLS protocols to encrypt data in transit. This prevents eavesdropping and tampering by malicious actors.

5.5. System Configuration

Figure 5.5.1

Network Logical Design View This figure shows the 3-layer hierarchical secured network design of the National University (NU), Oman.

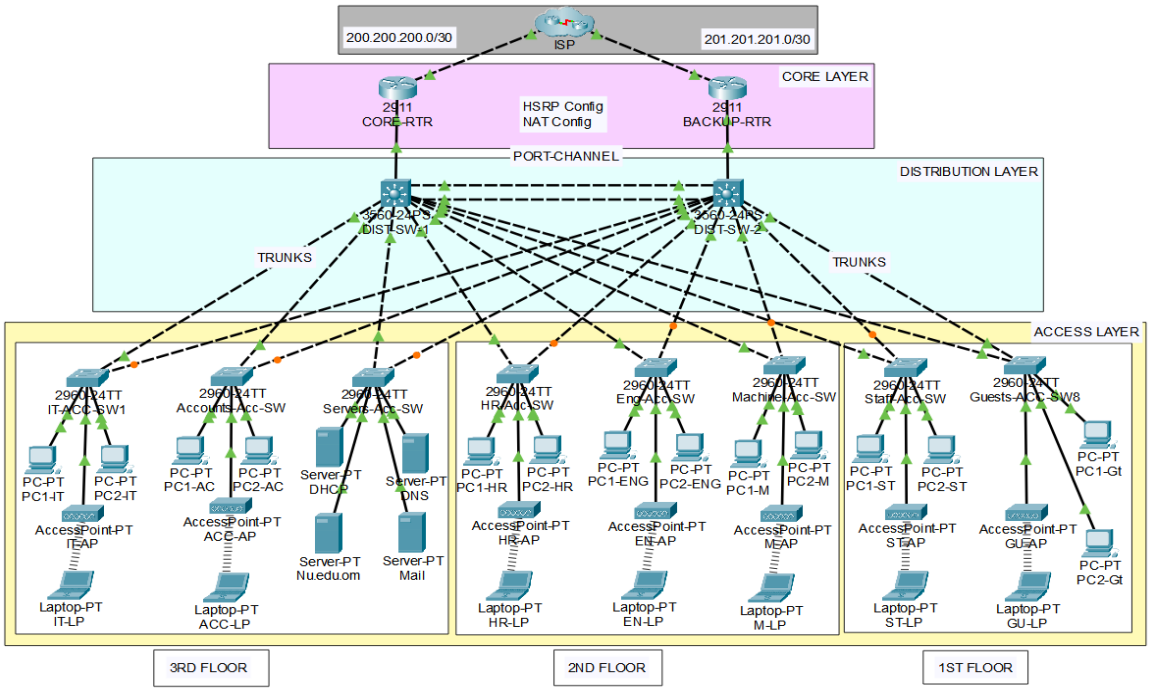
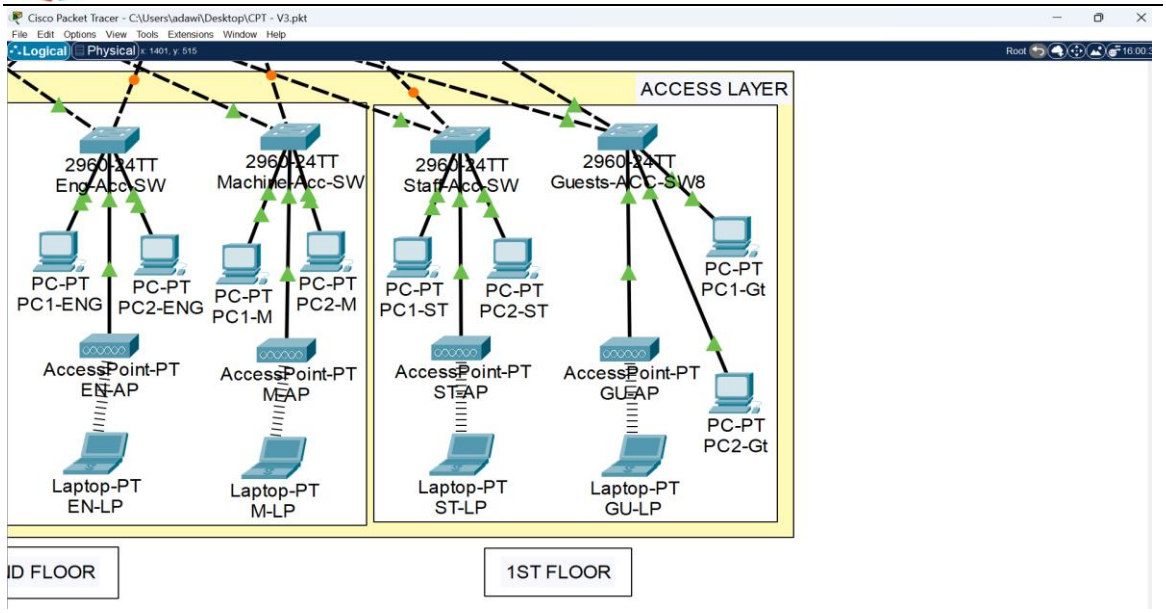


Figure 5.5.2

First Floor Configuration Departments: VLAN 80 (Guests), VLAN 70 (Staff) Displays the access layer setup for the first floor, which includes the Guests and Staff departments using VLANs 80 and 70, respectively.



5.5.1. Guests Department (VLAN 80)

Figure 5.5.3

Guests Access Switch Configuration The switch is configured with SSH, DHCP snooping, STP mode, and port assignments to VLAN 80 for guest users.

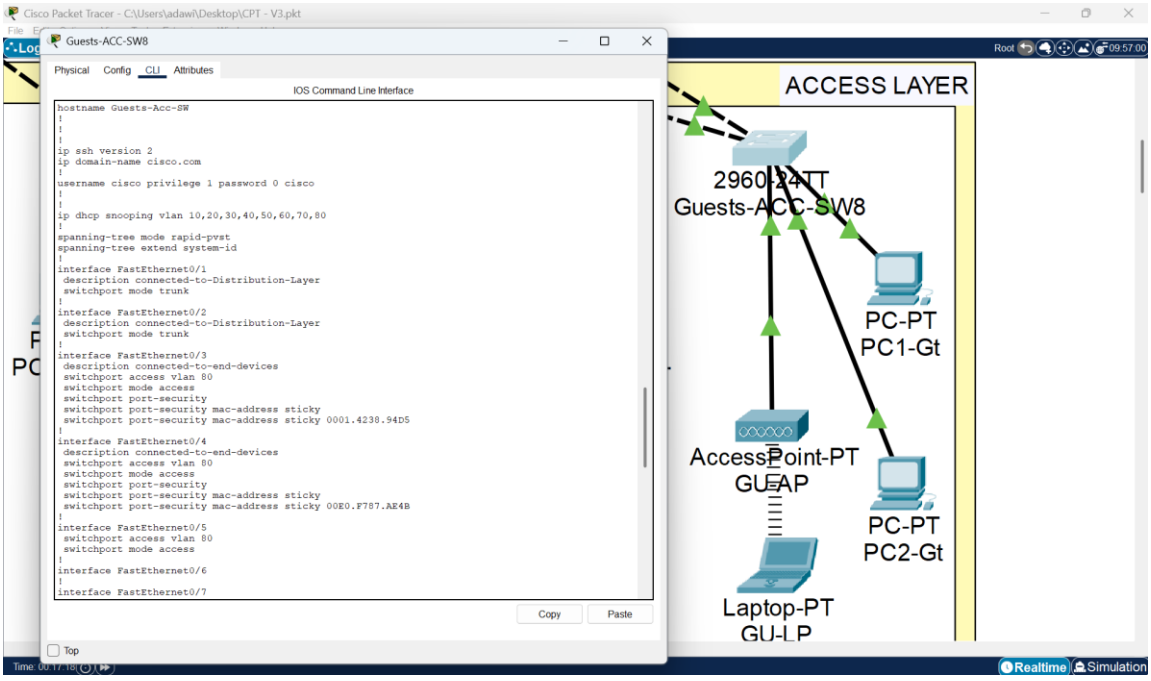


Figure 5.5.4

Guests Access Switch Management Configuration Sets the management VLAN and virtual teletype (VTY) lines for administrative remote access.

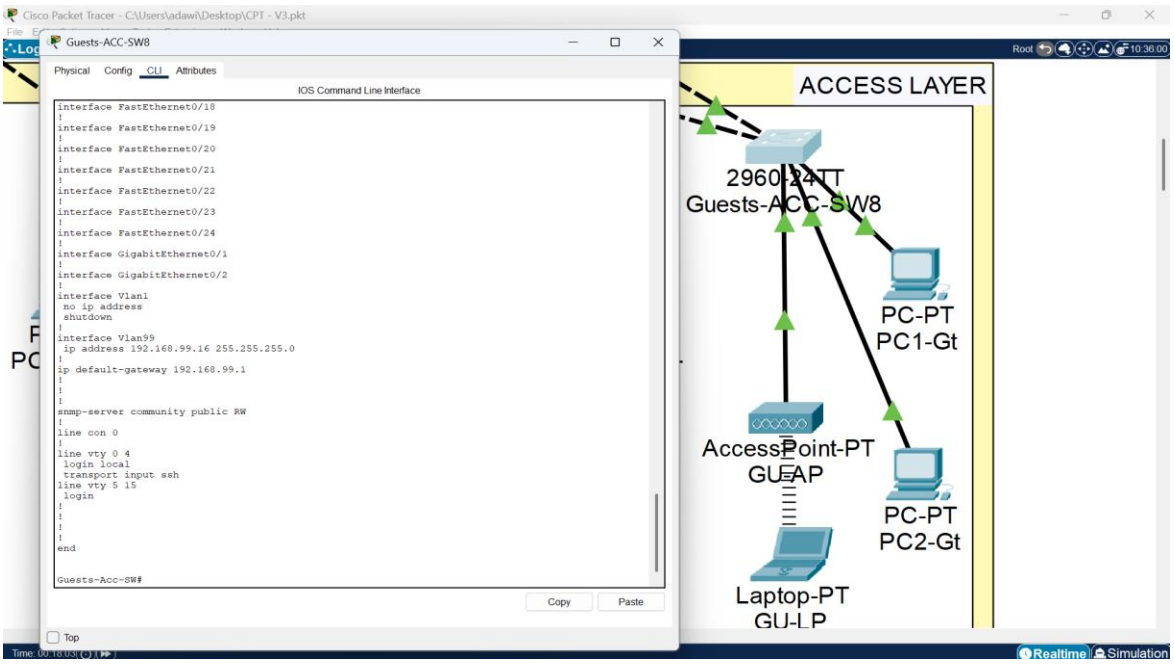


Figure 5.5.5

Guests PC1 Configuration Configured to obtain an IP address via DHCP under VLAN 80. Starting IP: 192.168.80.5, Gateway: 192.168.80.1 and DNS: 192.168.30.6.

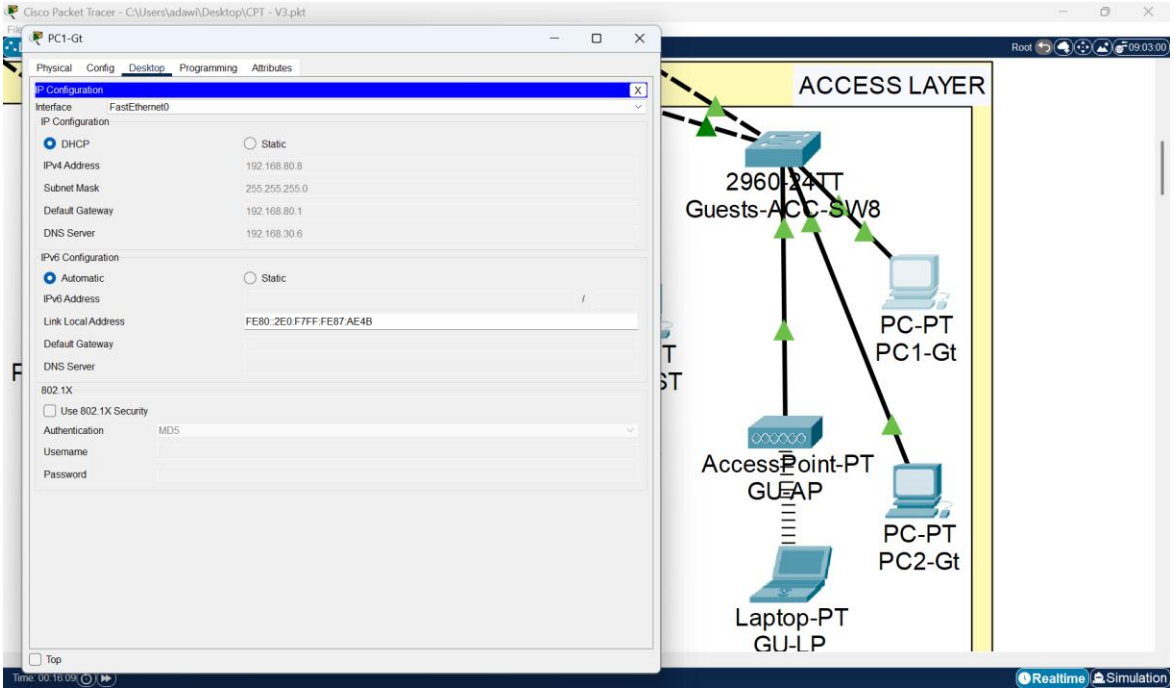


Figure 5.5.6

Guests VLAN Access Point Configuration SSID: GU, Coverage: 100 meters, PSK Pass Phrase: free1234. Provides wireless access to VLAN 80.

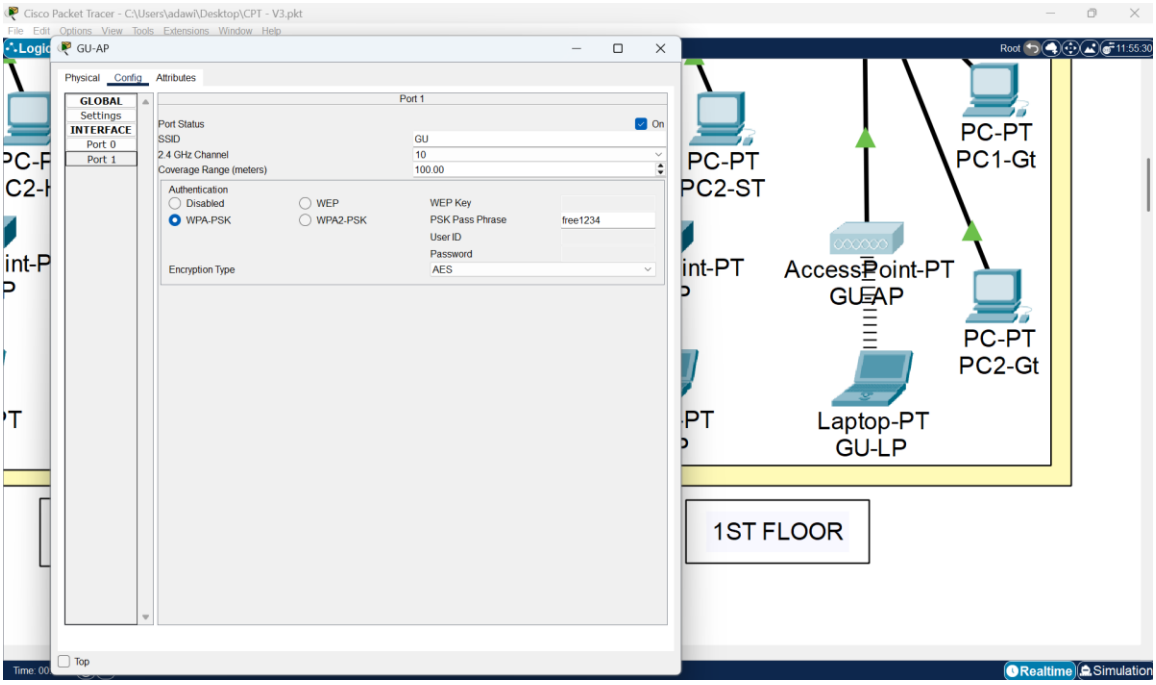


Figure 5.5.7

Guests PC2 Configuration, configured via DHCP under VLAN 80. Start IP: 192.168.80.5, Gateway: 192.168.80.1 and DNS: 192.168.30.6.

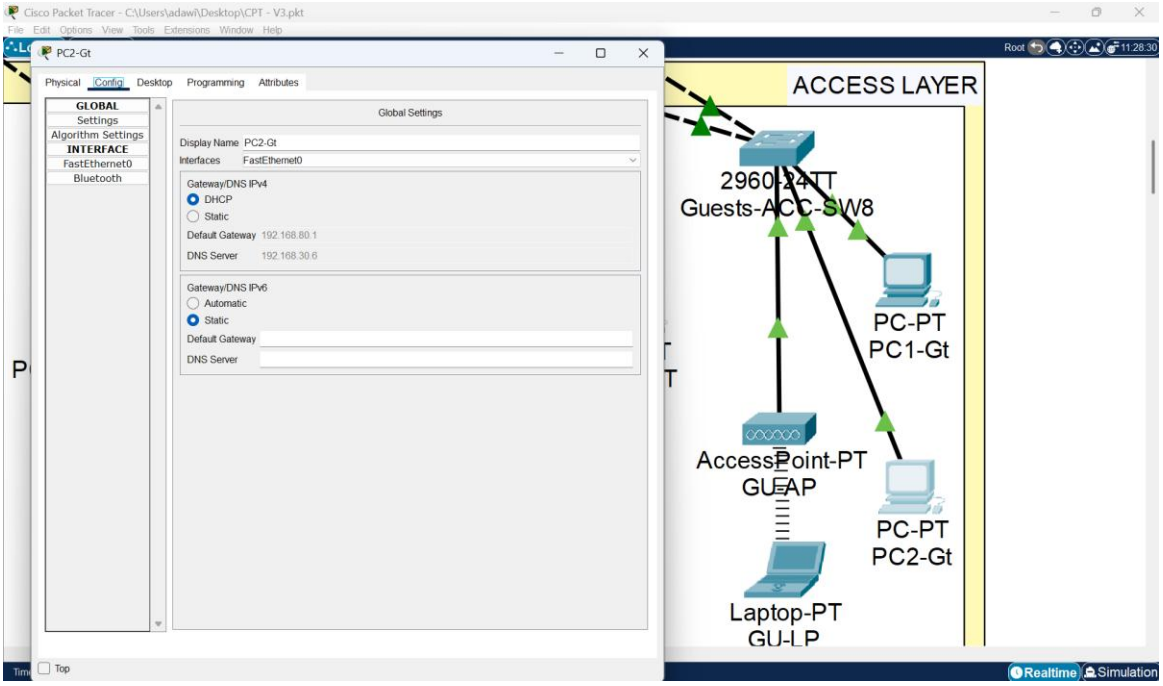
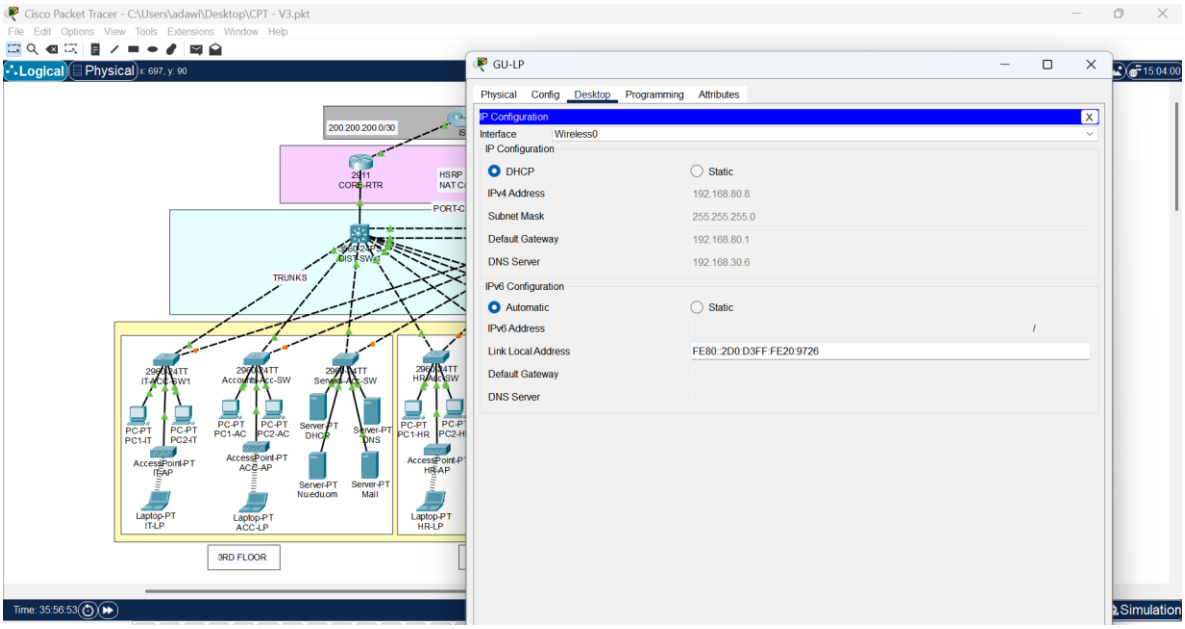


Figure 5.5.8

Guests Laptop Configuration Laptop receives IP via DHCP under VLAN 80. Start IP: 192.168.80.5, Gateway: 192.168.80.1 and DNS: 192.168.30.6.



5.5.2. Staff Department (VLAN 70)

Figure 5.5.9

Staff Access Switch Configuration The switch is configured with SSH, DHCP snooping, STP mode, and VLAN 70 port assignments for staff devices.

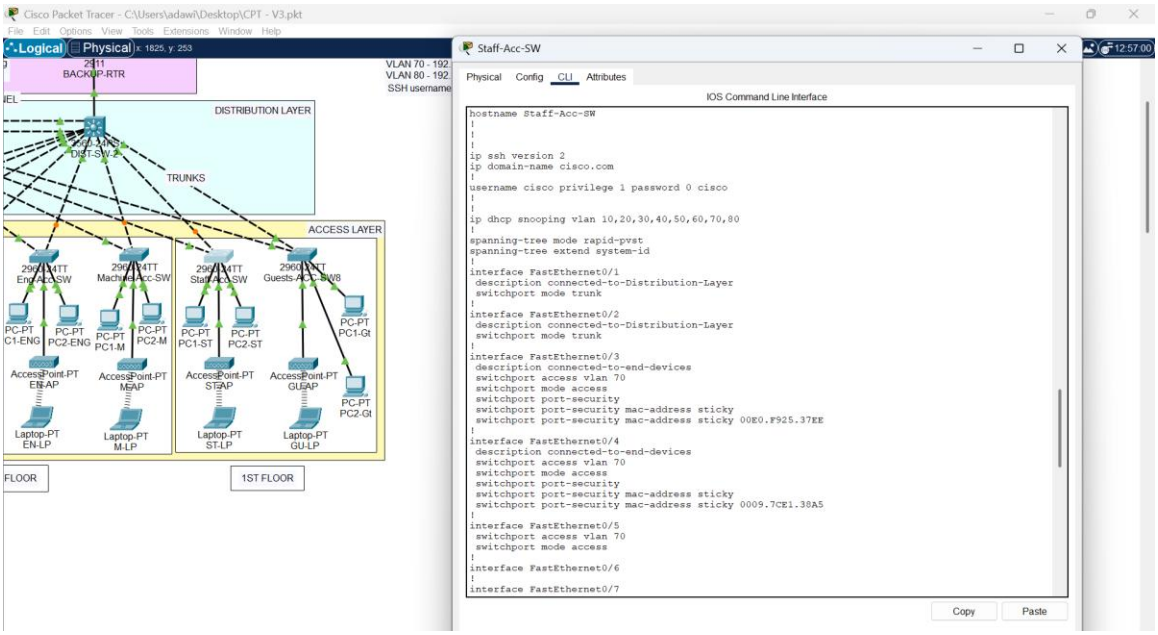


Figure 5.5.10

Staff Switch Management Configuration Configures the management VLAN and VTY lines for administrative remote access.

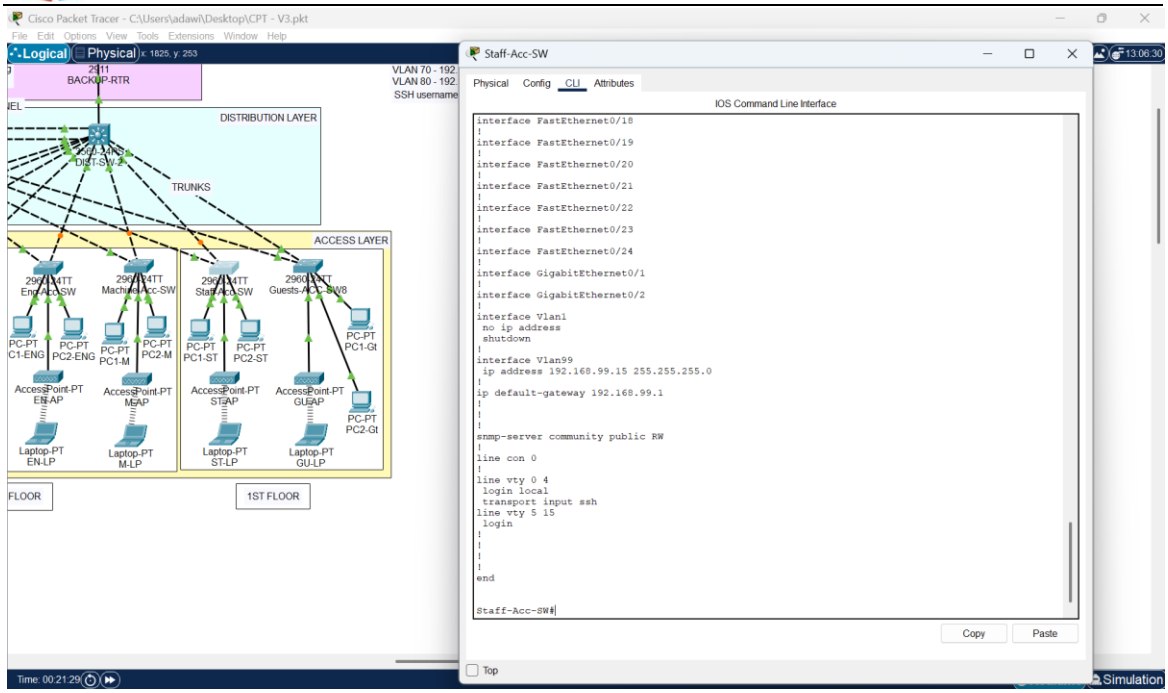


Figure 5.5.11

Staff PC1 Configuration DHCP configuration under VLAN 70. IP starts from 192.168.70.5 with Gateway: 192.168.70.1 and DNS: 192.168.30.6.

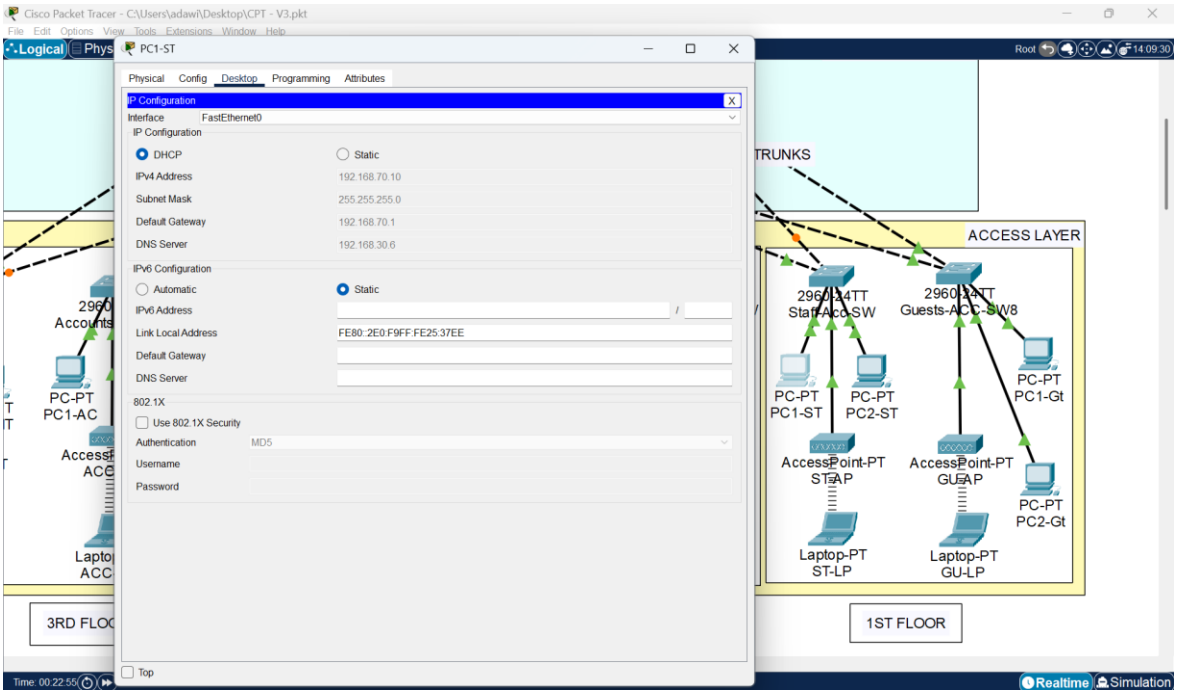


Figure 5.5.12

Staff PC2 Configuration Identical configuration as PC1. DHCP, Start IP: 192.168.70.5, Gateway: 192.168.70.1 and DNS: 192.168.30.6.

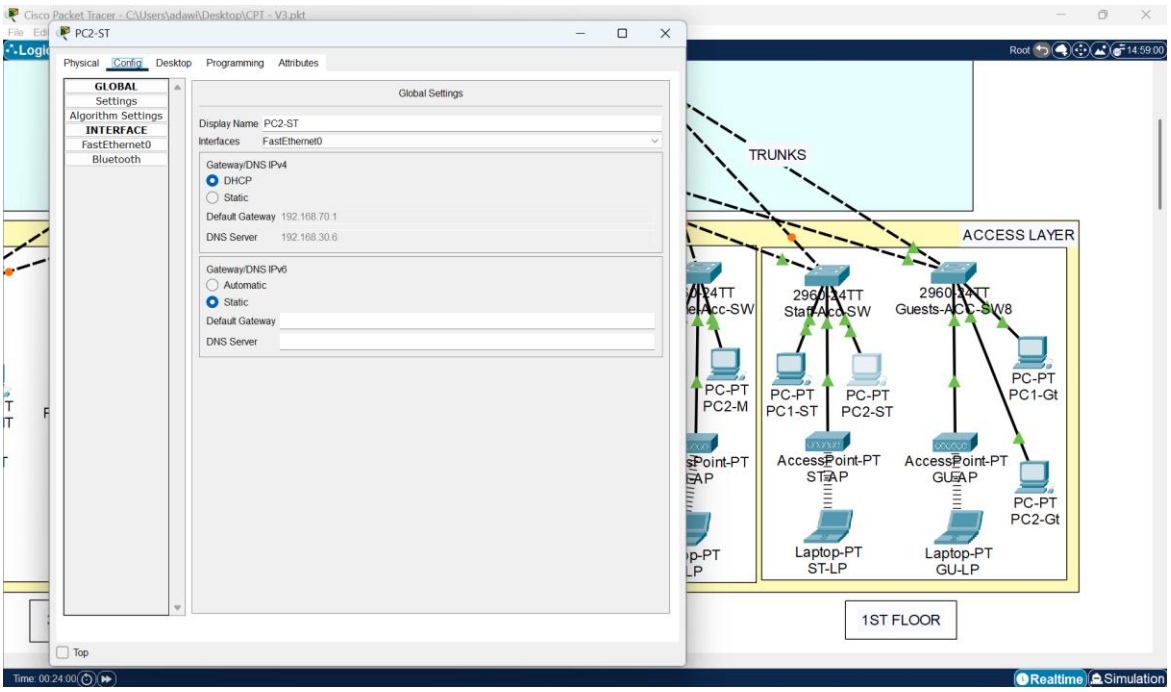


Figure 5.5.13

Staff VLAN Access Point Configuration SSID: ST, Coverage: 100 meters, PSK: cisco123. Provides wireless access to VLAN 70.

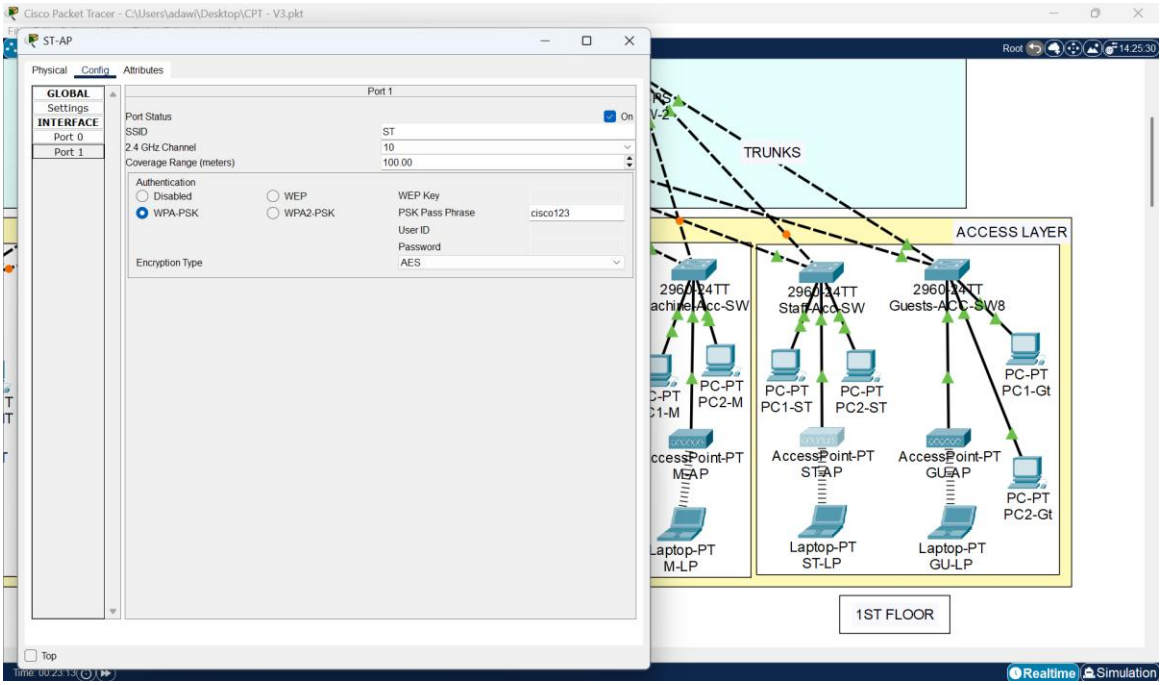


Figure 5.5.14

Staff Laptop Configuration Configured via DHCP in VLAN 70. Starting IP: 192.168.70.5, Gateway: 192.168.70.1 and DNS: 192.168.30.6.

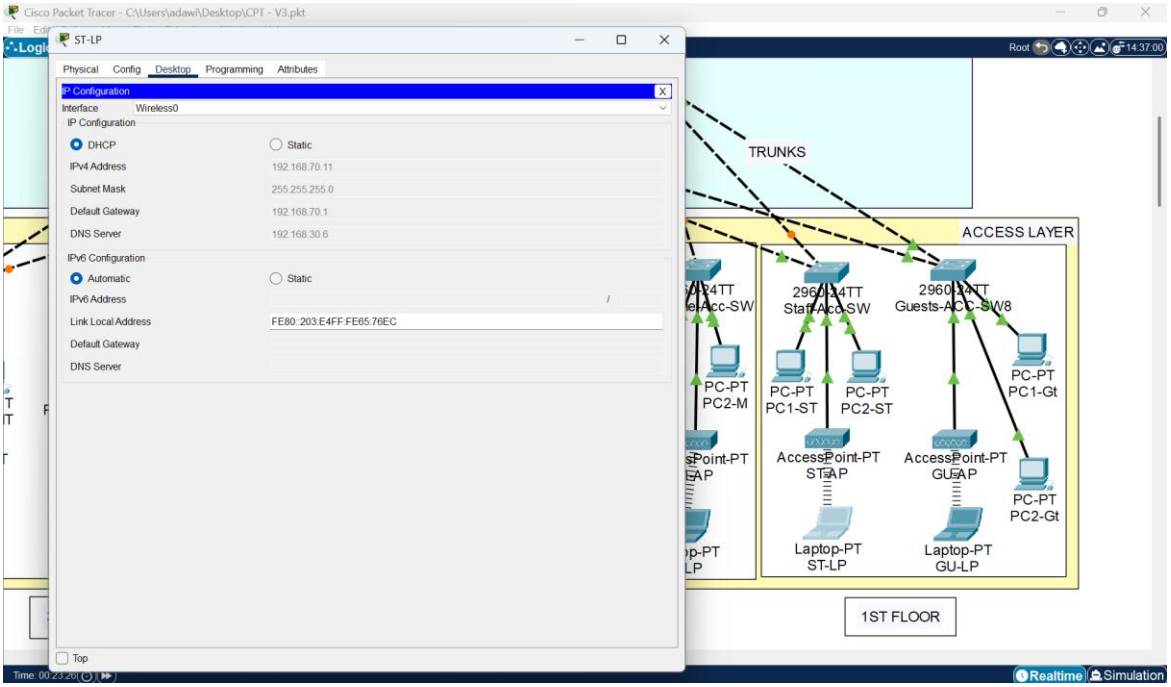
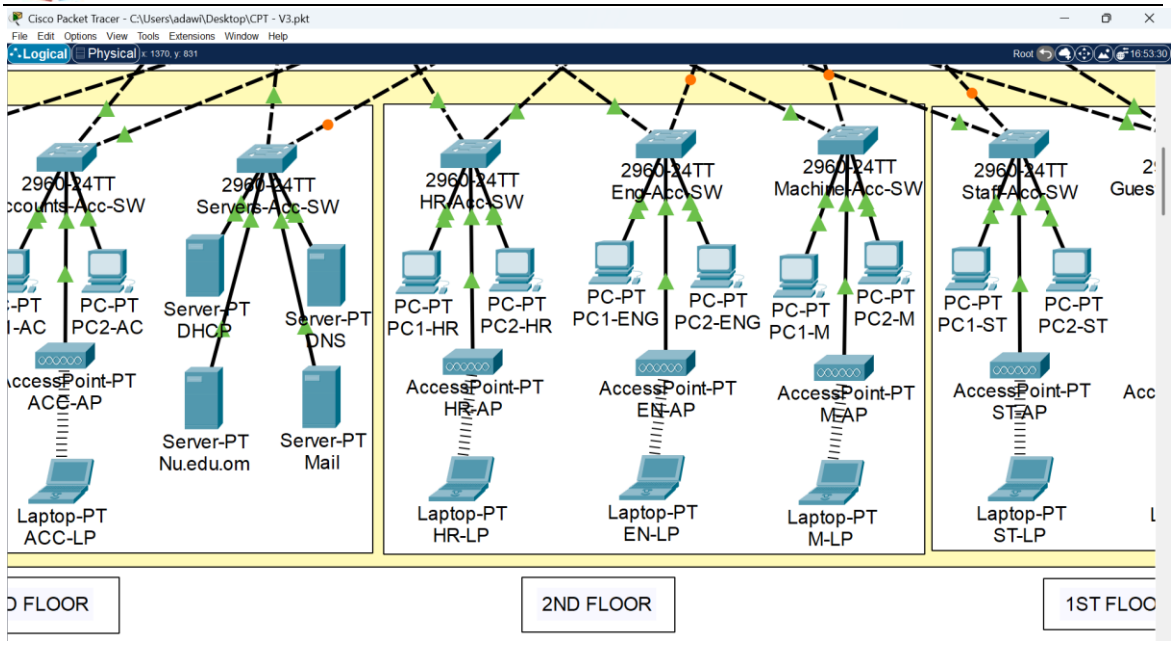


Figure 5.5.15

Second Floor Configuration Departments: VLAN 60 (Machines), VLAN 50 (Engineers), VLAN 40 (HR) Shows access layer for the second floor with Different VLANs



5.5.3. Machines Department (VLAN 60)

Figure 5.5.16

Machines Access Switch Configuration Configured for SSH, DHCP snooping, STP mode, and VLAN 60 port assignments.

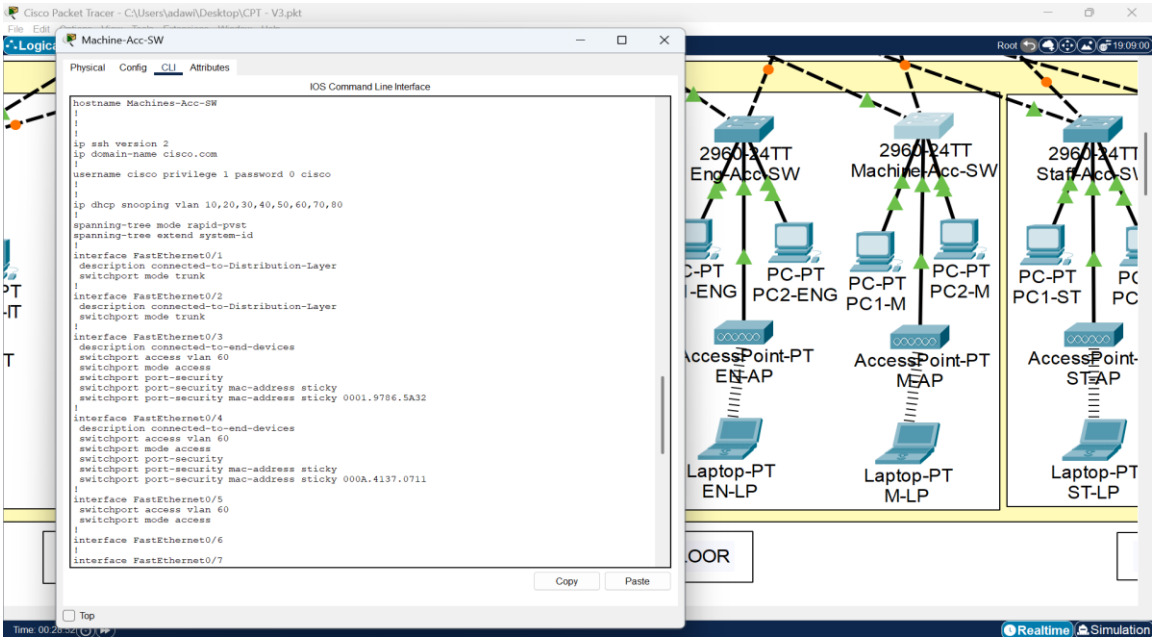


Figure 5.5.17

Machines Switch Management Configuration Sets the management VLAN and VTY settings for the Machines department switch.

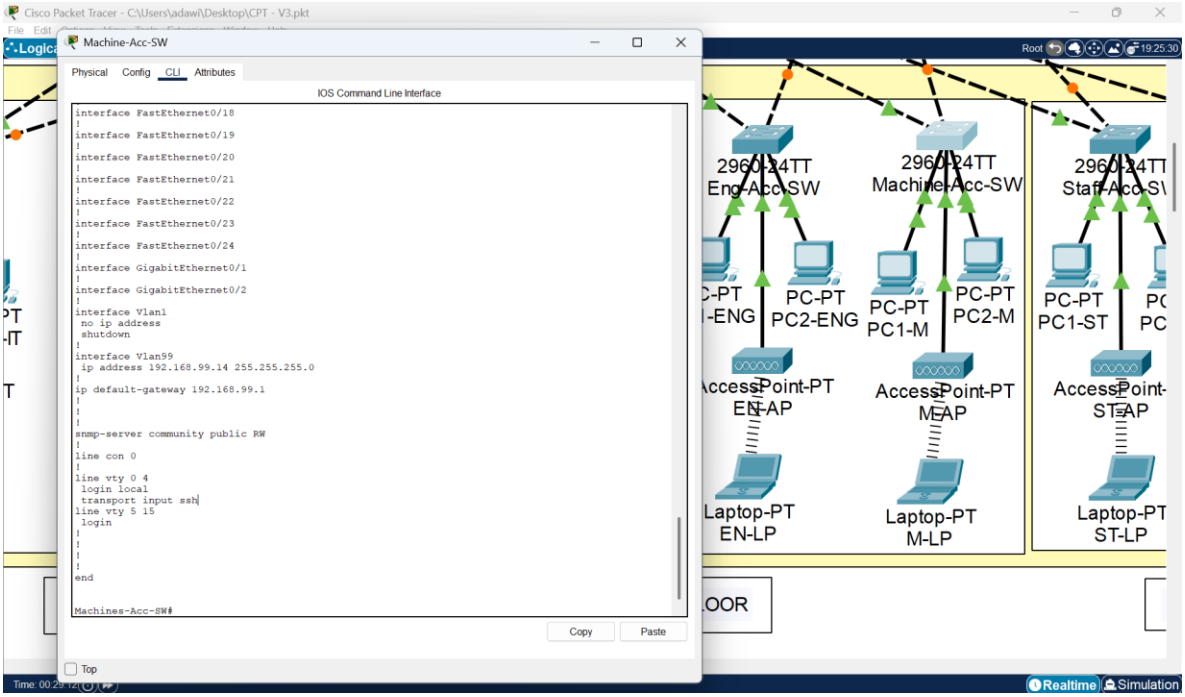


Figure 5.5.18

Machines PC1 Configuration DHCP configuration under VLAN 60. Starting IP: 192.168.60.5, Gateway: 192.168.60.1 and DNS: 192.168.30.6.

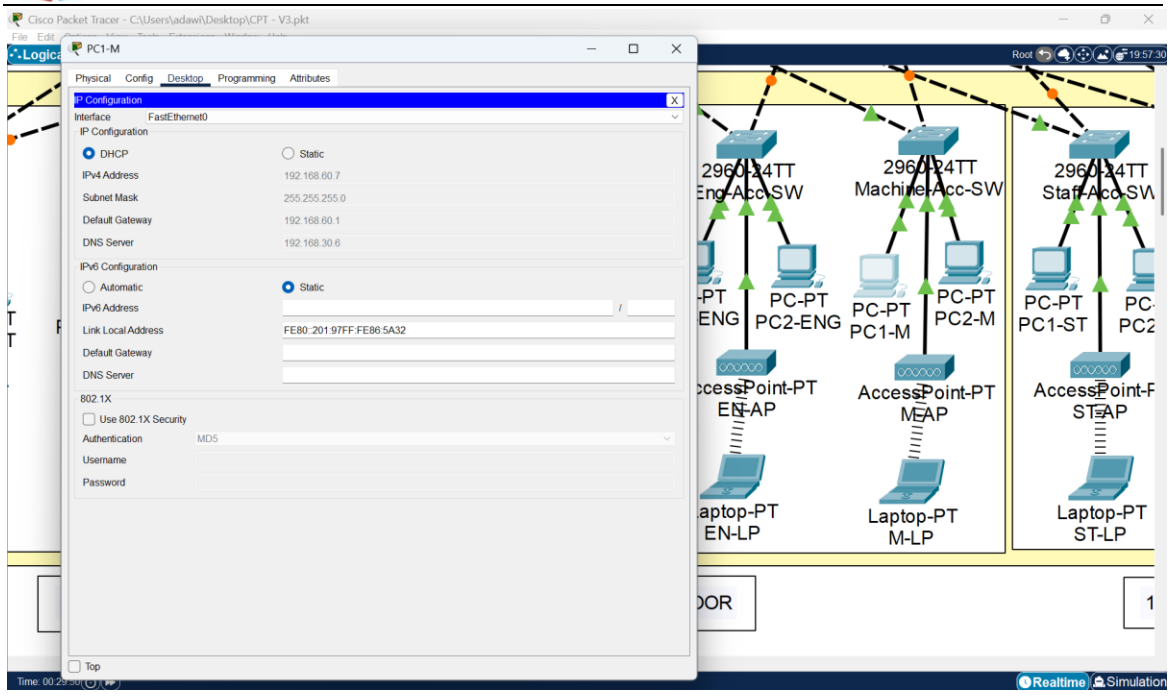


Figure 5.5.19

Machines PC2 Configuration DHCP configuration under VLAN 60. Starting IP: 192.168.60.5, Gateway: 192.168.60.1 and DNS: 192.168.30.6.

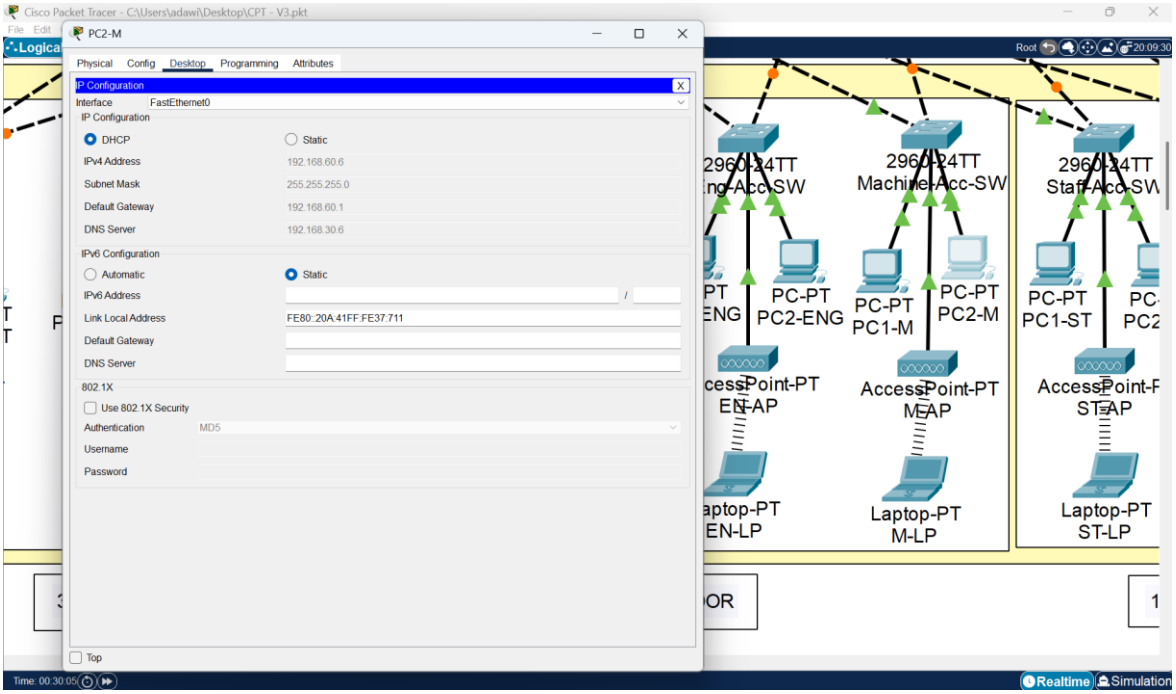


Figure 5.5.20

Machines VLAN Access Point Configuration SSID: ST, Coverage: 140 meters, PSK: cisco123. Provides wireless access to VLAN 60.

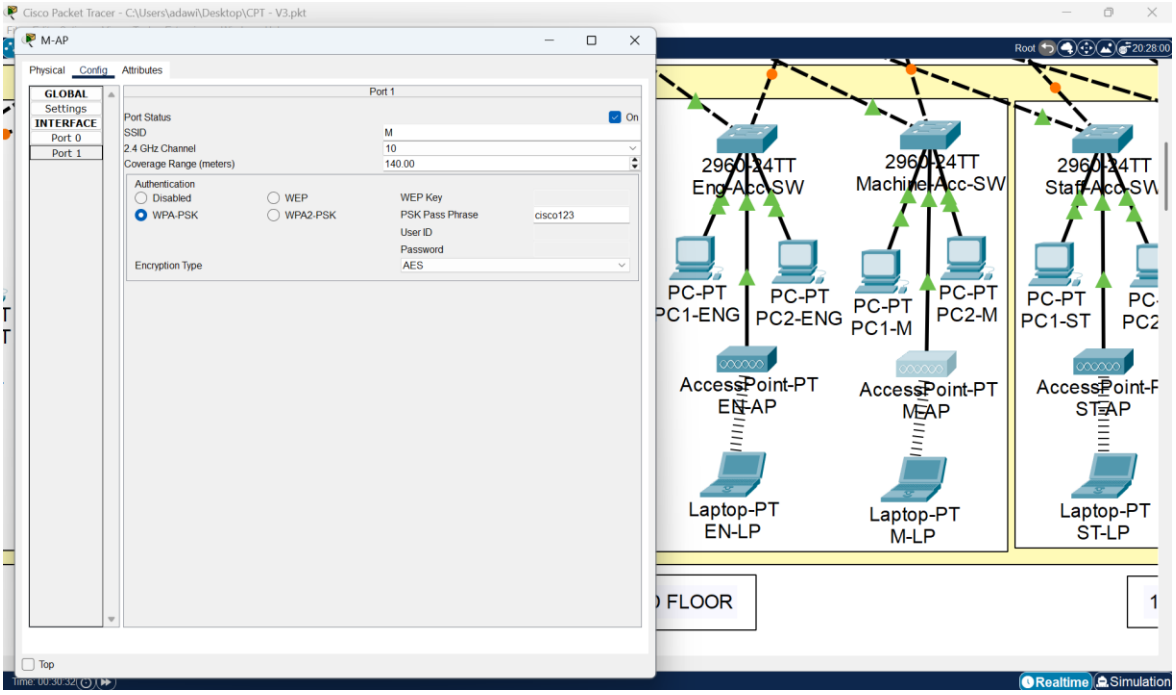
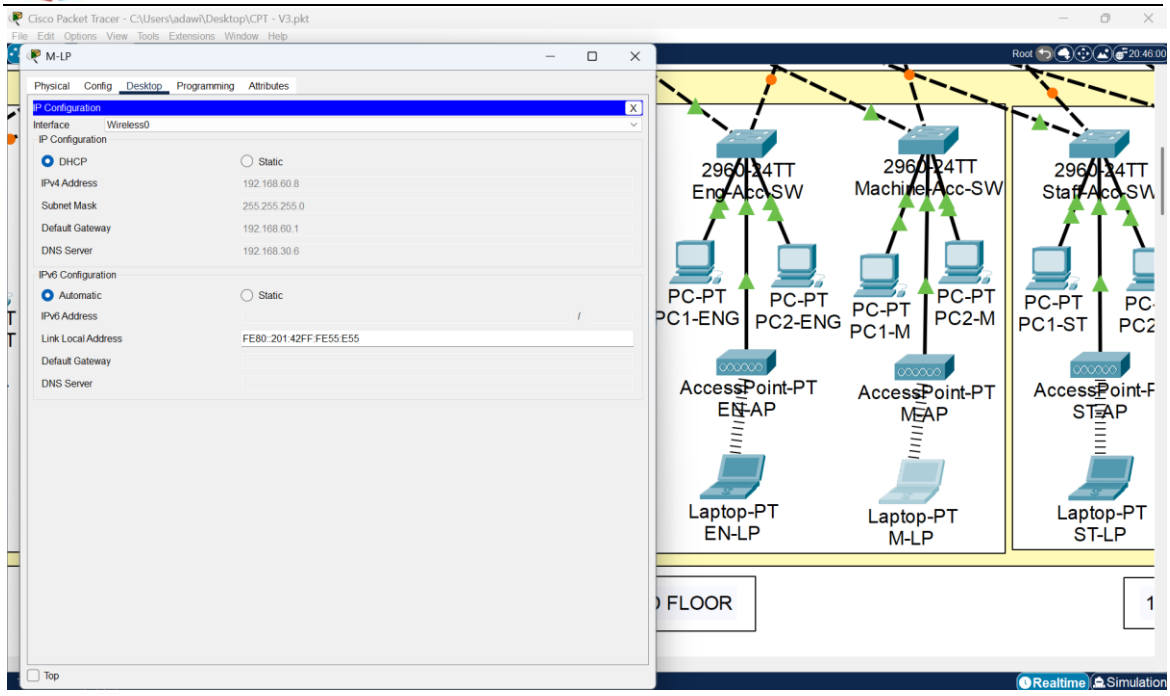


Figure 5.5.21

Machines Laptop Configuration Laptop connected via DHCP in VLAN 60. Starting IP: 192.168.60.5, Gateway: 192.168.60.1 and DNS: 192.168.30.6.



5.5.4. Engineering Department (VLAN 50)

Figure 5.5.22

Engineering Access Switch Configuration Switch configured for SSH, DHCP snooping, STP mode, and VLAN 50 port assignments.

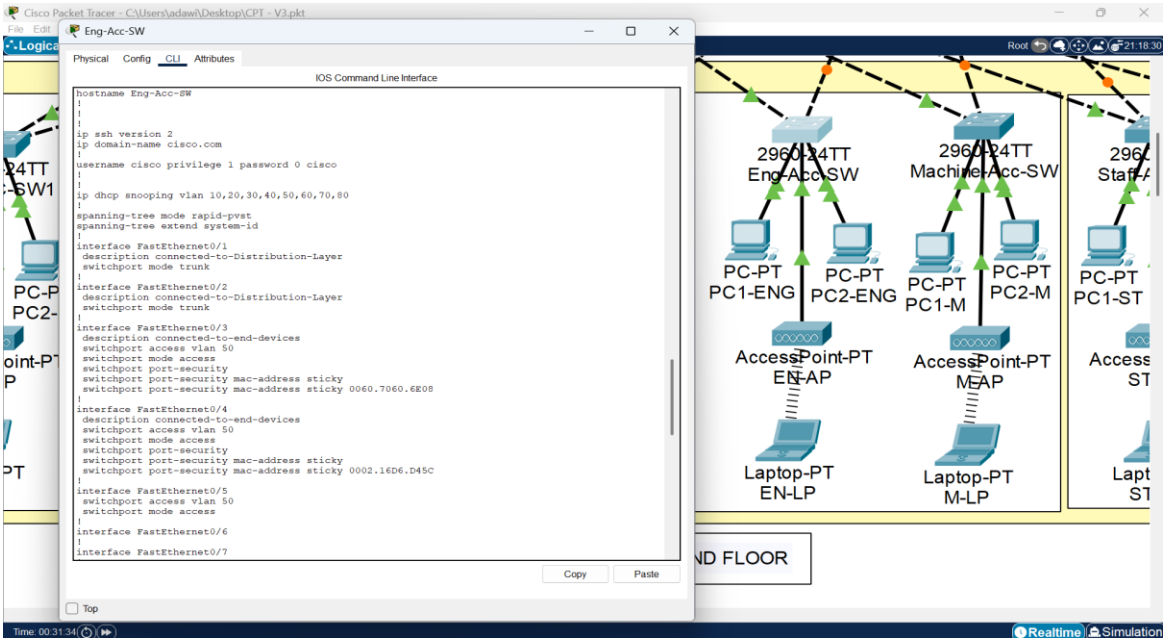


Figure 5.5.23

Engineering Switch Management Configuration Management VLAN and VTY settings applied.

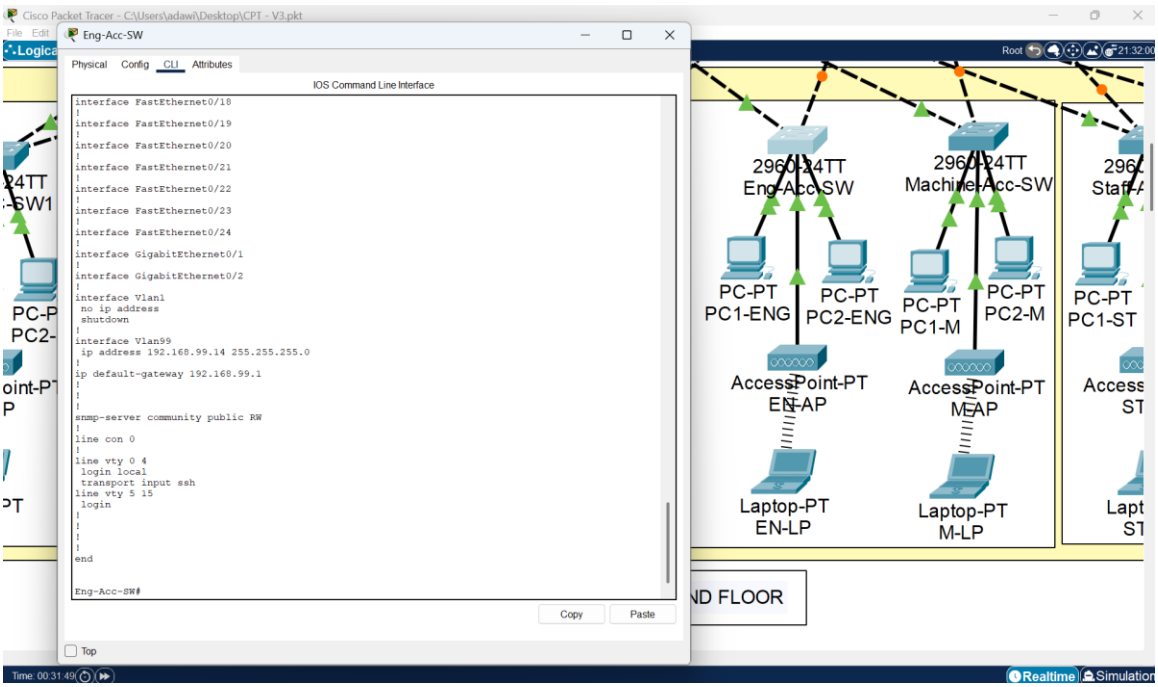


Figure 5.5.24

Engineering PC1 Configuration DHCP enabled under VLAN 50. Starting IP: 192.168.50.5, Gateway: 192.168.50.1 and DNS: 192.168.30.6.

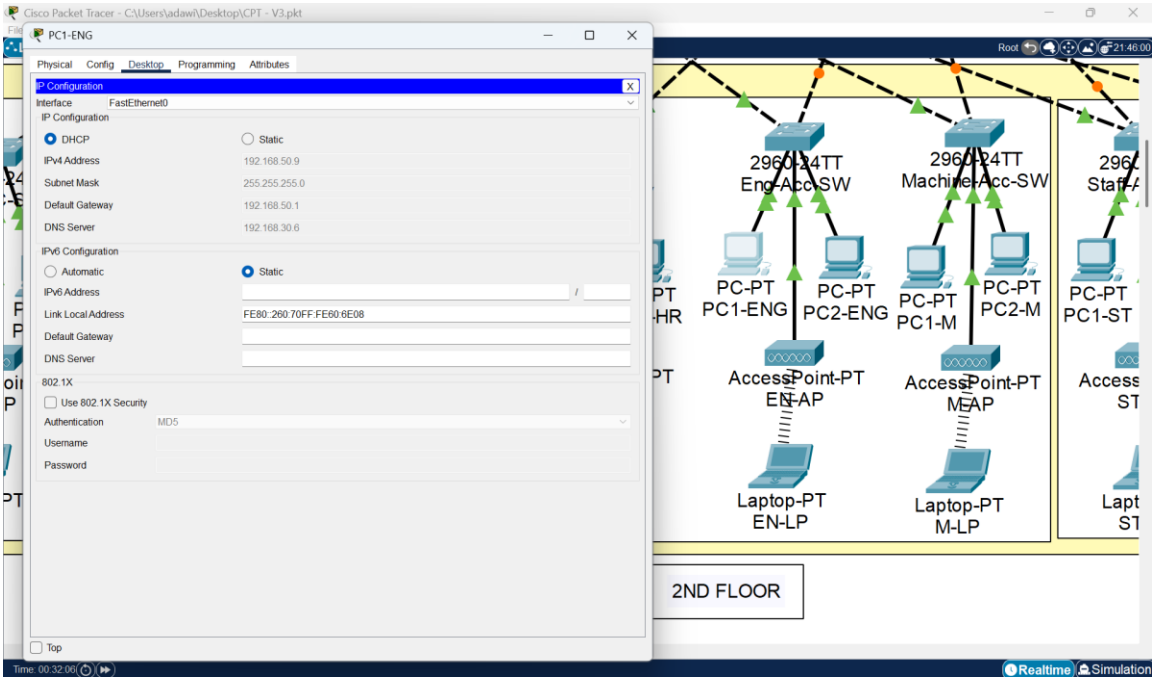


Figure 5.5.25

Engineering PC2 Configuration Same as PC1, configured under VLAN 50. Starting IP: 192.168.50.5, Gateway: 192.168.50.1 and DNS: 192.168.30.6.

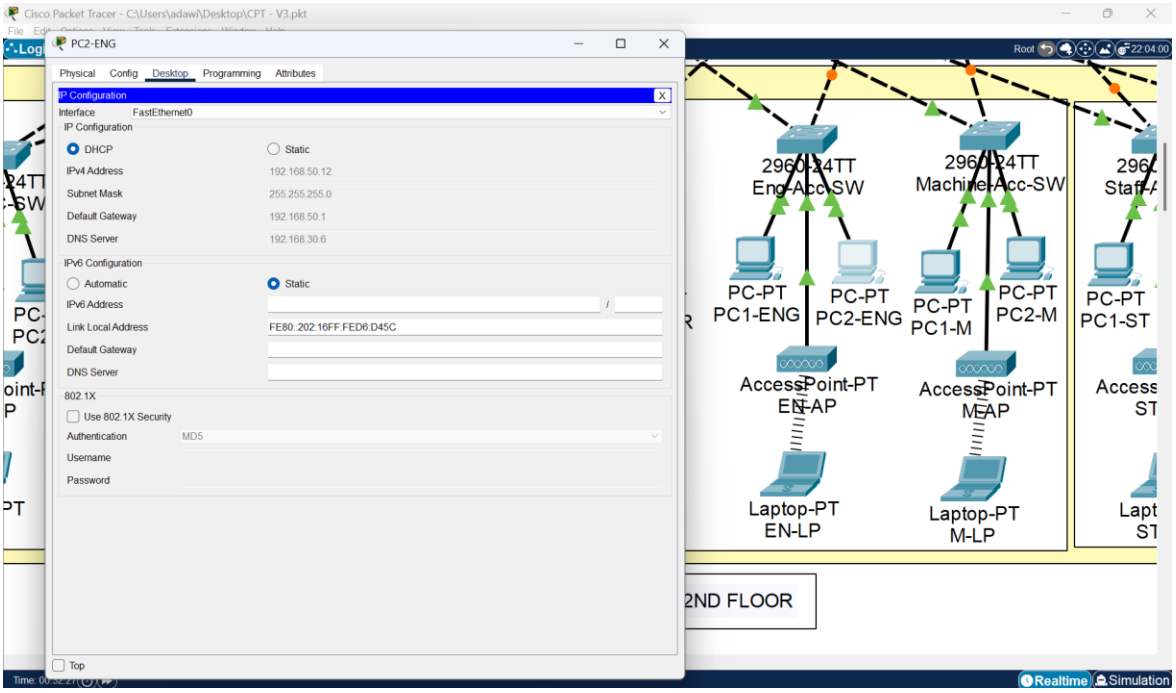


Figure 5.5.26

Engineering Laptop Configuration DHCP-enabled laptop connected to VLAN 50. Starting IP: 192.168.50.5, Gateway: 192.168.50.1 and DNS: 192.168.30.6.

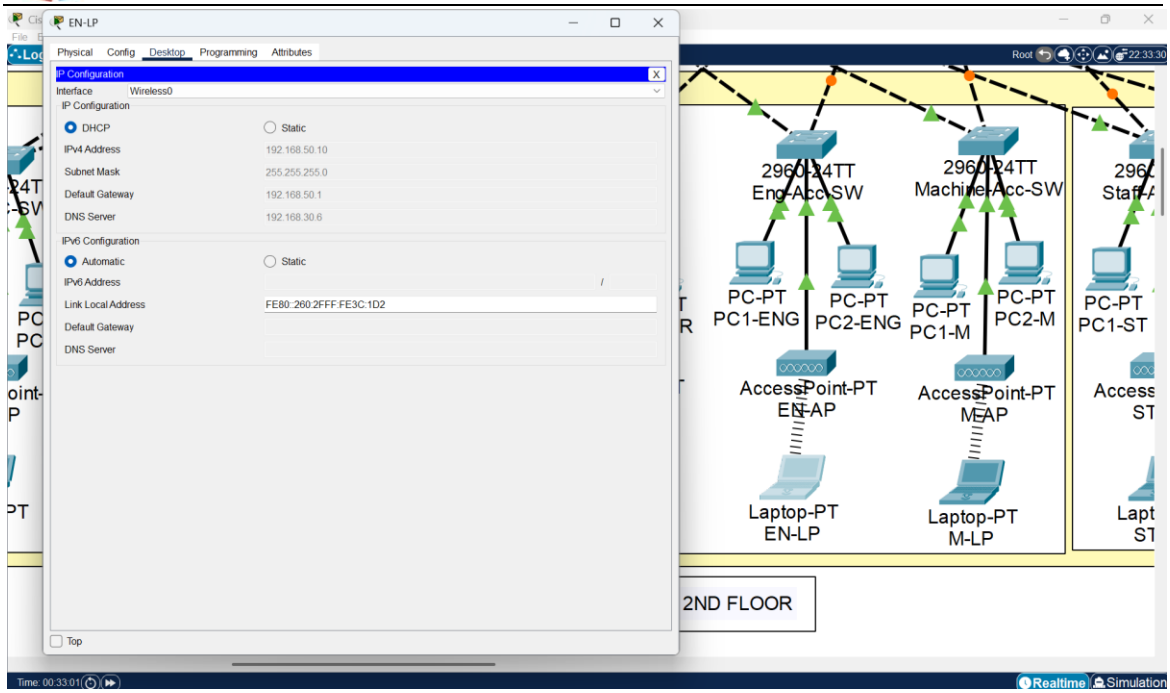
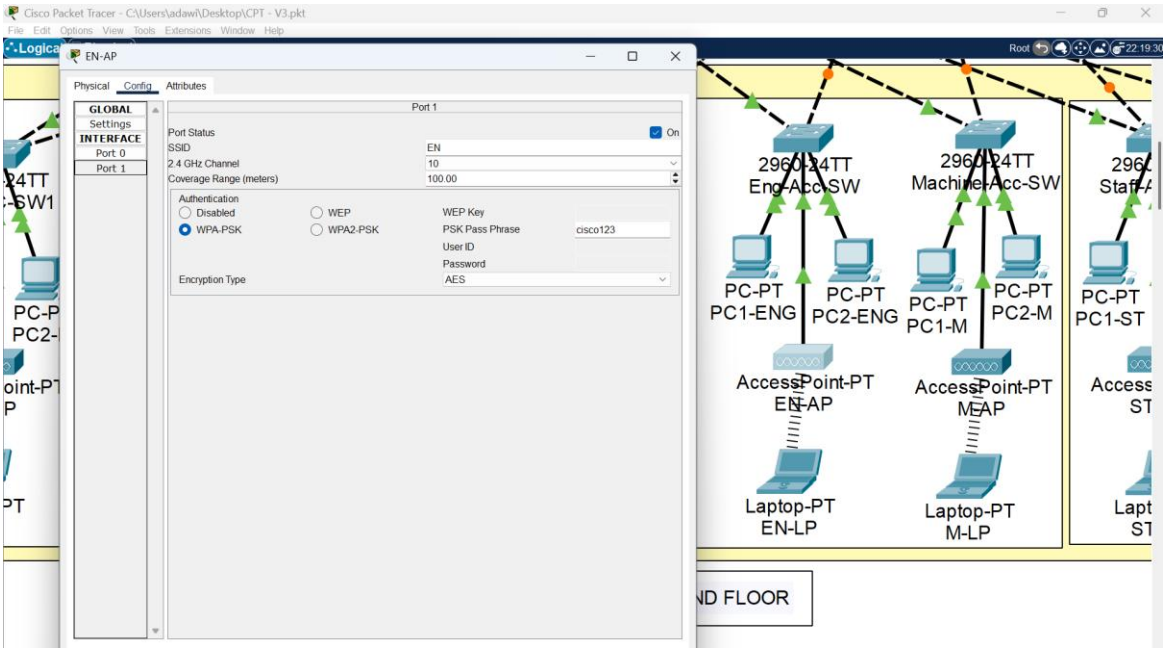


Figure 5.5.27

Engineering VLAN Access Point Configuration SSID: ST, Coverage: 100 meters, PSK: cisco123.



5.5.5. Human Resource Department (VLAN 40)

Figure 5.5.28

HR Access Switch Configuration Switch configured with SSH, DHCP snooping, STP mode, and VLAN 40 ports.

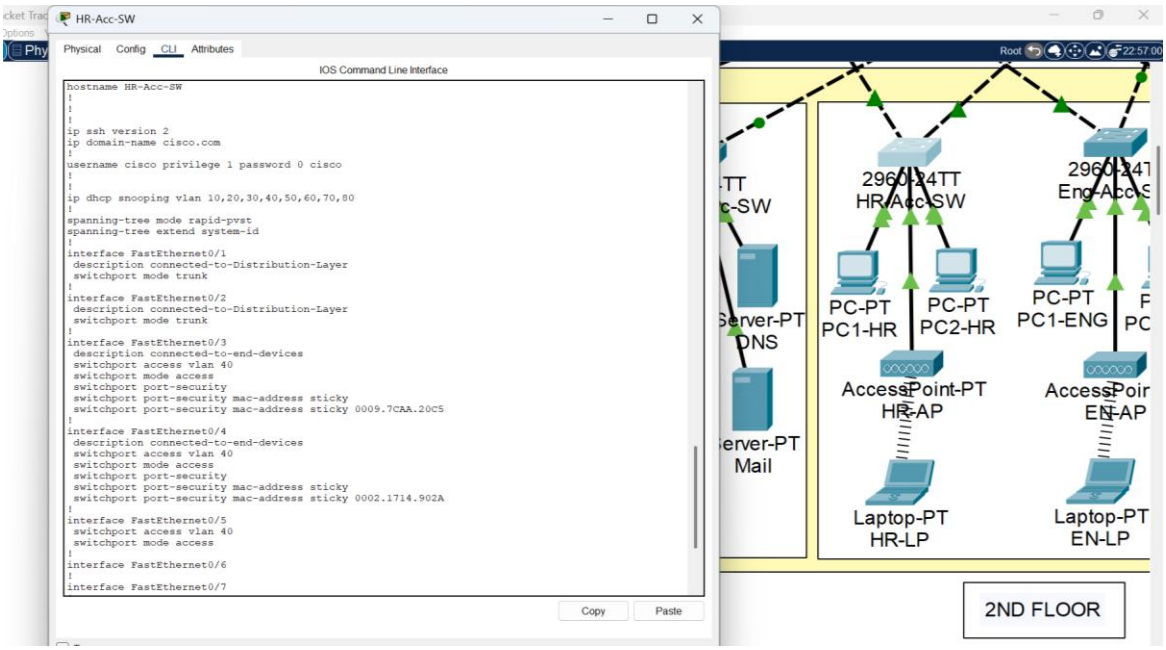


Figure 5.5.29

HR PC1 Configuration Configured under VLAN 40. Starting IP: 192.168.40.5, Gateway: 192.168.40.1 and DNS: 192.168.30.6.

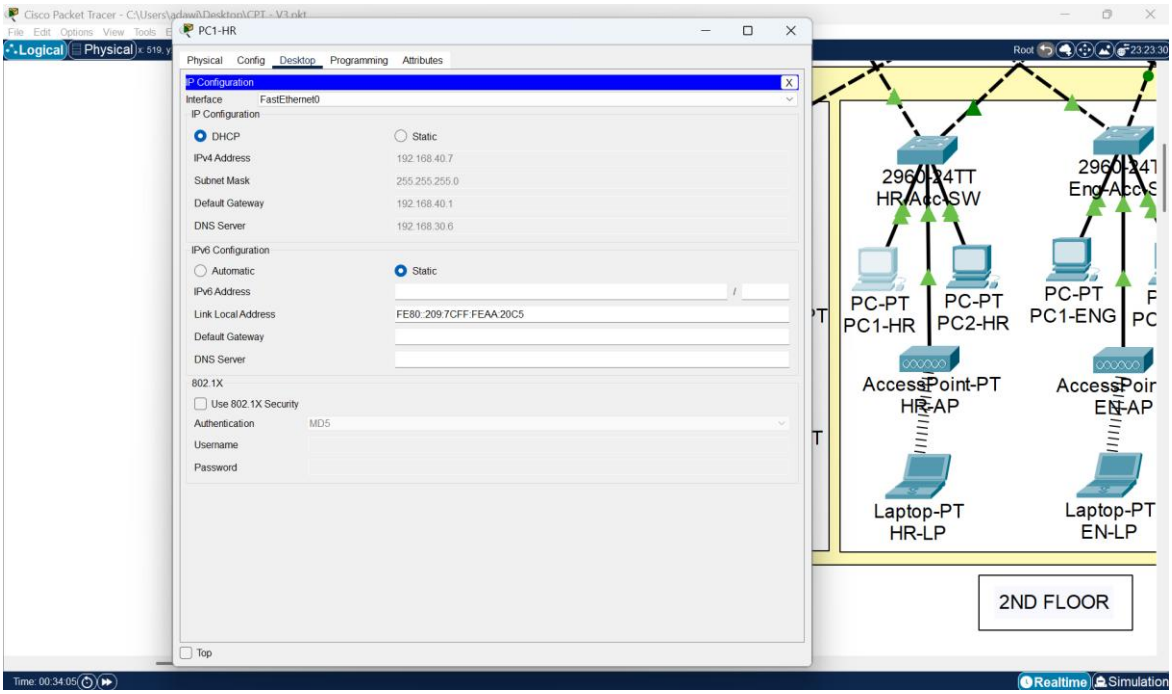


Figure 5.5.30

HR PC2 Configuration Configured under VLAN 40. Starting IP: 192.168.40.5, Gateway: 192.168.40.1 and DNS: 192.168.30.6.

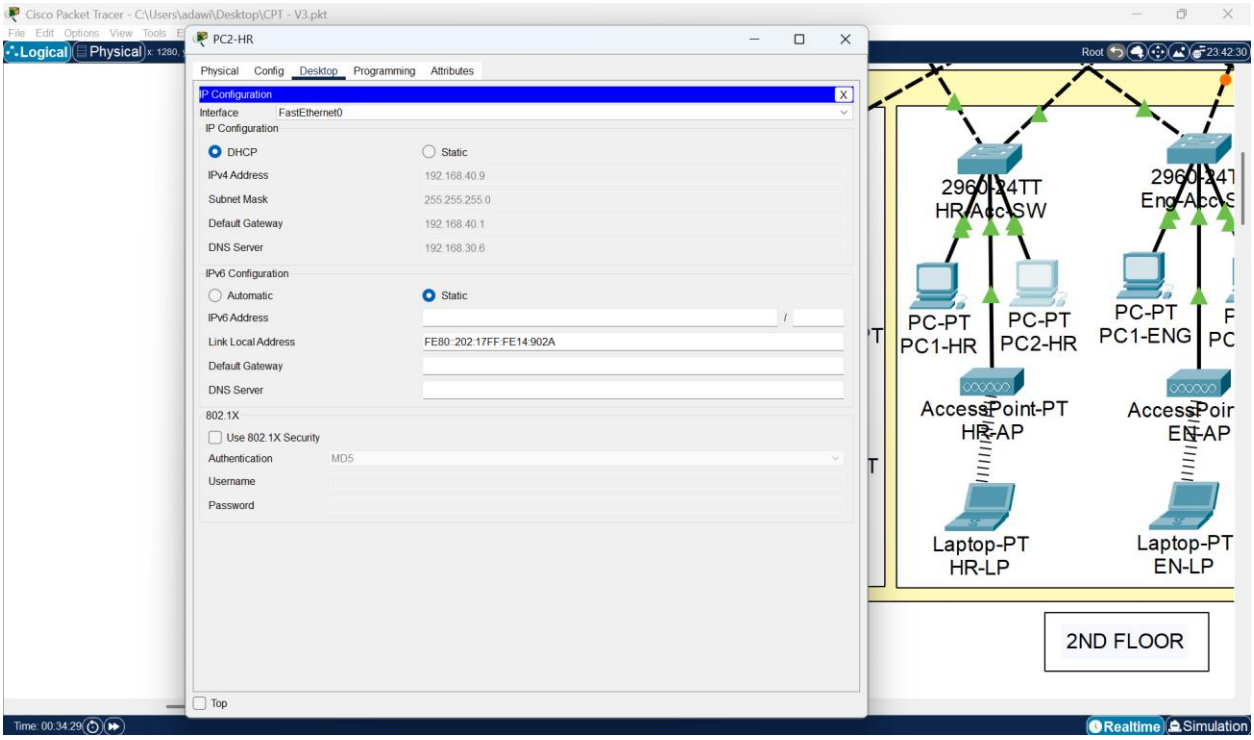


Figure 5.5.31

HR Laptop Configuration DHCP-enabled under VLAN 40. Starting IP: 192.168.40.5, Gateway: 192.168.40.1 and DNS: 192.168.30.6.

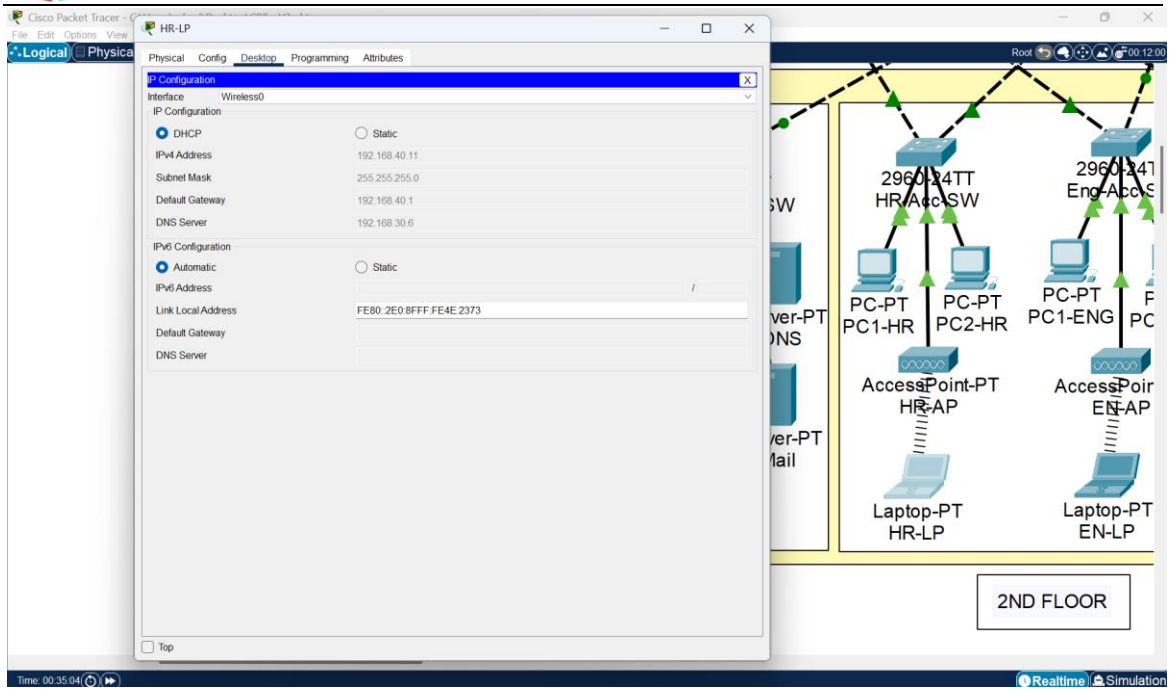


Figure 5.5.32

HR VLAN Access Point Configuration SSID: HR, coverage up to 100 meters. The access point provides wireless connectivity to HR VLAN 40 with a passphrase: cisco123.

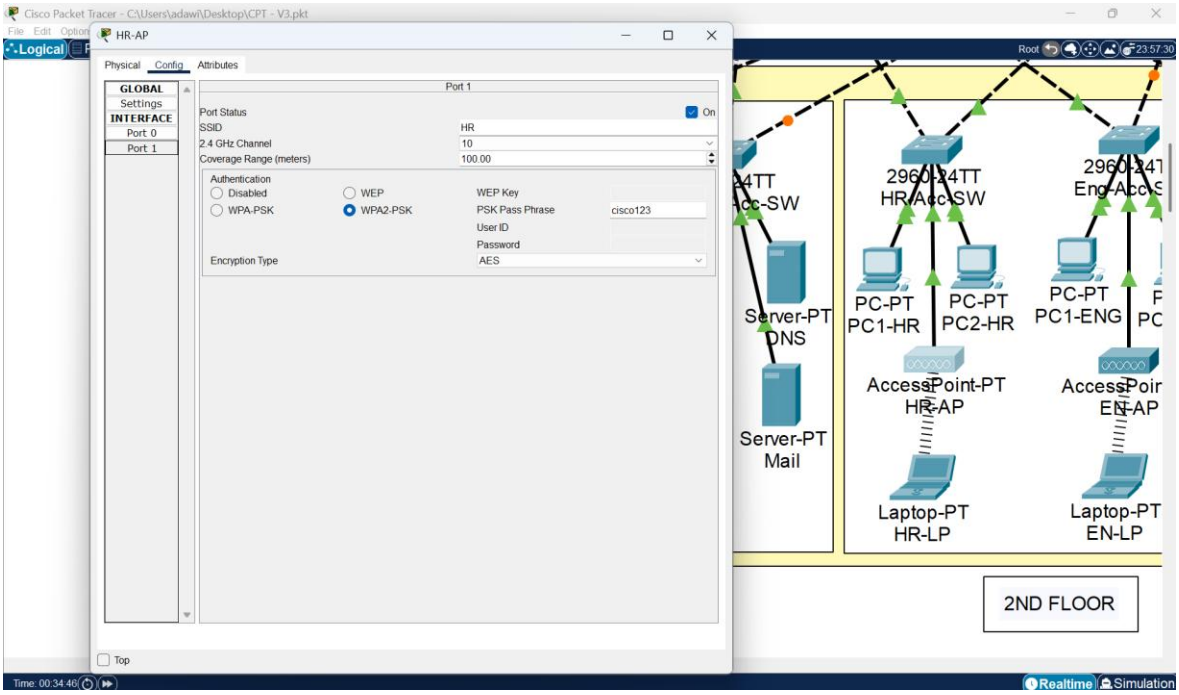
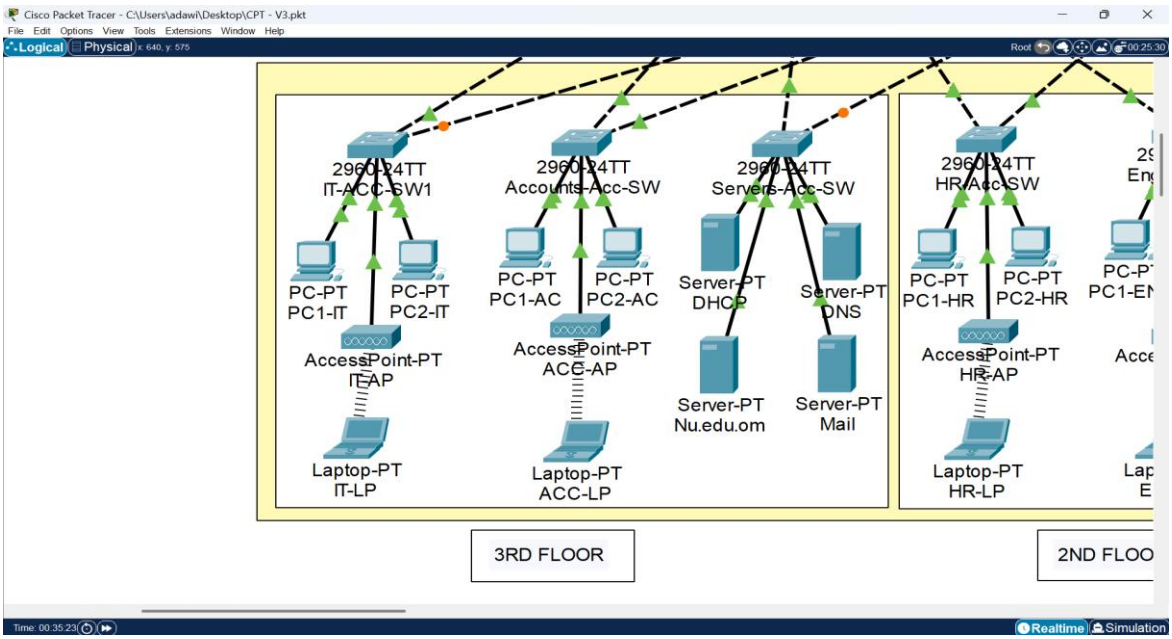


Figure 5.5.33

Third Floor Configuration Departments: VLAN 30 (Servers), VLAN 10 (Accounts), VLAN 20 (IT)



5.5.6. Servers Department (VLAN 30)

Figure 5.5.34

Servers Access Switch Configuration Configured with SSH, DHCP snooping, STP mode, and VLAN 30 port assignments.

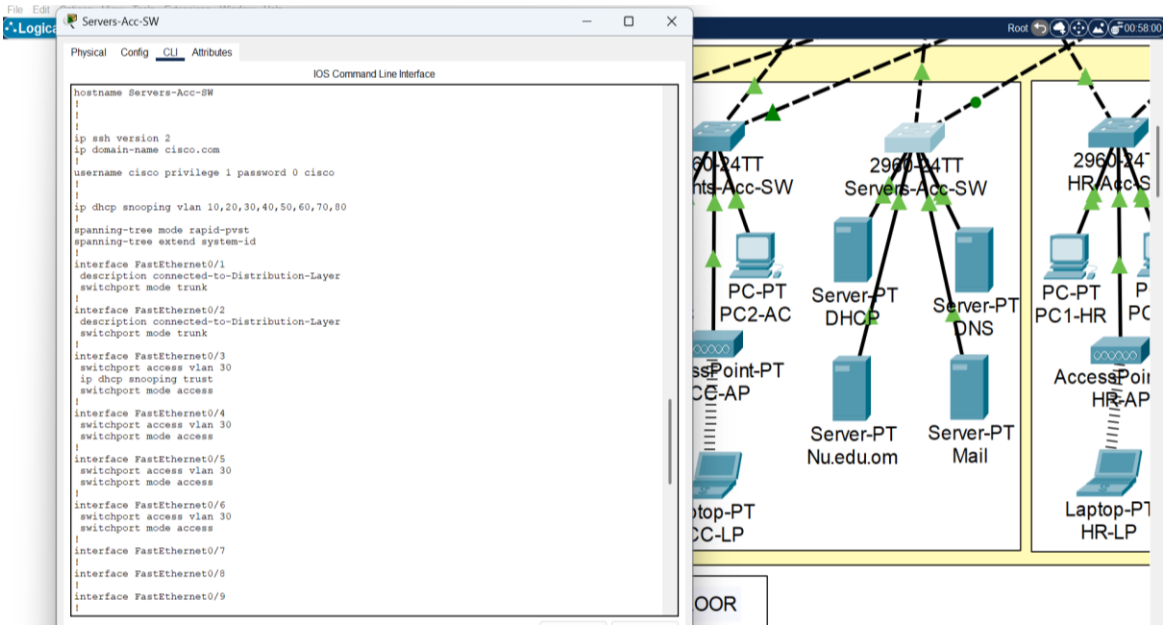


Figure 5.5.35

Servers Switch Management Configuration Includes management VLAN and VTY line settings.

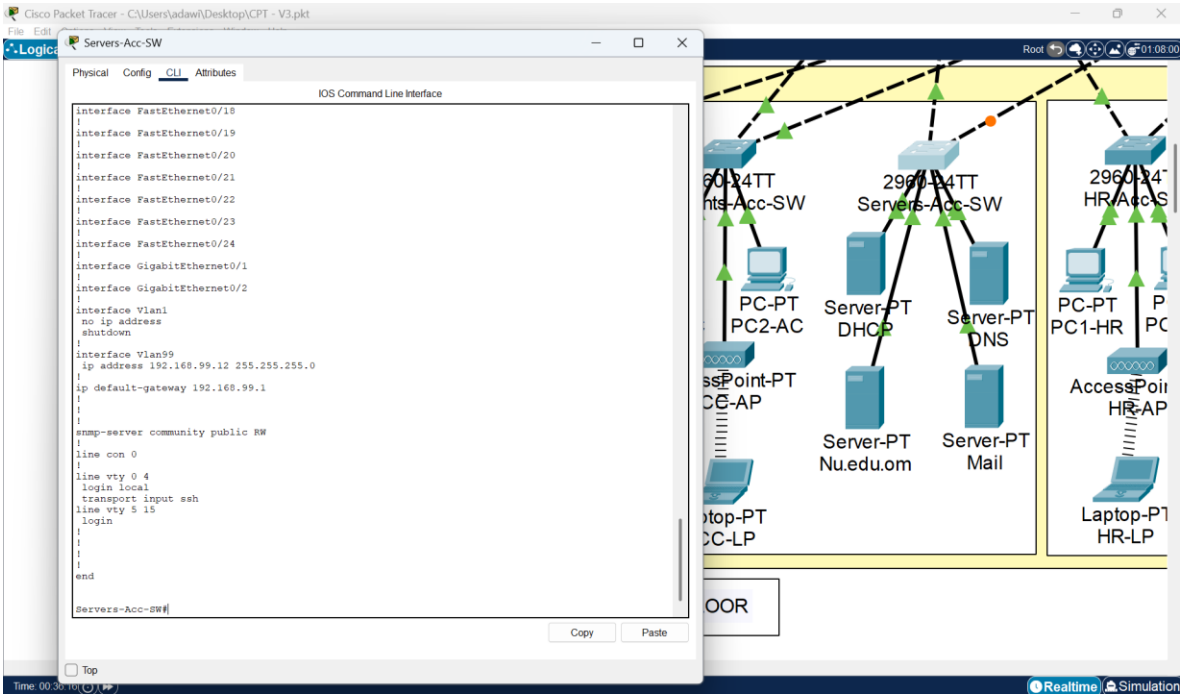


Figure 5.5.36

DHCP Server Configuration Static IP: 192.168.30.5, VLAN 30, Gateway: 192.168.30.1 and DNS: 192.168.30.6.

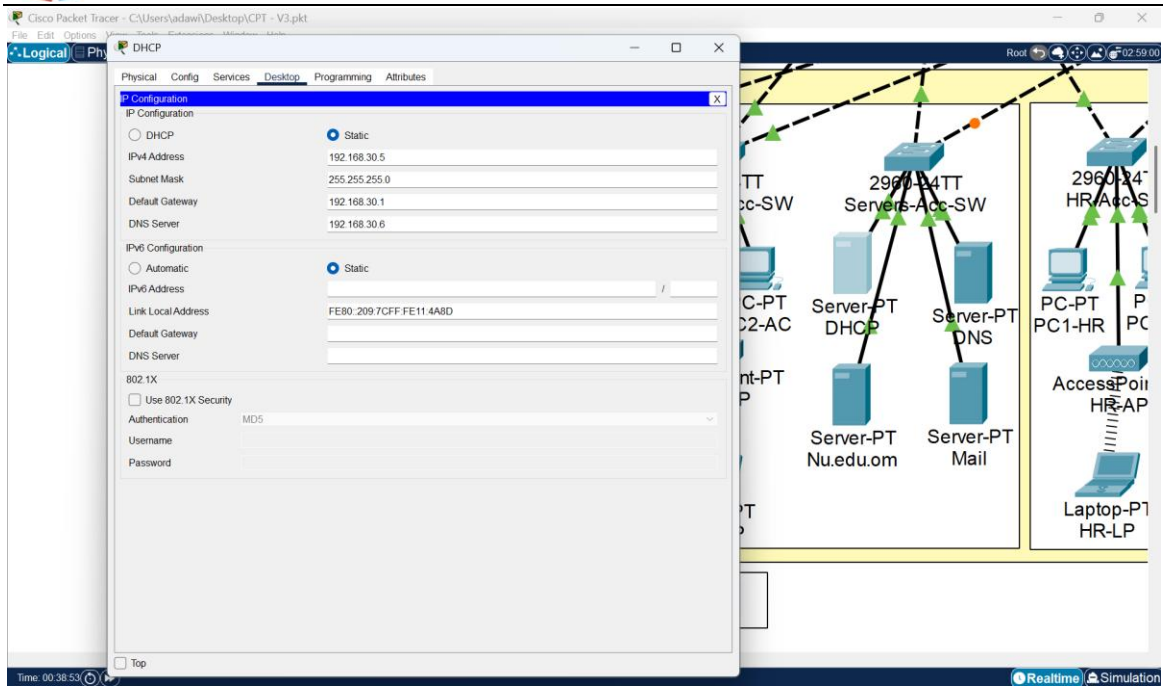
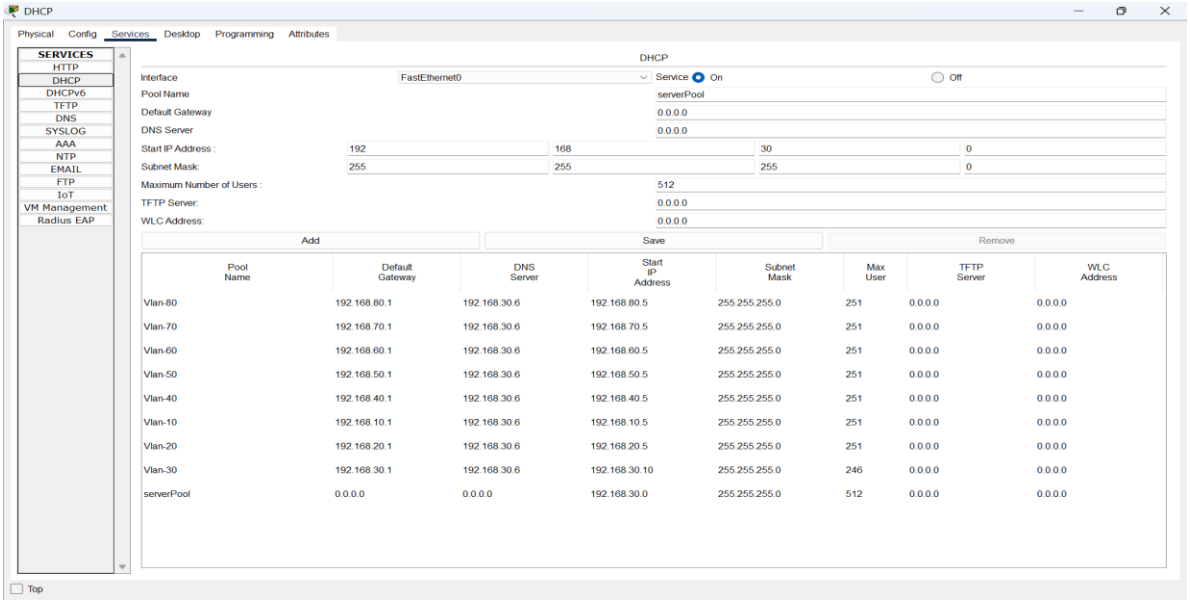


Figure 5.5.37

This figure shows DHCP Server Service Configuration for all VLANs including Default Gateways, DNS Server, Starting IP addresses, Subnet mask and maximum users.



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Vlan-80	192.168.80.1	192.168.30.6	192.168.80.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-70	192.168.70.1	192.168.30.6	192.168.70.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-60	192.168.60.1	192.168.30.6	192.168.60.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-50	192.168.50.1	192.168.30.6	192.168.50.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-40	192.168.40.1	192.168.30.6	192.168.40.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-10	192.168.10.1	192.168.30.6	192.168.10.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-20	192.168.20.1	192.168.30.6	192.168.20.5	255.255.255.0	251	0.0.0.0	0.0.0.0
Vlan-30	192.168.30.1	192.168.30.6	192.168.30.10	255.255.255.0	246	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.30.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Figure 5.5.38

DNS Server Configuration Static IP: 192.168.30.6, VLAN 30, Gateway: 192.168.30.1 and DNS: 192.168.30.6.

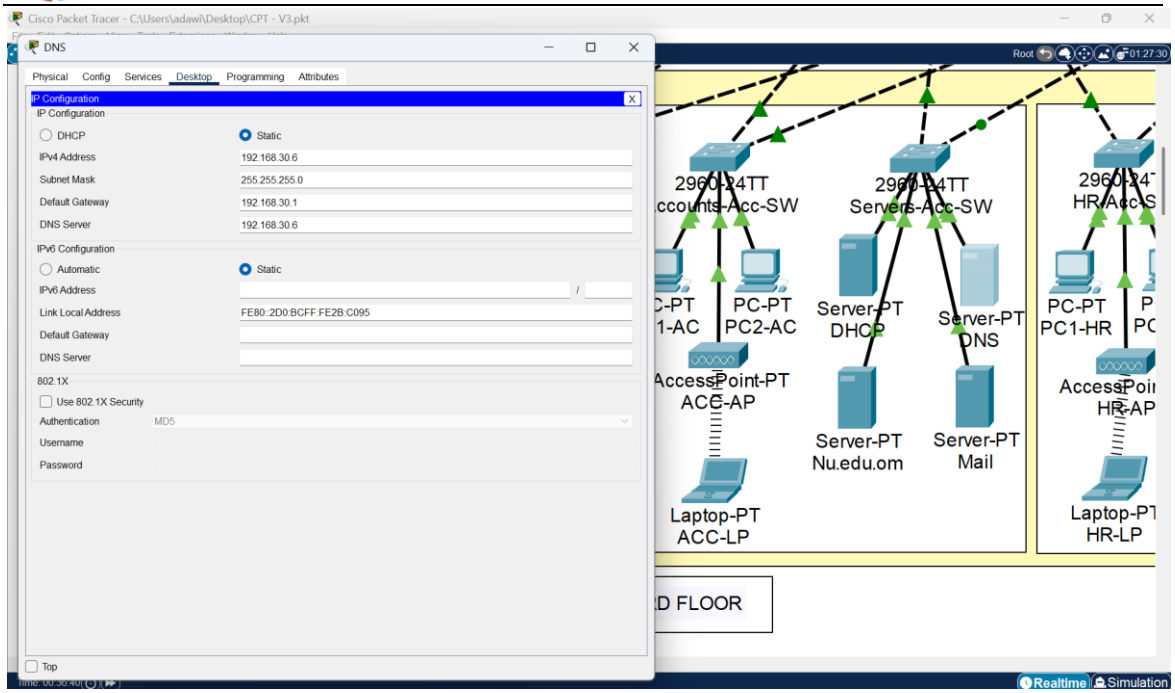


Figure 5.5.39

This figure shows DNS Service Domian name system configuration including 2 records: HRIS IP (192.168.30.6), Nu.edu.om IP (192.168.30.7)

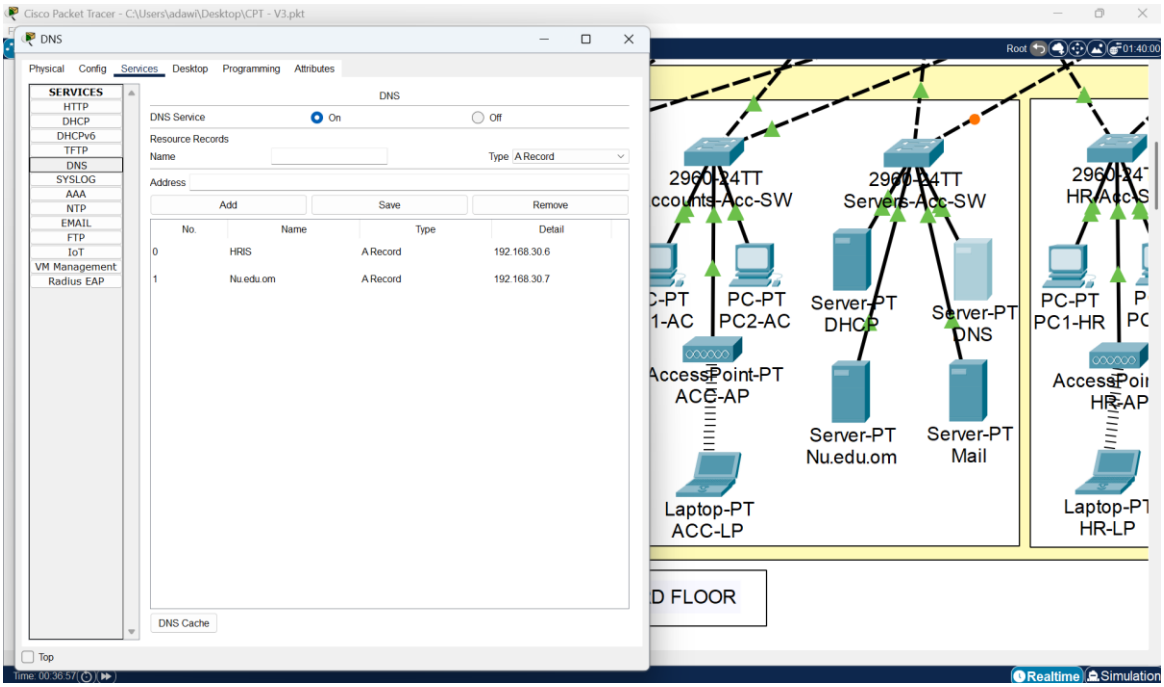


Figure 5.5.40

This figure shows DNS Server HTTP Service HTML code and naming the webpage (HRIS)

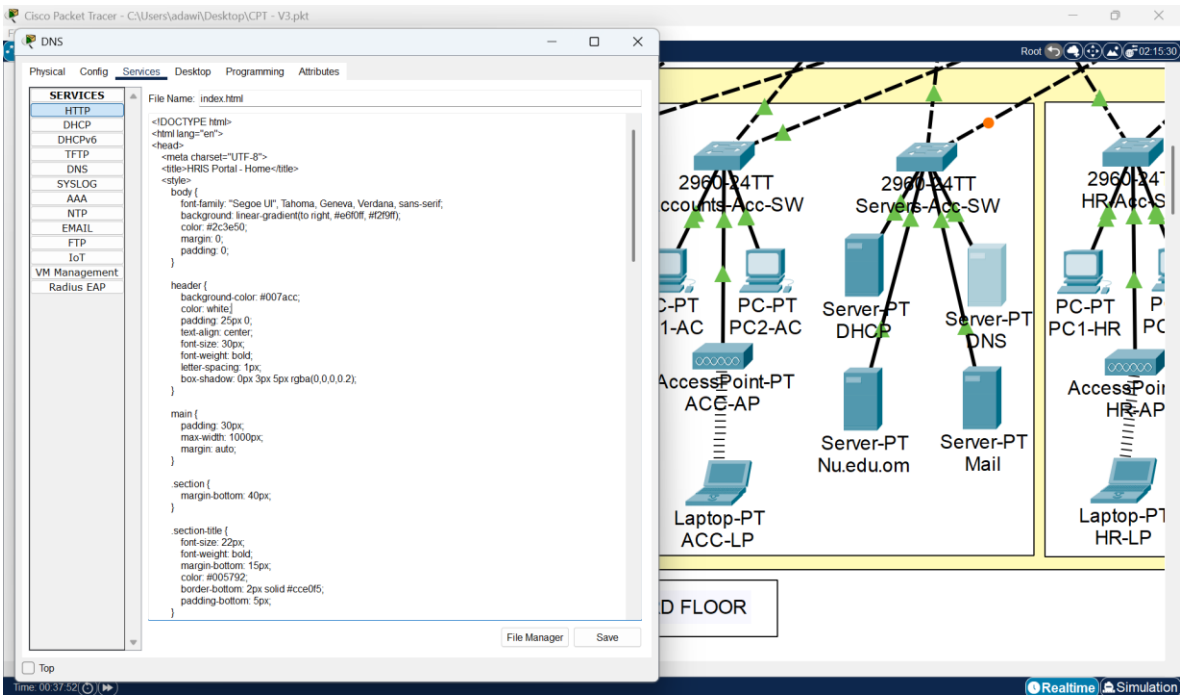


Figure 5.5.41

Mail Server Configuration Static IP: 192.168.30.8, VLAN 30, Gateway: 192.168.30.1 and DNS: 192.168.30.6.

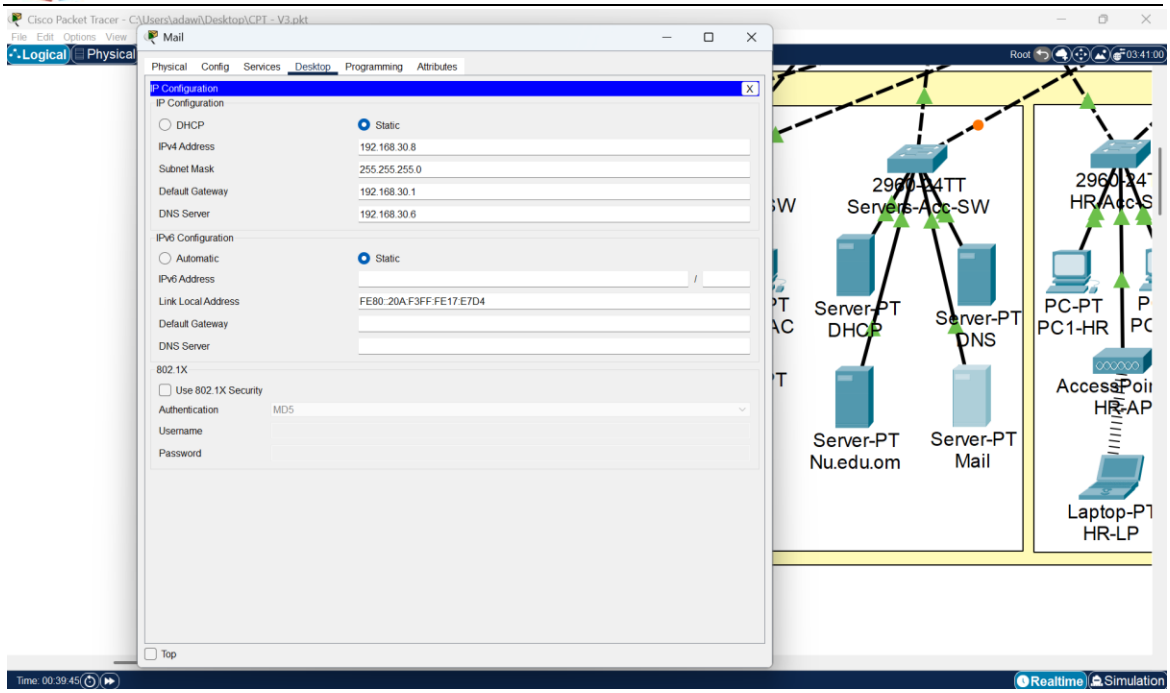


Figure 5.5.42

This figure shows Private Mail Implementation with domain name: nu.edu.om and many users (Students, Staff and Dean) of National University (NU) Oman.

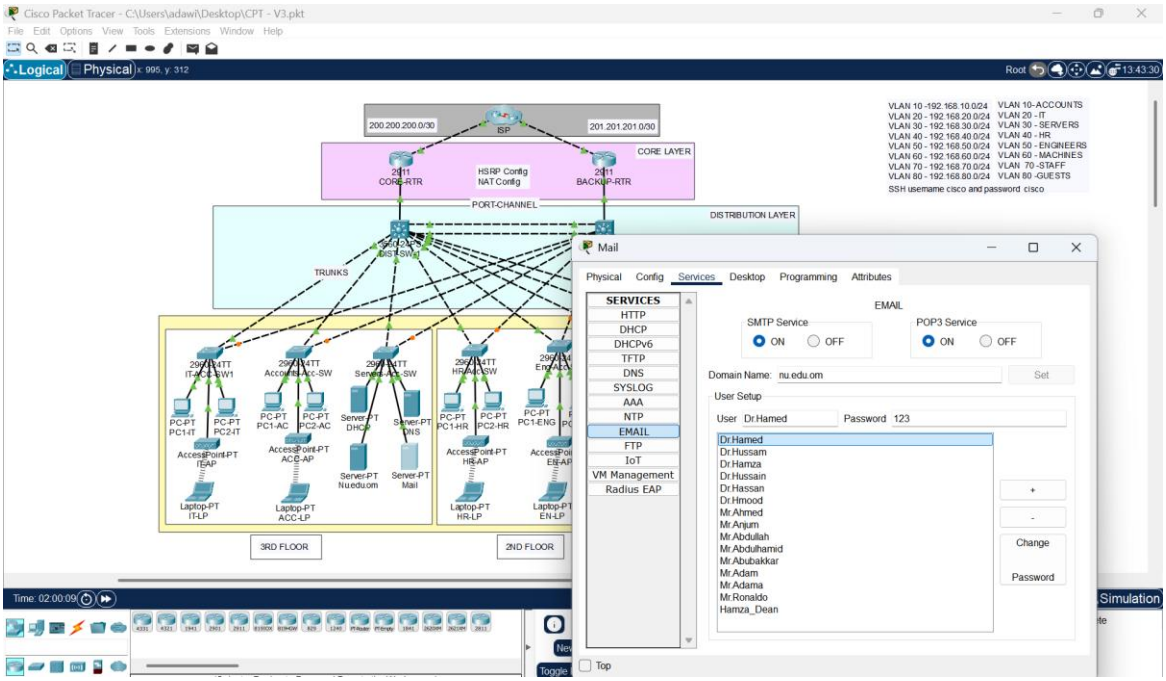


Figure 5.5.43

Web Server (NU.EDU.OM) Configuration Static IP: 192.168.30.7, VLAN 30, Gateway: 192.168.30.1 and DNS 192.168.30.6.

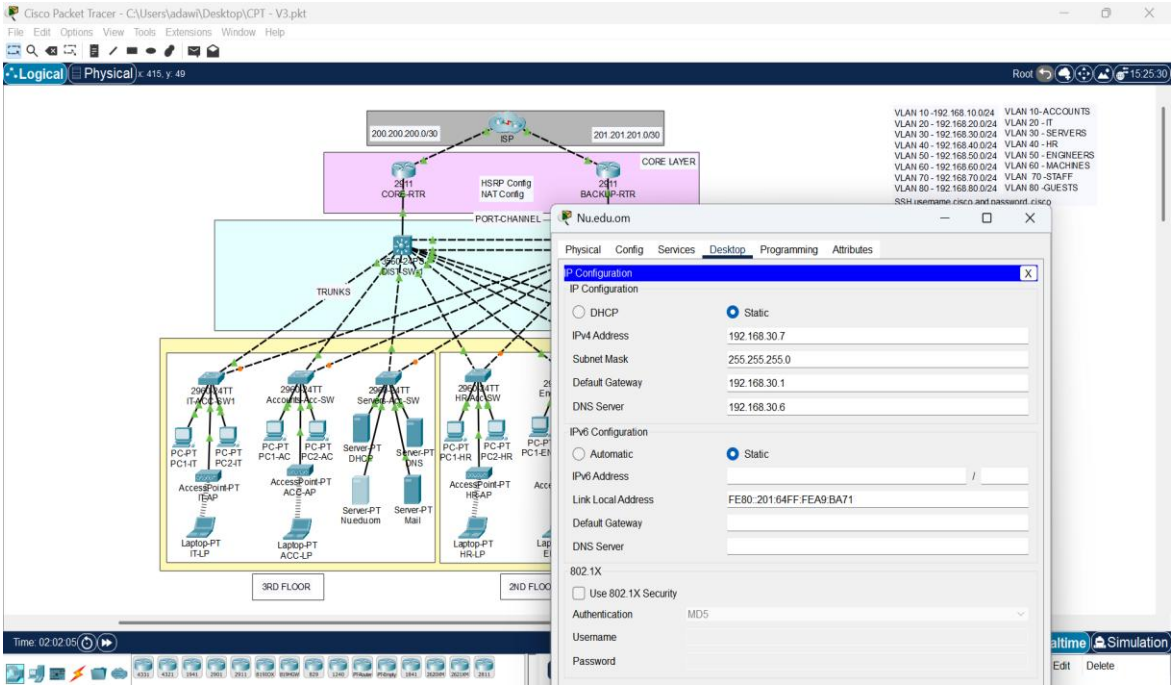
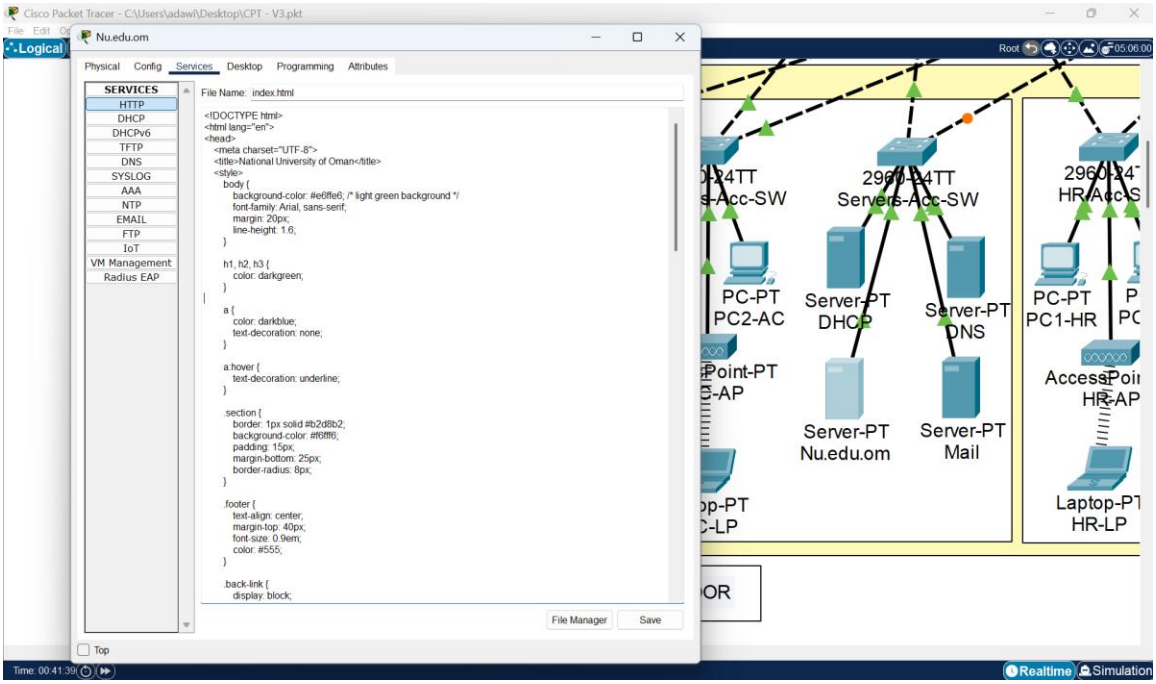


Figure 5.5.44

This figure shows the Web Server (NU.EDU.OM) HTTP Service HTML code and naming the webpage (Nu.edu.om).



5.5.7. Accounts Department (VLAN 10)

Figure 5.5.45

Accounts Access Switch Configuration SSH, DHCP snooping, STP mode, and VLAN 10 port assignment configured.

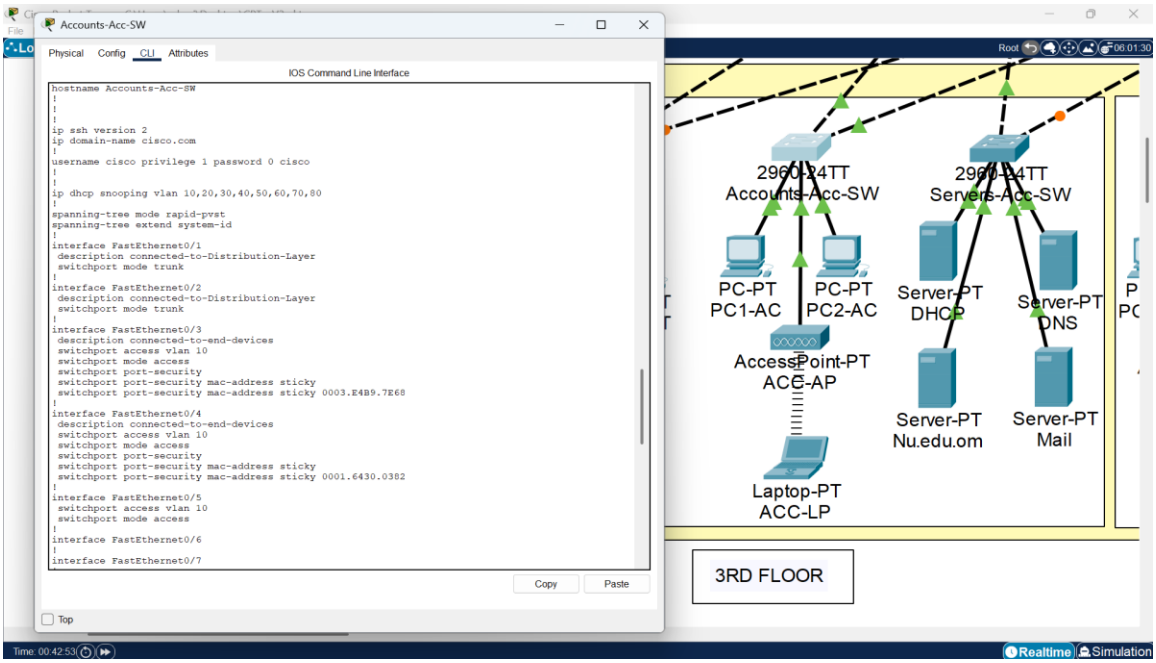


Figure 5.5.46

Accounts Switch Management Configuration Configured with management VLAN and VTY access.

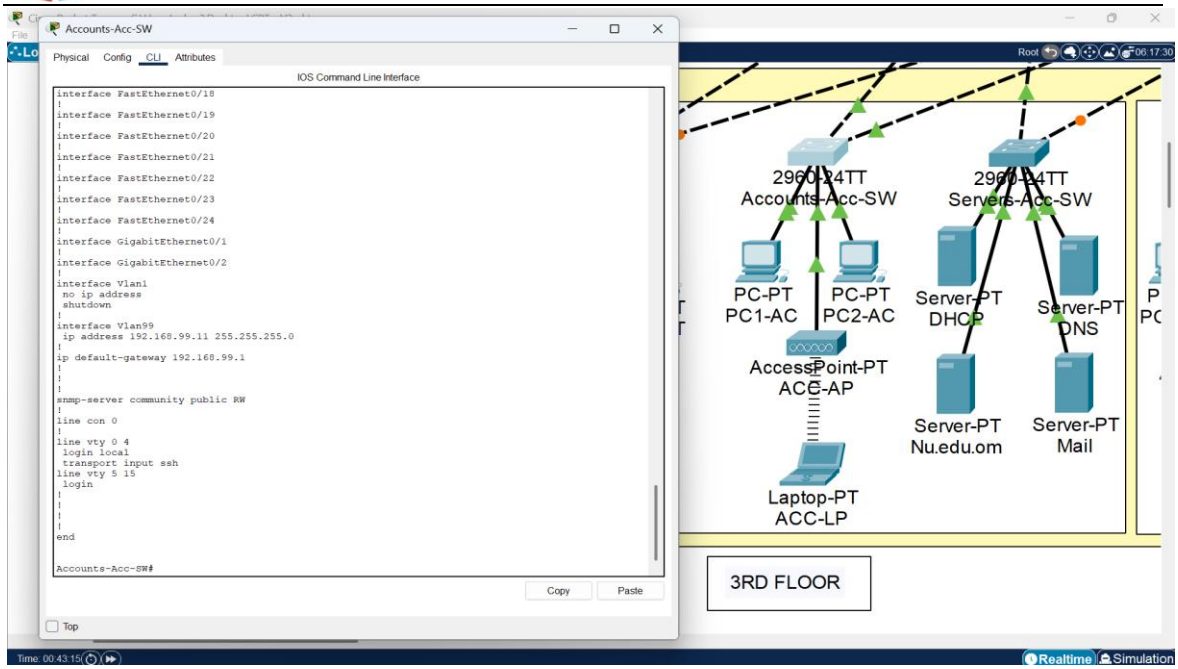


Figure 5.5.47

Accounts PC1 Configuration DHCP enabled, Starting IP: 192.168.10.5, Gateway: 192.168.10.1 and DNS: 192.168.30.6.

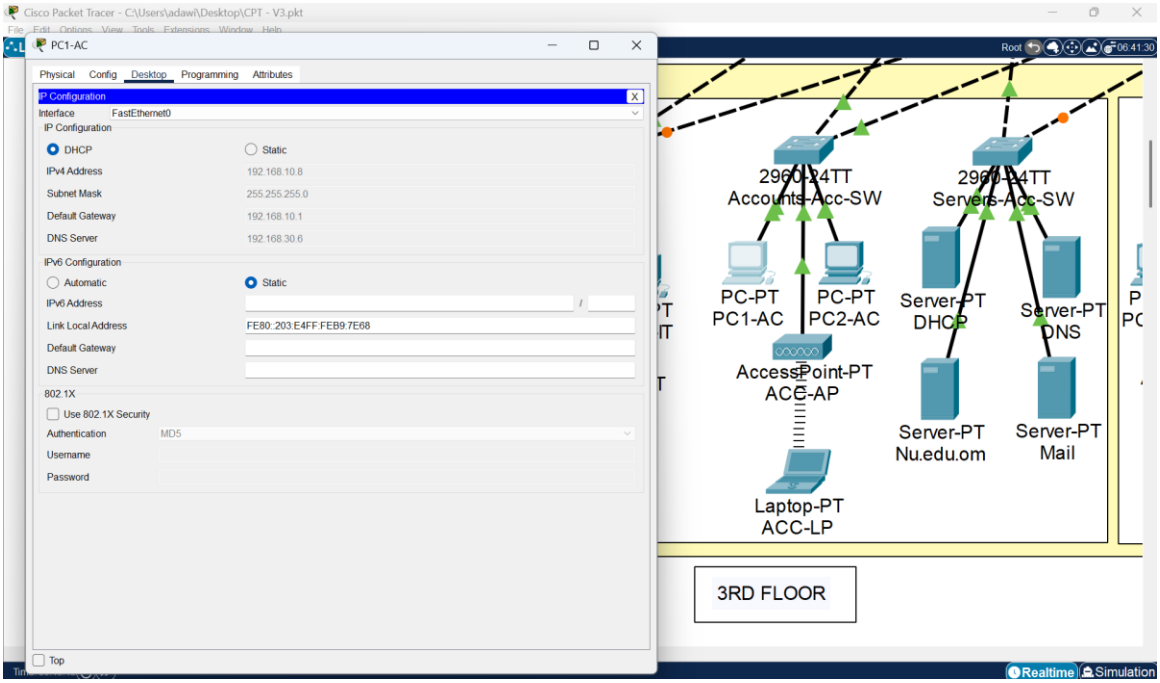


Figure 5.5.48

Accounts PC2 Configuration DHCP enabled, Starting IP: 192.168.10.5, Gateway: 192.168.10.1 and DNS: 192.168.30.6.

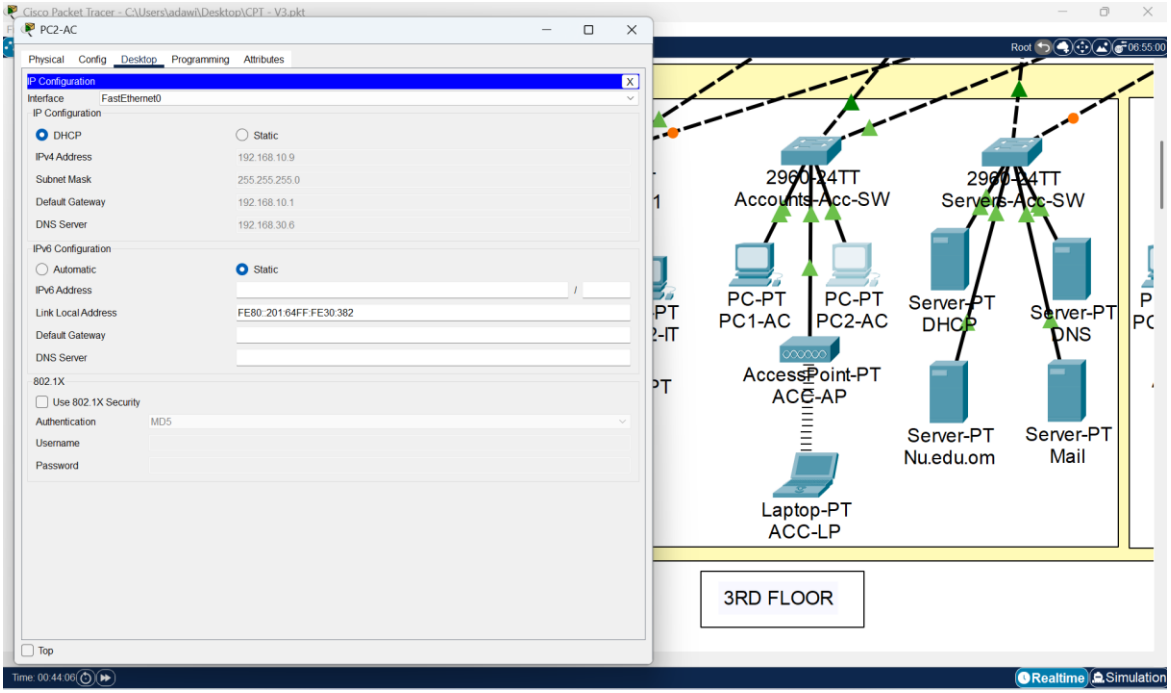


Figure 5.5.49

Accounts Laptop Configuration Same as PC1. DHCP, Starting IP: 192.168.10.5, Gateway: 192.168.10.1 and DNS: 192.168.30.6.

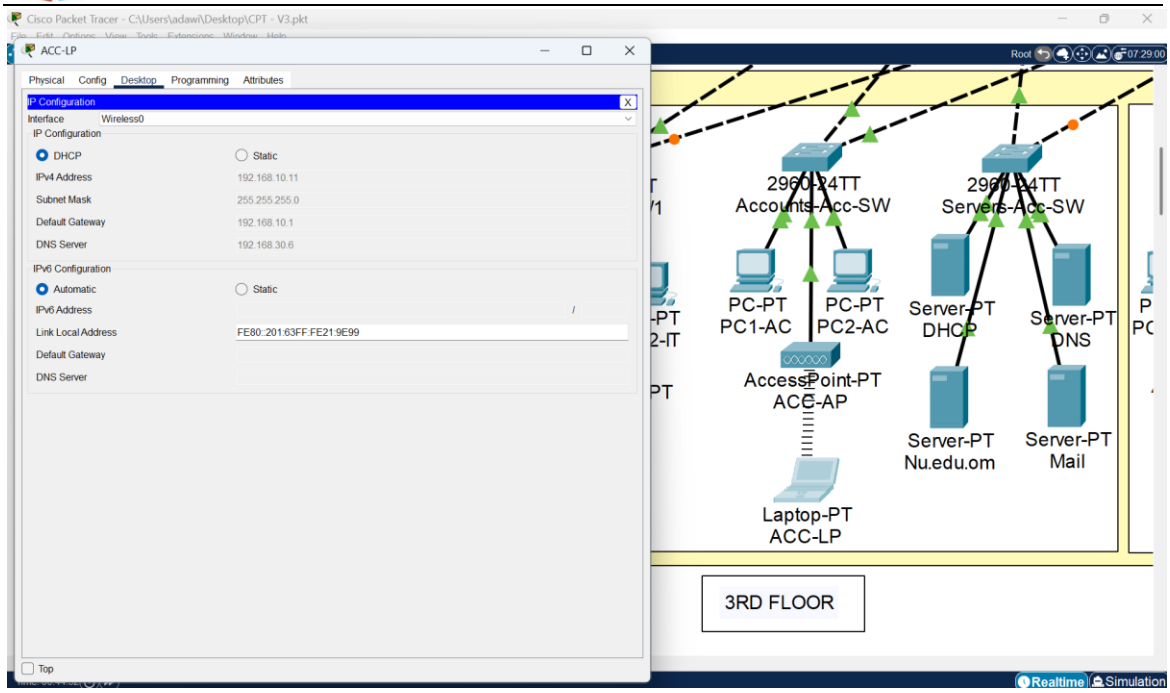
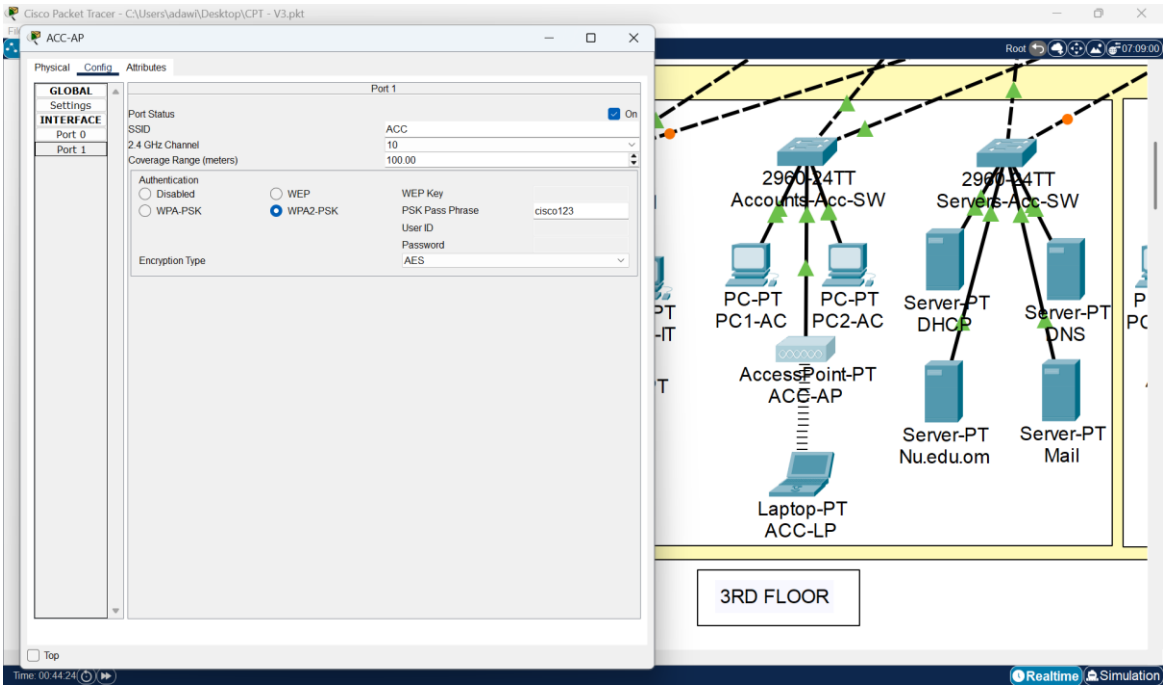


Figure 5.5.50

Accounts VLAN Access Point Configuration SSID: AC, coverage up to 100 meters. Provides wireless access to VLAN 10 using passphrase: cisco1234.



5.5.8. IT Department (VLAN 20)

Figure 5.5.51

IT Access Switch Configuration SSH, DHCP snooping, STP mode, and VLAN 20 port assignments configured.

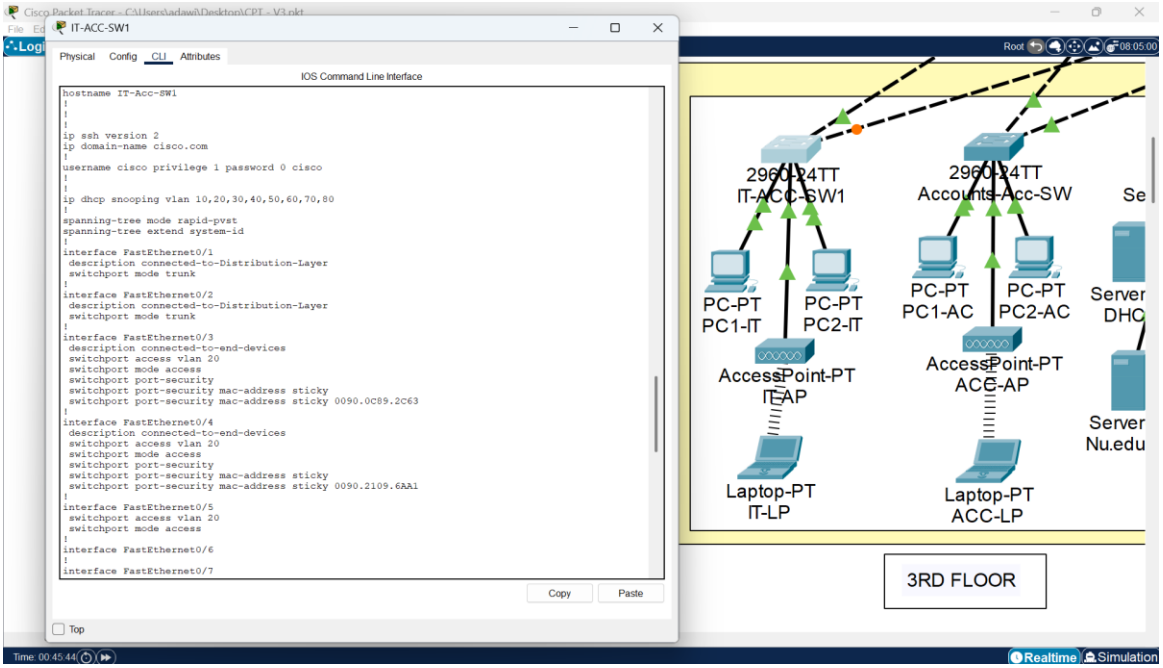


Figure 5.5.52

IT Switch Management Configuration Configured with management VLAN and VTY.

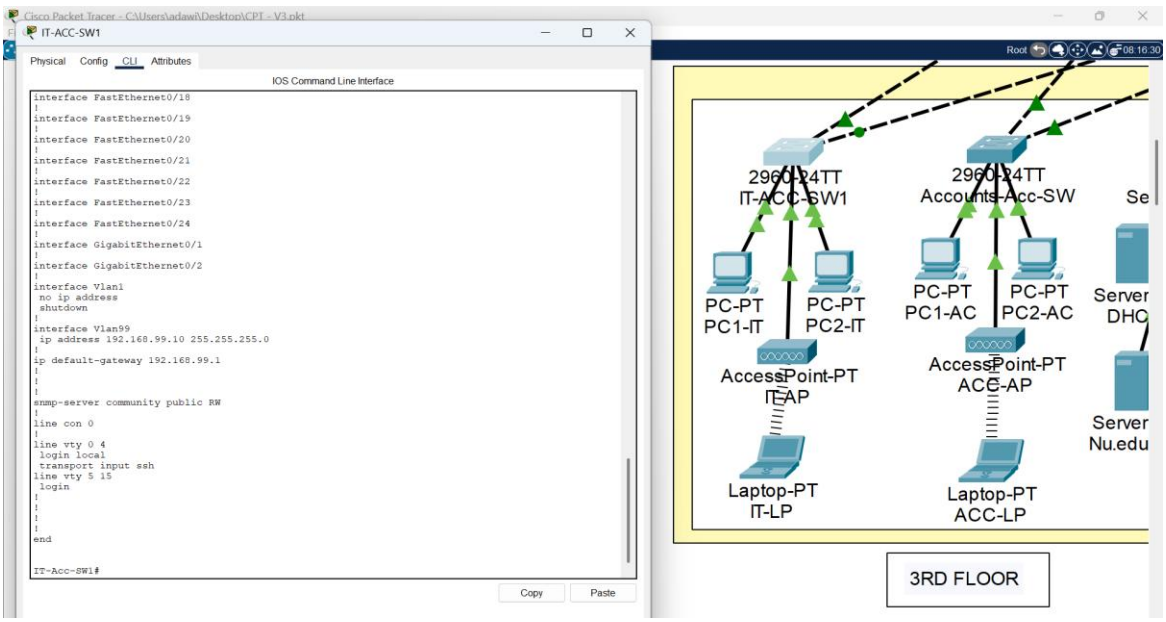


Figure 5.5.53

IT PC1 Configuration DHCP enabled, Starting IP: 192.168.20.5, Gateway: 192.168.20.1 and DNS: 192.168.30.6.

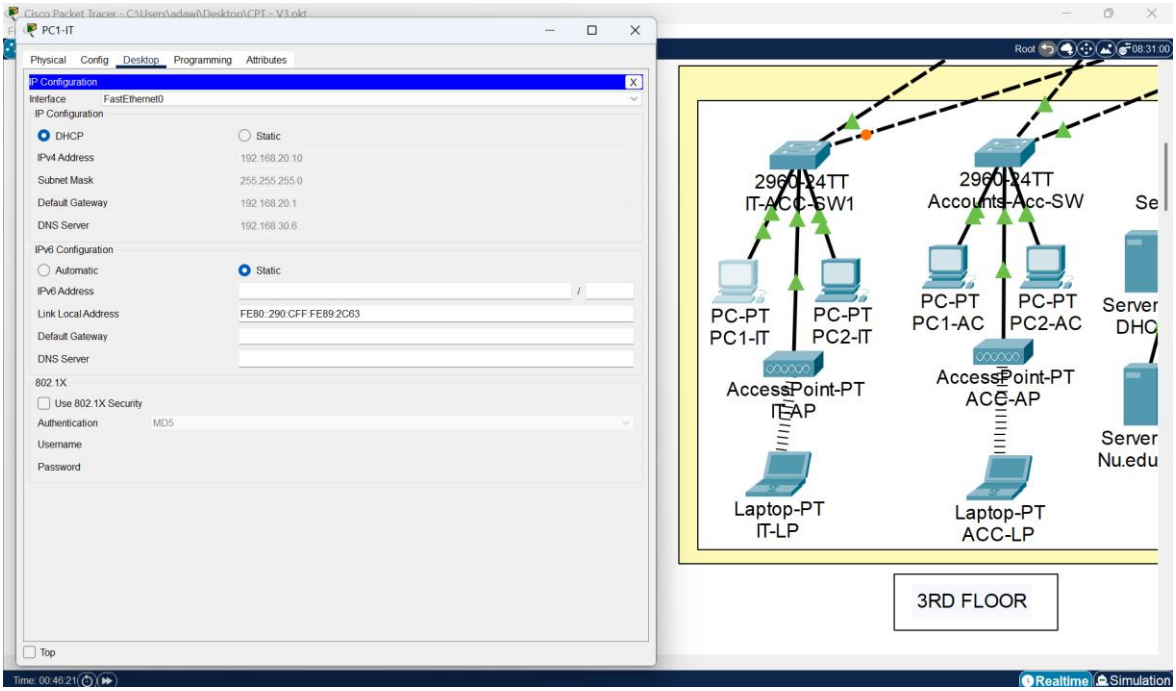


Figure 5.5.54

IT Laptop Configuration Configured via DHCP, Starting IP: 192.168.20.5, Gateway: 192.168.20.1 and DNS: 192.168.30.6.

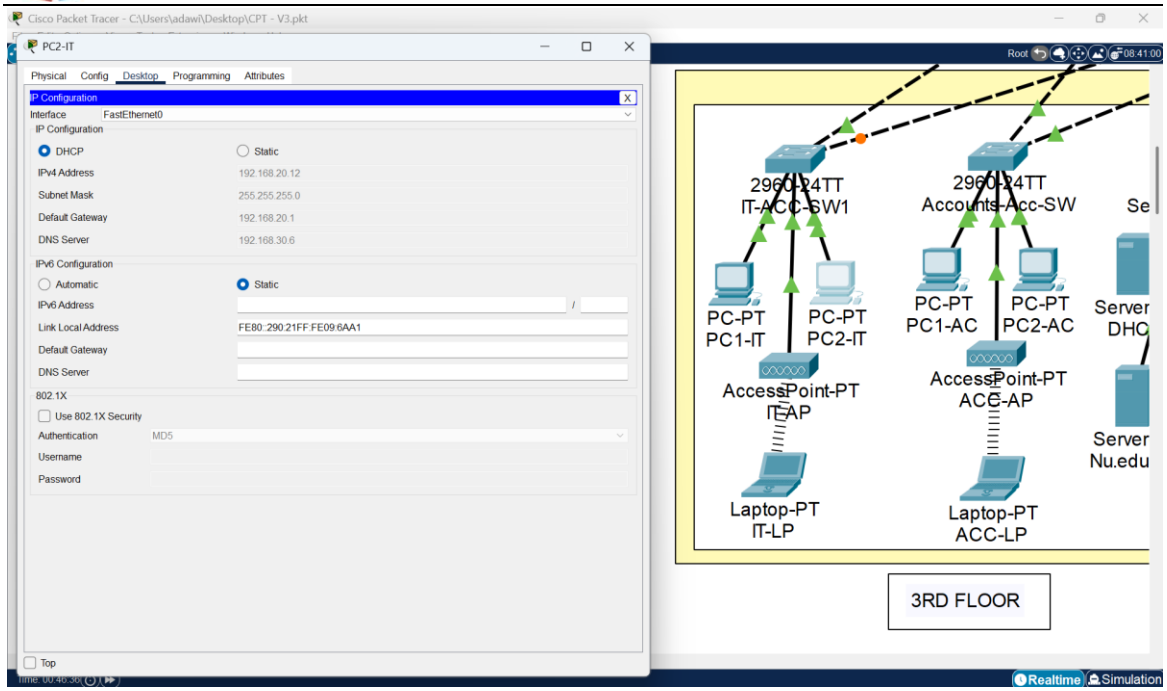


Figure 5.5.55

IT Laptop Configuration Configured via DHCP, Starting IP: 192.168.20.5, Gateway: 192.168.20.1 and DNS: 192.168.30.6.

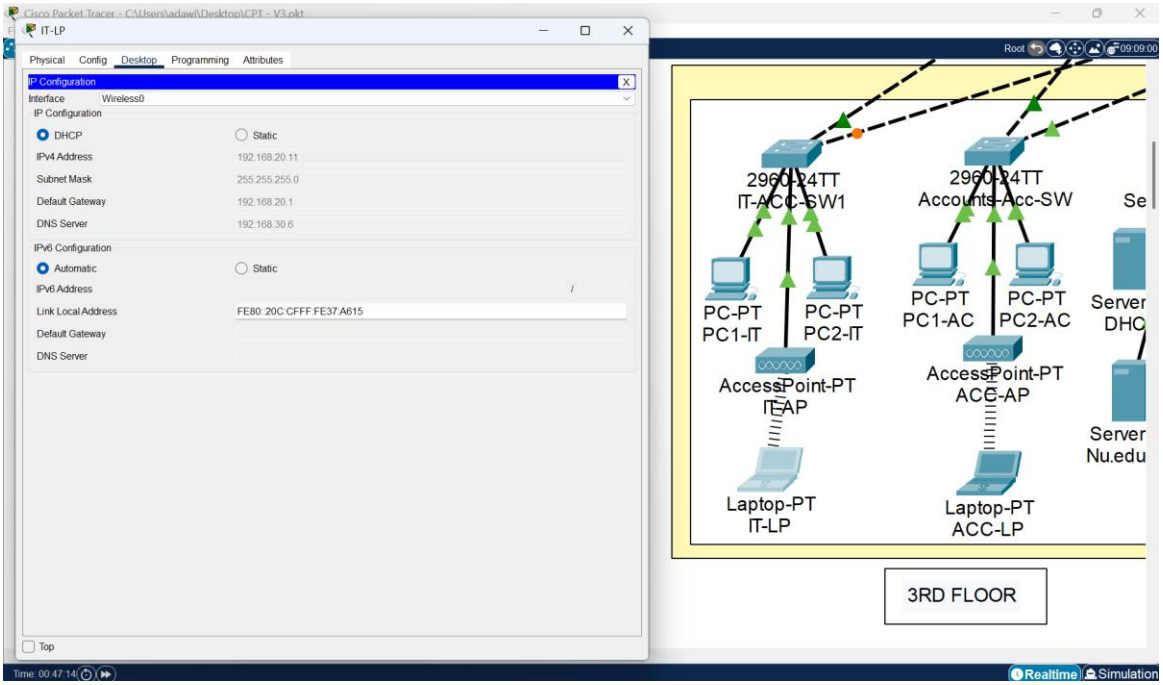
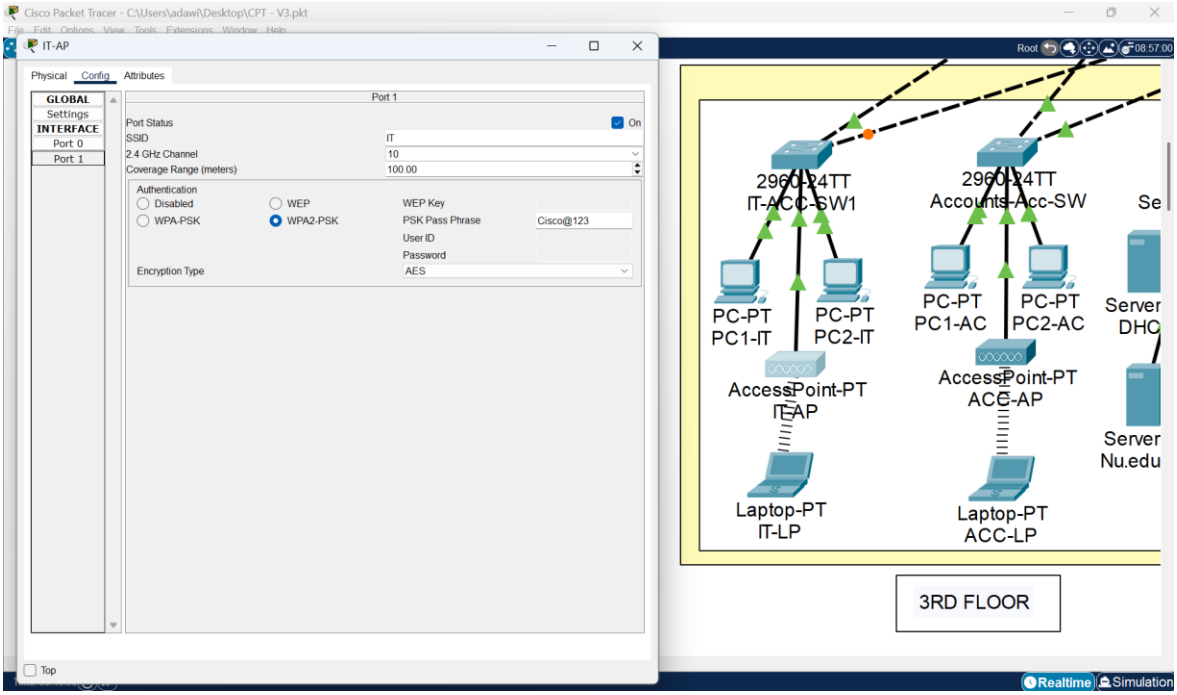


Figure 5.5.56

IT VLAN Access Point Configuration SSID: IT, coverage up to 100 meters. The access point provides wireless access to VLAN 20 using passphrase: cisco@123.



5.5.9. Network Distribution Layer

Figure 5.5.57

Hostname set and SSH enabled usage of domain name and crypto key for secure remote access. and routing between access switches and core routers.

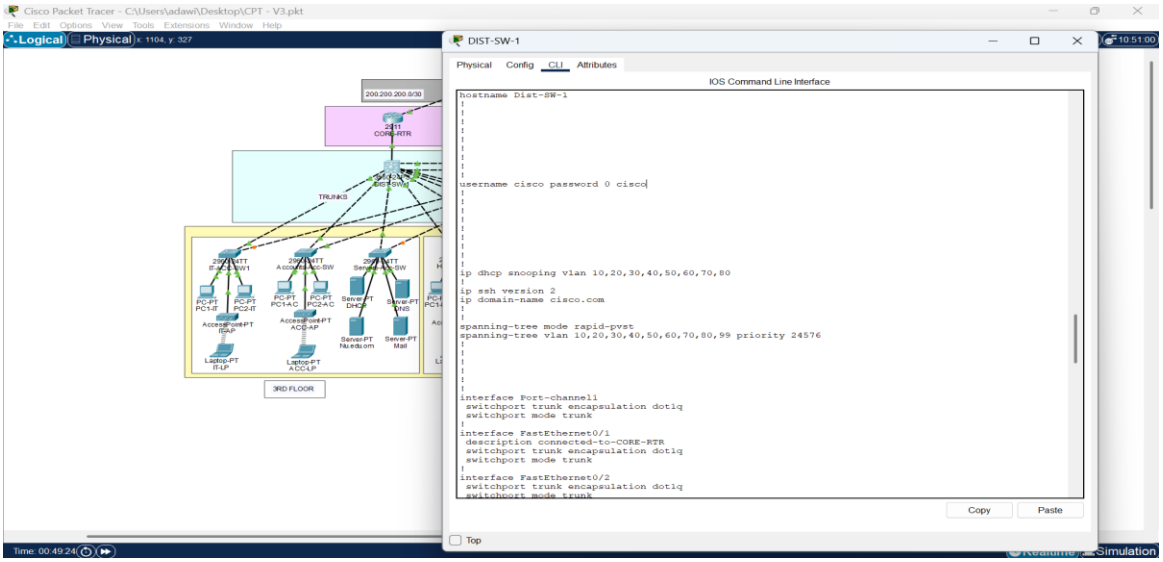


Figure 5.5.58

Trunk ports configured on uplinks; all VLANs allowed for inter-switch communication.

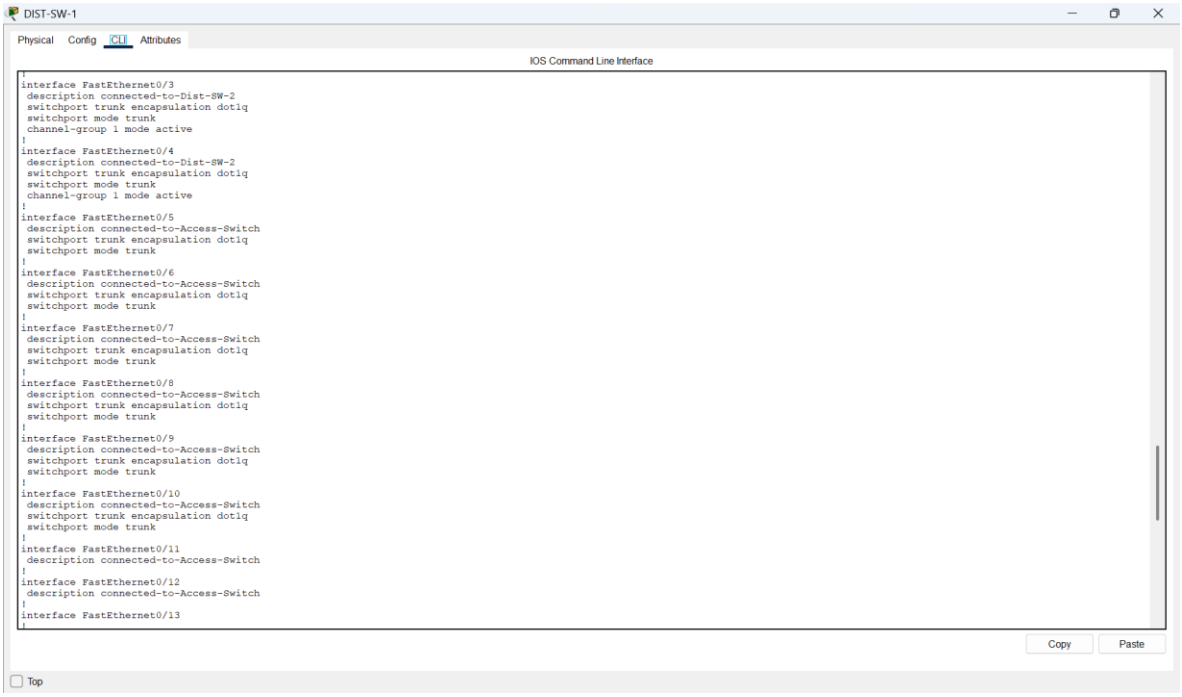


Figure 5.5.59

VLAN 99 created with specific mac-address for management and IP assigned. SSH lines managed

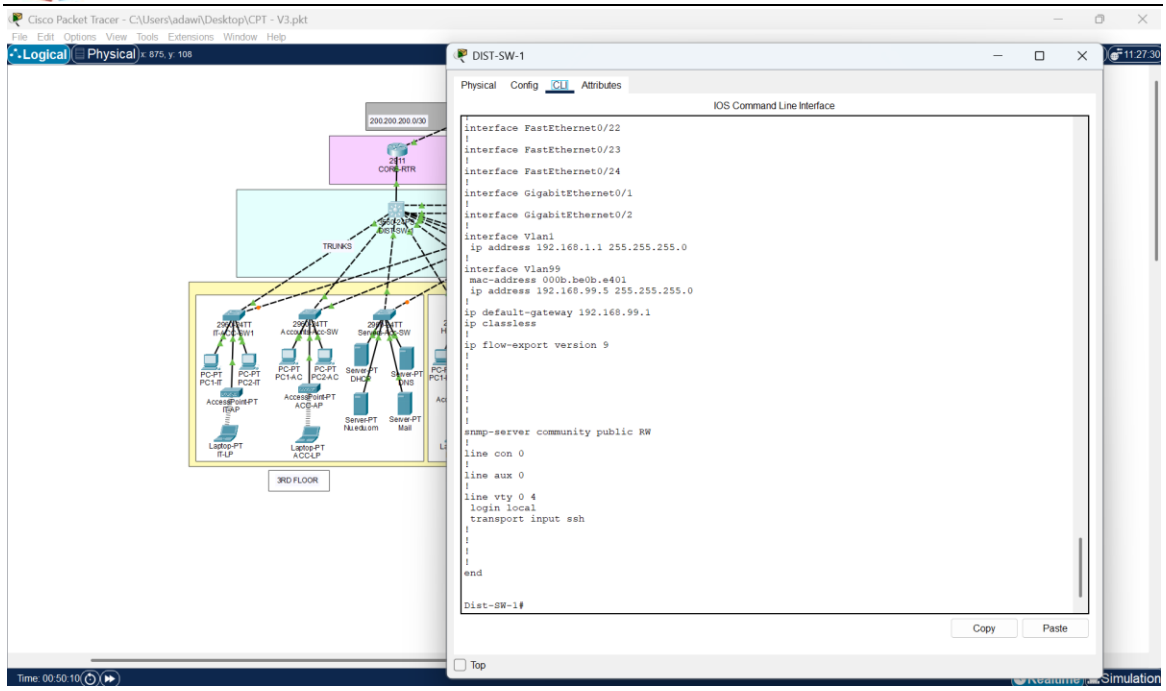


Figure 5.5.60

Hostname configured and SSH enabled with domain name and crypto key for secure access. also configured with HSRP and routing capabilities.

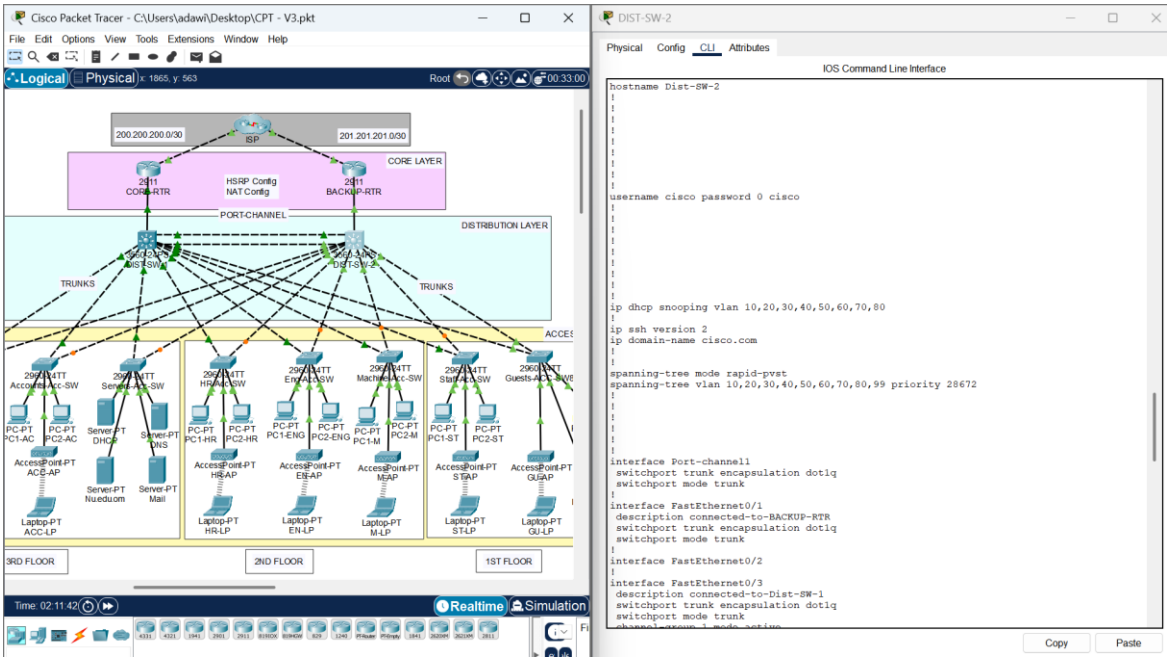


Figure 5.5.61

Trunk links established on uplink ports; all VLANs allowed for access and core connectivity.

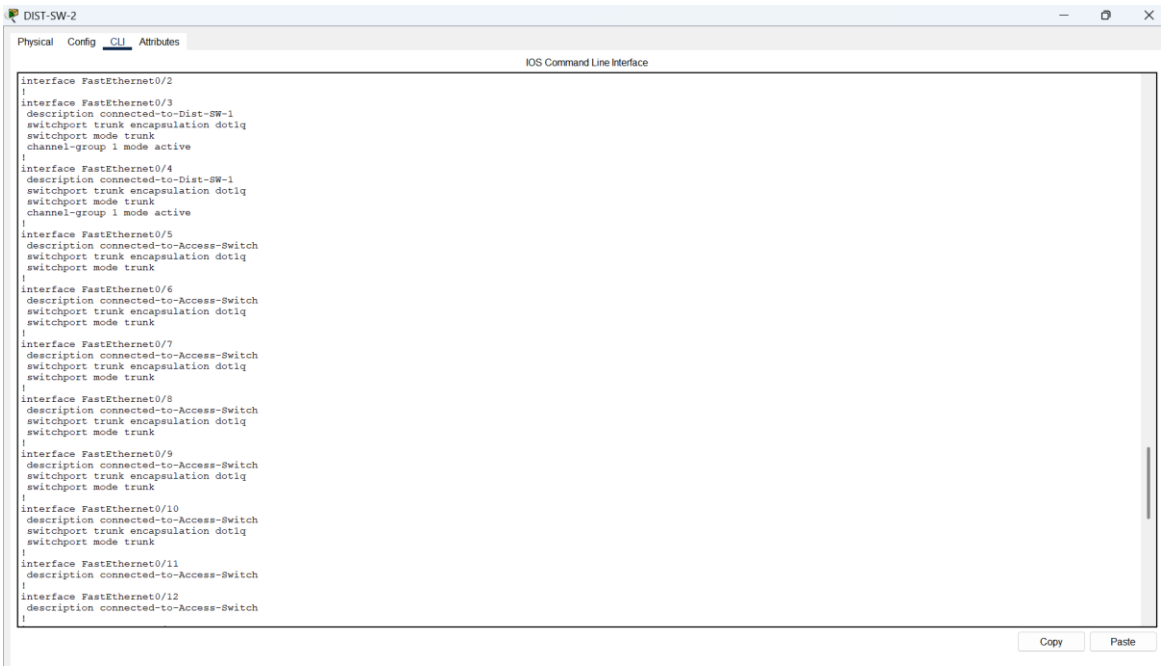
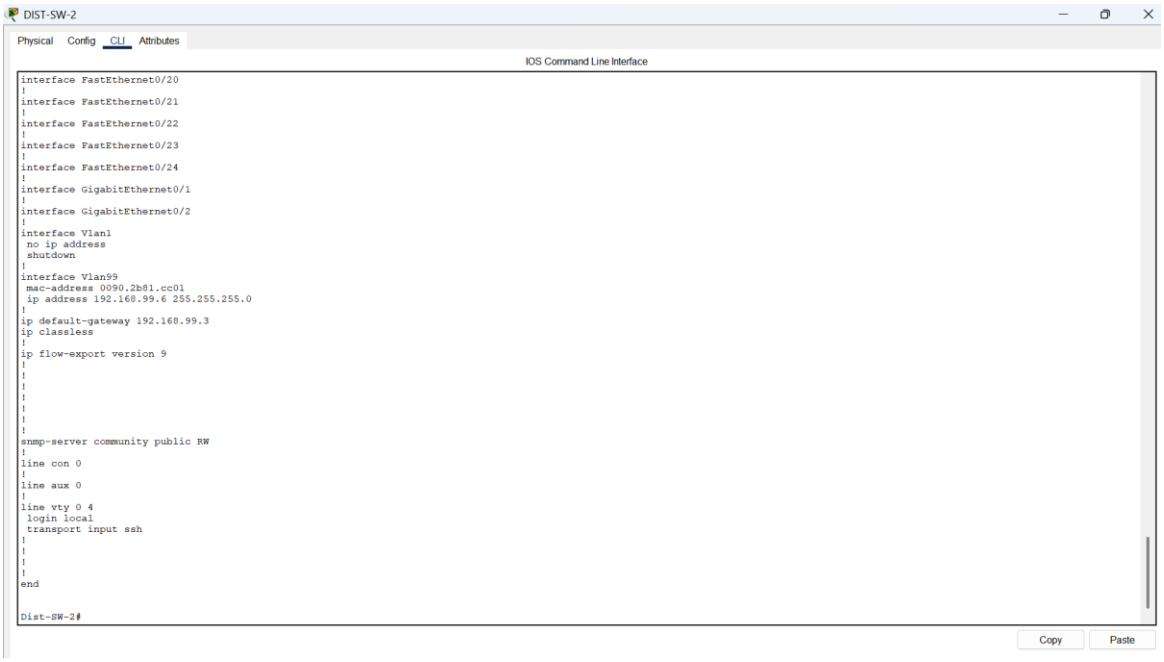


Figure 5.5.62

VLAN 99 created with specific mac-address for management and IP assigned. SSH lines managed



5.5.10. Network Core layer

Figure 5.5.63

Hostname CORE-RTR set, SSH enabled with domain name and version 2, local login created for secure remote access. Connected to both distribution switches.

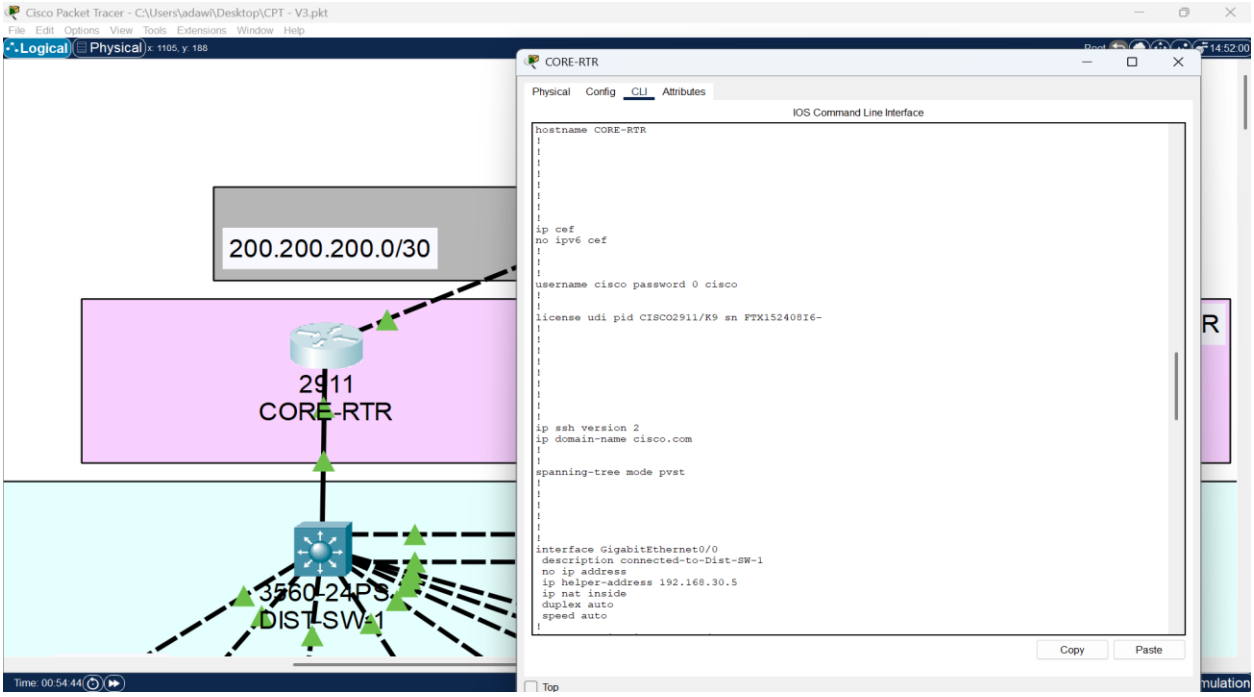


Figure 5.5.64

Sub-interfaces configured with dot1Q encapsulation and IPs for VLANs 10–99; HSRP and IP helper addresses enabled.

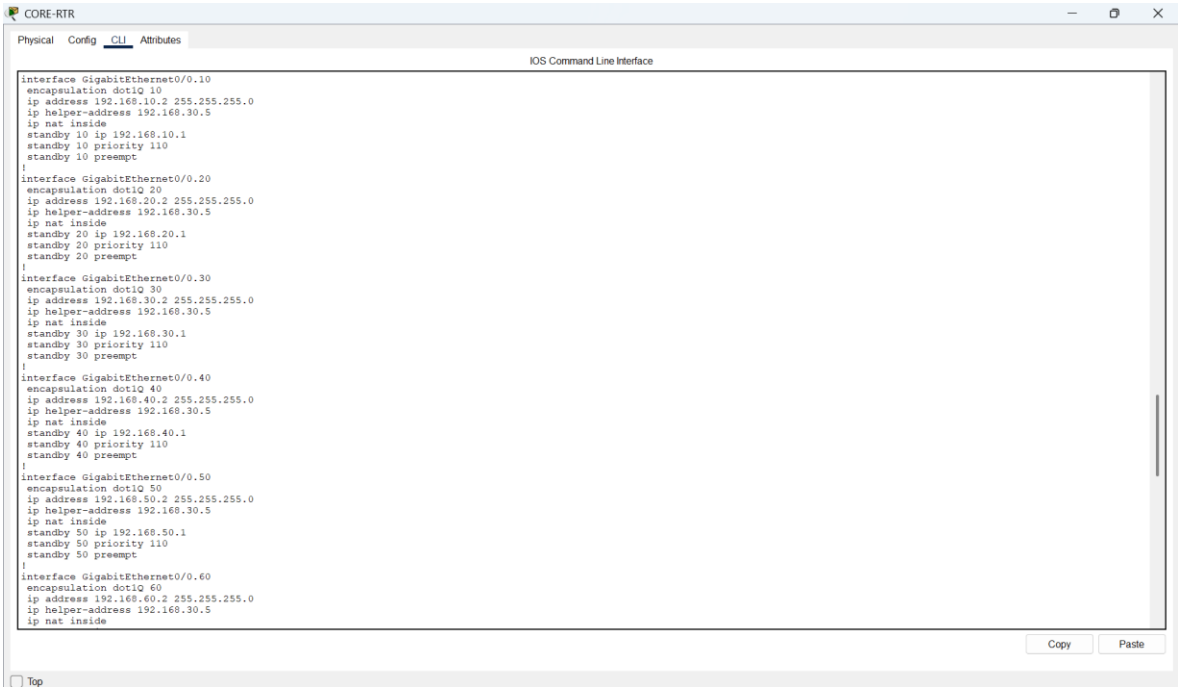


Figure 5.5.65

Sub-interfaces configured with dot1Q encapsulation and IPs for VLANs 10–99; HSRP and IP helper addresses enabled.

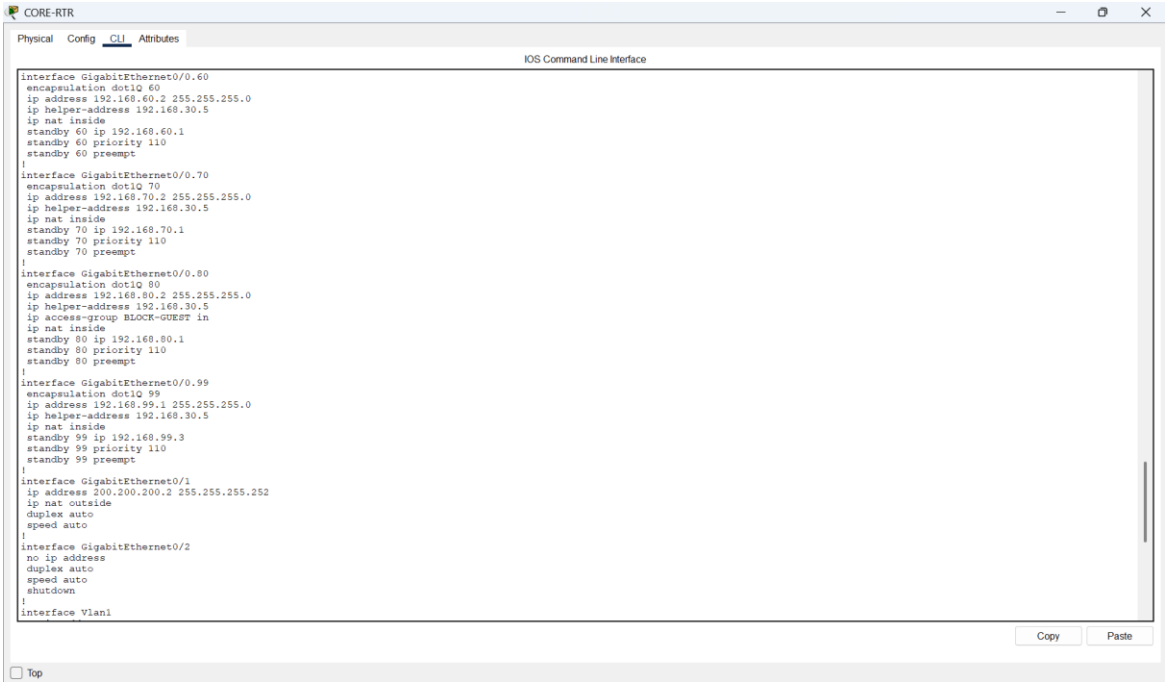


Figure 5.5.66

VLAN 99 used for management with IP 192.168.99.1; SSH and NAT restricted through ACLs and VLAN-specific settings.

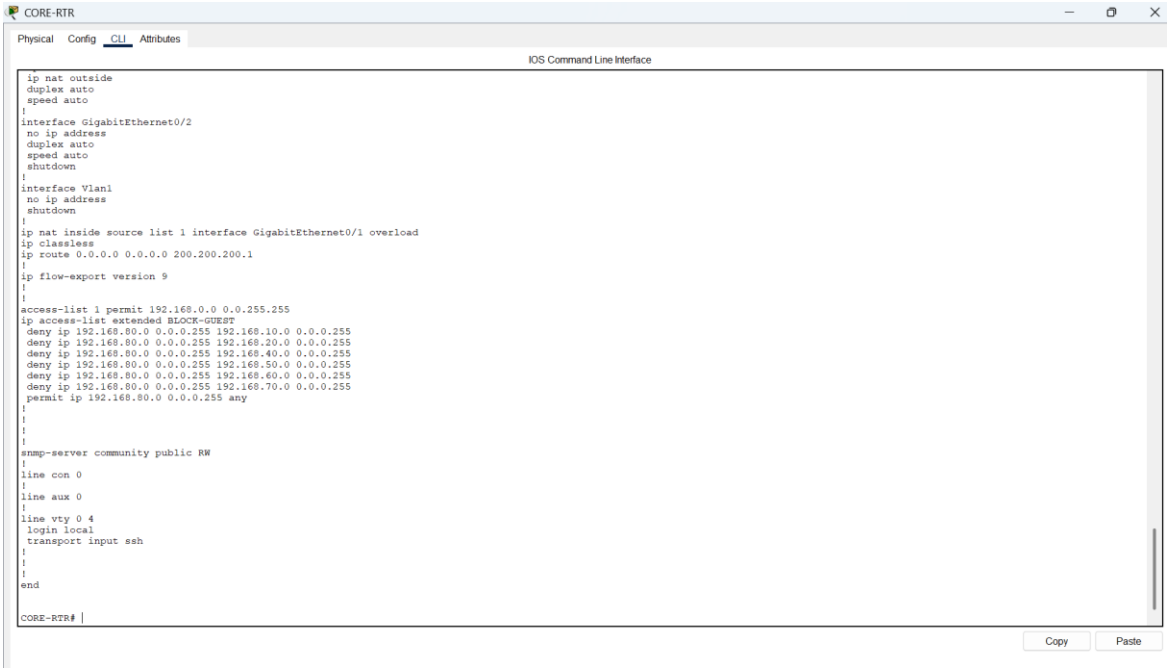


Figure 5.5.67

Hostname BACKUP-RTR configured; SSH enabled with domain name and local login for secure access. Connected to both distribution switches.

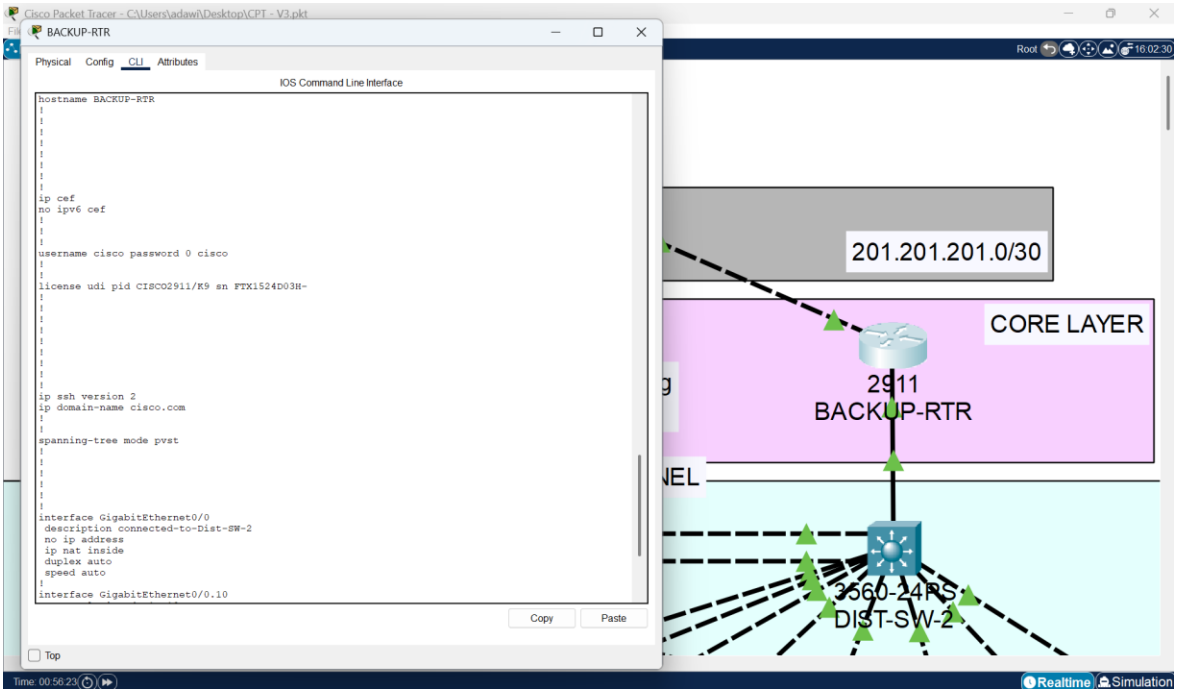


Figure 5.5.68

Sub-interfaces for VLANs 10–99 use dot1Q encapsulation with IPs and HSRP settings for redundancy.

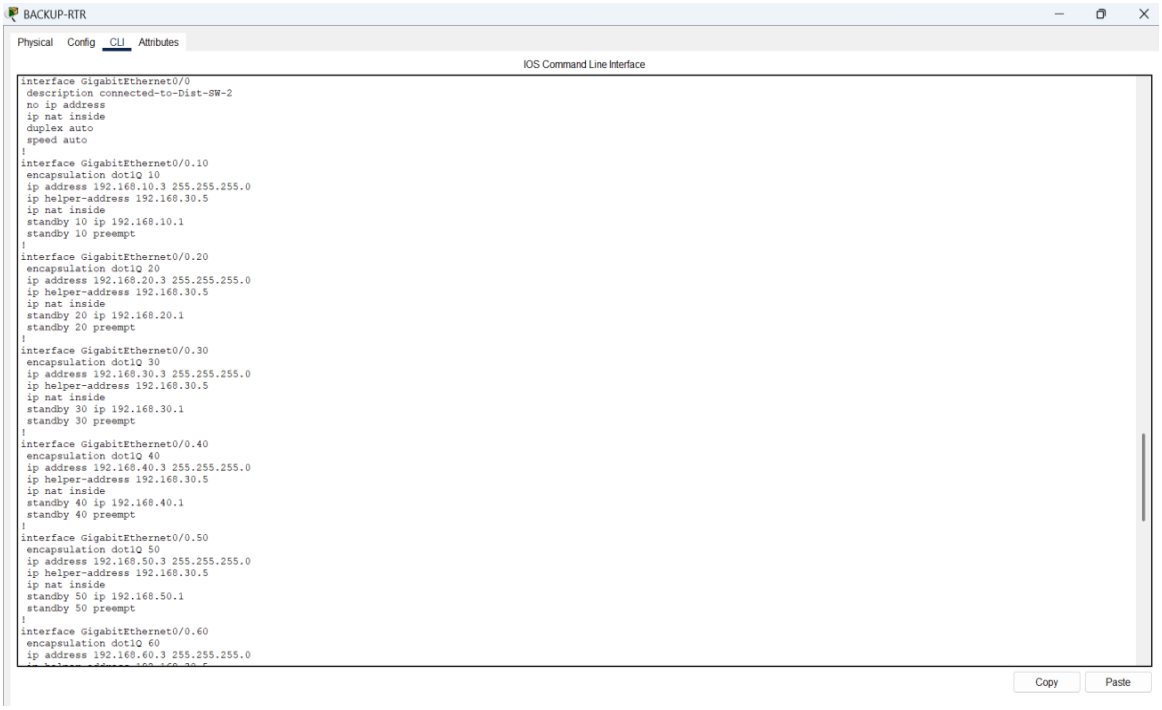


Figure 5.5.69

Sub-interfaces for VLANs 10–99 use dot1Q encapsulation with IPs and HSRP settings for redundancy.

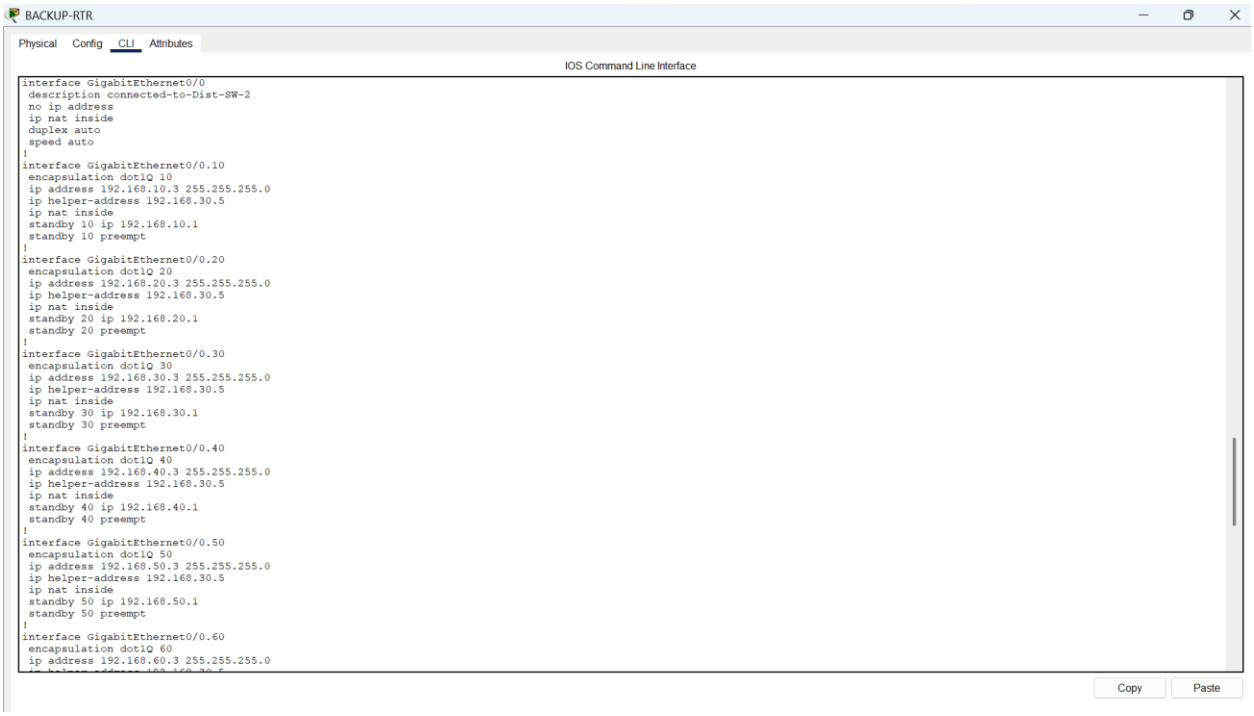


Figure 5.5.70

VLAN 99 assigned 192.168.99.2 for management; SSH access restricted, and NAT enabled with ACLs.

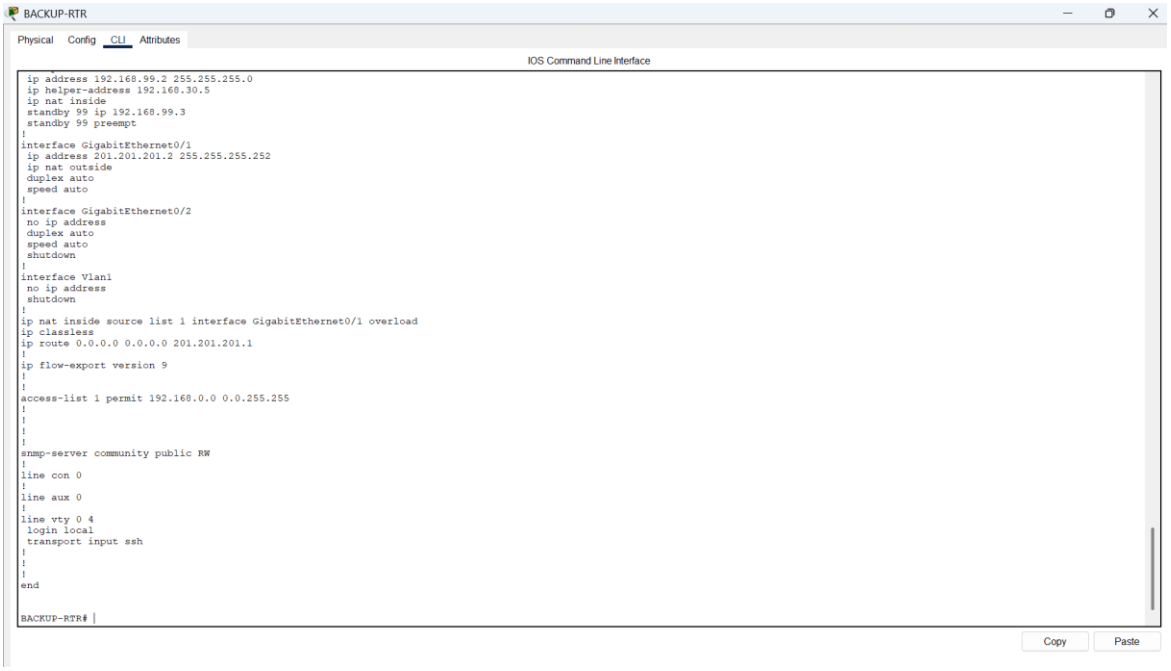


Figure 5.5.71

Internet Service Provider (ISP) Connection Provides the primary internet link. Hostname ISP configured; no SSH settings applied, used for simple routing setup. Connected to both the core and backup routers for redundancy and continuous internet access.

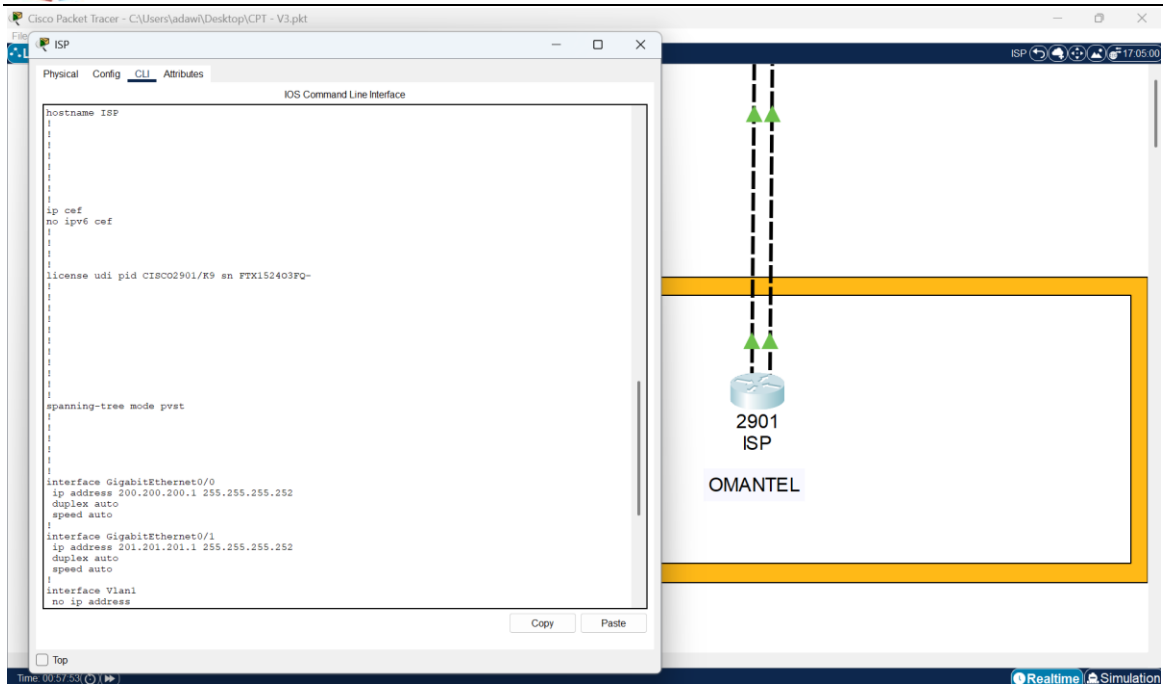
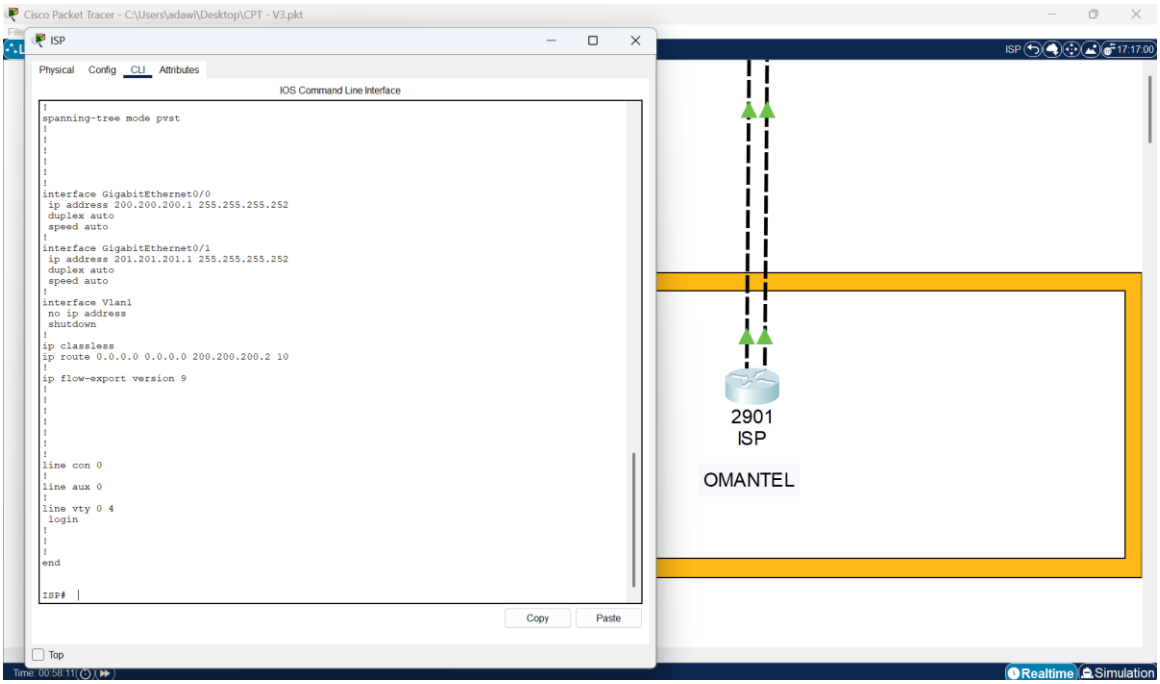


Figure 5.5.72

G0/0 and G0/1 configured with public IPs 200.200.200.1 and 201.201.201.1 for external connectivity (Core and Backup Routers).



5.5.11. System features

Figure 5.5.73

This figure shows Web Server (NU.EDU.OM) Successfully works in Network Computers which includes Welcome message, Cybersecurity Awareness Section, Cyber-attacks and ways for self-protection.

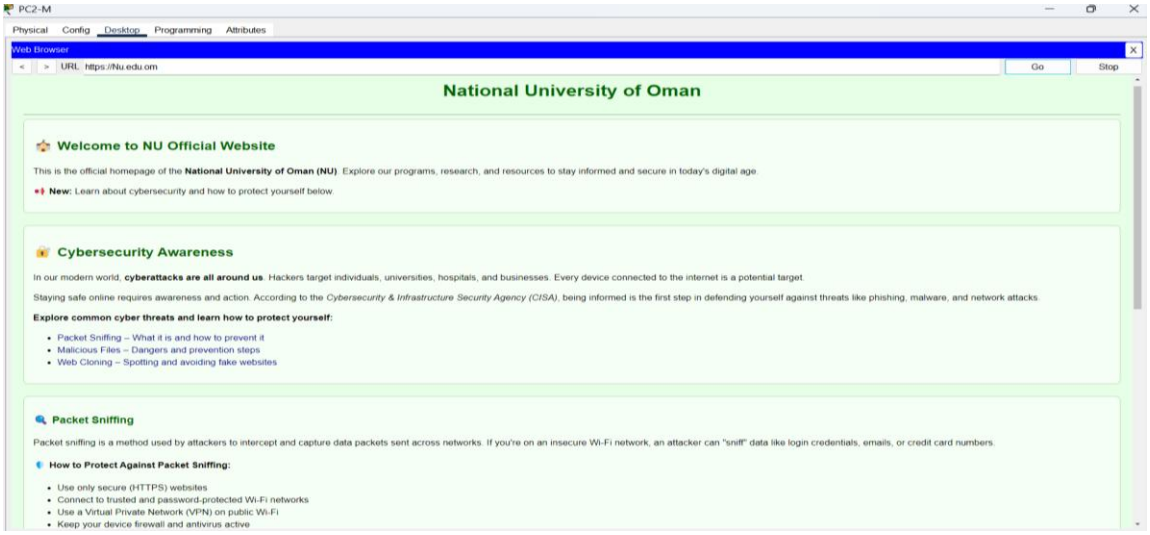


Figure 5.5.74

This figure shows the Web Server (NU.EDU.OM) attacks section which include information about: Malicious files and Web Cloning attack.

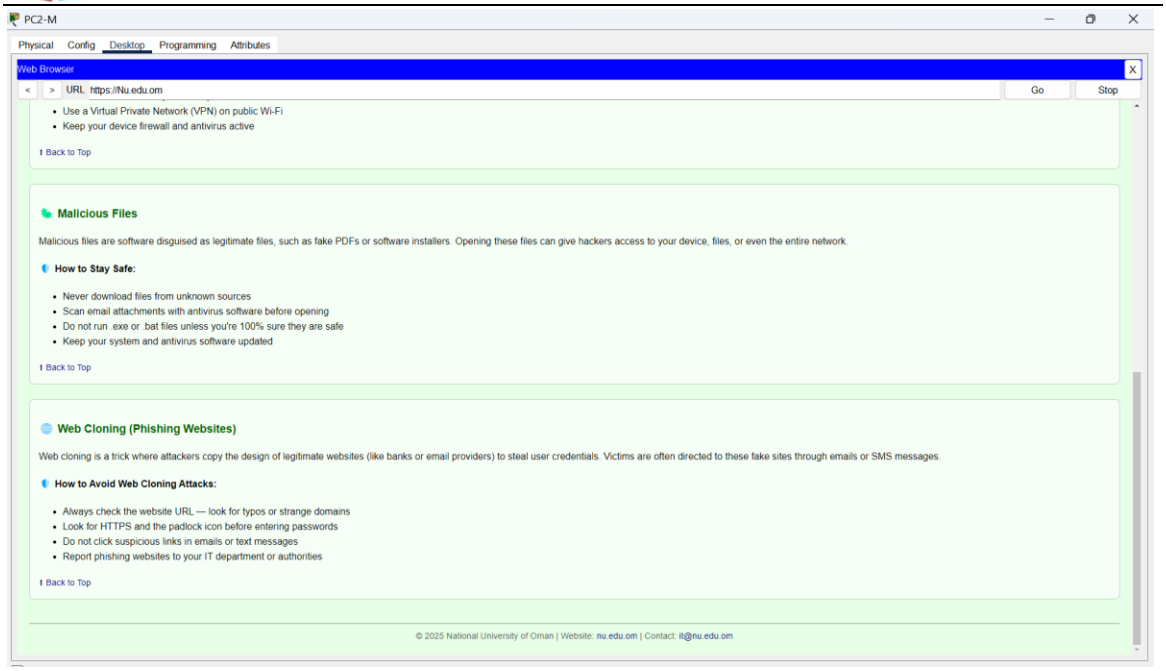
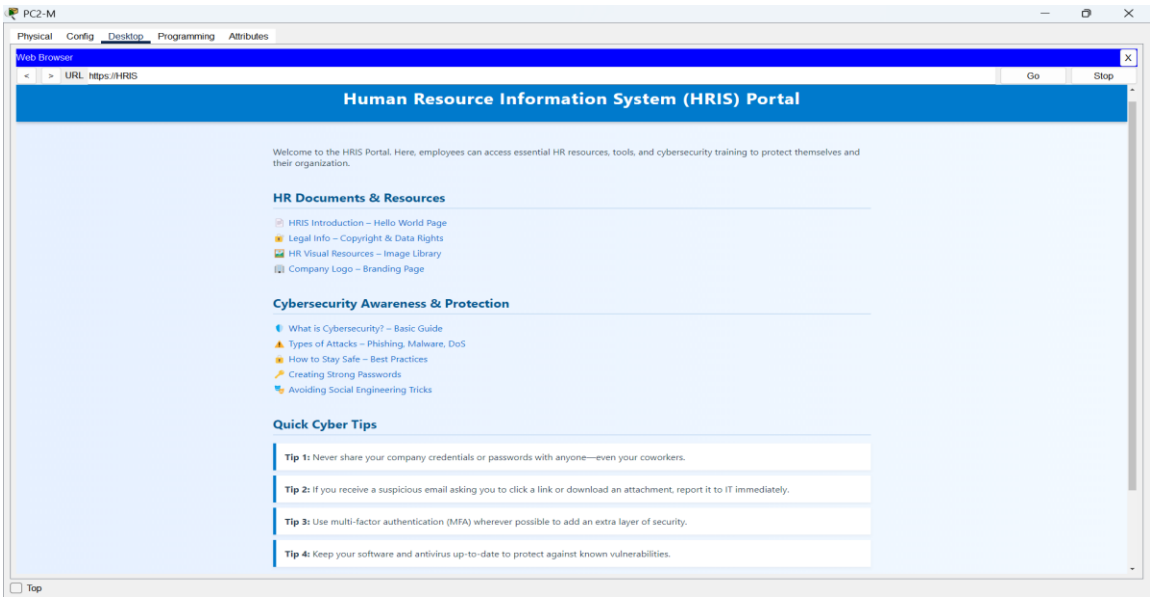


Figure 5.5.75

This figure shows the Human Resources Information System webpage (HRIS) for assuring good Cybersecurity Knowledge for staff and the page includes HR Documents and Resources, Cybersecurity Awareness and Quick Cyber Tips.



5.5.12. Security Settings – SSH

Figure 5.5.76

SSH This figure shows SSH configuration applied on the Core RTR. SSH ensures encrypted remote access, preventing credential theft during login.

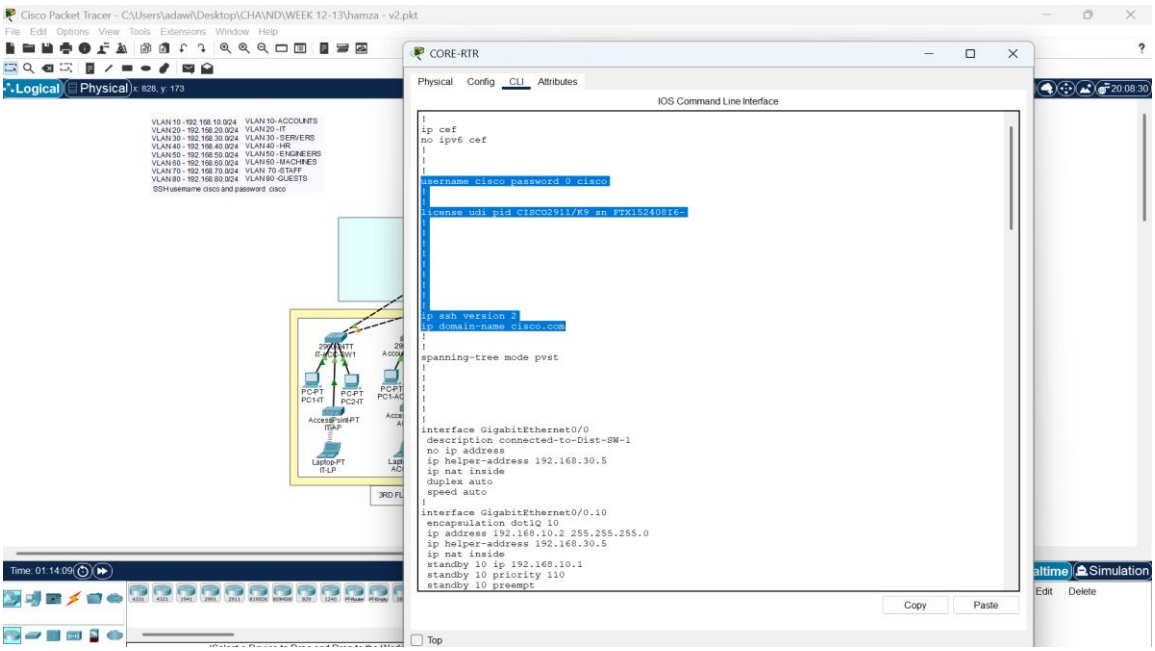


Figure 5.5.77

SSH This figure shows SSH configuration applied on the Backup RTR. SSH ensures encrypted remote access, preventing credential theft during login.

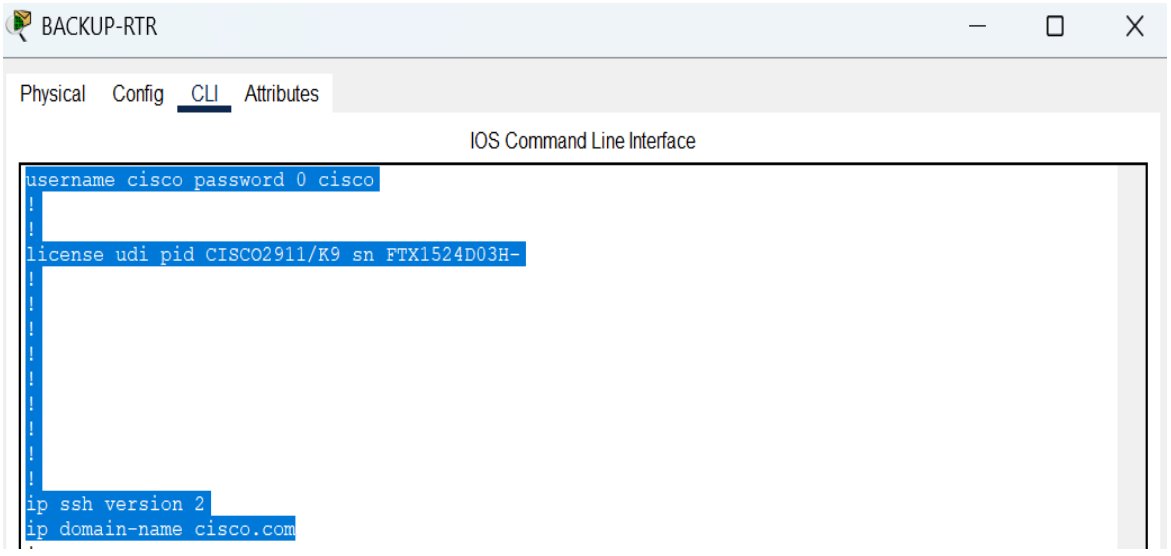


Figure 5.5.78

SSH on Staff Access Switch This figure highlights SSH setup on the staff switch. SSH helps protect login sessions by encrypting commands and credentials.

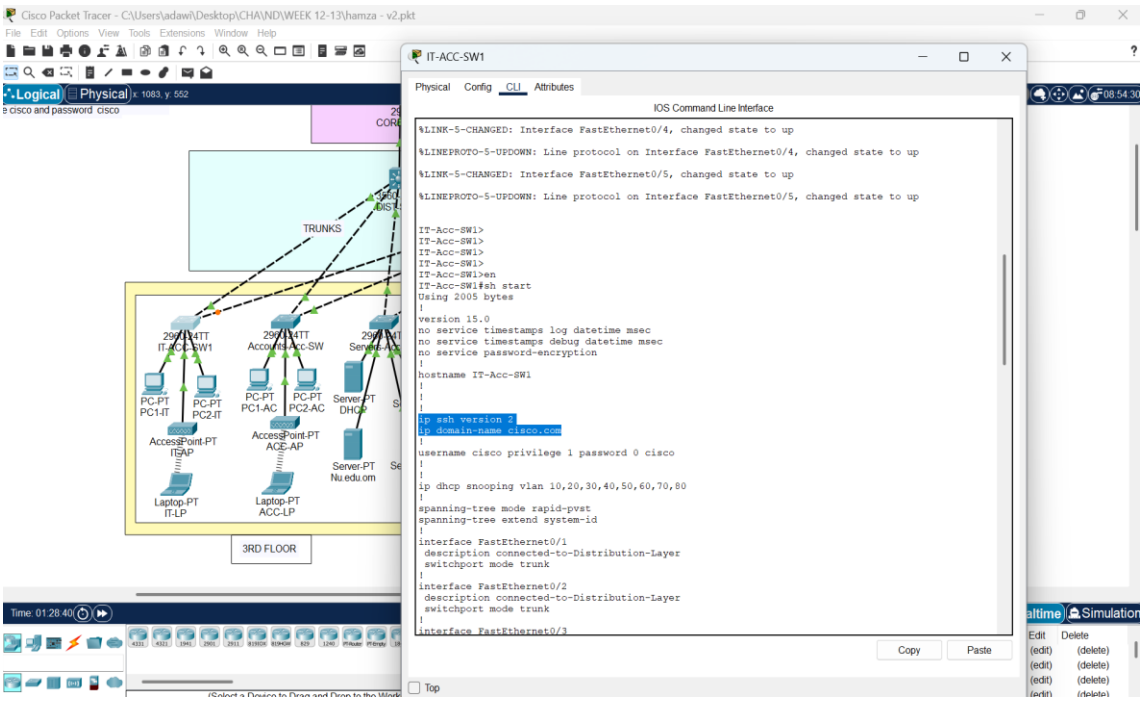


Figure 5.5.79

SSH was tested from end-user PCs to access switches and the core router. The connection was successful, secure remote access is working.

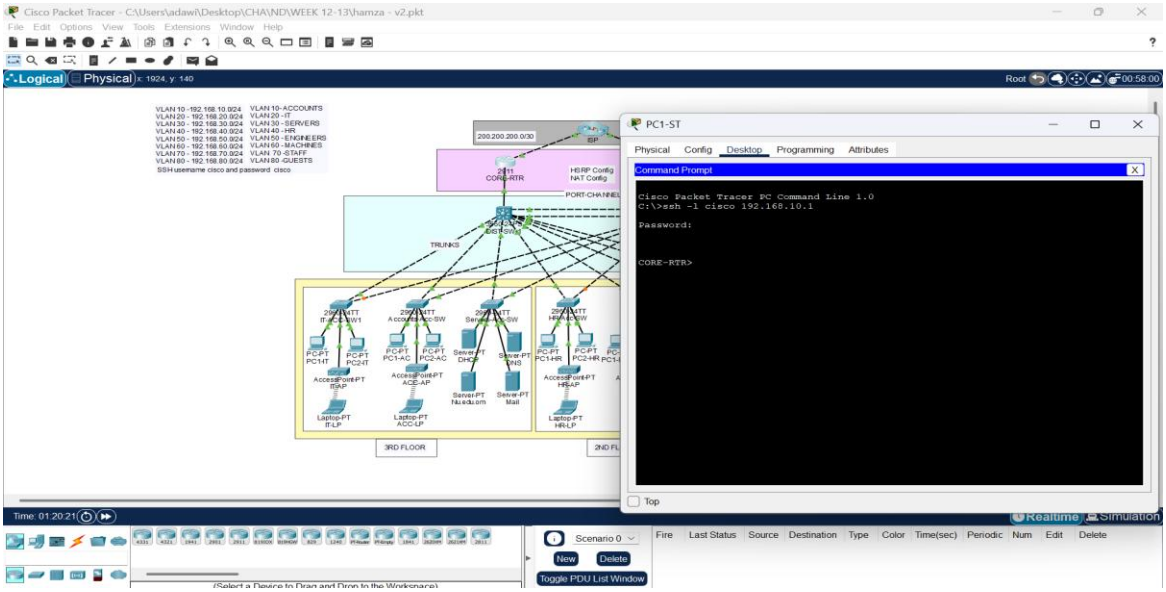


Figure 5.5.80

ACL Configuration on Core RTR for VLAN 80 – An access control list (ACL) was configured on the Core Router to deny traffic originating from VLAN 80. This setup ensures that guest devices are restricted from accessing internal departments.

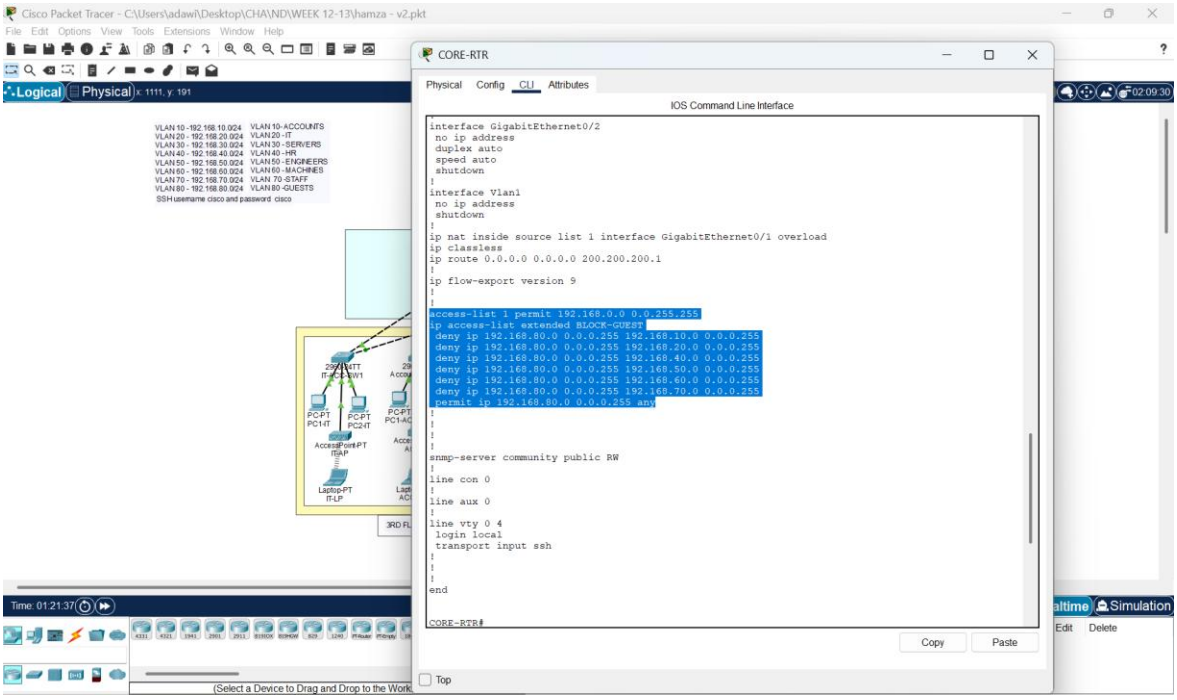


Figure 5.5.81

ACL Verification – VLAN 80 (Guest) – ACL testing confirmed that devices in VLAN 80 are denied access beyond allowed destinations. The restriction helps isolate guest users and protect internal resources. As the figure shows devices in VLAN 800 are unable to communicate with other VLANs.

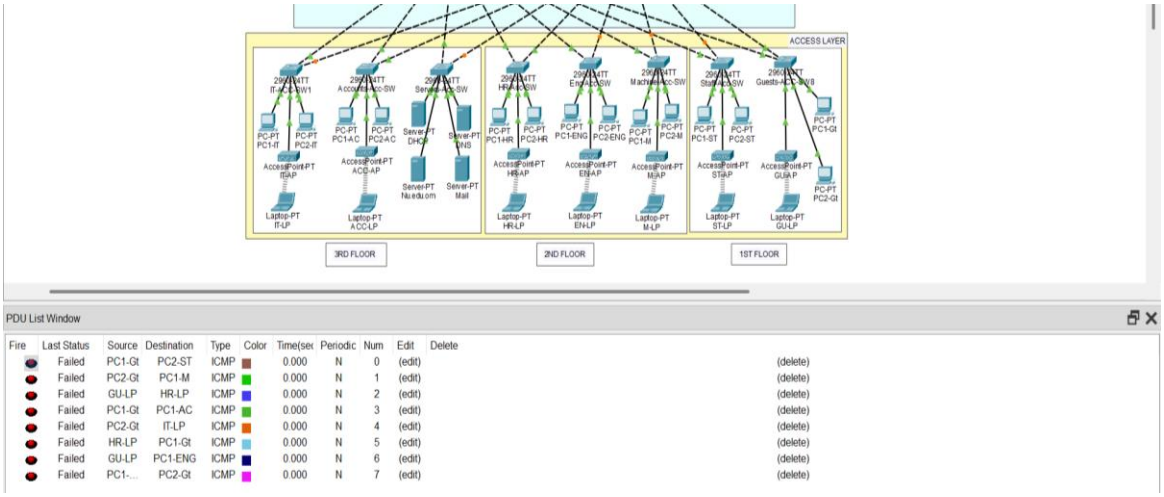
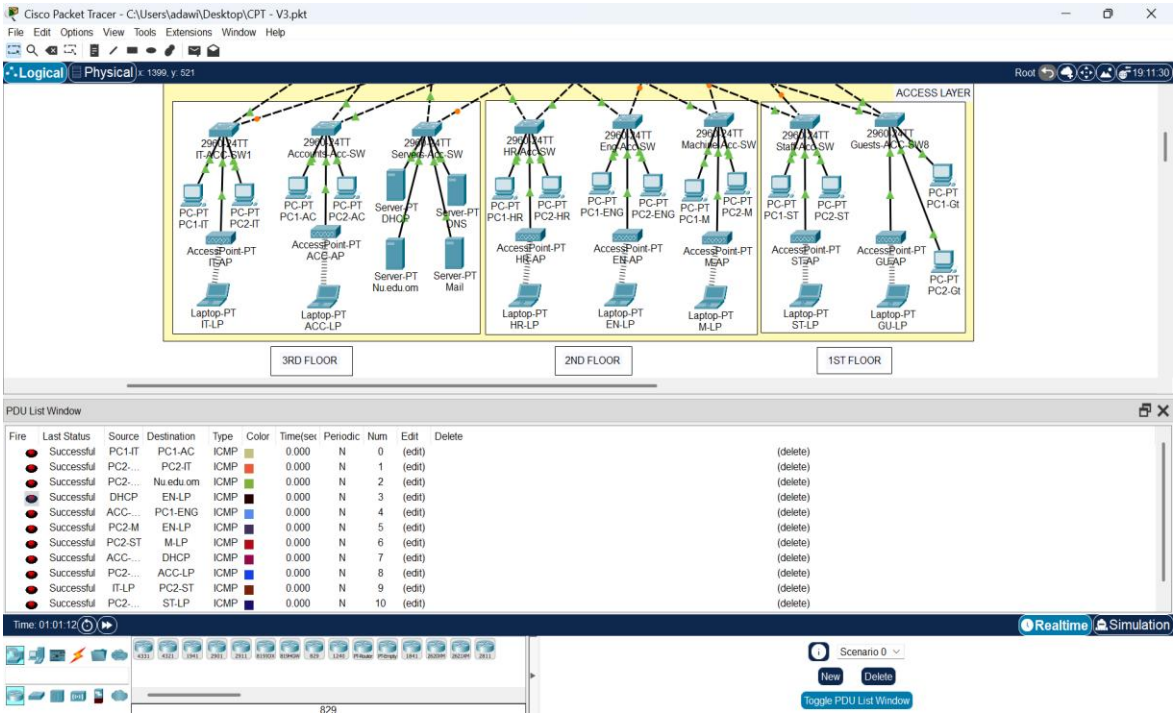


Figure 5.5.82

Inter-VLAN Communication with ACL Applied – Devices from all departments can communicate with each other through inter-VLAN routing, except for VLAN 80 can communicate or ping only servers VLAN 30.



5.5.13. Virtual Local Area Networks Configuration-VLANS

Figure 5.5.83

VLAN Verification on Access Switches – All VLANs were verified on access switches using the show VLAN command.

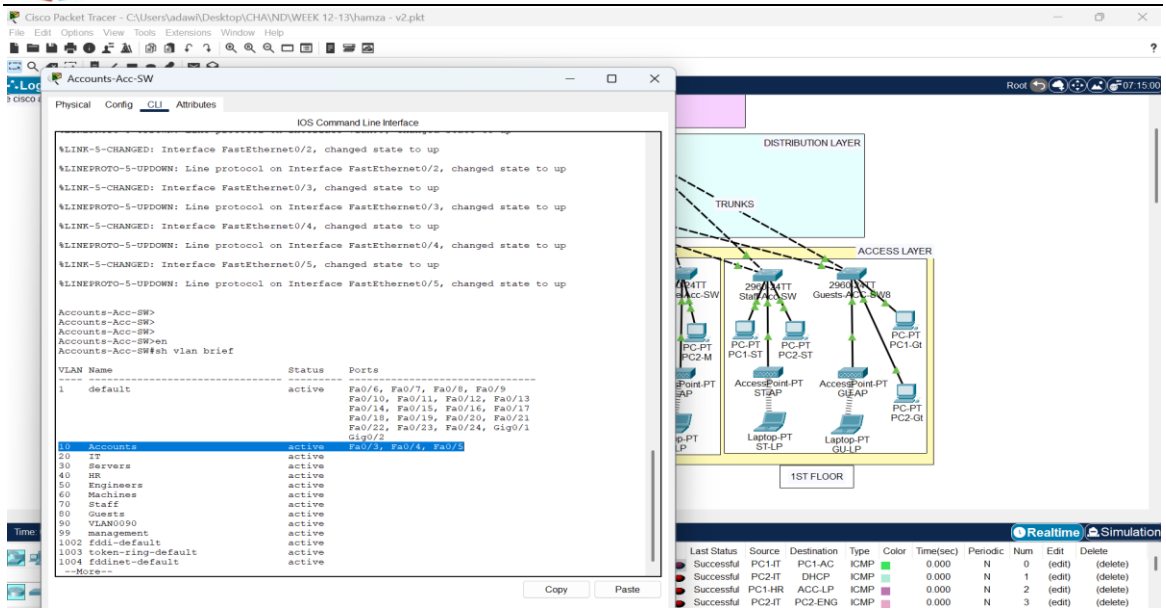


Figure 5.5.84

VLAN Verification on Access Switches – All VLANs were verified on access switches using the show VLAN command.

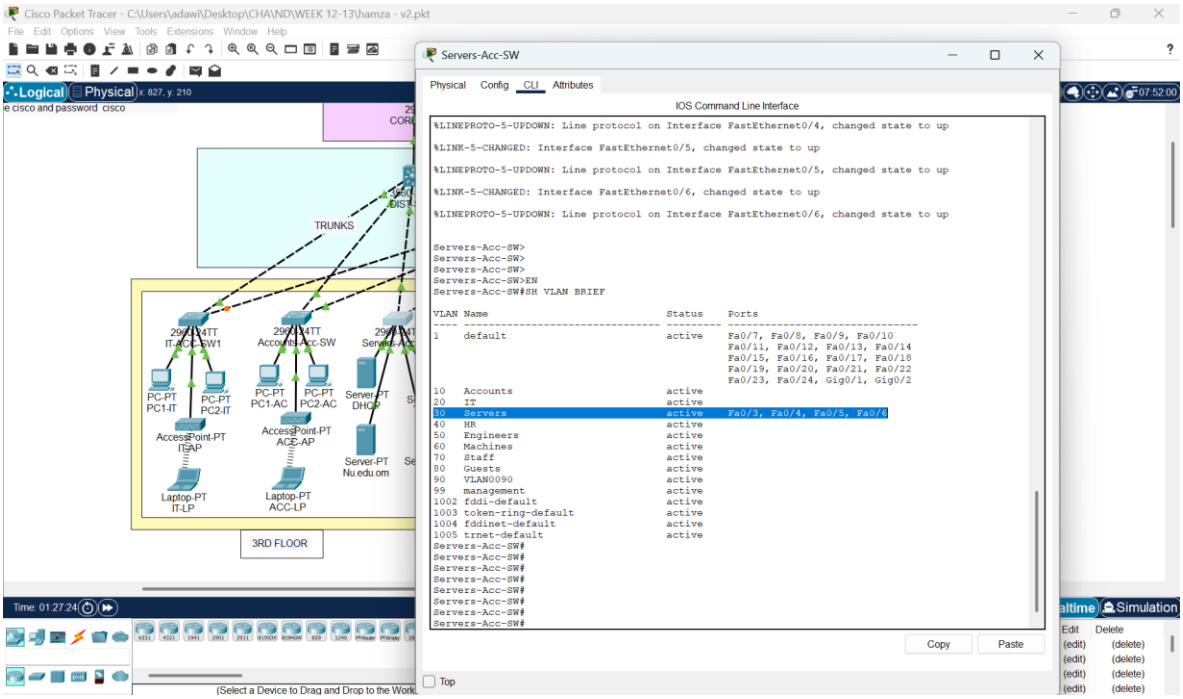


Figure 5.5.85

VLAN Verification on Distribution Switches – The distribution switches were checked for VLAN propagation using show VLAN.

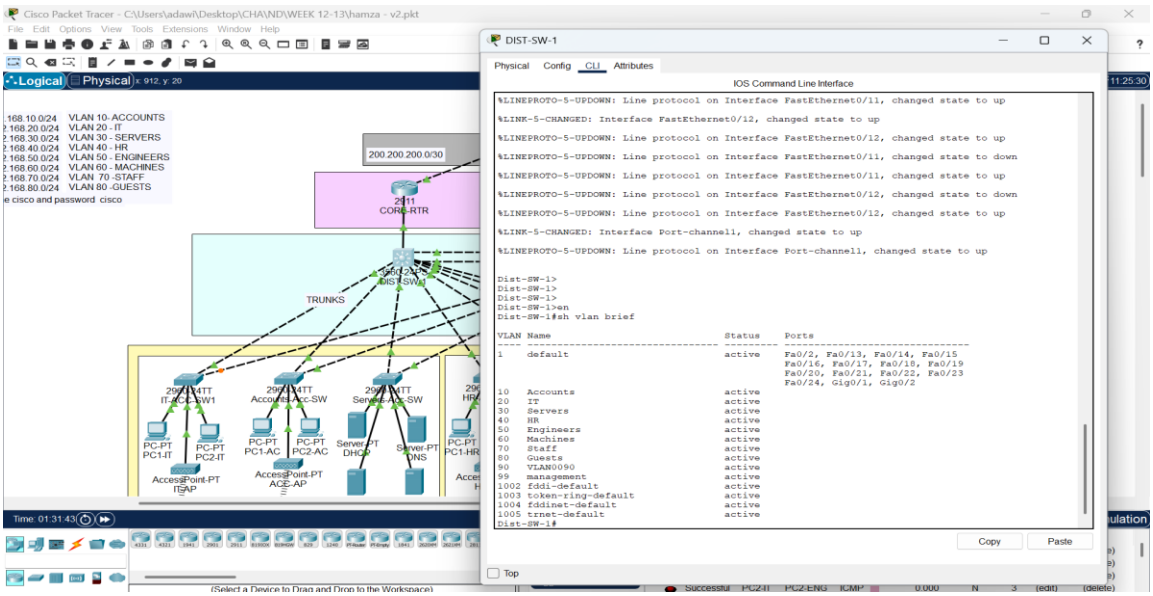
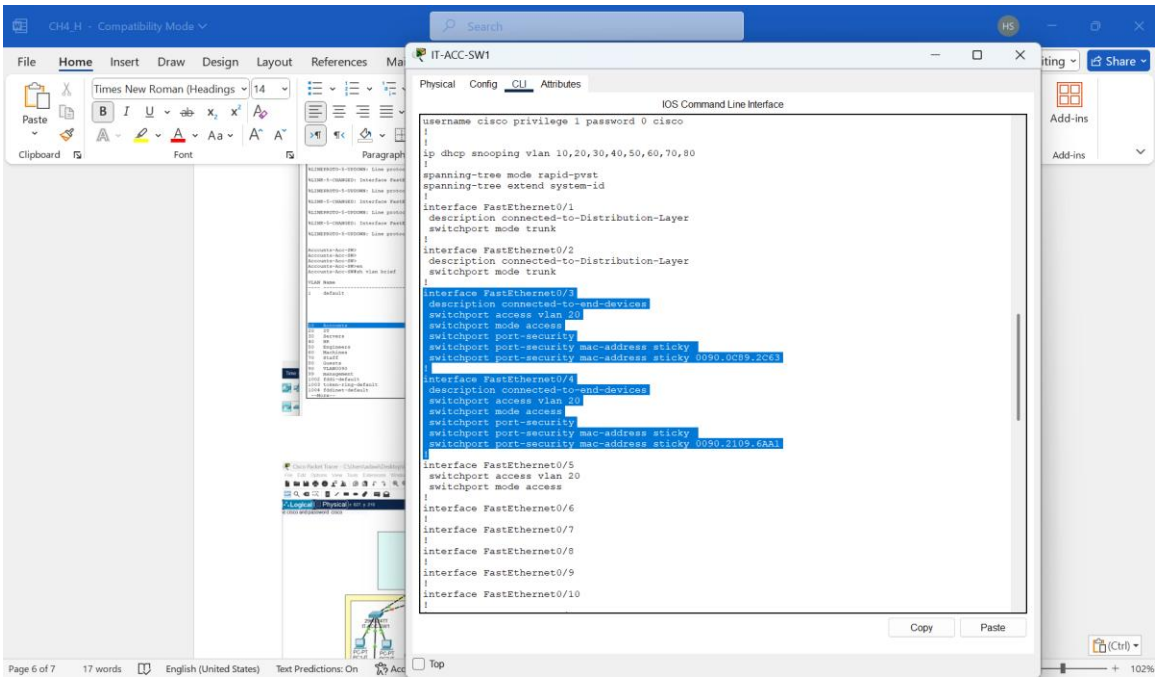


Figure 5.5.86

Port security was enabled on all access switches using the sticky MAC feature. This allows each port to dynamically learn and lock the first device's MAC address, to prevent unauthorized access.



5.5.14. Cyber Attacks Phase

Attack 1- Packet sniffing

Figure 5.5.87

Monitoring Packet Flow – The attacker Started capturing network traffic using Wireshark, passively observing all packet transmissions on the local network.

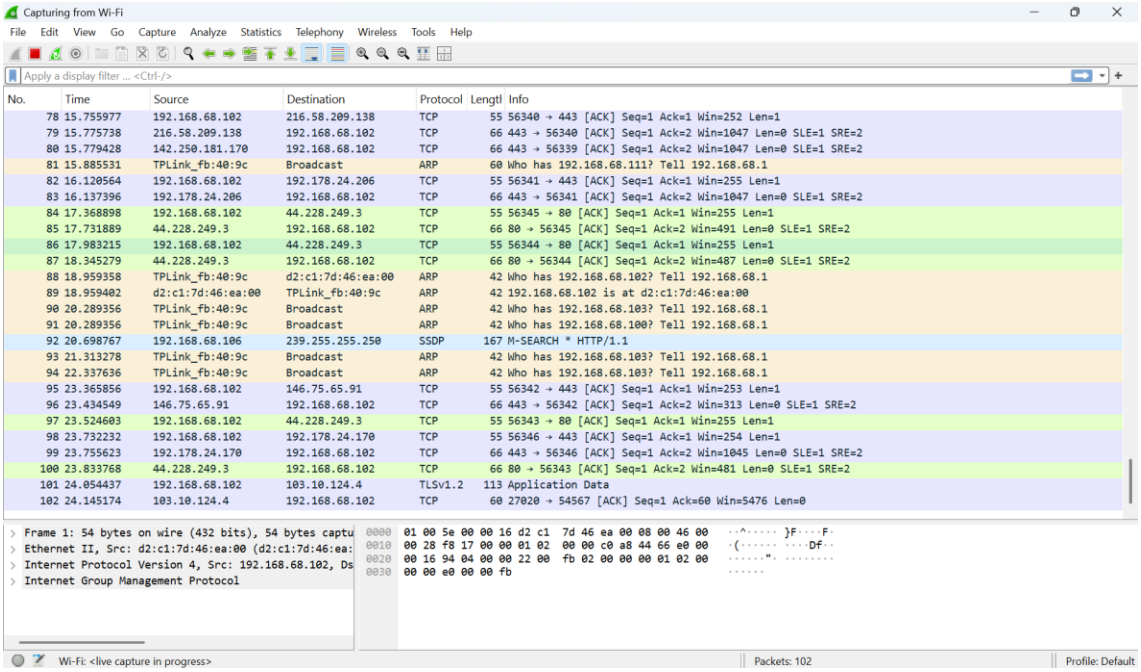


Figure 5.5.88

Victim Enters Credentials on HTTP Website unsecured – A user on the same VLAN accessed an unencrypted HTTP login page and entered their username and password without encryption.

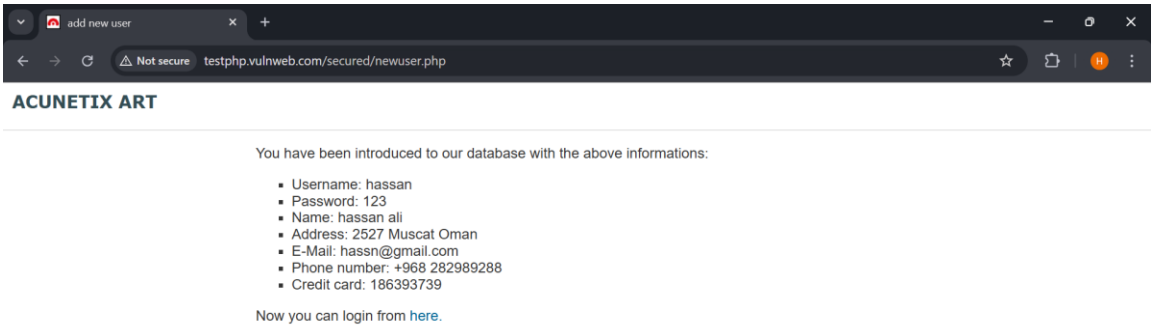
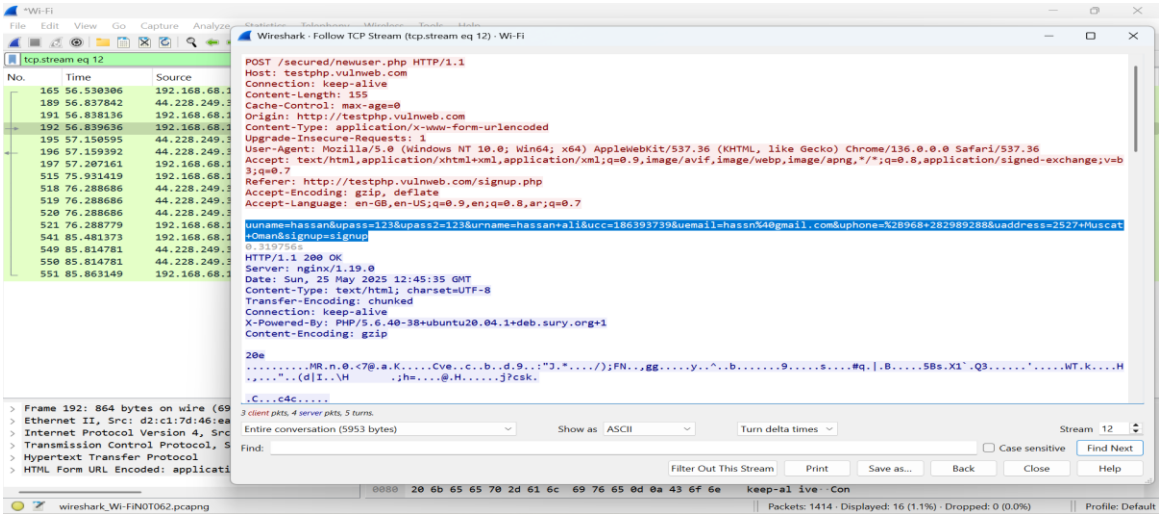


Figure 5.5.89

Captured Credentials Visible in Wireshark – The attacker filtered HTTP POST packets and clearly extracted the victim's username and password in plain text from the captured traffic.



Attack 2 - Web Cloning.

Figure 5.5.90

Selecting Web Cloning Module – In Kali Linux, the Social Engineering Toolkit (SET) was launched, and the website cloning option was selected. The target website URL was entered to create a clone. Inserting Attacker's IP Address – The attacker entered their local IP address to host the fake login page that mimics the real website.

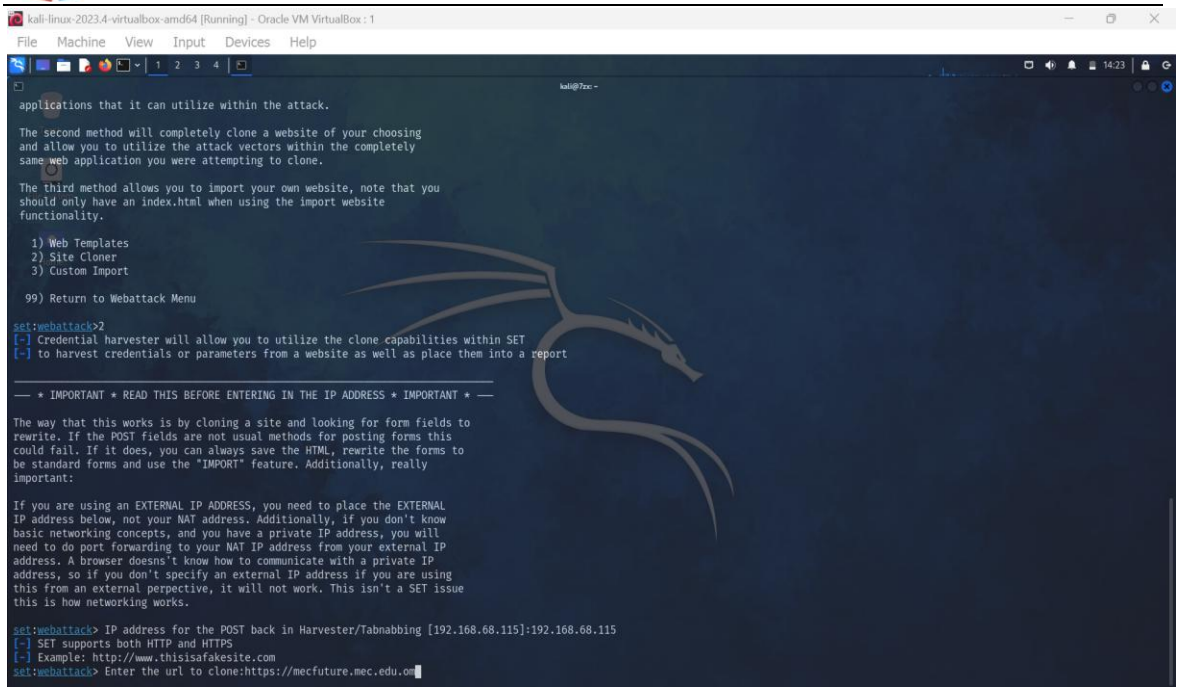


Figure 5.5.91

Victim Opens the Cloned Website – The victim accesses the fake website in a browser.

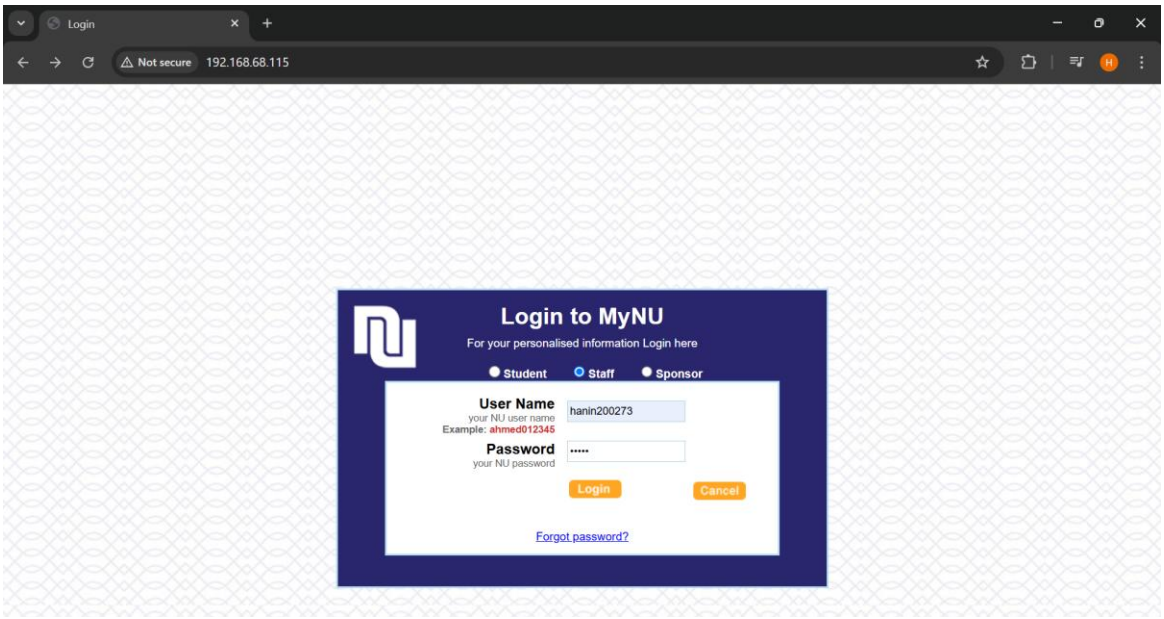


Figure 5.5.92

This figure shows the victim. After entering credentials in cloned web, the page reloads and redirects to the actual site to avoid suspicion.

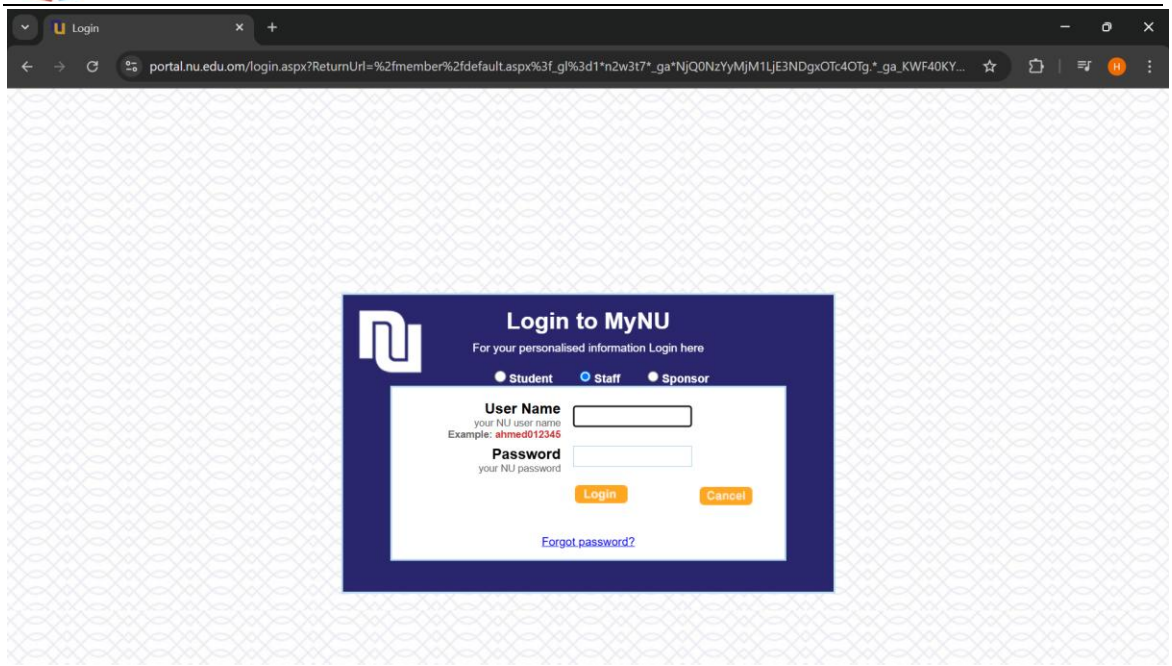
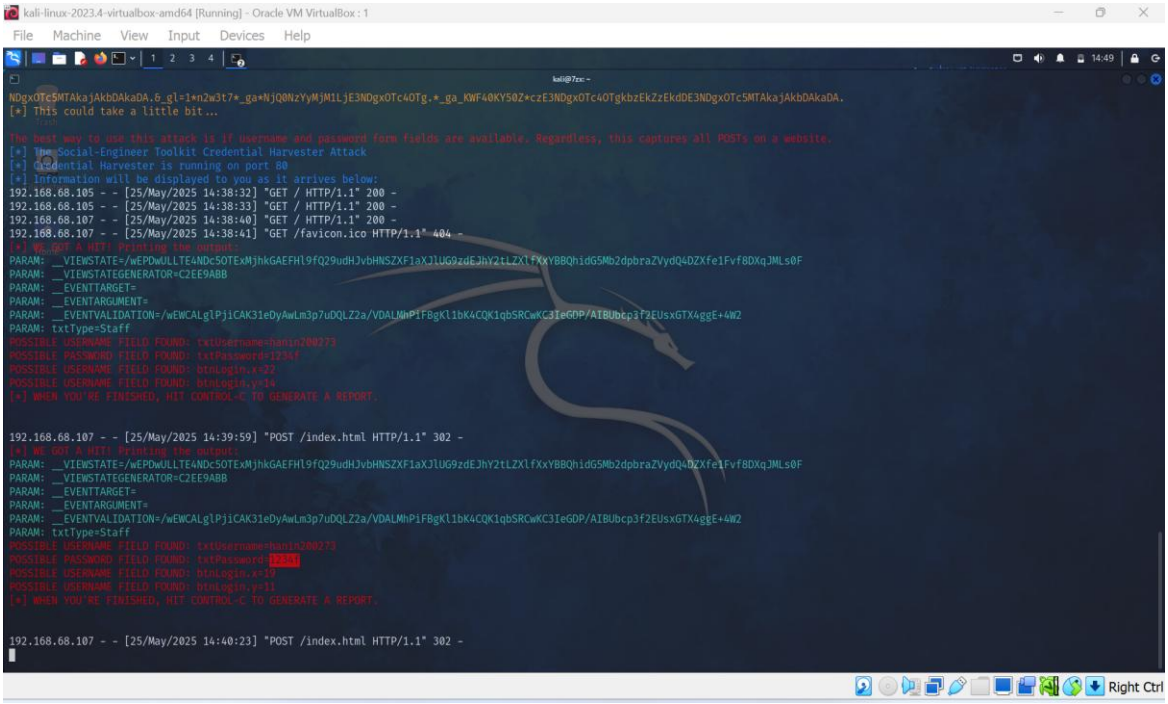


Figure 5.5.93

Captured Password Displayed in Terminal – The login credentials entered by the victim are captured and displayed in the attacker's SET terminal window.



Attack 3 - Reverse shell payload

Figure 5.5.94

Creating Reverse Shell Payload – A malicious .exe payload was generated using MSF console in Kali Linux with the attacker's IP and a listener port for reverse connection.

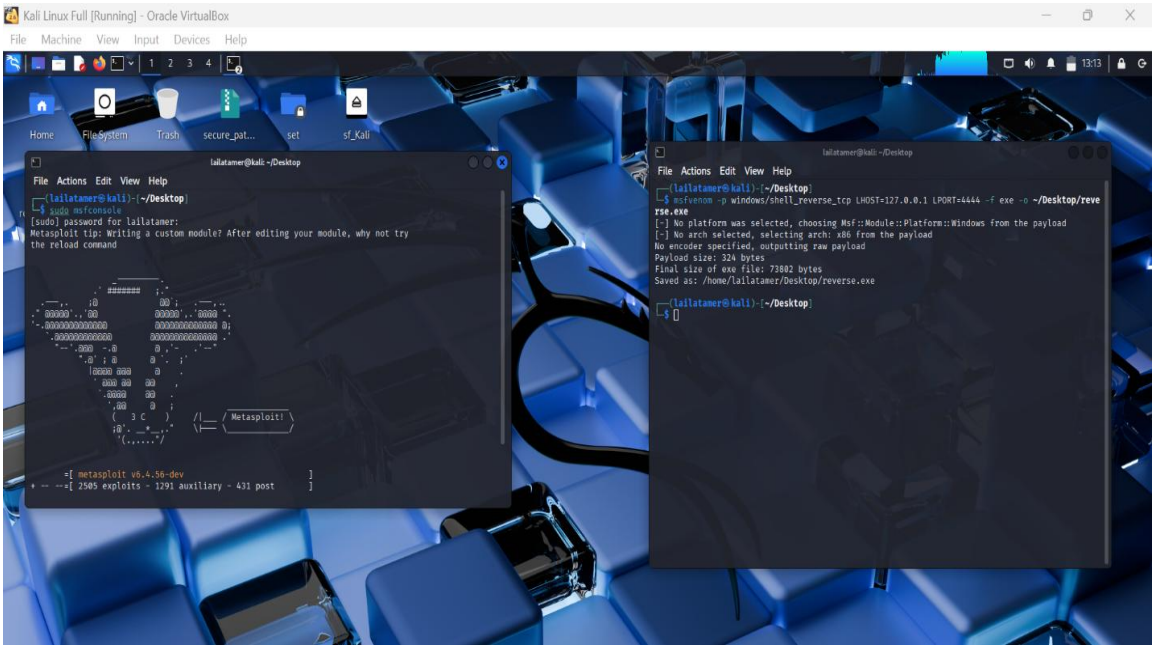


Figure 5.5.95

Executing Payload on Victim Machine – The victim unknowingly ran the payload file, triggering a reverse connection request to the attacker's system.

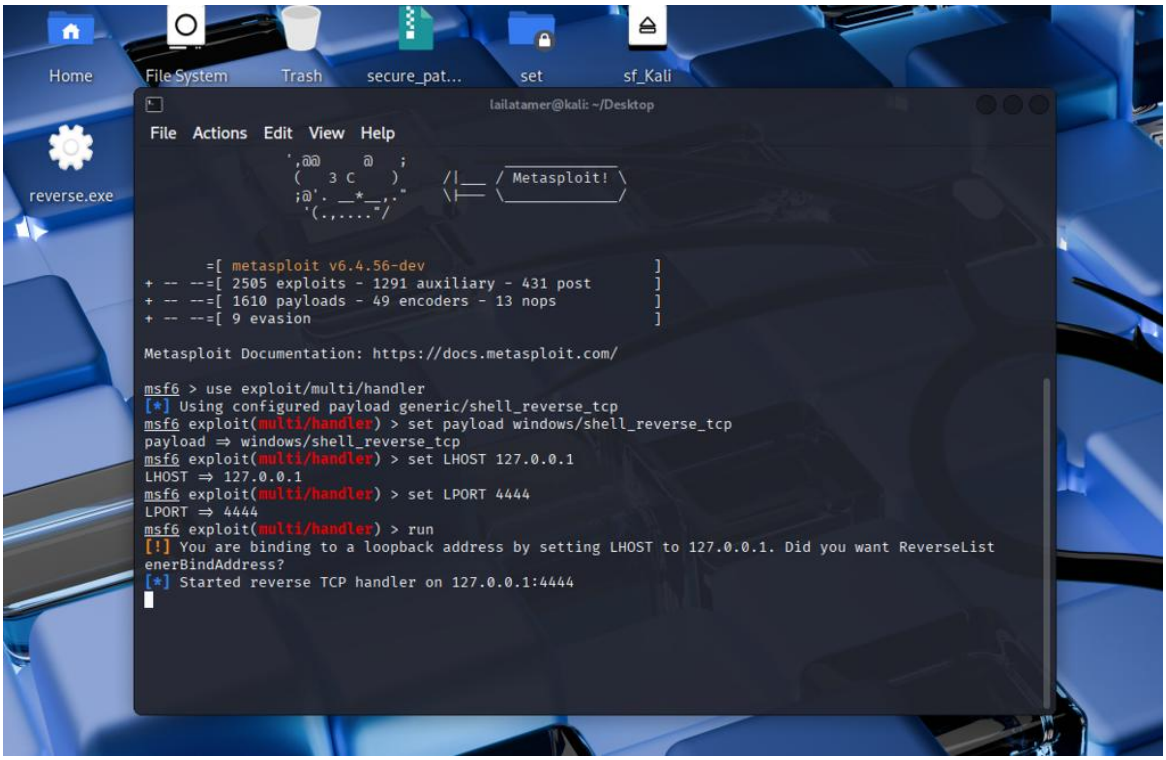
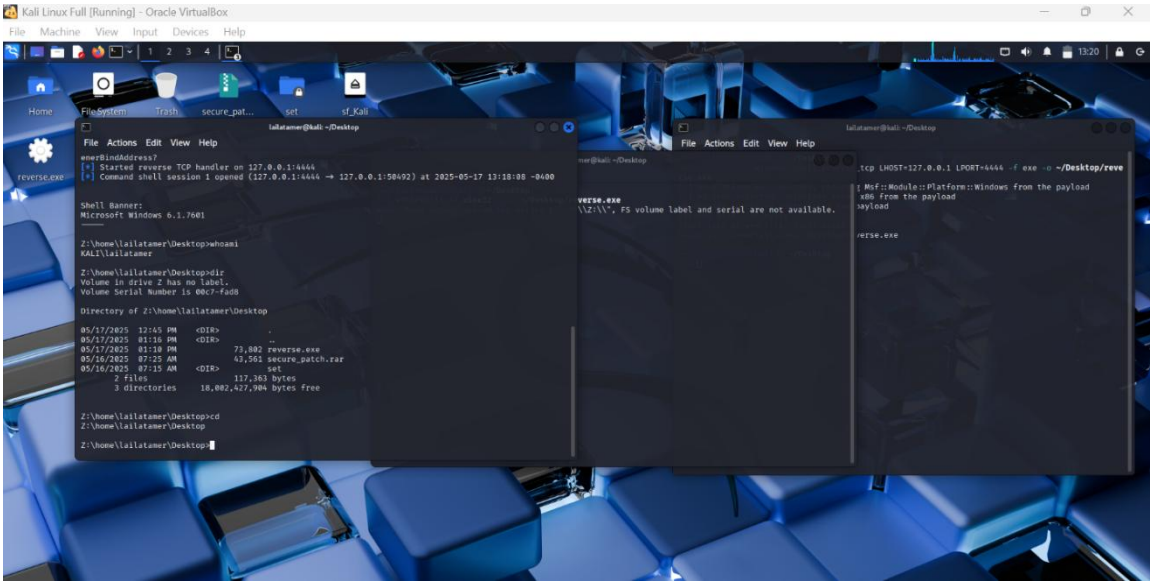


Figure 5.5.96

Attacker Gains Remote Shell Access – The attacker received a reverse shell session in the Metasploit console, gaining full remote control over the victim's machine.



5.5.15. Mail System Snapshot

Figure 5.5.97

Mail Test Message Sent – A test email was sent from one user to another using the internal mail server.

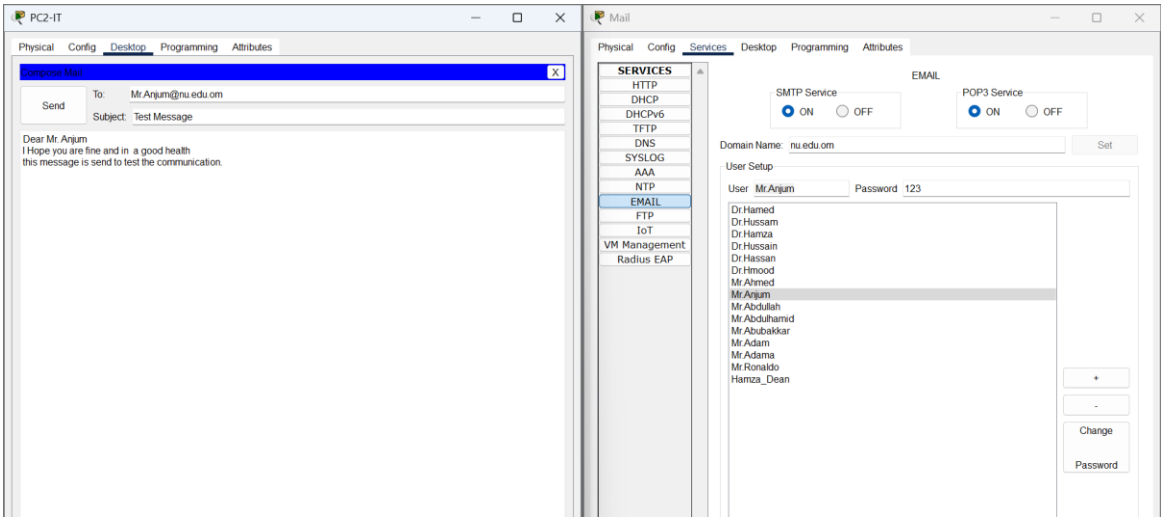
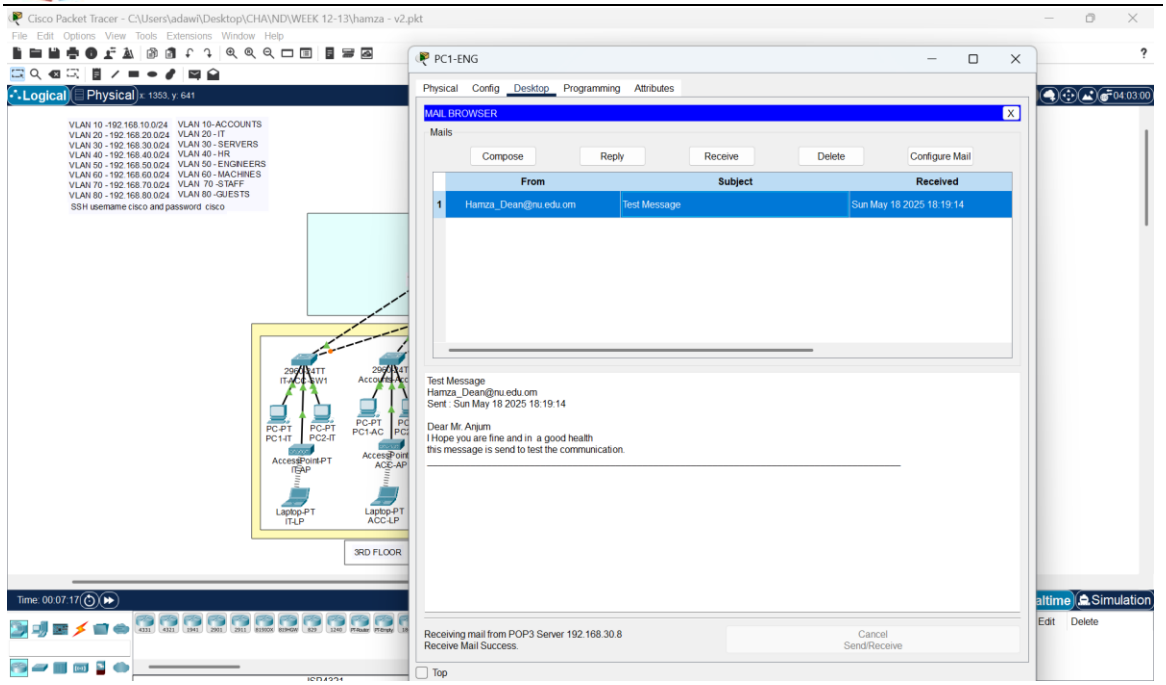


Figure 5.5.98

Email Communication Test – This figure shows a successful email exchange between users via the configured mail server. It confirms that internal email services are functioning properly for user communication.



5.5.16. Cybersecurity Awareness Training -Dashboard

Figure 5.5.99

Cybersecurity Dashboard and Awareness Content – A Power BI dashboard was created using questionnaire responses, presenting graphs and insights on user awareness. Three videos were added as QR code in the dashboard also produced and uploaded to YouTube to visually help in implementing Cyber-attacks.

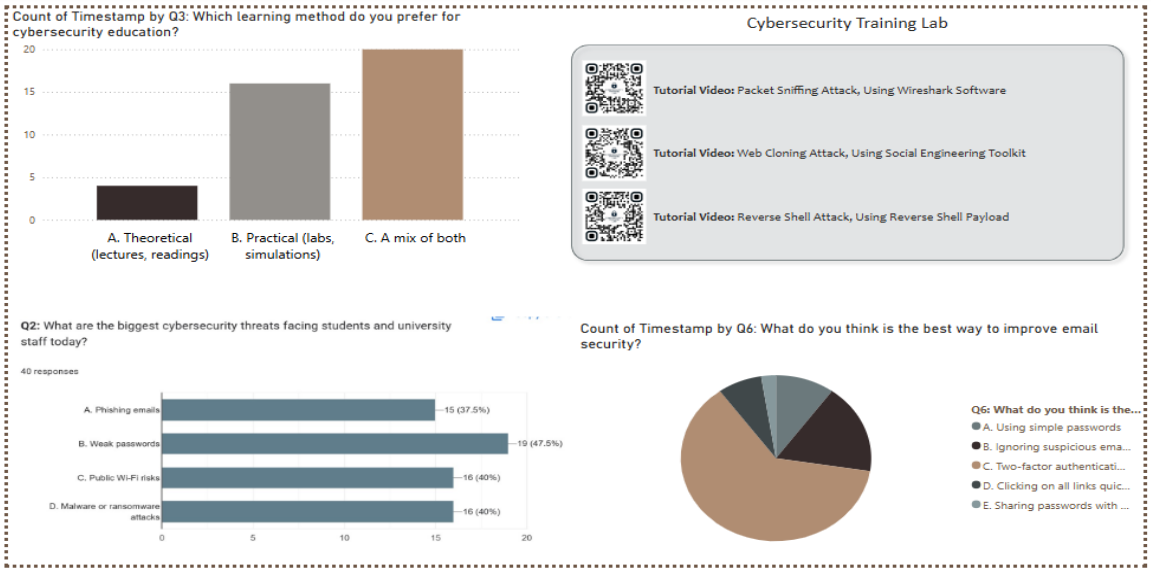
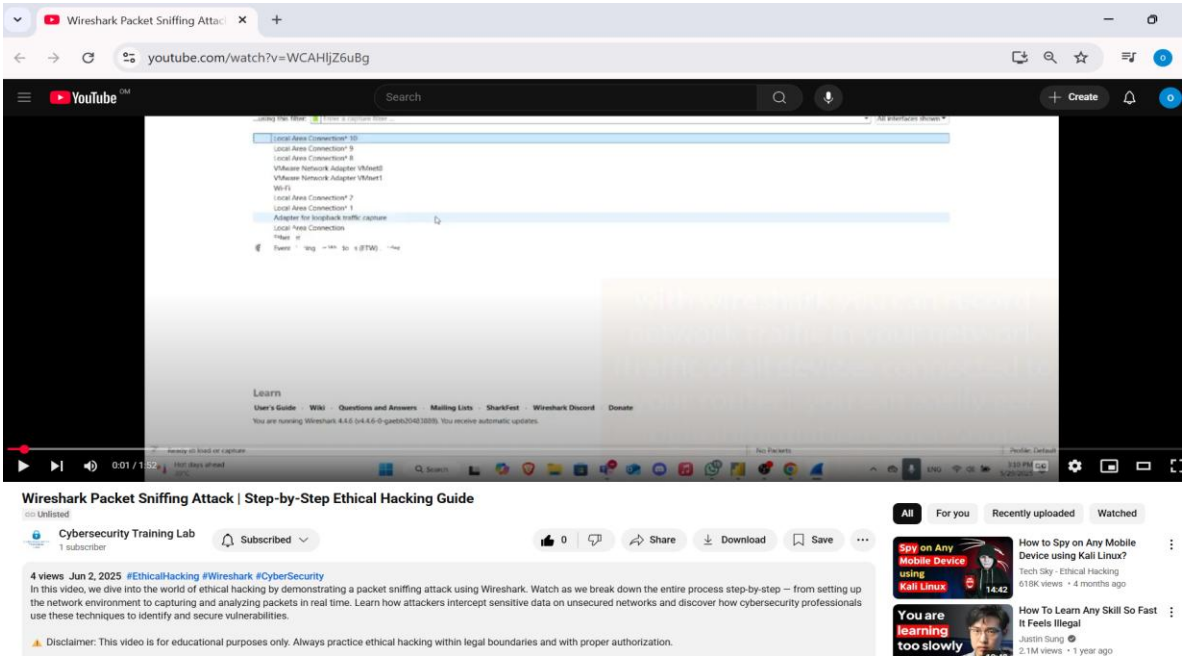


Figure 5.5.100

YouTube Channel and Video Publishing – A dedicated YouTube channel was created to host the three awareness videos which can be accessed only by QR codes in dashboard. Each video addressed different cybersecurity topics and was linked with the dashboard content for educational impact.



5.6. Configurations Summary

Cisco Packet Tracer was used to establish a comprehensive, safe network for the National University (NU), Oman, by designing it from an enterprise level. A three-layer hierarchical model (Access, Distribution, Core) is used, and each floor is separated into different VLANs (ranging from 10 to 99). The Access Layer connects user devices in departments such as Guests (VLAN 80), Staff (70), IT (20) and others, applying SSH for secure remote connection, DHCP snooping to guard against illegal servers and Port Security based on sticky MAC. Departments get their own IP range and wireless name which boosts separation of networks and access privileges. In the Distribution Layer, VLAN routing, trunking and inter-VLAN access take place and VLAN 99 is set aside for administrative activities. The Core Layer consists of routers that have sub-interfaces (dot1Q), use HSRP to provide backup and have ACLs to block guest networks. VLAN 30 hosts services such as DNS, DHCP, Mail and Web servers which are checked for proper operations and SSH was made sure to be enabled on every network level for encryption. This way of organizing networks makes them both flexible and secure and works very well in real institutions.

To train staff and spread awareness, Wireshark and Kali Linux were used in cybersecurity testing to simulate common cyber-attacks. A user visited an unsecured HTTP site, and Wireshark was used to pick up the user's password in plaintext by using packet filtering. In the Web Cloning attack, Kali's Social Engineering Toolkit (SET) was used to create a fake university login page and host it on the attacker's IP address; the victim's login information was captured by the attacker. The attacker followed this by generating a Reverse Shell payload, running it on the victim's system and using Metasploit to connect and access the entire system. Using the survey data, a Power BI dashboard was set up showing users' awareness of cybersecurity matters in the form of different graphs. As an addition, three informational videos about phishing, passwords and social engineering were added to YouTube and QR codes were provided for employees to watch them on the dashboard. It works as a teaching tool and a clear sign of the results from the university's work in cybersecurity.

5.7 Chapter Summary

This chapter focuses on creating a reliable and protected network for the National University (NU), Oman, using tools such as Cisco Packet Tracer, Wireshark, Kali Linux and Power BI. The goal included ensuring the system runs well and provides users with practical knowledge about online safety. The network was structured similarly to how professional organizations work, with each part of the business kept in its own secure section. Remote access secured network communication and blocking of suspicious traffic were provided to guarantee the system's efficiency as well as safety.

Yet, the project moved forward by adding services on top of the network. The team demonstrated how crucial proper security is by running fake attacks on the system through Wireshark and Kali Linux which allowed them to access unencrypted data and use phishing and reverse shell methods to get in. The group displayed the results of their survey by making a Power BI dashboard that highlighted how well employees knew about cybersecurity. They created three short videos for YouTube, accessible through QR codes, that explain common cyber threats. In brief, this chapter mixes technical tasks with useful assessment, proving that having an organized network supports education and awareness too.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1. Introduction

This chapter gives details about the project and discusses its outstanding achievements, main obstacles, and what can be done to support it in the future. The main goal while working on the project is to introduce students to cybersecurity concepts and give them a chance to use the tools and methods effectively in real-world cases. It is created to represent a structured and protected network, like what businesses today rely on. By adding important features such as VLAN, HSRP, ACLs, DHCP, SSH, and NAT, the project was successful in creating an environment that let students use and practice both defense and offensive cybersecurity methods. There were also educational videos, daily dashboards, and exercises where teams were given the opportunity to experiment with ethical hacking.

It also discusses the main problems experienced in the project, for example, the limits of the platform, issues with technology setup, and insufficient basic networking knowledge among students. Despite these challenges, everyone worked well together and proved adaptable, resulting in a good and informative lab model. Lastly, this chapter offers ideas for boosting the lab's potential, by bringing in advanced real-time simulations, strengthening security monitoring, and developing strict ethical guidelines. The goal of these recommendations is to sustain the lab as a top teaching source for cybersecurity basics. Chapter 6 puts the whole project together and highlights how it aids in preparing students to work in IT and security fields, as well as improving digital readiness in Oman as outlined by Oman Vision 2040.

6.2. Deployment

To effectively establish the Cybersecurity Awareness Training Lab at the National University of Science & Technology, we are going to follow a structured, collaborative, hands-on strategy that will provide institutional fitness and guarantee sustainability. The initial process requires developing a detailed communication strategy to officially involve the management and IT department of the university. It involves preparing and presenting a formal proposal to the IT Director and then arranging a presentation meeting with the cybersecurity team of the university. The objective is to clearly demonstrate the educational usefulness of the lab, its consistency with national cybersecurity objectives, and its possibility to increase awareness among students and staff. After getting some initial support, we will hold a stakeholder workshop that will include faculty members, IT technicians, cybersecurity personnel, and administrative representatives.

These hands-on sessions will be used to communicate the purpose of the lab, showcase its major functions and gather constructive feedback. This will ensure that the implementation will fulfill the academic needs of the university and will abide by internal IT and data protection policies. With official approval pending, student orientation sessions are to be presented- either incorporated into the established coursework or presented as extracurricular training modules.

The sessions will include navigation in the lab environment, practical use of tools, knowledge of attack simulations, and awareness outcomes. At the same time, in close collaboration with the IT department, we will determine the most suitable deployment model between a physical lab consisting of real networking and security devices, or a more economical virtual environment via Cisco Packet Tracer installed on university systems. This gradual and comprehensive strategy will assist in the establishment of a robust cybersecurity culture within the entire university, where the students and staff are ready to identify and react to cyber threats.

6.3. Challenges Faced During Project Implementation

some challenges and limitations appeared during the process, even though the project was successfully implemented. For example:

1. Basic Networking Concepts

Since the students working on this project were only in their second year, the more advanced networking concepts posed challenges. Learning how to use Cisco Packet Tracer, setting up HSRP, and configuring VLANs required additional time to understand and apply effectively.

2. Cybersecurity YouTube Channel Suspension

The goal of the YouTube channel was to provide project documentation and explanation videos, but the channel was suspended due to the sensitive cybersecurity topics.

3. YouTube Channel Suspension Cybersecurity

Simulated attack videos provided sufficient opportunity to showcase skills, but they also had significant challenges. Many cybersecurity tools that have been issued require being in full-screen mode, and switching between windows quickly made it hard to maintain a smooth workflow. Creating video recordings while multitasking to complete processes that require multiple steps done simultaneously tend to require many attempts to achieve clear and accurate recordings.

6.4. Limitations and Future Enhancements

System Limitations:

1. Awareness of Risks Based on Familiarity
   These attacks were mostly simple (e.g., phishing, spoofing, sniffing), and more elaborate ones such as moving sideways within a network, getting system rights, or setting up ransomware were not part of the vulnerability assessments.
2. A Lack of Fundamentals in Networking for Students

Some students found it hard to grasp details about dynamic routing, subnetting, and securing infrastructure, which prevented them from working on configuration and troubleshooting alone.

3. No Mechanism for Responding and Adapting

   No system existed to check each student's achievements, assess their learning, or find where they lacked skills by using live challenges or role-play.

4. Confused rules about what is permitted.

   Students lacked a proper system that ensures they follow legal and ethical rules when using these tools, increasing the chance that they might incorrectly handle responsible hacking.

5. No Access to Advanced Types of Cyberattacks

   Participants were not exposed to recently launched malware, hacking supply chains, or unique attacks that bring together physical and digital aspects.

Suggestions for Enhancement in the Future:

- Include Complex Threats in the System

  Start using advanced attack simulations, including ways to gain higher-level access, persistent malicious campaigns, widespread ransomware, and social engineering is powered by AI.

- Provide additional assistance in networking courses.

  Teach the main areas of networking (for instance, dynamic routing and firewall rules) before starting the actual courses.

- Making Assessments Smart

  Create mixed quizzes, lab performance charts, and instant skill assessment activities to give students personalized help and support learning.

- Ensure everyone follows ethical guidelines by having them sign a code and checking their actions.

  Students need to commit to safe internet practices and introduce artificial intelligence to monitor programs, noting any activity against the rules and informing educators of any breaches.

- Follow the directions of Threat Intelligence.

Stay updated in the lab by including threat intelligence research and case studies so students are aware of recent attack methods and occurrences.

6.5. Conclusion

The main objective of this research was to help NU Oman face rising cybersecurity threats by designing a Cybersecurity Awareness Training Lab using Cisco Packet Tracer. The purpose of this project was to establish a secure, practical and scalable place for training to help students, faculty and IT staff improve their cybersecurity skills and awareness. Its purpose was to deal with issues raised so far, including limited practical experience, risk of different cyber-attacks and having no central program for security awareness at the university.

Different phases were created for the project which led to several key achievements. Successful achievements included establishing a safe network hierarchy with VLAN segmentation and ACL functions, HSRP as backup and features for security such as DHCP snooping and SSH access from afar. It was found by surveys and interviews that the majority of people preferred hands-on, SET exercises and the most significant security worries were weak passwords, phishing scams and using public Wi-Fi. Wireshark and Kali Linux were used in this project to explore various cyberattacks and a dashboard on Power BI was made to track user awareness. Also, cybersecurity awareness videos are available to expand students' knowledge beyond what is covered in the lab.

The project is aimed at extending practical cybersecurity training through an easy-to-use lab-based solution. The Cybersecurity Awareness Training Lab is an adjustable system that combines the management of networks, simulations of security threats and evaluation of awareness in one spot. By using IT, it makes the institution stronger against cyber threats and gives students and faculty real experience facing security challenges and learn how to handle them. Constructing and working with the system has helped improve students' understanding and skills in a safe way.

Applications for this project can go beyond the National University of Science and Technology. The material from this Lab can be useful in teaching at colleges, vocational schools and companies that offer professional development in Oman. Because it can be easily changed, depends on commonly available programs and use interactive training, it is perfect for use in national cybersecurity education projects. Oman Vision 2040 is being followed by the project which aims to help the country with digital preparedness, job readiness and improving cyber awareness.

Overall, the project achieved its objectives by providing a solid, detailed and effective system for cybersecurity training. The actions addressed the problems found in the network by using strong network planning, wise risk control and teachable awareness tools. Combining practice exercises, simulations and educational campaigns has proven to be very useful in making educational environments more prepared for cybersecurity threats. Extra measures should be taken such as broadening training to address more severe cyberattacks, using assessment systems all the time and spreading the adoption of this approach to boost the country's cybersecurity.

6.6. Project Team Reflections

6.6.1. Laila Tamer Abdelhamid – 23F24083

Working on the development of the Cybersecurity Awareness Training Lab has been a rewarding learning experience that integrates knowledge with practice. As a second-year student majoring in Cybersecurity Engineering, the project gave me the opportunity to deal with secure network design and configuration using simulation tools like Cisco Packet Tracer, Wireshark, and Kali Linux.

From a Large-Scale Cybersecurity Project perspective, one of the most rewarding parts of the project was virtual LANs implementation along with inter-VLAN routing implemented by the stick router method. This contributed to my understanding of how organizations partition network traffic to improve security and performance. Along with these, the deployment of essential services like DHCP, DNS, web, and mail servers, helped me understand how real networks work every day and the risks related to each part

In terms of security, I successfully learned many strategic defensive configurations like Access Control Lists (ACLs), remote access via SSH, and port-based network access control. Also, the implementation of DHCP snooping and MAC address filtering improves the overall security of the network and allows me to understand how these elements mitigate different risks.

In addition to the more distinct technical aspects, this project was valuable in relation to my self-development professionally, personally, and socially. By showing initiative within a detailed risk management plan containing structured timelines, task schedules, and risk addressing workflows, I was able to more effectively manage risks during the project. My team participation developed my role-related communication skills including coordination, documentation writing, and presentation. Challenges were often shared and collectively resolved during team discussions and working meetings.

6.6.2. Yamen Hamed Al Dhanki – 23S23781

Participating in the Cybersecurity Awareness and Simulation Lab project has been one of the most valuable and eye-opening parts of my college life. Studying networking and cybersecurity, I found that working on this project connected my classroom learning with actual practices. It improved my technical abilities as well as my critical, independent and time management skills.

At the start, I knew some network basics, the different topologies and little about security measures. Still, manually creating every element of a simulated network using Packet Tracer made me feel really challenged. I had to approach problems from the standpoint of a network engineer, a cybersecurity expert and sometimes act like a system administrator. Every element, including planning IP schemes, setting up routing protocols and implementing VLANs and ACLs, demanded careful handling and close attention.

Reflecting on it, I see that this project has influenced my view of cybersecurity. Focusing on firewalls, protocols or intrusion detection is not enough; what's important is developing awareness, responsibility and resilience in people. The point is to help individuals and institutions defend themselves by providing the right knowledge and tools. Because of this project, I am more passionate than ever about pursuing cybersecurity in the future.

In short, the Cybersecurity Awareness and Simulation Lab was both a technical project and an individual journey of growth and discovery. It allowed me to visit places I have never been to, handle problems and make use of my talents. I appreciate all the experience I've had and feel sure that the knowledge and skills I possess will be helpful in shaping my future activities in cybersecurity and IT.

6.6.3. Taha Mohammed Al Balushi – 23F24590

Engaging in the Cybersecurity Awareness and Simulation Lab has been both pleasant and a beneficial part of my education. Doing projects in class, I could put what I learned in theory to use in actual tasks which improved my knowledge of networking and cybersecurity. The process helped me boost my abilities in programming as well as in resolving problems, connecting with others and managing time.

At first, I had only a basic idea of networking and some knowledge of Cisco Packet Tracer. Setting up the simulated network, along with adding VLANs, router protocols and access rules was a difficult process. Analyzing and fixing network issues in Packet Tracer required me to remain patient and thoughtful which helped my critical thinking.

Additionally, building network diagrams with Microsoft Visio initially proved to be quite a challenge. Soon after, I studied the tool's options and used them to draw network diagrams accurately which took me some effort yet turned out to be very helpful in learning how to document complex systems.

A major difficulty I had was ensuring the attack videos were recorded in a clear and efficient way. Getting the videos clear and covering all the important information was done only after several tries and detailed planning. This situation showed that it is necessary to clearly explain technical details of cybersecurity to people with different backgrounds.

This experience has made me realize that the project gave me a better understanding of cybersecurity. It includes configuring devices and setting up protocols as well as learning how to be responsible with cyber security. This understanding is necessary for organizations and people to keep their digital data safe. Working on this project has boosted my wish to learn more about this subject.

Overall, the Cybersecurity Awareness and Simulation Lab tested my abilities and shaped my character. Through it, I got to handle real cybersecurity examples, pick up new skills and work on my abilities. Gaining work experience lets me believe that I am well-equipped for any future cybersecurity projects.

6.6.4. Sheikha Rashid Al Hinai – 23F24676

During the process of Cybersecurity Awareness Training Lab project, I learnt a lot in terms of technique and personal feelings. I enhanced my knowledge on real-world cyber security tools and network setups through Cisco Packet Tracer (VLANs, ACLs NAT and Remote Access Configurations). Also, I learned how to effectively apply these concepts, and not only "by the book", but in practice.

The team performed well as a whole. Everyone did their part and respected the deadlines, which helped us stay organized. The work was separated according to each team members strengths and talents, and it made the process easier. One of the challenges was working on the Cisco Packet Tracer together and managing multiple Word documents without a shared file. This caused confusion and made it difficult to identify which version of the chapter was the most current.

Despite those difficulties I enjoyed it and was motivated. I enjoyed the process of having to solve problems and learning through hands-on practice. One thing that stood out to me was working on logical network design, it helped me understand how all the components come together to make a secure and functional system. If I were to do the project again, I would recommend using shared platforms something like Google Docs to make collaboration smoother and avoid confusion.

This experience relates very well to my field of study in networking and cybersecurity. It helped me turn what I learned in the classroom into practical skills and showed me how real networks are built and secured. I can use what I learned from this project to better understand how cybersecurity works in real life, especially how important hands-on practice and teamwork are. At the same time, the limit of my experience was that we practiced on a simulated network that does not represent the scale and pressure of live environments. Still, the project gave me good opportunities for personal and professional growth. My technical skills became stronger, improved my teamwork, and learned how to manage group work better. I believe I met most of my goals and came out of this project better prepared for future challenges in the field.

6.6.5. Hamza Suleiman Aladawi - 23F24607

Being involved in this project has proved to be one of the most meaningful and uplifting experiences in my education. I was able to study cybersecurity more, see how networks are organized, and get experience using these tools for real purposes. I first studied what various cyberattacks consist of and then investigated ways to secure networks from threats like phishing, snooping networks for information, and illegal access. I was able to understand tree topology, VLANs, ACLs, and SSH setup by doing a Cisco Packet Tracer course and watching many online tutorials. I designed a cybersecurity-focused questionnaire on the internet and looked at the results using Power BI by building a dashboard. It guided me and provided the information I needed to understand the problem. To make our research stronger, I interviewed a cybersecurity expert from the National University of Oman, gaining additional real-life insights into our topic.

At first, it was tough for us to arrange what we needed to do and organize our documentation. Later, modifications and practice made the group perform better as a team. I volunteered to take charge and delegated duties, followed the progress being made, and saw that everything stayed on time. This experience taught me the importance of being organized, cooperating with others, and explaining technical information in an easier way. We experienced some technical issues that we had to overcome. Initially, Intrusion Detection Systems (IDS) would have been useful, but Cisco Packet Tracer didn't have the option for them. Although we tried GNS3 and EVE-NG, our setup wasn't advanced enough, so we kept working on Packet Tracer instead.

During the project, I felt a range of emotions, from being frustrated to feeling motivated and always proud of the things we managed to accomplish. Whenever an idea didn't turn out as hoped, I felt nervous, but I always learned from those instances. Resolving network issues helped me understand the technology better and boosted my ability to solve problems. My experience shows that practicing by yourself is one of the most effective ways to learn technical skills.

The next time I work on a project, I recommend everything should be organized from initial stages, by creating deadlines for different parts, planning online meetings, and communicating more often with mentors regarding our work. It would help us as a group to accomplish tasks faster and without feeling pressured.

Overall, my participation in this project allowed me to use class knowledge and improve my leadership and technical abilities while growing my involvement in cybersecurity. Although it was tough, I achieved what I set out to do and now more confident about where I am headed in this area.

REFERENCES

1. Aleksic, M. (2022). What is ACL in networking & how to implement it? *phoenixNAP*. https://phoenixnap.com/kb/acl-network
2. AlexHost. (n.d.). What is MAC flooding? How to prevent it? https://alexhost.com/faq/what-is-mac-flooding-how-to-prevent-it/
3. Amin, D. (2019, February 12). *Chapter 5: Agile software development* [PowerPoint slides]. SlideShare. https://www.slideshare.net/slideshow/chapter-5-agile-software-development/131438690
4. Anomali. (n.d.). *Top 10 cybersecurity challenges enterprise organizations face*. https://www.anomali.com/blog/top-10-cybersecurity-challenges-enterprise-organizations-face
5. Ariganello, J. (2022). *Dealing with the cybersecurity challenges of digital transformation*. Anomali. https://www.anomali.com/blog/dealing-with-the-cybersecurity-challenges-of-digital-transformation
6. B&H Photo Video. (n.d.). *Cisco Catalyst 2960 24-Port PoE Ethernet switch with 2 dual-purpose uplinks*. https://www.bhphotovideo.com/c/product/745523-REG/Cisco_WS_C2960_24PC_L_Catalyst_2960_24_Port_PoE.html
7. Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., & Thomas, D. (2001). *Manifesto for agile software development*. https://agilemanifesto.org/
8. Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security, 78*, 350–364. https://doi.org/10.1016/j.cose.2018.07.008
9. Brace, I. (2018). *Questionnaire design: How to plan, structure and write survey material for effective market research* (4th ed.). Kogan Page.
10. Brand Logo Vector. (n.d.). *Microsoft Word logo vector*. https://brandlogovector.com/microsoft-word-logo-vector/
11. Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
12. BS-Concepts GmbH. (n.d.). *Microsoft Power BI, kostenlose Version*. https://www.bs-concepts.com/produkt/microsoft-power-bi-kostenlose-version/
13. CDW. (n.d.). *Cisco Business 140AC - wireless access point - Wi-Fi 5*. https://www.cdw.com/product/cisco-business-140ac-wireless-access-point-wi-fi-5/6285173
14. Chowdhury, M. M. H., Colley, S., Abdelgadir, A., & Gabrys, B. (2021). Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security, 105*, Article 102551. https://doi.org/10.1016/j.cose.2021.102551

15. Cisco. (2023). *Understand the Hot Standby Router Protocol features and functionality*. https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html
16. Cisco. (2025). *Spanning Tree Protocol*. https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html
17. Cisco. (2025). *Understand VLAN Trunk Protocol (VTP)*. https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html
18. Cisco. (n.d.-a). *Hot Standby Router Protocol (HSRP)*. https://www.cisco.com/c/en/us/tech/ip/hot-standby-router-protocol-hsrp/index.html
19. Cisco. (n.d.-b). *Overview of Layer 2 switched networks and communication*. https://community.cisco.com/t5/networking-knowledge-base/overview-of-layer-2-switched-networks-and-communication/ta-p/3128423
20. Cisco. (n.d.-c). *Configure and filter IP access lists*. https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html
21. Cisco. (n.d.-e). *Configure TFTP servers*. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU2/systemConfig/cucm_b_system-configuration-guide-1251su2/cucm_b_system-configuration-guide-for-cisco-1251su2_chapter_011111.pdf
22. Cisco. (n.d.-f). *Configure network address translation*. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html
23. Cisco. (n.d.-g). *What is a management VLAN? How to configure VLAN management*. https://community.cisco.com/t5/networking-blogs/what-is-a-management-vlan-how-to-configure-vlan-management/ba-p/5138052
24. Cisco. (n.d.-h). *SNMP configuration guide*. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book.html
25. Cisco. (n.d.-k). *Configuring port security* [PDF]. https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011111.pdf
26. Cisco. (n.d.-l). *Configure SSH on routers and switches*. https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
27. Cisco Networking Academy. (2023). *Packet Tracer tutored activity course: Troubleshoot a wireless connection*. https://www.netacad.com/launch?id=dc0847b7-ef6c-4597-bc31-38ddd6b07a2f&tab=curriculum&view=8c4538d2-d082-5f2f-98f2-6a7a5c4a2abc
28. Cisco Networking Academy. (n.d.). *Introduction to cybersecurity*. https://www.netacad.com/launch?id=dc0847b7-d6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=a3899440-d246-5b65-ba11-fb9077b7b8de

29. Cisco Systems. (2023). *Cisco Packet Tracer*. Cisco Networking Academy. https://www.netacad.com/courses/packet-tracer
30. CTC Union. (n.d.). *Access switch*. https://www.ctcu.com/en/category/CATE-Access-Switch.html
31. Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.
32. Dell Laptop. (n.d.). In *Exporters India*. https://www.exportersindia.com/product-detail/dell-laptop-6004650.htm
33. Domínguez, M., Prada, M. A., Reguera, P., Fuertes, J. J., Alonso, S., & Morán, A. (2017). Cybersecurity training in control systems using real equipment. *IFAC-PapersOnLine, 50*(1), 12179–12184. https://doi.org/10.1016/j.ifacol.2017.08.2151
34. Fowler, M. (n.d.). *The new methodology*. MartinFowler.com. https://martinfowler.com/articles/newMethodology.html
35. Freepik. (n.d.). *YouTube logo*. Retrieved June 1, 2025, from https://www.freepik.com/free-photos-vectors/youtube-logo
36. GeeksforGeeks. (2024). *Difference between trunk port and access port*. https://www.geeksforgeeks.org/difference-between-trunk-port-and-access-port/
37. GeeksforGeeks. (2024). *Types of network topology*. https://www.geeksforgeeks.org/types-of-network-topology/
38. GNS3 Documentation. (2023). *GNS3 and cloud simulation environments*. https://docs.gns3.com/docs/
39. Glas, M., Vielberth, M., Reittinger, T., Böhm, F., & Pernul, G. (2023). Improving cybersecurity skill development through visual programming. *Information and Computer Security, 31*(3), 509–529. https://doi.org/10.1108/ICS-11-2022-0170
40. Haiilo. (2023). *What is team communication, why it matters, and how to get it right*. https://blog.haiilo.com/blog/team-communication/
41. Hayudini, M. A. (2021). Network infrastructure management: Its importance to the organization. *Natural Sciences Engineering and Technology Journal, 2*(1), 62–67. https://doi.org/10.37275/nasetjournal.v2i1.15
42. Heusser, M. (2013, August 12). *Has agile software development gone mainstream? CIO*. https://www.cio.com/article/288838/agile-development-has-agile-software-development-gone-mainstream.html
43. Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game-based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)* (pp. 68–73). ACM. https://doi.org/10.1145/3159450.3159591
44. Kävrestad, J., & Nohlberg, M. (2021). Evaluation strategies for cybersecurity training methods: A literature review. In N. Clarke & S. Furnell (Eds.), *Human aspects of information security and assurance* (Vol. 613, pp. 102–112). Springer. https://doi.org/10.1007/978-3-030-81111-2_9

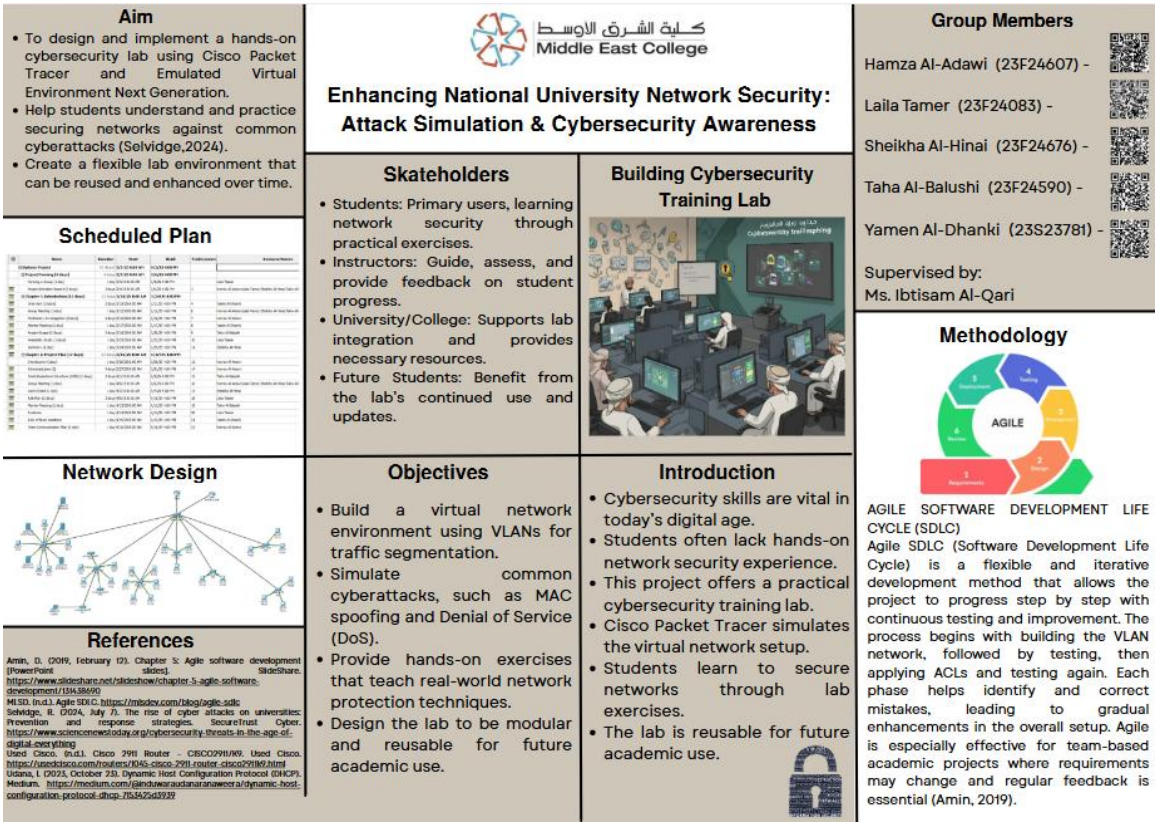
45. Lewis, L., & Lewis, A. (2020, September 7). *Chapter structure: How to write the perfect chapter*. The Novel Smithy. https://thenovelsmithy.com/chapter-structure/
46. LinuxServer.io. (n.d.). *linuxserver/wireshark*. Retrieved June 1, 2025, from https://docs.linuxserver.io/images/docker-wireshark/
47. Logos-world.net. (2024, April 12). *Canva logo, symbol, meaning, history, PNG, brand*. https://logos-world.net/canva-logo/
48. Logos-World. (2025, April 4). *CapCut logo*. Retrieved June 1, 2025, from https://logos-world.net/capcut-logo/
49. Love Tech AI. (2024, December 16). *Advantages and disadvantages of campus area network*. https://lovetechai.com/advantages-and-disadvantages-of-campus-area-network/
50. ManageEngine. (n.d.). *Switching loops*. https://www.manageengine.com/network-monitoring/tech-topics/switching-loops.html
51. Microsoft. (2018, September 26). *Fundamentals of computer networking*. Microsoft Learn. https://learn.microsoft.com/en-us/training/modules/network-fundamentals/
52. Microsoft. (2023). *Microsoft Visio*. Microsoft Corporation. https://www.microsoft.com/visio
53. Microsoft Teams. (n.d.). *Microsoft Teams* [Online tool]. Microsoft. https://www.microsoft.com/en/microsoft-teams/group-chat-software
54. MS Codes. (2023). *Building a cybersecurity lab environment in EVE-NG*. https://ms.codes/blogs/cybersecurity/cybersecurity-lab-environment-in-eve-ng
55. National Institute of Standards and Technology. (2023). *Cybersecurity framework*. https://www.nist.gov/cyberframework
56. National University of Science & Technology. (2022). *History*. https://nu.edu.om/history
57. Networks Learning. (n.d.). *Cisco Packet Tracer*. https://networkslearning.com/cisco-packet-tracer/
58. Networking. (2021, December 16). *Networking project simulating XYZ company network design using Cisco Packet Tracer* [Video]. YouTube. https://youtu.be/kqoSYlqEu64?si=0votGyMbeRoJaxpd
59. Nikhil Computers. (n.d.). *Dell laptop*. In *Exporters India*. https://www.exportersindia.com/product-detail/dell-laptop-6004650.htm
60. Odom, W. (2020). *CCNA 200-301 official cert guide, volume 1*. Cisco Press. https://elhacker.info/manuales/Redes/Cisco/CCNA%20Ebooks/CiscoPress-CCNA-200-301-Official-Cert-Guide-Volume-1.pdf
61. Patnaik, M. (2024, January 11). *What are the features of cyber security? A complete guide*. AlmaBetter. https://www.almabetter.com/bytes/articles/features-of-cyber-security
62. Prümmer, J., van Steen, T., & van den Berg, B. (2023). A review of cybersecurity training strategies in the current research landscape. *Computers & Security, 112*, Article 102458. https://doi.org/10.1016/j.cose.2021.102458

63. Project Management Academy. (2022). *Introduction to risk management plan*. https://projectmanagementacademy.net/resources/blog/introduction-to-risk-management-plan/
64. ProjectManager.com. (2024). *How to make a risk management plan (template included)*. https://www.projectmanager.com/blog/risk-management-plan
65. Qawasmeh, S. A.-D., AlQahtani, A. A. S., & Khan, M. K. (2025). Navigating cybersecurity training: A comprehensive review. *Computers and Electrical Engineering, 123*, Article 110097. https://doi.org/10.1016/j.compeleceng.2025.110097
66. Queen's University Belfast. (2025, March 11). *Introduction to Microsoft Visio*. QUB Blogs. https://blogs.qub.ac.uk/digitallearning/event/introduction-to-microsoft-visio/
67. Rouse, M. (2022). *Virtual LAN (VLAN)*. TechTarget. https://www.techtarget.com/searchnetworking/definition/virtual-LAN
68. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & M, N. J. J. C. (2020). An effective cybersecurity training model to support an organizational awareness program. In *IGI Global eBooks* (pp. 174–188). https://doi.org/10.4018/978-1-7998-7705-9.ch008
69. ScienceDirect Topics. (n.d.). *Work breakdown structure*. Retrieved April 19, 2025, from https://www.sciencedirect.com/topics/engineering/work-breakdown-structure
70. Seek Logo. (n.d.). *Microsoft PowerPoint 2013 logo PNG vector (SVG) free download*. https://seeklogo.com/vector-logo/298302/microsoft-powerpoint-2013
71. Selvidge, R. (2024, July 7). The rise of cyber attacks on universities: Prevention and response strategies. *SecureTrust Cyber*. https://www.sciencenewstoday.org/cybersecurity-threats-in-the-age-of-digital-everything
72. Sequeira, D. (2020). Router-on-a-stick inter-VLAN routing. Cisco Press. https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=5
73. Shiksha. (2024). *Tree topology: Features and advantages*. https://www.shiksha.com/online-courses/articles/tree-topology-features-advantages-and-disadvantages/
74. Shutterstock. (n.d.). *DNS server icon communication technology concept*. https://www.shutterstock.com/image-vector/dns-server-icon-communication-2220378645
75. Stallings, W. (2016). *Network security essentials: Applications and standards* (6th ed.). Pearson. https://bayanbox.ir/view/449483728521785029/Network-security-essentials-6th-edition-william-stallings.pdf
76. Stallings, W. (2020). *Network security essentials: Applications and standards* (6th ed.). Pearson. https://api.pageplace.de/preview/DT0400.9781292154916_A37747529/preview-9781292154916_A37747529.pdf
77. StickPNG. (n.d.). *Microsoft Teams logo*. Retrieved June 1, 2025, from https://www.stickpng.com/img/icons-logos-emojis/video-conference-software-providers/microsoft-teams-logo

78. StickPNG. (n.d.). *Google Docs logo and symbol*. Retrieved June 1, 2025, from https://www.stickpng.com/img/icons-logos-emojis/iconic-brands/google-docs-logo-and-symbol
79. Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer networks* (5th ed.). Pearson Education. https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf
80. Telkom University. (n.d.). *DNS server is: Definition, how it works and its functions*. https://bif.telkomuniversity.ac.id/en/what-is-dns/
81. Tunc, C., Hariri, S., De La Peña Montero, F., Fargo, F., & Satam, P. (2015, September 1). CLaaS: Cybersecurity Lab as a Service – Design, analysis, and evaluation. *2015 IEEE International Conference on Cloud and Autonomic Computing (ICCAC)*, 279–285. https://doi.org/10.1109/ICCAC.2015.34
82. Udana, I. (2023, October 23). *Dynamic Host Configuration Protocol (DHCP)*. Medium. https://medium.com/@induwaraudanaranaweera/dynamic-host-configuration-protocol-dhcp-7153425d3939
83. Used Cisco. (n.d.). *Cisco 2911 router - CISCO2911/K9*. https://usedcisco.com/routers/1045-cisco-2911-router-cisco2911k9.html
84. Wadhwa, K. (2024). *The role of Gantt chart in project management* [bachelor's thesis, Laurea University of Applied Sciences]. Theseus. https://www.theseus.fi/handle/10024/865913
85. Xie, N. (2018). Interval grey number-based project scheduling model and algorithm. *Grey Systems: Theory and Application, 8*(1), 100–109. https://doi.org/10.1108/GS-11-2017-0035

Appendix

Project Poster



Approval Form

كـــلية الشـــرق الأوســـط
Middle East College

Certificate of Ethical Approval

RollNumber 23F24607

Student Name HAMZA SULEIMAN RASHID AL ADAWI

Semester 2025 Spring

Project Title

Enhancing National University Network Security: Attack Simulation & Cybersecurity Awareness

This is to certify that the above named student has completed the Middle East College Ethical Approval process and their project has been confirmed and approved as Low Risk.

Supervisor Ibtisam Al Qari

Date of Approval Jun 18, 2025

Interview Questions

Q1. Our project enhances NU network security using Cisco Packet Tracer, Wireshark, Kali Linux OS, and MS Visio. It also includes creating a website and a dashboard containing quizzes and videos for awareness. What important features should we consider enhancing our project?

Q2. How can we ensure the cybersecurity lab is isolated and doesn't risk infecting or compromising the campus network?

Q3. What specific topics or types of attacks should we prioritize for training students and staff in our cybersecurity lab?

Q4. From your experience, what are the most effective ways to raise cybersecurity awareness among students and staff beyond just traditional lectures?

Q5. How can our project support Oman Vision 2040 goals related to digital transformation and the knowledge-based economy?

Questionnaire

Q1: What is your major?

Q2: What are the biggest cybersecurity threats facing students and university staff today?

Q3: Which learning method do you prefer for cybersecurity education?

Q4: How would you rate your current knowledge of cybersecurity?

Q5: Do you think that university students need to focus more on practical cybersecurity training?

Q6: What do you think is the best way to improve email security?

Q7: Which of the following cybersecurity practices do you follow?

Q8: In your opinion, which of the following topics should be included in a cybersecurity training lab?

Q9: Do you believe hands-on labs are important for learning cybersecurity? Why or why not?

Project Testing

Project Title:			
Specialization:		Test Date:	
Team	**Student ID**	**Student Name**	
	23F24607	HAMZA SULEIMAN RASHID AL ADAWI	
	23F24083	LAILA TAMER ABDELHAMID ELSAYED MEKHIMAR	
	23F24676	SHEIKHA RASHID SHAIKHAN AL HINAI	
	23F24590	TAHA MOHAMMED ALI AL BALUSHI	
	23S23781	YAMEN HAMED YAHYA AL DHANKI	

Tester Name	Signature	Date
Ibtisam Al Qari (Supervisor)		

The Implementation Test:

Test #	Environment	Description	Expected Result	Actual Result	Pass/ Fail	Comment
1	Packet tracer	Creating different vlans	**Communication between different devices in different vlans**	**work**	**pass**	**-**

2	Packet tracer	Access Control Lists (ACLs)	**to manage the flow of traffic connecting various VLANs**	**work**	**pass**	
	Packet tracer	Configure SSH	**to give secure, remote access to network devices through encryption**	**work**	**pass**	
	Packet tracer	DHCP	**TO assign IP addresses automatically for devices**	**work**	**pass**	
	Packet tracer	Two routers	**For backup**	**work**	**pass**	**-**
	Packet tracer	Trunk ports	**To allow all VLANs for inter-switch communicatio n**	**work**	**pass**	**-**
	Packet tracer	Email Service	**Simulated email server used to test sending/receivi ng messages within the network.**	**work**	**pass**	

	Packet tracer	Wireless Network	**Wireless Access Points are configured to provide Wi-Fi connectivity to clients.**	**work**	**pass**	
	Packet tracer	HSRP	**Hot Standby Router Protocol ensures gateway redundancy between two routers.**	**work**	**pass**	
	Wireshark	Packet Sniffing attack	**Capturing and analyzing packets to demonstrate network vulnerability to sniffing.**	**work**	**pass**	
	Kali Linux	payload	**A crafted code used to exploit systems**	**work**	**pass**	
	Kali Linux	Web cloning	**Cloning a legitimate website to capture login credentials**	**work**	**pass**	

Pre-Graduation Program Certificates

كلية الشرق الأوسط
Middle East College

Enterprising, Resillient, Impactful

CERTIFICATE
OF COMPLETION

Proudly presented to :

LAILA TAMER ABDELHAMID MEKHIMAR

for successfully completing the Pre-Graduation Program - Spring 2025 at Middle East College. This program is aimed to enhance graduates' employability and readiness to the World of Work.

Director - Employability and Partnerships

Head of World of Work Services

كلية الشرق الأوسط
Middle East College

Enterprising, Resillient, Impactful

CERTIFICATE
OF COMPLETION

Proudly presented to :

SHEIKHA RASHID SHAIKHAN AL HINAI

for successfully completing the Pre-Graduation Program - Spring 2025 at Middle East College. This program is aimed to enhance graduates' employability and readiness to the World of Work.

Director - Employability and Partnerships

Head of World of Work Services


كـلية الشـرق الأوسـط
Middle East College
Enterprising, Resilient, Impactful
CERTIFICATE
OF COMPLETION
Proudly presented to :
TAHA MOHAMMED ALI AL BALUSHI
for successfully completing the Pre-Graduation Program - Spring 2025 at Middle East College. This program is aimed to enhance graduates' employability and readiness to the World of Work.
Director - Employability and Partnerships
Head of World of Work Services

List of Abbreviations

Abbreviation	Full Form
VLAN	Virtual Local Area Network
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
MAC	Media Access Control
SSH	Secure Shell
S/MIME	Secure/Multipurpose Internet Mail Extensions
PGP	Pretty Good Privacy
HTTPS	Hypertext Transfer Protocol Secure
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SNMP	Simple Network Management Protocol
ACL	Access Control List
TCP/IP	Transmission Control Protocol / Internet Protocol
DNS	Domain Name System
QoS	Quality of Service
NU	National University
PSK	Pre-Shared Key
VTY	Virtual Teletype

STP	Spanning Tree Protocol
HR	Human Resources
HRIS	Human Resources Information System
HSRP	Hot Standby Router Protocol
ISP	Internet Service Provider
SET	Social Engineering Toolkit
PC	Personal Computer
RTR	Router (used as part of CORE-RTR and BACKUP-RTR)
QR	Quick Response (as in QR code)