UNIVERSITY OF COMPUTER STUDIES, HINTHADA

INTERNSHIP PROJECT

MIN HTET MOE YAN

B.C.Tech. **AUGUST, 2025**

CAMPUS LOCAL AREA NETWORK MANAGEMENT SYSTEM
(Web Hosting, Security Management, and Monitoring)

By

MIN HTET MOE YAN

A Dissertation Submitted in Partial Fulfillment of
the Requirements for the Degree of
Bachelor of Computer Technology
(B.C.Tech.)
of the

UNIVERSITY OF COMPUTER STUDIES, HINTHADA
AUGUST, 2025

CONTENT

PAGES

ACKNOWLEDGEMENT i

ABSTRACT ii

CHAPTER 1 INTRODUCTION 1

1.1 Experience of Internship 2

1.2 Motivation 2

1.3 Objectives of the System 3

1.4 Summary of the Project Book 3

CHAPTER 2 BACKGROUND THEORY 5

2.1 Windows Servers 2022 5

2.2 Oracle VirtualBox 7

2.3 Windows 10 Pro 8

2.4 IIS Web Server 8

2.5 File Sharing with Security Permissions 9

2.6 Remote Desktop 10

2.7 Group Policy Objects (GPOs) 11

2.8 Window PowerShell 12

CHAPTER 3 SYSTEM DESIGN 13

3.1 Network Diagram 13

3.2 Functional Block Diagram 14

3.3 System Flow Diagram 15

CHAPTER 4 IMPLEMENTATION 17

4.1 Server Configuration 17

4.1.1 IIS Web Server Configuration 17

4.1.2 File Sharing with Security Permissions configuration 21

4.1.3 Drive Mapping and Account Logout Policy with GPO Configuration 25

4.2 Client Configuration 27

4.2.1 Remote Desktop Configuration 27

4.3 Implementation Result 28

4.3.1 Local Host Web Page in LAN 28
4.3.2 File Sharing with Security Permissions 29
4.3.3 Drive Mapping and Account Logout Policy with GPO (Group Policy Object) LAN 31
4.3.4 Network Traffic Monitoring Using Wireshark 32
4.3.5 Remote Desktop Using PowerShell Script DHCP Monitoring 33
CHAPTER 5 CONCLUSION AND FUTURE WORK 34
5.1 Advantages of the Project 34
5.2 Limitation and Future Work 35
REFERENCES

LIST OF FIGURES **PAGES**

Figure 2.1 Logo for Windows Server 2022 6
Figure 2.2 Oracle VirtualBox..... 8
Figure 2.3 Windows 10 Professional..... 9
Figure 2.4 IIS Web Server 10
Figure 2.5 Waterfall Permission Model.....11
Figure 2.6 Example Picture of Remote Desktop 12
Figure 2.7 Sample Architecture of GPO..... 13
Figure 2.8 Windows PowerShell..... 13
Figure 3.1 Network Diagram 14
Figure 3.2 Functional Block Diagram 15
Figure 3.3 System Flow Diagram 17
Figure 4.1 Managing Add Roles and Features..... 18
Figure 4.2 Role-based or Feature-based Installation 19
Figure 4.3 Destination Server Selection 19
Figure 4.4 Server Roles Selection 20
Figure 4.5 IIS Web Server Manager 21
Figure 4.6 IIS Configuration of ucsh.edu.mm/fcst Webpage 21
Figure 4.7 Website Hosting Folder Path 22
Figure 4.8 Sample Hosted Webpage (HTML, CSS and Images) 22
Figure 4.9 Share Folder: Admins and Students 23
Figure 4.10 Security Group..... 24
Figure 4.11 Add Permission in Teachers Folder 25
Figure 4.12 Add Permission in Students Folder 25
Figure 4.13 Mapped Drives Policy..... 26
Figure 4.14 Drive Maps 26
Figure 4.15 Setting Drive Label in Group Policy Drive Map Properties 27
Figure 4.16 Account Lockout Policy in Group Policy Management Editor 28
Figure 4.17 Run System.cpl 29
Figure 4.18 Allow Remote Connection 29
Figure 4.19 Web Page of FCST..... 30
Figure 4.20 Login with an Admin Account on a Client PC 31
Figure 4.21 Login with a Student Account on a Client PC 31

Figure 4.22 Show Drives in Network Location 32
Figure 4.23 Lock Account 33
Figure 4.23 Wireshark Monitoring UI..... 33
Figure 4.23 Remote Desktop Connection 33
Figure 4.22 Remote Desktop Server to Client 32

LIST OF TABLES **PAGES**

Table 2.1 Detail of Windows Server 2022..... 6
Table 2.2 Requirement of Oracle VirtualBox..... 7

ACKNOWLEDGEMENT

I want to express my gratitude to **Prof. Dr. Tun Myat Aung,** Vice-Rector of the University of Computer Studies, Hinthada for giving me the chance to work on a project. He helped me comprehend many concepts and provided all the assistance and direction I needed to finish the project properly. He provided the necessary components and guidance for the project and we are very grateful.

Another thing I would like to thank is the Head of Department, Faculty of Computer Systems and Technologies, **Dr. Khin Kyu Kyu**, Professor, for her support, wise advice, and insightful comments.

I would like to especially thank to my project supervisor and course coordinator, **Daw Thida Soe,** Associate Professor who showed a genuine interest in my work and led me throughout the entire process by giving me all the information I needed to create a successful system. Her advice was helpful to me throughout the entire project. I could not have envisioned a more ideal mentor for my project.

I would like to thank my internship supervisor, **Daw May Thae Sue** (Team Lead of Microsoft), for providing me with group internship possibilities and guiding me while I worked on intriguing projects across a variety of industries.

In addition, I would like to express my gratitude to my friends. I am very grateful to my friend, who patiently told me what I did not understand while I was compiling the text and actively helped me. Finally, I would like to express my gratitude to my parents and family members for their unwavering support, assistance, and encouragement.

ABSTRACT

The Campus Local Area Network Management System, developed using Windows Server 2022, is designed to provide secure, efficient, and reliable resource management within a university environment. The system integrates key services such as Active Directory Domain Services (AD DS), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Group Policy Objects (GPO) to centralize user and device management. An internal website is hosted via Internet Information Services (IIS), ensuring convenient access to academic and administrative resources. File sharing with security permissions enforces role-based data access, while GPO policies automate drive mapping and session control. PowerShell scripts are employed to monitor active and inactive devices in the DHCP scope, and AD DS logs are analyzed to track domain user logon and logoff activities for accountability. Remote Desktop provides administrators with efficient troubleshooting capabilities, and Wireshark supports continuous traffic monitoring for performance and security. Together, these solutions deliver a secure, reliable, and well-organized campus-wide IT infrastructure.

CHAPTER 1
INTRODUCTION

A secure and well-structured Local Area Network (LAN) is essential for modern educational institutions, as it provides the foundation for centralized management, efficient communication, and seamless resource sharing.

This project focuses on implementing a comprehensive Campus LAN Management System using Windows Server 2022. The system is engineered to deliver a reliable, scalable, and secure IT infrastructure that supports both academic and administrative functions.

At the core of this system, Internet Information Services (IIS) hosts a campus web portal, providing students, faculty, and staff with a unified platform to access resources, announcements, and administrative services.

This centralization enhances availability, consistency, and ease of management. Secure file sharing with granular, role-based permissions ensures that sensitive data is protected, allowing only authorized users to access or modify files. This prevents unauthorized access and maintains data integrity across the network.

To streamline operations and bolster security, Group Policy Objects (GPO) automate essential functions such as network drive mapping, automatic logoff, and session lock enforcement across different user groups.

For enhanced monitoring, PowerShell scripts identify active and inactive devices within the DHCP scope, giving administrators real-time visibility into all network clients. Additionally, Active Directory Domain Services (AD DS) event logs are analyzed to monitor user logon and logoff activities, which is critical for auditing and accountability.

For administrative efficiency, Remote Desktop allows secure access to client computers, enabling timely troubleshooting, software updates, and remote system management.

Alongside this, Wireshark provides continuous network traffic monitoring, assisting in identifying performance bottlenecks, unusual activity, or potential security threats.

By combining centralized hosting, secure access controls, automation, monitoring, and remote management, this system offers a comprehensive and future-

ready campus LAN solution that meets the evolving demands of a modern educational environment.

1.1 Experience of Internship

I completed a three-month internship from March to July, which offered valuable opportunities to enhance my technical skills, deepen my knowledge, and gain hands-on experience in my field. The internship program was designed to help students develop practical abilities, gain real-world exposure, and improve social and professional interactions. During this period, I learned about Hybrid IT Infrastructure Implementation, which provided insights into integrating on-premises systems with cloud technologies for efficient operations. Additionally, I gained substantial practical experience by working on projects such as the Student Attendance Tracker Application and the design and testing of an AI Chatbot, which strengthened my problem-solving, programming, and analytical skills.

Throughout the internship, I collaborated closely with experienced colleagues, observing their approaches and learning from their expertise. This mentorship and teamwork significantly enhanced my professional development, communication skills, and confidence in applying theoretical knowledge to real-world scenarios. Overall, the internship was an enriching experience that prepared me for future challenges in my field.

1.2 Motivation

In modern educational institutions, effective management of network resources is critical for smooth academic and administrative operations. A campus LAN connects multiple devices, servers, and services, enabling students, faculty, and staff to access information, collaborate, and communicate efficiently. However, as the number of users and devices grows, managing network configurations, security, and resource allocation manually becomes time-consuming, error-prone, and inefficient.

The motivation behind developing a Campus LAN Management System is to centralize control, enhance network security, and improve operational efficiency. By integrating services such as Active Directory, DHCP, DNS, file sharing, and network monitoring, the system ensures that network resources are allocated automatically, user accounts and permissions are managed consistently, and network performance can be tracked in real time.

Moreover, the system supports remote administration, reducing the need for on-site intervention and allowing IT staff to respond to issues quickly. With a LAN management system, educational institutions can reduce downtime, enforce security policies effectively, and provide seamless access to digital resources, thus fostering a productive and technologically advanced campus environment.

1.3 Objectives of the System

The Campus Local Area Network Management System using Windows Server 2022 provides secure, efficient, and centralized management of campus resources. The server was configured with AD-DS for user and device control, along with DNS and DHCP for domain resolution and IP allocation. GPOs were applied to enforce password, account lockout, and drive mapping policies. For resource sharing, I implemented file sharing with access control and hosted web resources using IIS. PowerShell was used for DHCP monitoring, while Remote Desktop Services enabled remote administration and client support. The objectives of this project are:

- To host campus web resources and provide easy access to internal information.
- To enable secure file sharing with proper access permissions.
- To monitor network traffic effectively and troubleshoot issues in real time.
- To allow administrators to remotely manage and support client machines efficiently.
- To implement GPO settings for password policy, account lockout, and drive mapping.
- To enhance network usability, security, and overall operational efficiency.
- To manage users, groups, and devices centrally through Active Directory Domain Services (AD-DS).
- To provide automated IP address allocation and management using DHCP.
- To ensure reliable domain name resolution and network connectivity with DNS.

1.4 Summary of the Project Book

This project presents the design and implementation of a Campus Local Area Network (LAN) Management System using Windows Server (2022) as the core platform. The system was deployed and tested in a virtualized environment using Oracle VirtualBox, with Windows 10 Pro serving as the client operating system.

In Chapter 2, the background theory explores the foundational technologies that support the system. It begins with Windows Server 2022, which provides the backbone for centralized network services. Oracle VirtualBox enables virtualization for testing and deployment, while Windows 10 Pro acts as the client interface. The chapter also discusses the use of IIS Web Server for hosting internal web pages, file sharing with security permissions for controlled access, Remote Desktop for remote administration, Group Policy Objects (GPOs) for enforcing organizational policies, and Windows PowerShell for automating administrative tasks.

In Chapter 3, the system design is illustrated through a network diagram, a functional block diagram, and a system flow diagram. These visual tools guided the implementation process and clarified the interaction between server and client components, ensuring a structured approach to system development.

In Chapter 4, the implementation details are presented. The server was configured to support IIS Web Server for hosting a local web page, secure file sharing with defined permissions, and drive mapping with logout policies using GPOs. On the client side, Remote Desktop was configured to enable secure access to the server. The results confirmed that the system successfully delivered a LAN-accessible web page, ensured secure file sharing, and applied policy enforcement through GPOs.

Finally, in Chapter 5, the conclusion highlights the project's success in achieving centralized management, enhanced security, and scalability within a campus network. The advantages include simplified administration and improved control over network resources. The limitations and future work suggest expanding the system to support more clients, integrating cloud-based backups, and refining automation scripts to handle broader administrative tasks.

CHAPTER 2

BACKGROUND THEORY

The development of a Campus Local Area Network (LAN) addresses the need for centralized management, secure communication, and efficient resource sharing in educational institutions. As campuses expand, managing multiple users and devices requires a structured and reliable network infrastructure. Key components include IIS Web Server for hosting internal websites, file sharing with security permissions to control access, and Group Policy Objects (GPOs) to enforce policies such as automatic account logout and restricted network access.

To improve monitoring, PowerShell scripts are used to identify active and inactive devices within the DHCP scope, while Active Directory Domain Services (AD DS) logs track user logon and logoff activities, supporting auditing and security management. A challenge arose with a client machine running Windows 10 Home Single Language; Oracle VirtualBox was used to create a Windows 10 Pro virtual machine, configured with a bridge adapter to join the domain. Remote Desktop, along with switches, client PCs, and network cables, completes the implementation of a secure and functional campus LAN.

2.1 Windows Server 2022

Windows Server 2022 is a modern server operating system developed by Microsoft, designed to provide a secure, reliable, and scalable platform for managing centralized IT infrastructure. It enables organizations, including educational institutions, to efficiently control users, devices, applications, and network resources. By providing centralized management, resource sharing, and network monitoring, Windows Server 2022 supports the smooth operation of a campus LAN, ensuring that students, staff, and administrators can access required services securely and efficiently. Its integration with modern management tools allows IT teams to streamline administrative tasks and reduce downtime across the network.

One of the most important aspects of Windows Server 2022 is its enhanced security. Features such as Secured-core server protection, advanced threat detection, and secure communication protocols like TLS 1.3 and DNS-over-HTTPS help safeguard the network against cyber threats. The operating system also supports Active Directory Domain Services (AD DS) and Group Policy Objects (GPOs), enabling centralized authentication, policy enforcement, and consistent configuration

management across all connected devices. These features are crucial for maintaining control, user accountability, and security within a campus LAN environment.

Table 2.1 Detail of Windows Server 2022

Technical Overview	Key Features and Specifications
Developer	Microsoft
Written in	C, C++, Rust, C#, Assembly language
OS family	Window Server
Working state	Current
Source model	Closed source
Released to manufacturing	May 24, 2021; 4 years ago
General availability	August 18, 2021; 3 years ago[1]
Latest release	21H2 (10.0.20348.4052) (August 12, 2025)
Marketing target	Business
Available in	110 languages
Update method	Windows Update, Windows Server Update Services, SCCM
Package manager	Window Package Manager
Supported platforms	x86-64
Kernel type	Hybrid (Windows NT kernel)
Default user interface	Window Shell
License	Proprietary

Windows Server 2022 also offers improved storage and networking capabilities, including Storage Migration Services, SMB over QUIC, and support for high-speed network adapters, which enhance performance and data accessibility.

Built-in virtualization through Hyper-V and Remote Desktop Services allows administrators to manage client PCs, create virtual environments, and provide secure remote access. Additionally, its hybrid cloud integration with Microsoft Azure enables backup, monitoring, and centralized management across on-premises and cloud resources.

In a campus LAN setting, these features ensure efficient management, reliable connectivity, and scalable infrastructure, making Windows Server 2022 an ideal choice for implementing a secure, well-organized, and centrally controlled network.

Figure 2.1 Logo for Windows Server 2022

2.2 Oracle VirtualBox

Oracle VirtualBox is a powerful open-source virtualization software that allows users to run multiple operating systems simultaneously on a single physical computer. Developed originally by Innotek GmbH in 2007 and later acquired by Oracle Corporation, it supports a wide range of guest operating systems, including Windows, Linux, macOS, and others. VirtualBox works by creating virtual machines (VMs), each with its own virtual hardware such as CPU, memory, storage, and network interfaces, while sharing the physical resources of the host computer. It provides features like snapshots, seamless mode, shared folders, and virtual networking, making it ideal for software testing, development, training, and learning environments. By enabling isolated environments without affecting the host system, VirtualBox enhances flexibility, security, and efficiency, making it a widely used tool for IT professionals, educators, and students in both personal and enterprise computing.

Table 2.2 Requirements of Oracle VirtualBox

System Requirements	Minimum and Recommended Specifications
Host Os	Windows 8/10/11, Linux (Ubuntu, Fedora, Debian, Red Hat), macOS 10.13+, Solaris
Processor	x86 or AMD64 CPU with virtualization (Intel VT-x / AMD-V)
RAM	Minimum 4 GB (8 GB+ recommended)
Storage	Minimum 10 GB free per VM
Graphics	Standard graphics; 3D acceleration optional
Optional Software	VirtualBox Extension Pack (USB, RDP, advanced features)
Network	Internet access for downloads and updates

Figure 2.2 Oracle VirtualBox

2.3 Windows 10 Pro

Windows 10 Pro is a specialized version of Microsoft's operating system designed for business and professional use. Its core philosophy centers on enhanced security, management, and productivity features not found in the Home edition. Key to its design is BitLocker, which provides full disk encryption to protect sensitive data from unauthorized access. The operating system also enables centralized control through Group Policy Management, allowing IT administrators to enforce security settings and configurations across a network of devices. For connectivity and remote work, Windows 10 Pro includes Remote Desktop functionality and the ability to join a Windows Domain. It further supports virtualization with Hyper-V, making it an ideal platform for power users, developers, and businesses requiring a secure and controllable computing.

Figure 2.3 Windows 10 Professional

2.4 IIS Web Server

Internet Information Services (IIS) is a Microsoft-developed web server designed for the Windows operating system, with a core theory of providing a modular, secure, and extensible platform for hosting web content. At its heart, IIS is built on a request-response model where a kernel-mode driver, HTTP.sys, efficiently handles incoming requests and routes them to the appropriate application. This driver's direct interaction with the kernel provides high performance by reducing the need for context switching. The server's design separates the core functionality from specific features,

allowing administrators to install only the modules they need. This modularity not only minimizes the server's memory footprint and potential attack surface but also makes it highly customizable and extensible. .

A key architectural principle of IIS is process isolation, achieved through the use of Application Pools. An Application Pool is a container that holds one or more web applications and runs within a dedicated worker process (w3wp.exe). This is a crucial design choice because it ensures that if one web application crashes, it will not affect other websites or applications running on the same server, thereby enhancing the server's stability and reliability. The Windows Process Activation Service (WAS) manages these worker processes, starting, stopping, and recycling them as needed to maintain health and performance. This separation of concerns ensures that the failure of one application does not cascade across the entire server.

Furthermore, IIS is designed to be deeply integrated with the Windows security and management ecosystem. It supports a wide range of authentication and authorization methods, including Windows Authentication, which allows for seamless integration with Active Directory environments. The server's security is enhanced through features like request filtering and URL rewriting, which help protect against common web attacks. For management, IIS provides a comprehensive graphical user interface, IIS Manager, along with command-line tools and scripting capabilities for automation. This tight integration with the Windows platform and its emphasis on security and management are central to its design, making it a powerful and reliable choice for hosting web applications in a corporate or enterprise environment.

Figure 2.4 IIS Web Server

2.5 File Sharing with Security Permissions

File sharing with security permissions is a method that allows multiple users or computers to access and exchange files over a network while controlling who can view, modify, or delete them. This concept became important with the rise of Local Area Networks (LANs), where multiple users needed access to shared resources like

documents, applications, and printers. Security permissions are used to restrict access, ensuring that sensitive data is protected from unauthorized users. Permissions are typically managed using operating system features, such as Windows NTFS file permissions, which allow administrators to assign rights like read, write, modify, or full control. Implementing secure file sharing improves collaboration while maintaining data confidentiality, integrity, and accountability, making it an essential practice in offices, educational institutions, and enterprise networks.

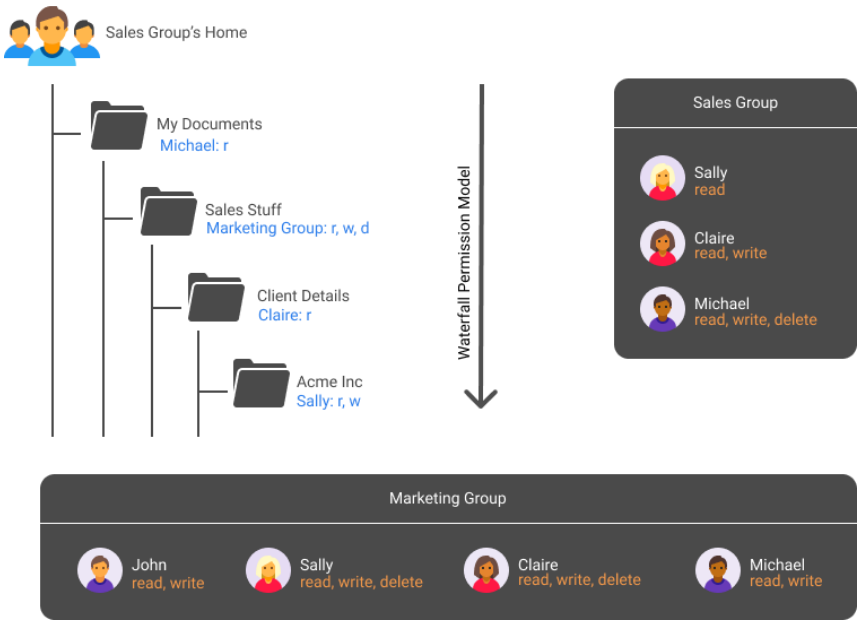

Figure 2.5 Waterfall Permission Model

2.6 Remote Desktop

Remote Desktop is a technology that allows a user to connect to and control a computer from a different location over a network or the internet. It provides access to the computer's desktop, applications, and files as if the user were physically sitting in front of it. Developed by Microsoft as part of the Windows operating systems, Remote Desktop uses protocols such as RDP (Remote Desktop Protocol) to transmit screen images, keyboard inputs, and mouse movements between the host and client computers. This technology is widely employed for remote administration, technical support, troubleshooting, and teleworking, enabling IT administrators to manage servers, workstations, and user machines efficiently from anywhere. Remote Desktop also improves productivity by reducing the need for physical presence while supporting secure connections through authentication and encryption measures. By providing centralized access and control, it has become an essential tool in modern networked

environments, facilitating collaboration, maintenance, and real-time support across distributed locations.

Figure 2.6 Example Picture of Remote Desktop

2.7 Group Policy Objects (GPOs)

Group Policy Objects (GPOs) are a fundamental feature of Microsoft Windows Server environments, allowing administrators to centrally manage and configure operating systems, applications, and user settings across a network.

First introduced with Windows 2000, GPOs enable the consistent enforcement of security policies, software installations, account restrictions, desktop configurations, and network settings on multiple computers and users within an Active Directory (AD) domain. By leveraging GPOs, organizations can ensure system consistency, enhance security, and maintain compliance, significantly reducing the need for manual configuration on each individual machine.

Policies can be applied at different levels, including site, domain, or organizational unit (OU), and can be filtered or overridden when necessary to meet specific requirements. In enterprise environments, GPOs are widely used to manage password policies, control user access, standardize desktop environments, and regulate overall system behavior, making them an essential tool for efficient network administration and centralized IT management.

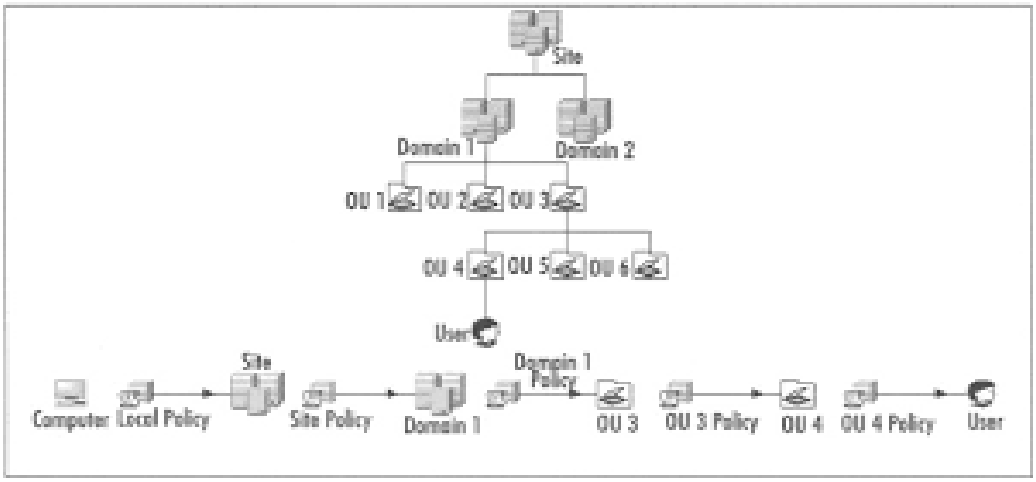

Figure 2.7 Sample Architecture of GPO

2.8 Windows PowerShell

Windows PowerShell is a Microsoft automation and configuration tool built on .NET, combining a command-line interface with a scripting language. Unlike traditional shells, it works with objects, enabling structured data handling through properties and methods. Using cmdlets and pipelines, it allows system administration, automation, remote management, and integration with services like Active Directory and Azure. Its object-oriented and extensible design makes it powerful for network management, security auditing, and software deployment.

Figure 2.8 Windows PowerShell

CHAPTER 3

SYSTEM DESIGN

3.1 Network Diagram

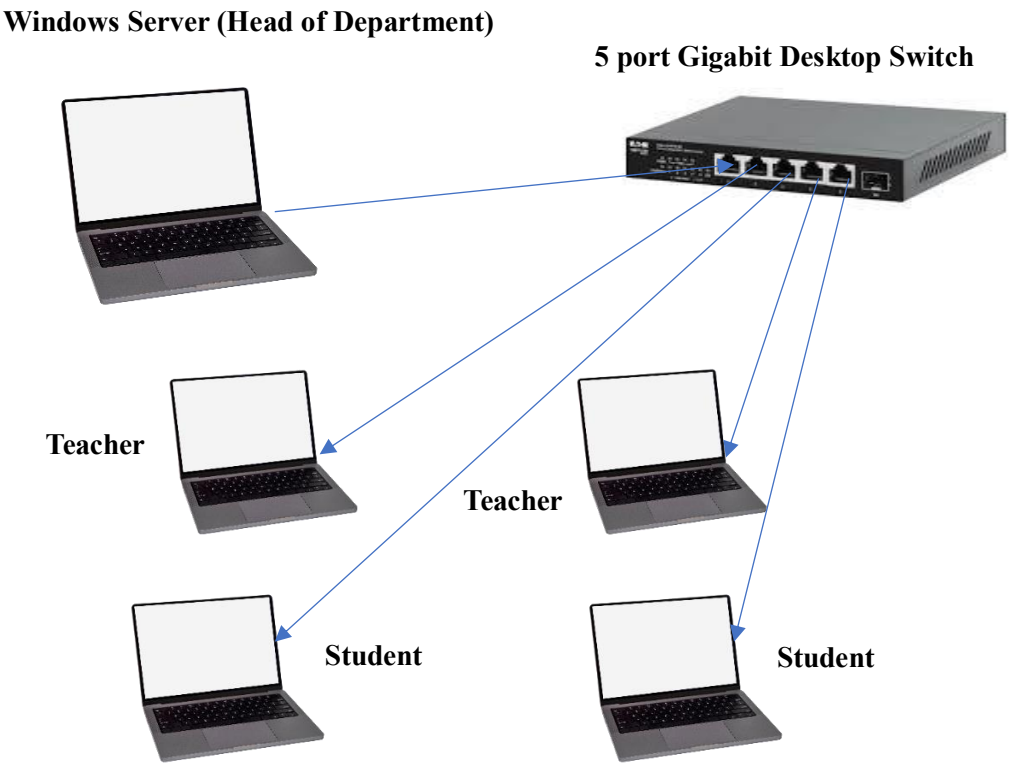

Figure 3.1 Network Diagram

Figure 3.1 describes a small computer network using a star topology. In this configuration, all devices specifically, a Windows Server(Head of department), teacher's laptop, and student's laptop are connected to a central 5-port Gigabit Desktop switch. This central switch acts as the hub, directing data traffic efficiently between all connected devices. The Windows Server 2022 is the core of the network, providing essential services like file sharing and user authentication, which are crucial for network security and resource management. Both the teacher's and student's laptops function as client devices, accessing resources and communicating with each other through the switch.

This topology is highly favored due to its reliability and scalability. A key advantage is its fault tolerance: if one device or its connecting cable fails, the rest of the network remains operational, which simplifies troubleshooting. Expanding the network is also straightforward, as new devices can be added simply by connecting them to an

open port on the central switch, making it an excellent choice for small-scale environments like a classroom.

3.2 Functional Block Diagram

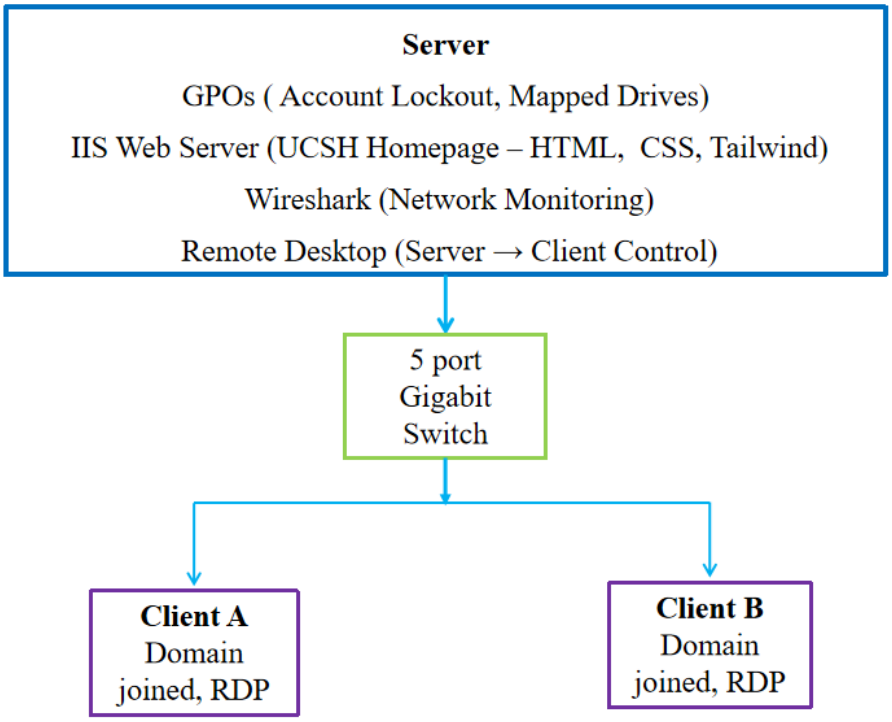

Figure 3.2 Functional Block Diagram

Figure 3.2 illustrates a centralized network architecture in which a Server functions as the core component, connected to two user computers, Client A and Client B, through a 5-port Gigabit Switch.

The server provides essential administrative and service roles, including the enforcement of Group Policy Objects (GPOs) for security and resource management, such as account lockouts and mapped drives.

It also operates as an IIS Web Server, hosting the homepage of the FCST organization, and employs Wireshark for monitoring network activity.

Furthermore, the server can manage client machines remotely via the Remote Desktop Protocol (RDP), with both Client A and Client B configured as domain-joined systems.

Acting as the central hub, the Gigabit Switch ensures high-speed data transmission and directs traffic efficiently between the server and client devices, thereby enabling seamless communication and centralized management within the network.

3.3 System Flow Diagram

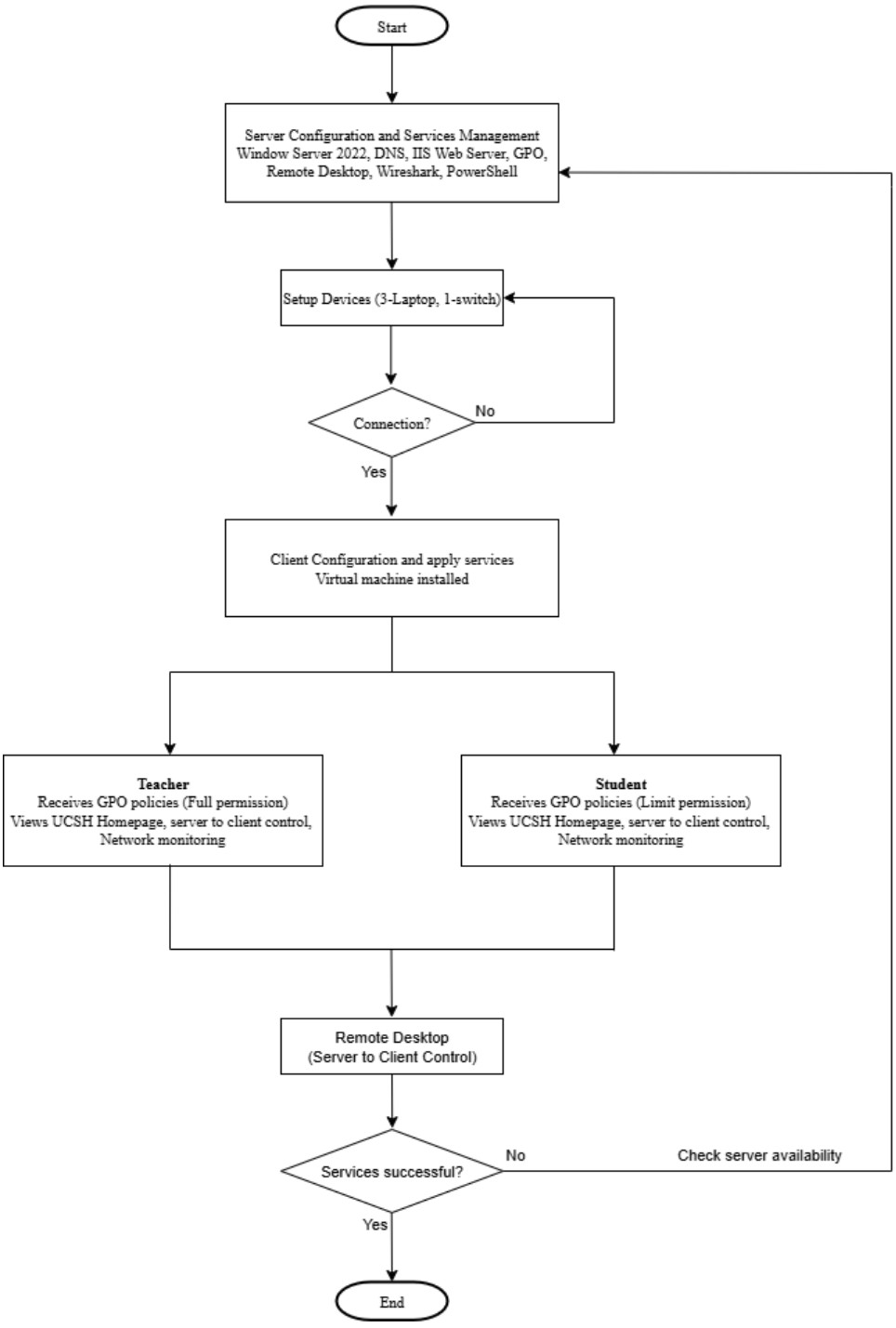

Figure 3.3 System Flow Diagram

Figure 3.3 illustrates a detailed flowchart showing the complete process of setting up and managing a server-client network system. The process begins with server configuration and management, which serves as the foundation of the entire network. At this stage, Windows Server 2022 is installed and configured with essential features to ensure efficient operation, robust security, and centralized administration.

Group Policy Objects (GPOs) are applied to enforce organizational policies, manage user accounts, and control access to network resources, including account lockouts, folder redirection, and mapped drives. An IIS Web Server is configured to host the UCSH homepage, providing centralized access to client computers within the campus network. Network monitoring and troubleshooting are carried out using Wireshark, while Remote Desktop Protocol (RDP) is enabled to allow administrators to remotely manage both the server and client devices, enhancing efficiency and responsiveness.

Following server setup, physical devices are connected, including five laptops and a 5-port Gigabit Switch, which acts as the central hub to efficiently direct data traffic between devices. A connectivity test is performed to verify proper communication and network stability.

Client computers are then configured with role-based access permissions: Teacher clients receive full administrative rights to access all resources, while student clients are granted limited access to ensure security and controlled usage. Finally, Remote Desktop is enabled from the server, followed by a comprehensive management and verification check, ensuring centralized control, secure access, and reliable performance of the network system for all users.

CHAPTER 4

IMPLEMENTATION

4.1 Server Configuration

4.1.1 IIS Web Server Configuration

To install and configure IIS on a Windows Server for hosting a website in a LAN, begin by opening Server Manager. Click on Manage and select Add Roles and Features.

In the Add Roles and Features Wizard, choose Role-based or feature-based installation and click Next, then select the target server and continue.

Figure 4.1 shows the diagram for managing the add roles and features.

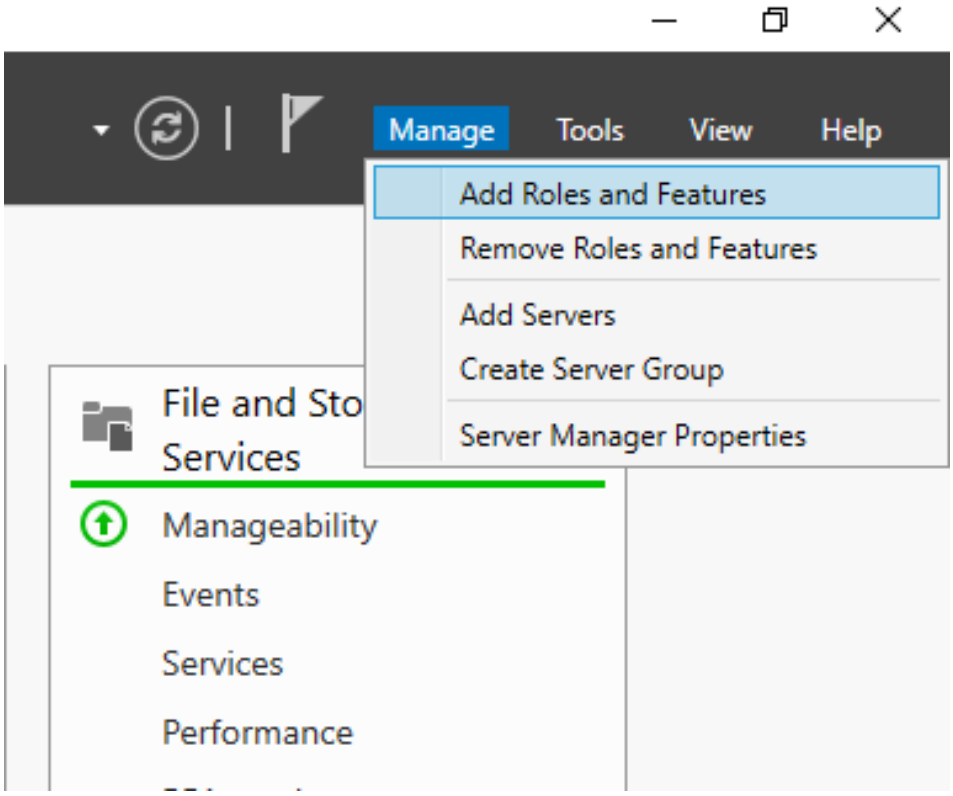

Figure 4.1 Managing Add Roles and Features

Follow the prompts to install the Web Server (IIS) role, along with any required features. Once the installation is complete, can use the IIS Manager to create and configure websites.

This powerful tool allows to easily manage application pools, ensuring web applications have the necessary resources and are isolated for security.

Figure 4.2 show the diagram for role-based or feature-based installation.

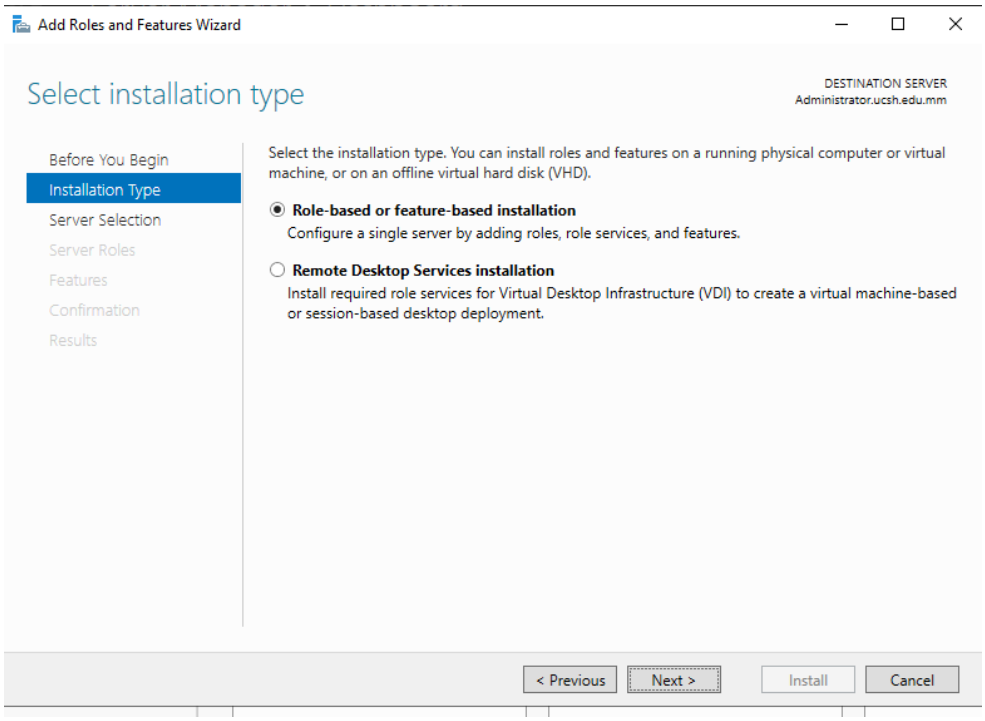

Figure 4.2 Role-based or Feature-based Installation

Destination Server selection is shown in Figure 4.3. In the diagram select a server from the server pool. Then, check the name, IP address and operating system.

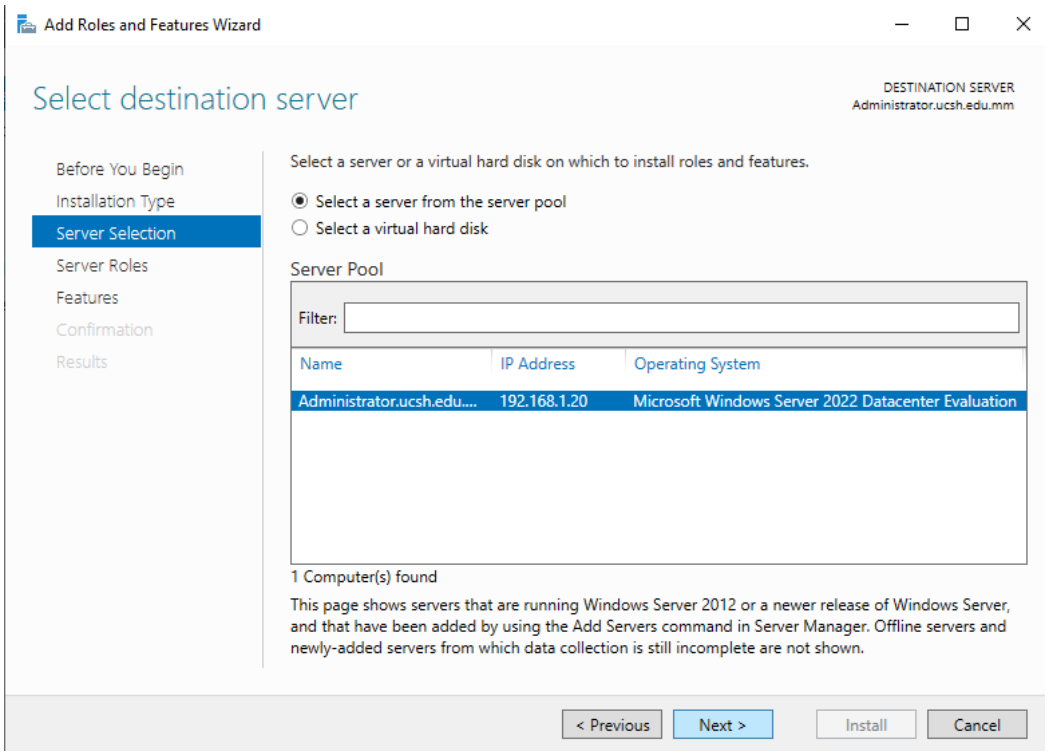

Figure 4.3 Destination Server Selection

Server role selection is shown in Figure 4.4. And then, Web Server IIS installation is finished.

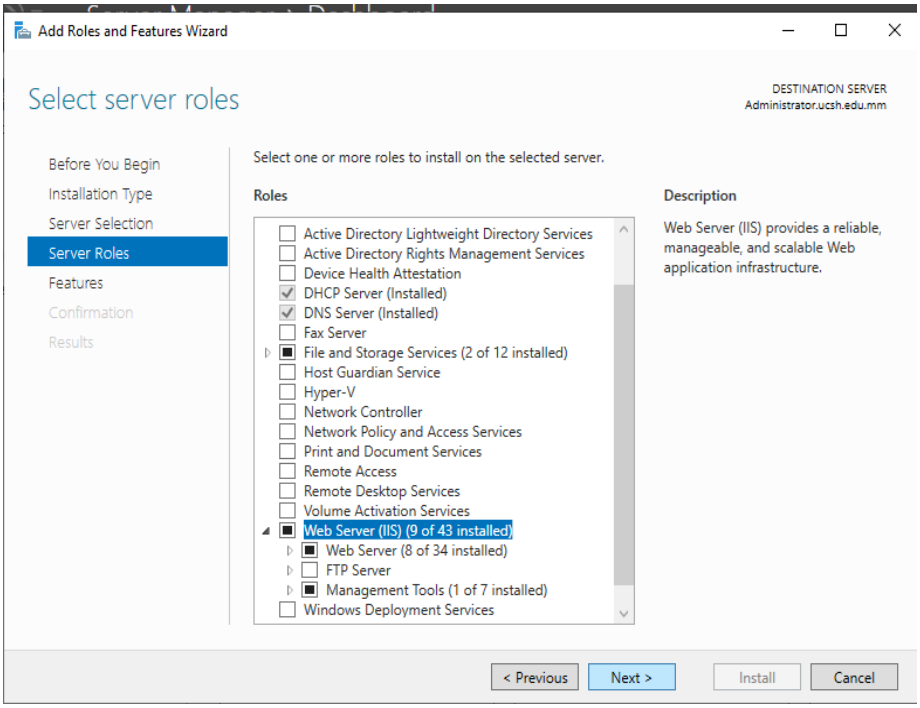

Figure 4.4 Server Roles Selection

After installing IIS on my Windows Server, configured it to host website within the LAN. Opened IIS Manager by pressing Win + R, typing inetmgr, and pressing Enter. That process is shown in Figure 4.5.

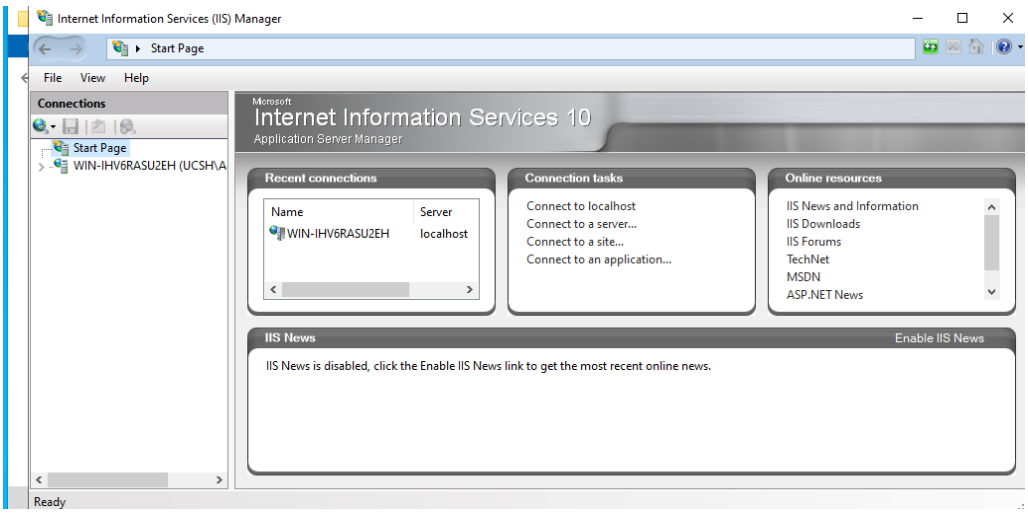

Figure 4.5 IIS Web Server Manager

IIS Configuration for ucsh.edu.mm/fcst Webpage is shown in Figure 4.6. In the connections panel, expanded the server node and selected sites, where the Default Web Site was displayed. To add new website, right-clicked Sites and chose Add Website.

Then, entered the Site name as ucsh.edu.mm and set the Physical path to C:/inetpub/wwwroot/ucsh.edu.mm, which contained all my HTML, CSS, and other supporting web files used to create the web pages.

For the binding, selected the server IP 192.168.1.20 and port 80. After verifying the settings, clicked OK to create the site.

The new website then appeared in IIS Manager, and was able to access it from any client connected to the LAN using the server's IP address.

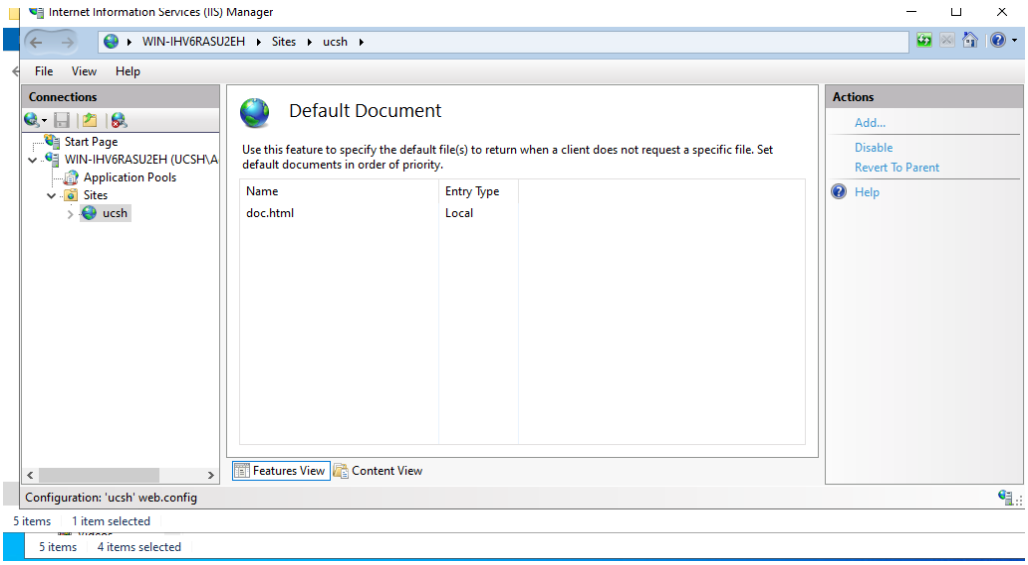

Figure 4.6 IIS Configuration for ucsh.edu.mm/fcst Webpage

Figure 4.7 illustrates the website's hosting folder path, which plays a critical role in enabling local network accessibility. To facilitate access via the domain name ucsh.edu.mm within the LAN, a web.config file was strategically placed in the site's directory.

This configuration file is essential for defining application settings and ensuring proper DNS-based routing. By using a domain name instead of a static local IP address, users benefit from simplified navigation and improved scalability.

This setup also centralizes website hosting and management, allowing administrators to apply updates, enforce security policies, and maintain consistency from a single location. The use of domain-based access enhances user experience and supports future network expansion.

Overall, this configuration ensures reliable, seamless access to the hosted website across the campus network, aligning with best practices in enterprise-level web deployment.

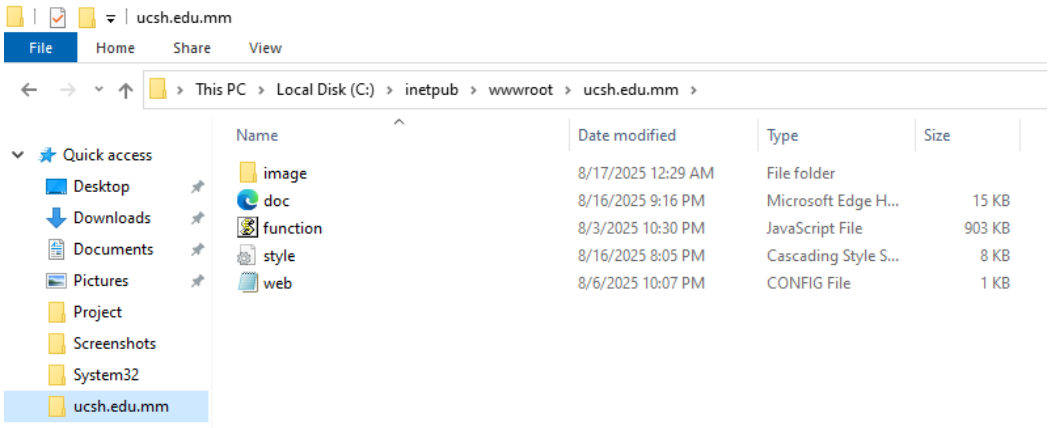

Figure 4.7 Website Hosting Folder Path

The sample hosted website is shown in Figure 4.8. In figure, doc.html is the main part of the page.

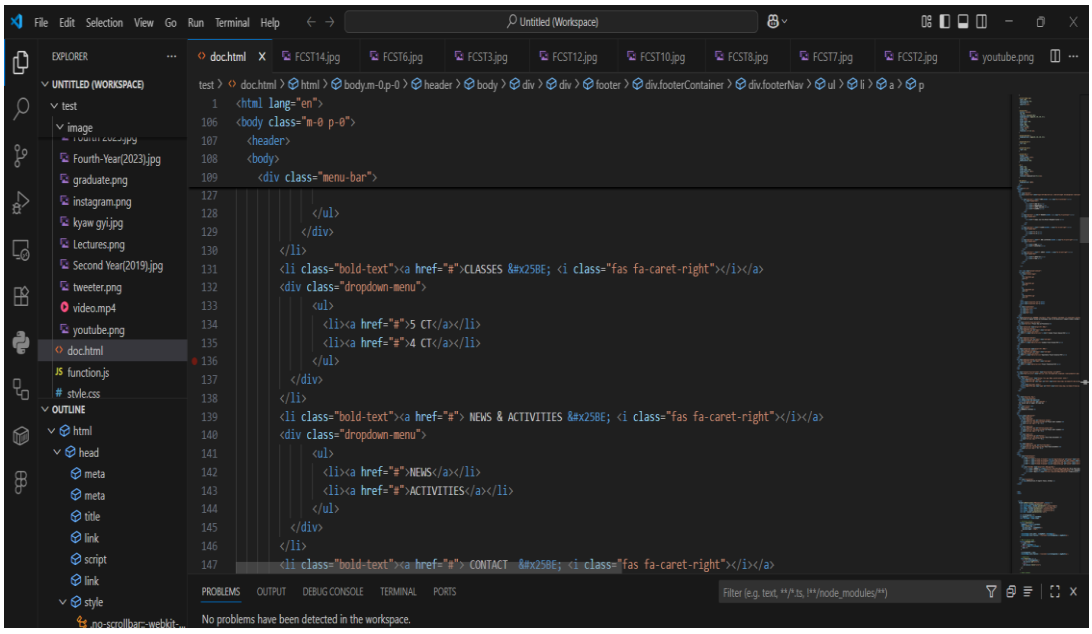

Figure 4.8 Sample Hosted Webpage (HTML, CSS, and images)

4.1.2 File Sharing with Security Permissions Configuration

As shown in Figure 4.9 a main shared folder named Share Folder was created to act as the central repository for all important files within the organization. To ensure organized storage and proper access management, two sub-folders were created inside Share Folder: Teachers and Students. The Teachers folder is intended to store sensitive administrative documents, accessible only by members of the administrative group.

The Students folder, on the other hand, is designed to hold files relevant to students, organized by their respective departments or years.

This structure not only keeps data organized but also enforces role-based access, ensuring that users can only access files appropriate to their role within the institution.

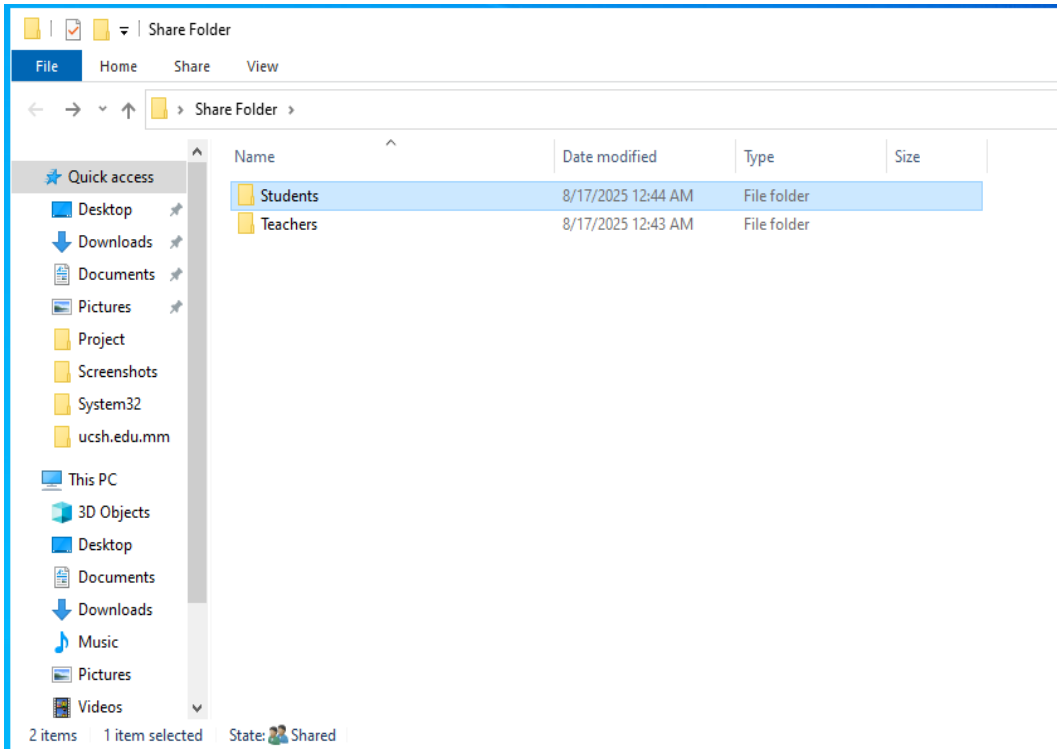

Figure 4.9 Share Folder: Teachers and Students

To manage access efficiently within the shared folder, five specific security groups were created: Teachers, Students classes such as 2CT, 3CT, 4CT, and 5CT. These groups were assigned specific, granular permissions for the various sub-folders inside the main share. The Teachers group was granted Full Control over the Teachers folder, a critical step to ensure that only authorized personnel could access and modify sensitive administrative files. This strict control adheres to the principle of least privilege, a fundamental security practice that minimizes potential vulnerabilities.

As represented in Figure 4.10, the student groups (2CT, 3CT, 4CT, and 5CT) were given permissions corresponding to their respective folders within the main Students sub-folder. For instance, a student in the 2CT group would have read and write access to their designated folder but be prevented from accessing files in other class folders. This robust structure facilitates a secure, role-based access system, simplifying administration by allowing permissions to be managed at the group level rather than for individual users. It maintains clarity and centralized control over who can view, edit, or delete data within each designated folder, providing a professional and organized network environment for all users.

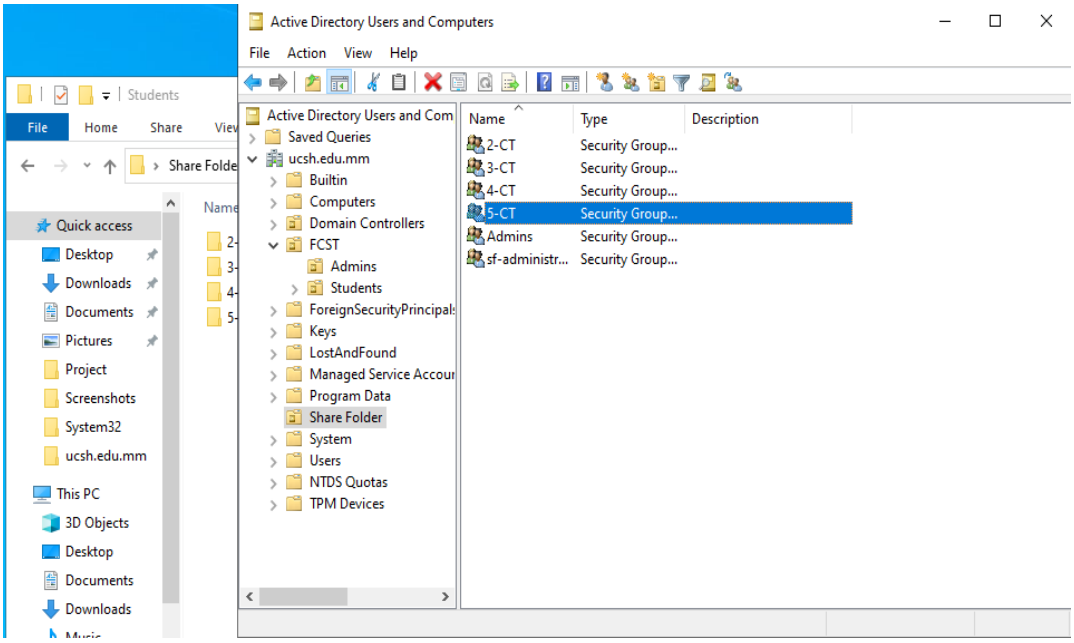

Figure 4.10 Security Groups

The share permission for the main folder, Share Folder, was intentionally set to everyone for Full Control. This broad setting provides a seamless initial connection for all users across the network, enabling them to easily locate and access the shared resources without any immediate restrictions.

This configuration prioritizes user convenience, simplifying basic network accessibility for everyone. To counteract this broad permission and maintain a high level of security, NTFS security permissions were applied to enforce precise, granular access controls.

This two-tier approach is a fundamental best practice for balancing ease of use with robust data protection. As a key example, and as shown in the Figure 4.11, within the Share Folder, the Admins sub-folder was meticulously configured to grant Full Control exclusively to the Admin group.

This critical restriction ensures that unauthorized users are fully blocked from accessing, modifying, or deleting the folder's contents. By applying precise permission settings, sensitive administrative files remain protected, and the integrity of system management data is preserved. This method demonstrates the effectiveness of combining NTFS and share permissions to enforce strict access control, enhancing overall server security and maintaining operational stability within the network environment.

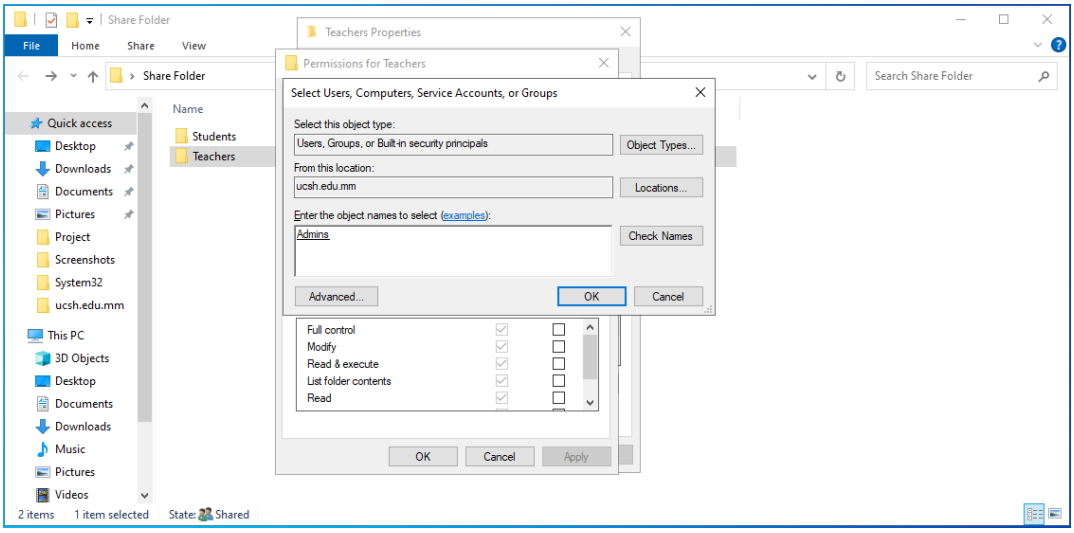

Figure 4.11 Add Permission in Teachers Folder

As depicted in Figure 4.12, student sub-folders were assigned permissions based on their respective security groups, allowing organized, role-based access according to department, class, or year.

This combination of broad Share permissions and targeted NTFS restrictions creates a powerful and balanced security model. The Share permissions grant general network access, simplifying connectivity for all users. Meanwhile, the more restrictive NTFS permissions provide granular control over specific files and sub-folders, dictating precise user actions like reading, writing, or modifying.

This two-tiered approach effectively balances user convenience with strong data protection, ensuring a secure, structured, and efficient file-sharing environment for all users on the network.

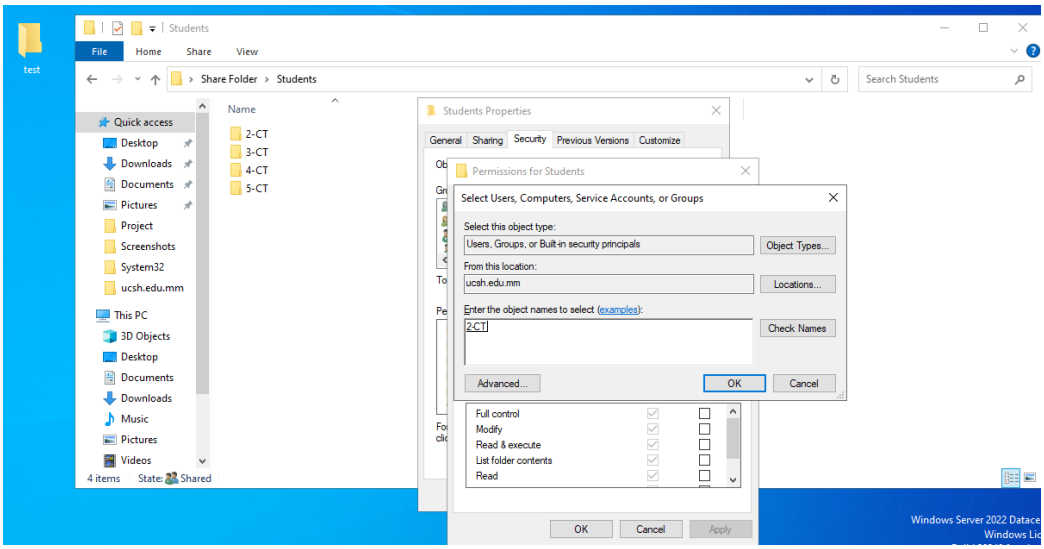

Figure 4.12 Add Permission in Students Folder

4.1.3 Drive Mapping and Account Logout Policy with GPO Configuration

As display in the Figure 4.13, a Group Policy Object (GPO) named Mapping-Drives was created to manage the assignment of network drives automatically to users within the domain. The GPO ensures that shared resources are consistently available across client computers without requiring manual configuration on each workstation.

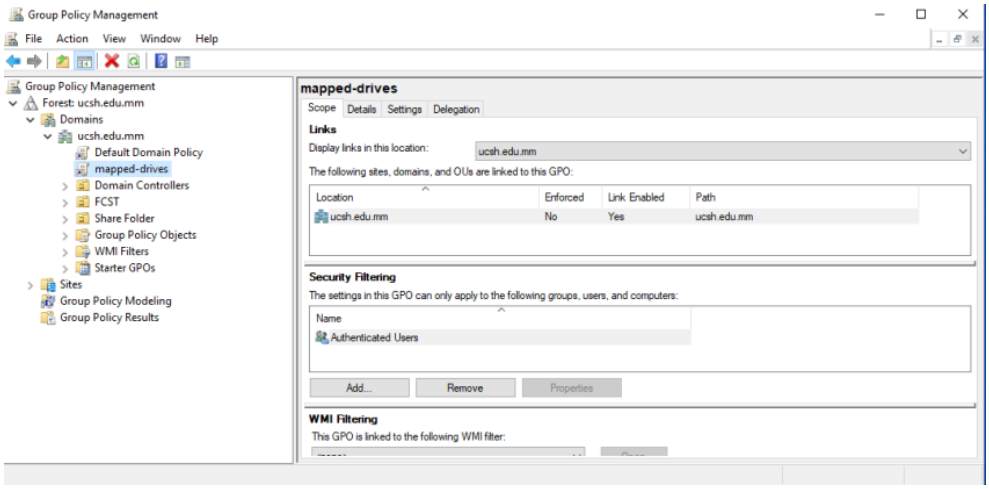

Figure 4.13 Mapped Drives Policy

The GPO was linked to the Organizational Unit (OU) containing the target users to ensure that only intended accounts receive the drive mapping configuration.

Under User Configuration, then Preferences, then Windows Settings, then Drive Maps, a new mapped drive was configured. The New, then Mapped Drive option was selected to create the mapping.

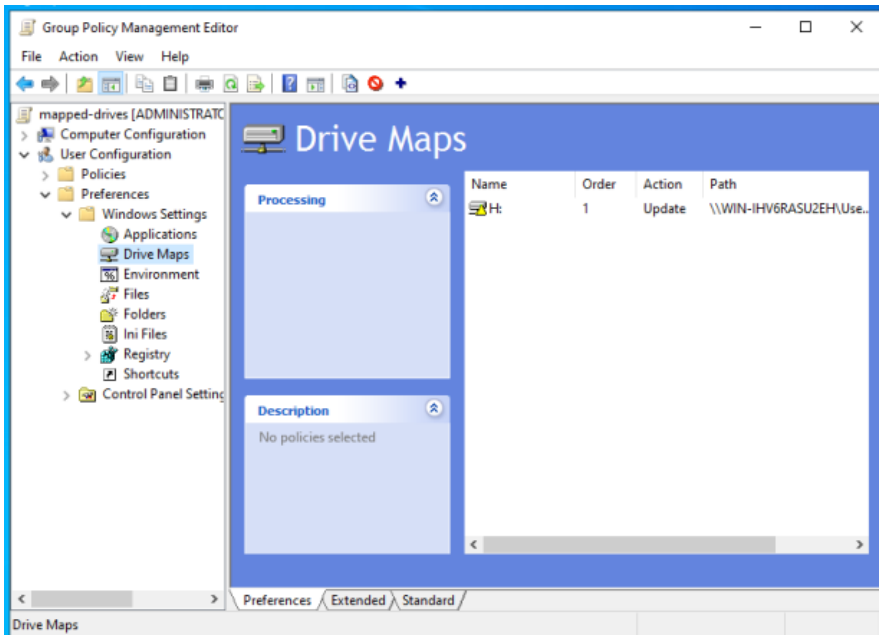

Figure 4.14 Drive Maps

As indicated in the Figure 4.15, the drive was assigned a specific drive letter to maintain consistency across all client machines. A descriptive name was provided for easier identification, and the network share path (for example, \\192.168.1.20\ShareFolder) was entered to point to the shared resource.

The action was set to Create, ensuring that the drive is added automatically if it does not already exist on the client computer. Additional options, such as reconnecting the drive at logon, were configured to maintain access during future sessions.

After configuration, the GPO was applied to the target OU. All users within the OU receive the mapped drive automatically upon logging into their accounts. If the mapped drive does not appear immediately, the policy can be refreshed on the client by running the command gpupdate /force, which forces the application of Group Policy settings. The use of GPO for drive mapping provides a standardized method for distributing network resources, reduces the likelihood of configuration errors, and simplifies IT management in the long term. This configuration ensures that all users have secure, reliable, and consistent access to required shared folders throughout the organization.

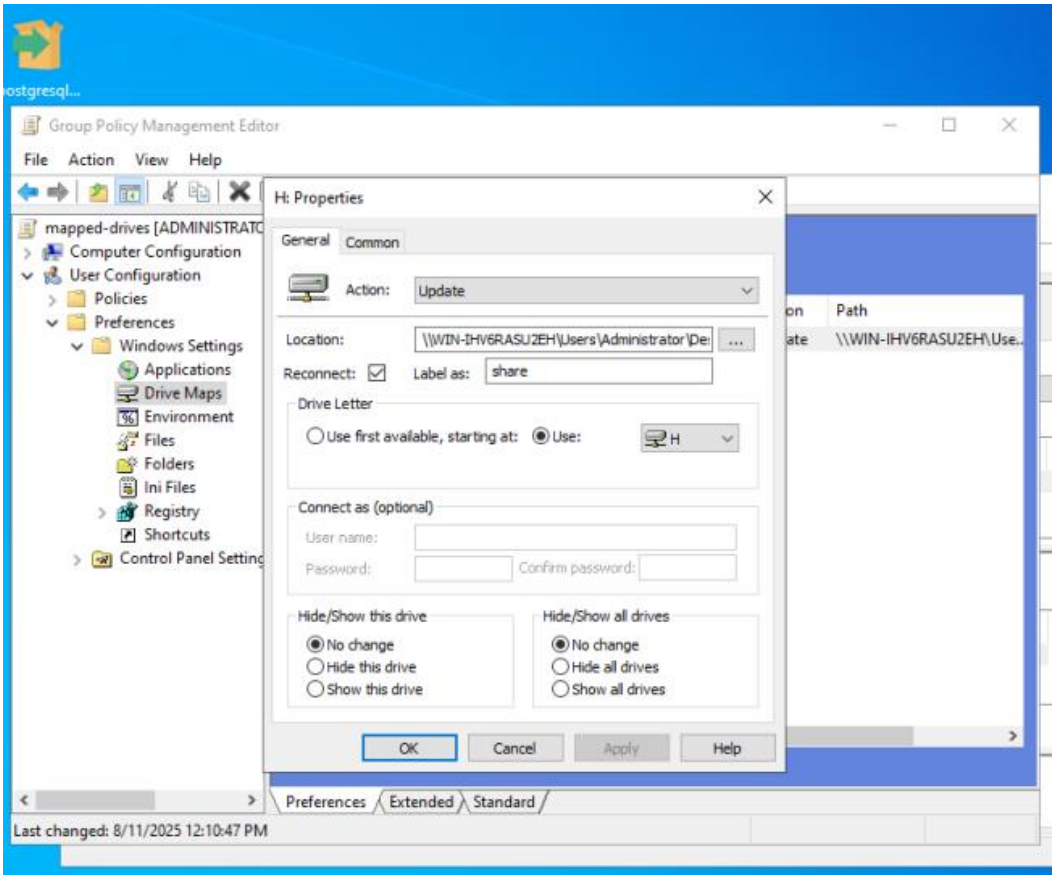

Figure 4.15 Setting Drive Label in Group Policy Drive Map Properties

According to Figure 4.16, an Account Lockout Policy was configured in the Default Domain Policy under Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies, Account Lockout Policy to enhance security against unauthorized access attempts.

The account lockout threshold was set to three invalid logon attempts, ensuring that if a user enters the wrong password three times, the account will be automatically locked. Additional settings such as account lockout duration and reset account lockout counter after can be defined to determine how long the account remains locked or when the failed attempt counter resets.

This policy helps protect domain accounts from brute force attacks while maintaining centralized control through Group Policy.

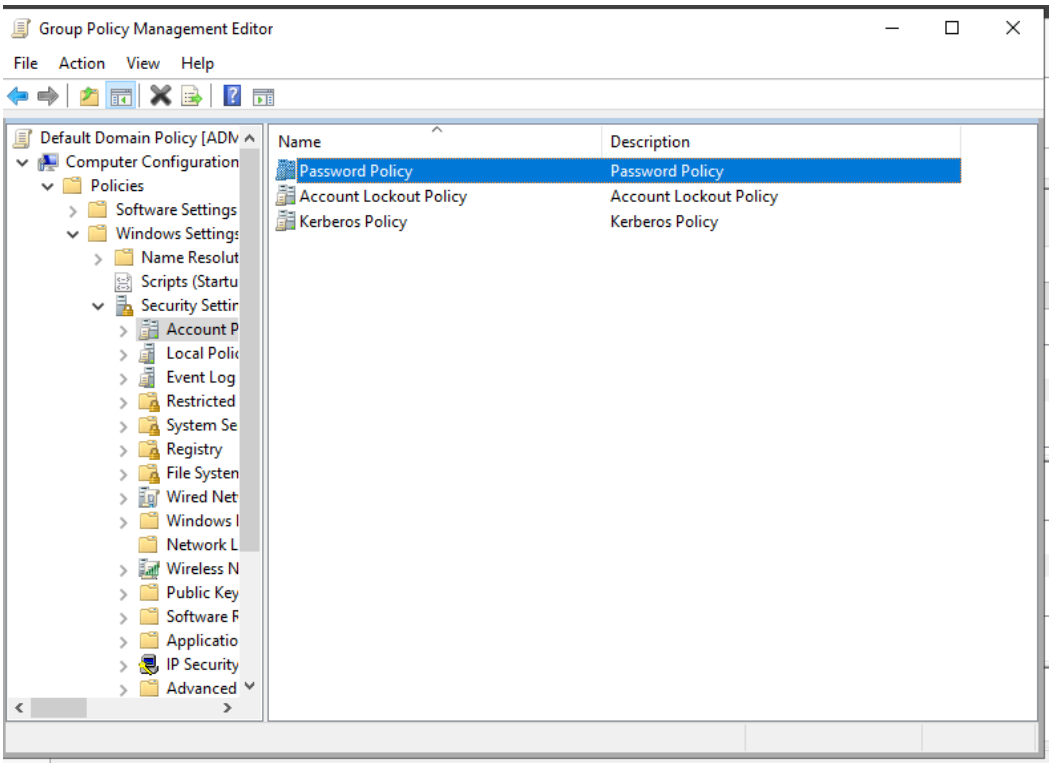

Figure 4.16 Account Lockout Policy in Group Policy Management Editor

4.2 Client Configuration

4.2.1 Remote Desktop Configuration

As point out in the Figure 4.17, Remote Desktop was configured on the client PC by opening System Properties using Win + R, typing sysdm.cpl, and pressing Enter.

This action launches the System Properties window, where the Remote tab can be accessed to enable Remote Desktop.

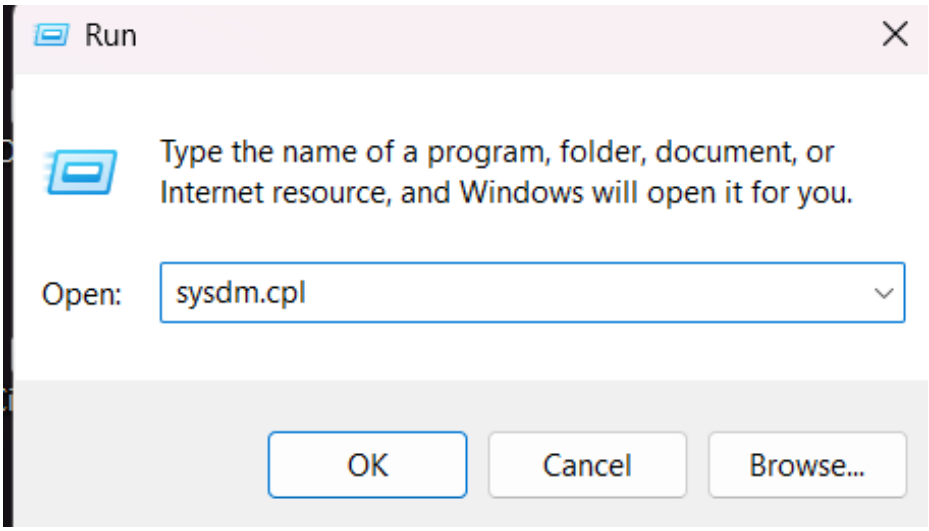

Figure 4.17 Run Sysdm.cpl

The System Properties window, the Remote tab was selected, and under the Remote Desktop section, the option Allow remote connections to this computer was enabled to permit remote access is displayed in the Figure 4.18.

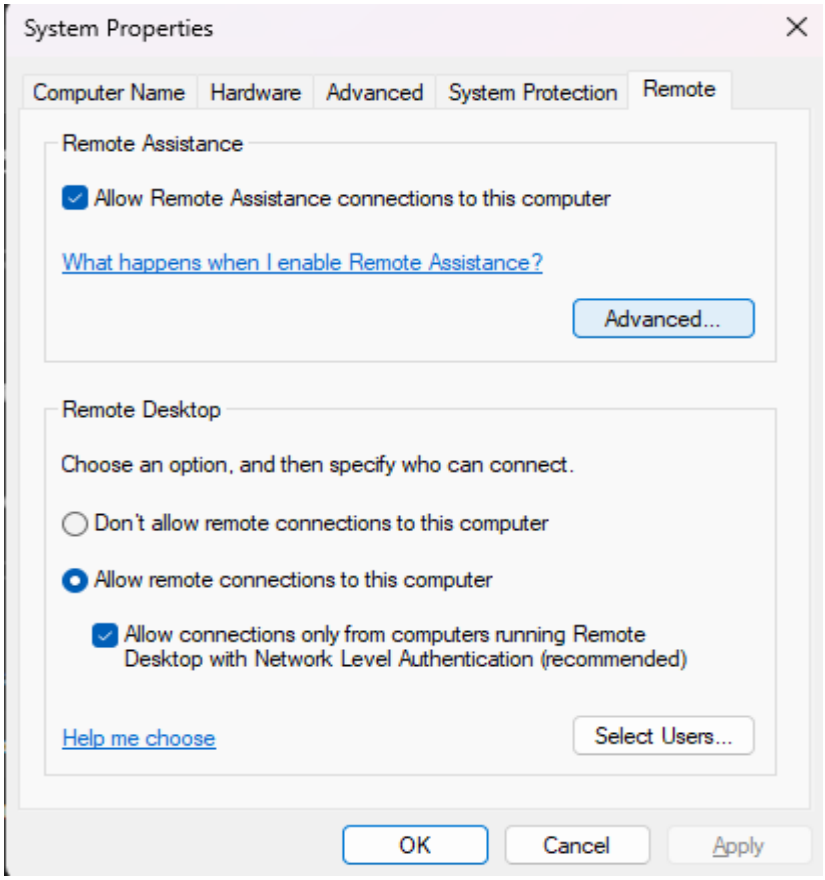

Figure 4.18 Allow Remote Connection

4.3 Implementation Result

4.3.1 Local Host Web Page in LAN

After the IIS Web Server was installed and configured on the Windows Server, the hosted website became fully accessible across the Local Area Network using the assigned DNS name instead of the raw IP address.

A DNS record was created so that the server's IP address correctly resolved to the domain name ucsh.edu.mm, making it easier and more convenient for users to remember and access the site.

As a result, whenever the DNS name ucsh.edu.mm was typed into the browser of any client computer connected to the LAN, the designed webpage loaded successfully without errors. This confirmed that the IIS setup was properly configured, the DNS service was accurately resolving the domain name, and the network connectivity between the server and clients was stable.

The successful display of the webpage on multiple client machines proved that the hosted site was functioning as expected and was available to all authorized users within the campus network environment. The result is presented in the Figure 4.19.

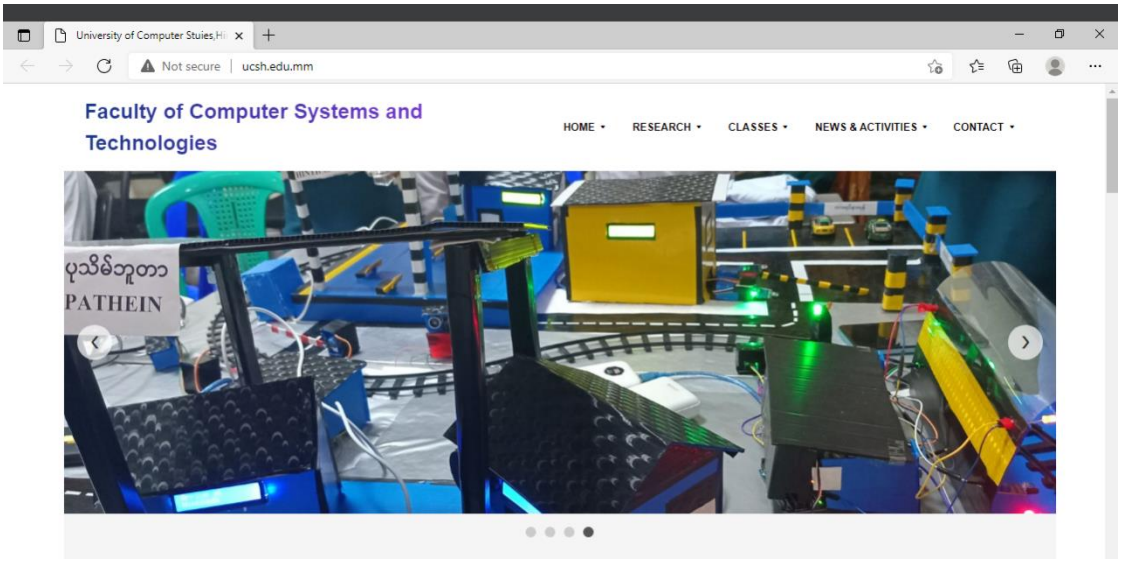

Figure 4.19 Web Page of FCST

4.3.2 File Sharing with Security Permissions

File sharing within the campus Local Area Network was configured using a combination of NTFS permissions and Group Policy Objects (GPOs), allowing the administrator to apply fine-grained control over how resources were accessed by different categories of users.

The primary goal of this configuration was to ensure security, role-based accessibility, and proper organization of data while maintaining an efficient user experience for both administrators and students.

As shown in Figure 4.20, when users logged in with an Admins account, they were granted full control of all the folders and files stored in the shared directory. This included the ability to create new folders, add and edit files, restructure existing data, and even delete content when necessary. Such unrestricted privileges ensured that administrators retained the authority to perform maintenance, manage sensitive information, and keep the overall system up to date without facing access limitations.

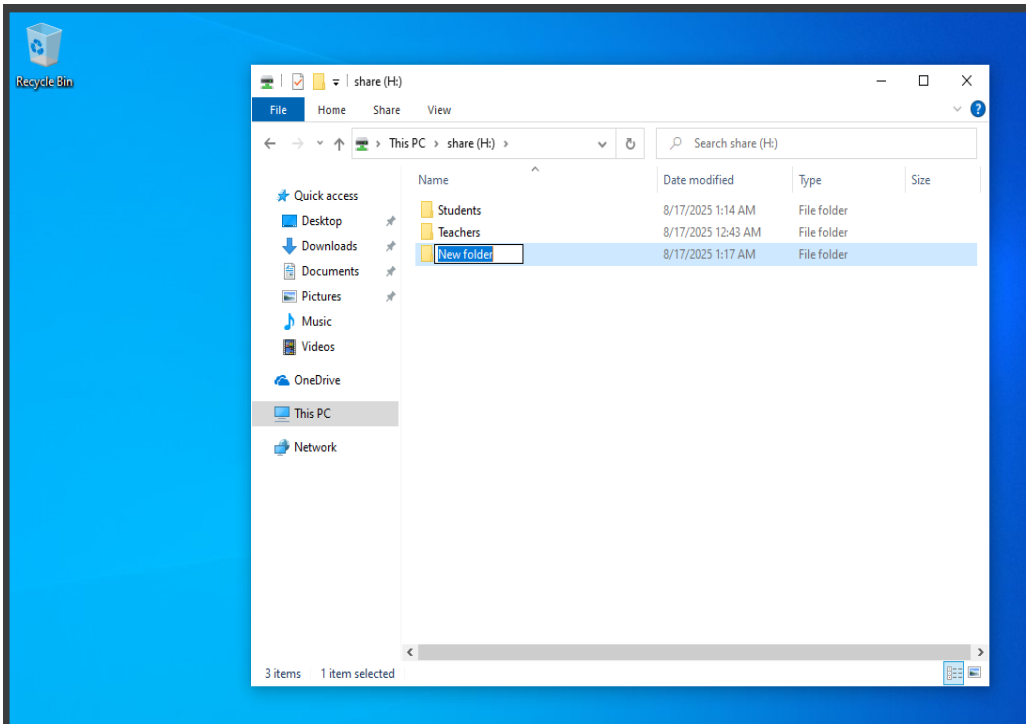

Figure 4.20 Log in with an Admins Account on a Client PC

Displayed in the Figure 4.21, users with a Students account were restricted by NTFS security rules and GPOs so that they could only access their assigned class or year folder. If they attempted to open folders belonging to another group, the system automatically displayed an "access denied" message, effectively preventing unauthorized usage. This demonstrated that access policies were working as intended and that the division between administrative and student rights was clearly enforced.

Overall, this implementation confirmed the successful application of role-based file sharing. Sensitive administrative data remained secure, while students benefited from organized and reliable access to their academic resources, achieving a balanced approach between security and usability.

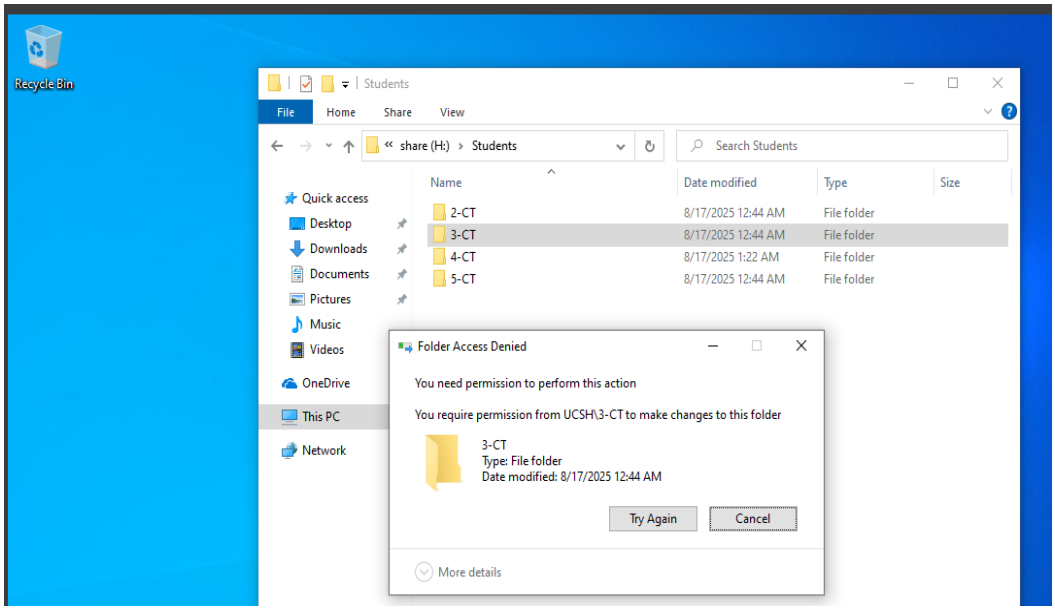

Figure 4.21 Log in with a Student Account on a Client PC

4.3.3 Drive Mapping and Account Logout Policy with GPO

When domain users log in to a client PC, the Group Policy Object (GPO) automatically maps network drives according to their group membership.

The assigned drive appears under Network Locations in File Explorer, using the specific drive letter configured in the GPO. This ensures users immediately have access to their designated shared folders without manually mapping drives.

Additionally, the Account Logout Policy enforced via GPO ensures that when users log out, any session-specific settings or cached credentials are cleared, maintaining security and preventing unauthorized access on shared computers.

This setup confirms that the GPO is functioning correctly, providing seamless drive mapping and consistent enforcement of logout policies for all domain users. The result of the policy is shown in Figure 4.22.

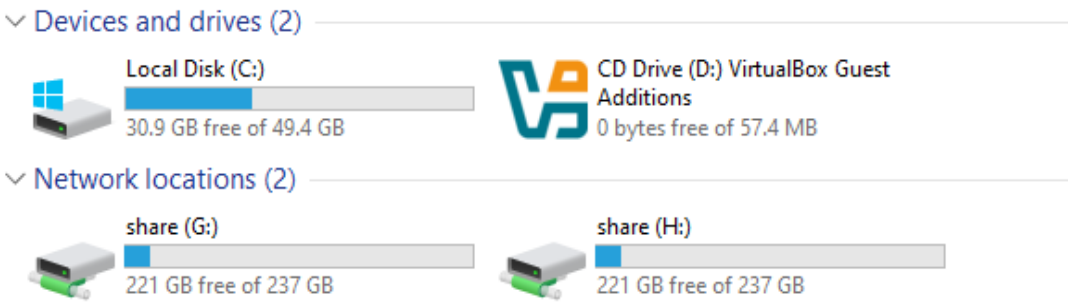

Figure 4.22 Mapping Drives in Network Location

Illustrated in the Figure 4.23, the Account Lockout Policy was implemented to enhance security by limiting repeated failed login attempts. According to the policy, if a user enters an incorrect password three times, their account is automatically locked out. During the lockout period, set to 30 minutes, the user cannot access their account even if the correct password is entered. To regain access immediately, the user must contact an Administrator, who can manually unlock the account using Active Directory Users and Computers. This approach prevents unauthorized login attempts while ensuring that account recovery is controlled and secure.

The policy balances security with administrative oversight, protecting sensitive resources on the network from potential breaches caused by repeated incorrect login attempts. It also enforces awareness among users regarding proper password management and the consequences of multiple failed logins.

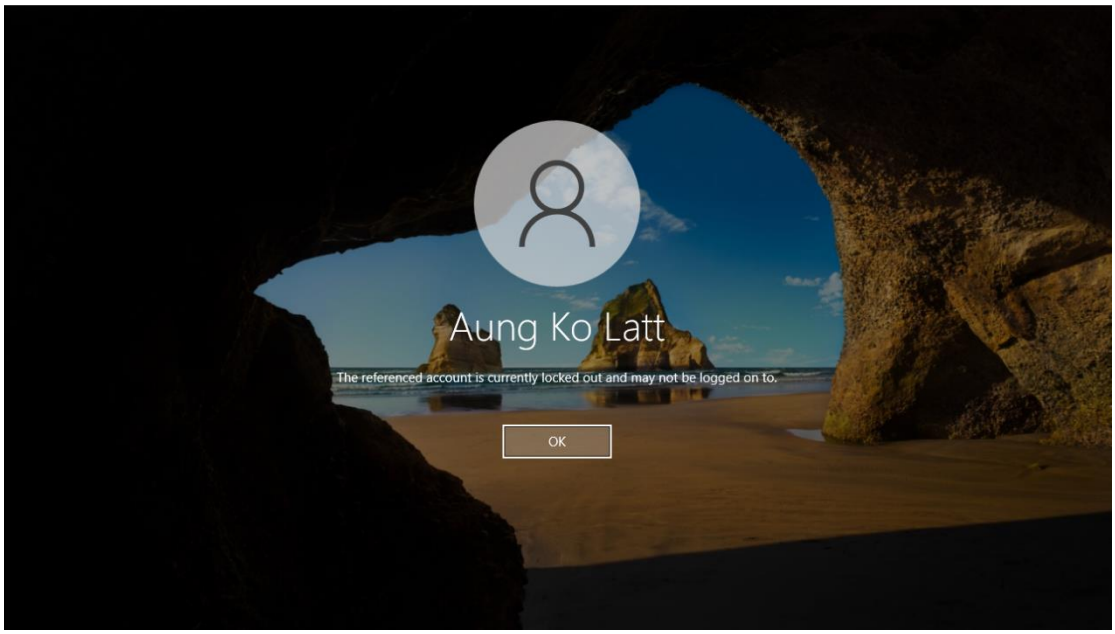

Figure 4.23 Lock Account

4.3.4 Network Traffic Monitoring Using Wireshark

After installing Wireshark, open the application and select the active network interface, such as Wi-Fi or Ethernet, then start capturing by clicking the blue shark fin icon. Wireshark will immediately begin displaying live traffic in real time, showing details such as the source, destination, protocol, and packet size. To make monitoring easier, display filters can be applied to focus on specific types of traffic. For example,

filtering by tcp.port 80 and tcp.port == 443 shows only web traffic, dns displays DNS queries, and ip.addr 192.168.1.50 isolates traffic for a specific device.

In addition to viewing packets, Wireshark provides built-in monitoring tools under the Statistics menu. The Protocol Hierarchy option shows the percentage of different protocols being used, while the Conversations window highlights which devices are exchanging the most traffic.

The IO Graphs feature is particularly useful for visualizing traffic volume over time, helping to detect spikes or unusual activity. Once monitoring is complete, capturing can be stopped by pressing the red square button, and the session may be saved as a .pcapng file for later review. This workflow allows Wireshark to function as a real-time monitoring tool, offering insights into active devices, bandwidth usage, and overall network activity.

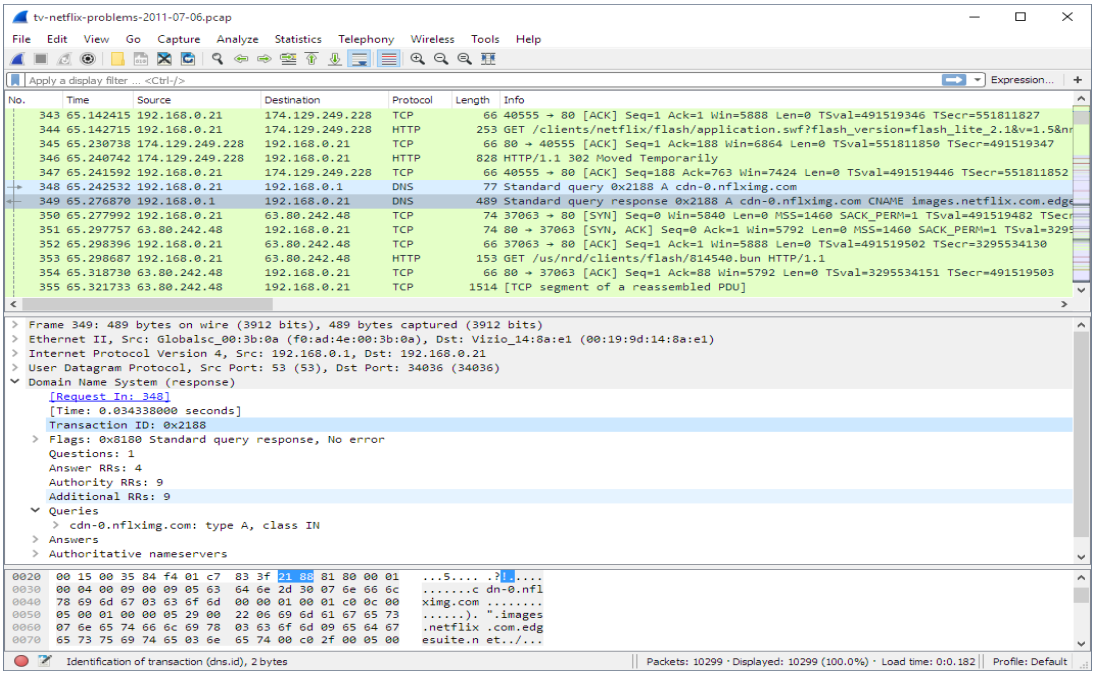

Figure 4.24 Wireshark Monitoring UI

4.3.5 Remote Desktop Using PowerShell Script DHCP Monitoring

The DHCP monitoring process can be automated using a PowerShell script that queries the DHCP server for active leases and checks whether each device is currently responding. The script retrieves all assigned IP addresses and hostnames using the Get-DhcpServerv4Lease cmdlet and then tests connectivity with Test-Connection. If a device replies, it is marked as True, indicating that the device is active, while a failure to respond is marked as False. For devices marked as False, further checks can be performed remotely using Remote Desktop Services.

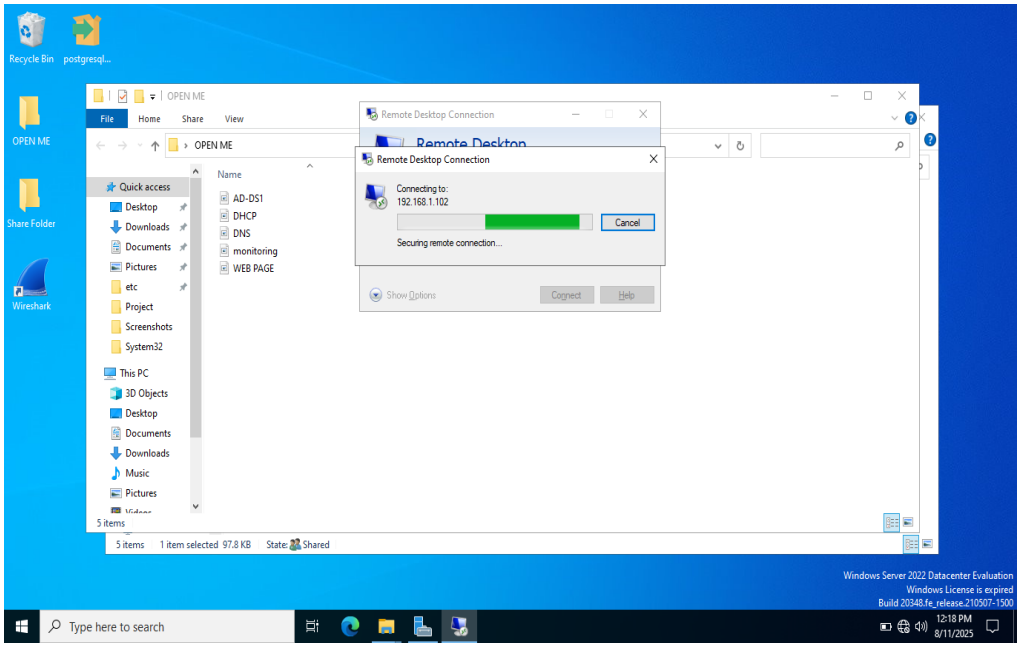

Figure 4.25 Remote Desktop Connection

PowerShell can be used to establish a remote session to the affected client and verify whether essential services are running. If a required service, such as Remote Desktop Services or another critical network service, has stopped, the script can attempt to restart it automatically using Restart-Service or prompt the administrator to take corrective action.

This approach ensures continuous monitoring of devices through DHCP, quick detection of inactive or unreachable hosts, and immediate remote intervention to restore services when failures are identified.

Figure 4.26 Remote Desktop Server to Client

CHAPTER 5
CONCLUSION

The Campus Local Area Network Management System implemented on Windows Server 2022 provides a secure, efficient, and well-organized IT infrastructure for the university. By integrating key services such as Active Directory Domain Services (AD DS), DHCP, DNS, and Group Policy Objects (GPO), the system centralizes management of users and devices, ensuring consistent configurations and controlled access across the network. Hosting an internal website via Internet Information Services (IIS) allows convenient access to academic and administrative resources, while role-based file sharing permissions ensure data security and structured access for different user groups. GPO policies automate administrative tasks such as drive mapping and session control, reducing manual intervention. PowerShell scripts monitor active and inactive devices in the DHCP scope, and analyzing AD DS logs provides accountability for user logon and logoff activities. Administrators can efficiently troubleshoot client systems using Remote Desktop, and Wireshark supports continuous traffic monitoring to enhance performance and security. By combining these tools, the system balances accessibility, efficiency, and protection. Overall, this Campus LAN Management System delivers a reliable, scalable, and secure network environment, supporting both academic and administrative functions while enabling administrators to maintain full control and oversight of network operations.

5.1 Advantages of the Project

The Campus Local Area Network Management System offers significant benefits by providing centralized and efficient management of university IT resources. Integration of Active Directory Domain Services (AD DS), DHCP, DNS, and Group Policy Objects (GPO) allows administrators to control users, devices, and network configurations from a single location. Role-based file sharing permissions, log monitoring, and network traffic analysis using Wireshark enhance data security, ensuring sensitive academic and administrative information is protected

Automation through GPO policies reduces manual workload by managing drive mappings, session controls, and software deployment, increasing overall efficiency

and minimizing errors. Hosting an internal website via IIS ensures reliable access to academic and administrative resources for all users.

Additionally, the system provides robust monitoring and accountability features. PowerShell scripts track active and inactive devices in the DHCP scope, and AD DS logs record user logon and logoff activities. Administrators can manage and troubleshoot client systems remotely using Remote Desktop, improving responsiveness to technical issues. The network is highly scalable, allowing easy integration of new users, devices, or services as the campus grows. Overall, the system strengthens security, streamlines administration, and ensures a reliable and well-organized campus network.

5.2 Limitation and Future Work

Despite its advantages, the Campus Local Area Network Management System has some limitations. The system is primarily designed for a controlled university environment, so its performance may be affected in larger or more complex networks with a high number of simultaneous users and devices. Initial setup and configuration require technical expertise, and any misconfiguration in Active Directory, DHCP, DNS, or GPO could lead to network disruptions. Remote access and monitoring tools such as Remote Desktop and Wireshark rely on consistent network connectivity, which may be limited by hardware or bandwidth constraints. Additionally, the system currently lacks advanced security features such as intrusion detection, automated threat response, or cloud integration, which could enhance resilience against modern cyber threats.

For future work, the system can be expanded to include advanced security solutions, such as firewalls, intrusion detection systems (IDS), and automated backup and recovery mechanisms. Integration with cloud services can enable scalable resource access and centralized data storage, allowing for hybrid campus-cloud networks. Artificial intelligence and analytics could be incorporated to predict network issues, optimize performance, and automate administrative tasks further. Moreover, expanding the system to support mobile devices and remote learning environments would increase flexibility and accessibility for students and staff. These enhancements will ensure the system remains robust, secure, and adaptable to future campus network needs.

REFERENCES

[1] Andi Purnomo, "Implementation of DHCP Snooping Method to Improve Security on Computer Networks". bit-Tech (Binary Digital–Technology), Vol. 6, No. 3, Komunitas Dosen Indonesia, April 2024.

[2] Adam Bertram, "PowerShell for Sysadmins: Workflow Automation Made Easy", No Starch Press, San Francisco, California, USA,2022.

[3] Andrew S. Tanenbaum, David J. Wetherall, "Computer Networks", Pearson (Prentice Hall), United States, 5th Edition, 2010.

[4] Behrouz A. Forouzan, "Data Communications and Networking", McGraw-Hill Education, United States, 5th Edition, 2012.

[5] BroadCom, "How to Configure Certain Settings for the Agent for IIS Manually.", CA Technologies, Inc, United States,2012.

[6] Cai, L., Yu, S., Zhou, J.-L, "Research and Implementation of Remote Desktop Protocol Service over SSL VPN", IEEE International Conference on Services Computing (SCC 2004), United States, October 2004.

[7] Chengjin Mou, "International Journal of Advanced Network Monitoring and Controls", Sciendo, Poland, 2023.

[8] Gerardus Blokdyk, "Windows Server A Complete Guide, 2021 Edition", 5STARCooks, United States, October 15, 2020

[9] Jordan Krause, "Mastering Windows Server 2022, Fourth Edition", 2022.

[10] James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach", Pearson Education, United States, 8th Edition, 2021.

[11] Jordan Krause, "Mastering Windows Server 2019", Third Edition, United Kingdom July 29, 2021.

[12] Kara, A, "Secure Remote Access from Office to Home", Germany, 2001.

[13] Robbie Allen, "Active Directory Cookbook 4ed (Cookbooks – O'Reilly)", United States (Sebastopol, CA), June 18, 2013.

[14] Steve Clines, "Karen Lockhart, Active Directory for Dummies", United States, 2015.

[15] W. Panek, MCSA "Windows Server 2016 Complete Study Guide", United States, 2018.