

CHAPTER 1

INTRODUCTION

In today educational institutions, a reliable and secure network infrastructure plays a vital role in supporting daily academic and administrative operations. Local Area Networks (LANs) enable efficient communication, centralized resource management, and secure data sharing among users within the same organization.

This project focuses on the implementation of a Campus Local Area Network Management System using one Windows Server 2022 and two Windows client machines. The system can operate in either a Switch-Based LAN setup without internet access depending on the requirements and available infrastructure.

Windows Server 2022 provides a variety of powerful services that enhance network management. These include Active Directory Domain Services (AD DS) for user authentication and access control, DHCP for automatic IP address assignment, and DNS for hostname resolution. Additional tools such as PowerShell, Task Scheduler, Windows Admin Center, and Performance Monitor are used to monitor, configure, and manage devices and network traffic efficiently.

By implementing this system, the university can achieve better control, visibility, and security within its local network, supporting both academic and administrative functions effectively.

1.1 Experiences of Internship

Securing an internship provided me with valuable firsthand experience in my chosen field. It allowed me to move beyond theoretical knowledge and apply it in a real-world setting. This opportunity helped me become familiar with the professional environment and acquire essential skills relevant to my role.

One of the most significant lessons I learned was the importance of punctuality. Recognizing that time is a precious commodity in the workplace, I understood that effective time management is crucial for success. Prioritizing tasks, meeting deadlines, and minimizing procrastination became fundamental aspects of my daily routine. In any field, managing communication requires one to use their voice effectively. During my internship, I worked with individuals who had more experience than I did. Being assertive and clear in my communication helped me gain trust and establish positive relationships with colleagues. I learned that every question is important. Admitting when I needed help or was unsure about something was a sign

of intelligence, not weakness. Mistakes happened, and instead of criticizing myself, I focused on correcting them and moving forward. Maintaining professionalism, being punctual, and responding promptly to messages helped me build a positive image in the workplace, which is valuable for my future career.

1.2 Motivation

Active Directory Domain Services (AD DS) helps organizations manage users, computers, and groups in one central place. It ensures that only authorized people can access the network and its resources. Domain Name System (DNS) works like a phonebook, translating easy-to-remember names into IP addresses, allowing computers to find each other on the network. Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and other network settings to devices when they connect, so there's no need to set them up manually. Together, these three services make network management easier, more secure, and more efficient.

I learned how to check network connection using PowerShell. From the DHCP client, I used the command ping “192.168.1.20” to test if the device could connect to another computer in the network. This helped me see if the connection was working and if there was any delay or data loss. It was a simple and useful way to check if the network was running properly. This task helped me understand basic network troubleshooting.

1.3 Objectives of the System

A Campus Local Area Network (LAN) Management System is crucial for effectively connecting and managing devices across a university campus. It enables centralized resource sharing, such as file servers, printers, and applications, allowing students, faculty, and staff to access and exchange information smoothly. The system also supports centralized data management, simplifying system maintenance, software deployment, and routine backups while ensuring operational efficiency. In addition, a properly implemented LAN strengthens security by regulating user access, protecting sensitive information, and reducing risks of unauthorized intrusion. Overall, a Campus LAN Management System delivers a reliable, secure, and scalable network infrastructure that enhances academic activities, administrative operations, and campus-wide communication. 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 book presents the design and implementation of a Windows Server 2022-based network infrastructure, emphasizing centralized management through Active Directory Domain Services (AD DS), DHCP, DNS, and Group Policy Objects (GPOs). It reflects the practical knowledge and hands-on experience gained during an internship while also outlining the motivation, objectives, and execution of the system.

Chapter One introduces the project by describing the internship experience, explaining the motivation for developing a scalable and secure network, defining the objectives such as automating IP assignment, centralizing user authentication, and enforcing security policies, and finally summarizing the overall work.

Chapter Two provides the theoretical background by covering key technologies including Windows Server 2022, AD DS, DHCP, DNS, GPOs, as well as essential networking hardware like unmanaged switches and Cat6 cables. Chapter Three focuses on system design, presenting the architecture through a network diagram, block diagram, and flowchart.

Chapter Four describes the implementation process in detail, including server configuration for AD DS, DHCP, DNS, and GPOs, along with client setup for DHCP-based IP assignment and domain joining, followed by verification of successful deployment.

Finally, Chapter Five concludes the project by highlighting its advantages, such as centralized control, automated IP management, and enhanced security, while also discussing limitations and proposing future improvements, including backup integration and possible expansion to cloud-based services.

CHAPTER 2

BACKGROUND THEORY

A campus LAN management system uses modern network technology and centralized IT tools to provide a secure, scalable, and easy-to-manage network for educational institutions. Old methods that require manual IP setup and local user control are slow, error-prone, and hard to expand. This improved system uses Active Directory Domain Services (ADDS) for managing logins, permissions, and resources, Dynamic Host Configuration Protocol (DHCP) to automatically assign IP addresses, and Domain Name System (DNS) to translate domain names into IP addresses for easier access to servers. By combining Windows Server, ADDS, DHCP, DNS, GPO and client computers, the network is managed efficiently, users are controlled centrally, and campus resources are quickly accessible.

2.1 Windows Server 2022

Windows Server 2022 is the latest long-term servicing channel (LTSC) release of Microsoft's server operating system, officially launched in August 2021. It is designed to deliver enhanced security, improved performance, and strong support for hybrid cloud environments. Building on Windows Server 2019, it introduces Secured-core server technology, which integrates protections at the hardware, firmware, and driver levels to defend against advanced cyberattacks. Additionally, Windows Server 2022 includes TLS 1.3 for stronger data encryption and Microsoft Defender Advanced Threat Protection for early detection and mitigation of potential security threats, making it a reliable and secure platform for enterprise environments.

The operating system also provides improved scalability, faster network speeds with lower latency, and enhanced container performance for modern applications. Its hybrid capabilities allow seamless integration with Microsoft Azure, enabling centralized management through Azure Arc and simplified maintenance with Azure Auto manage. These features make Windows Server 2022 suitable for both traditional on-premises data centers and hybrid cloud deployments.



Overall, it provides organizations with a secure, flexible, and reliable platform for operating essential business applications, efficiently managing networks, and delivering centralized IT services, while effectively supporting modern cloud-based solutions and hybrid IT infrastructures, ensuring seamless performance, scalability, and robust management across diverse enterprise environments.

Figure 2.1 Windows Server 2022

2.2 Active Directory Domain Services (AD DS)

Active Directory Domain Services (AD DS) is a feature of Windows Server that allows centralized management of users, computers, and network resources. It helps administrators organize and control access to the network efficiently, ensuring that only authorized users can use specific resources.

AD DS includes domains, domain controllers, organizational units, users, groups, and group policies. When a user logs in, the domain controller checks their credentials and grants access according to permissions. This makes the network secure, easier to manage, and scalable for future growth.

2.3 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that automates the assignment of IP addresses and other network configuration parameters to devices on a TCP/IP network. Developed as an extension of the Bootstrap Protocol (BOOTP), DHCP was first defined in RFC 1531 in October 1993 and later updated in RFC 2131 in March 1997. Unlike its predecessor, DHCP introduces the concept of leasing IP addresses for a finite period, allowing for efficient reuse of IP addresses and reducing the administrative burden of manual configuration. DHCP operates on a client-server model, where a DHCP server dynamically assigns IP addresses and other network configuration parameters to client devices. The protocol facilitates seamless network connectivity by enabling devices to obtain necessary configuration

information, such as IP address, subnet mask, default gateway, and DNS server addresses, without manual intervention. This automation simplifies network management, enhances scalability, and ensures consistent configuration across devices within a network. DHCP uses the User Datagram Protocol (UDP) for communication, with the server listening on UDP port 67 and the client listening on UDP port 68. These well-known port numbers are reserved specifically for DHCP operations, ensuring that messages are directed to the correct endpoints within the network.

The DHCP process involves several key components: the DHCP server, which holds a pool of IP addresses and configuration information; the DHCP client, which requests configuration information; and the DHCP relay agent, which forwards requests between clients and servers when they are on different subnets. The DHCP client initiates the process by broadcasting a DHCPDISCOVER message to locate available servers. In response, the DHCP server offers an IP address and configuration parameters through a DHCPOFFER message. The client then requests the offered parameters by sending a DHCPREQUEST message, and the server acknowledges the request with a DHCPACK message, completing the lease process. This mechanism allows for dynamic IP address allocation, reducing the need for manual configuration and minimizing the risk of address conflicts. Additionally, DHCP supports features like address reservation, where specific IP addresses are permanently assigned to particular devices, and lease renewal, which allows clients to extend their IP address leases before they expire. The use of fixed port numbers for both client and server ensures that DHCP messages are correctly routed and processed, even when clients do not have an IP address assigned at the time of the request.

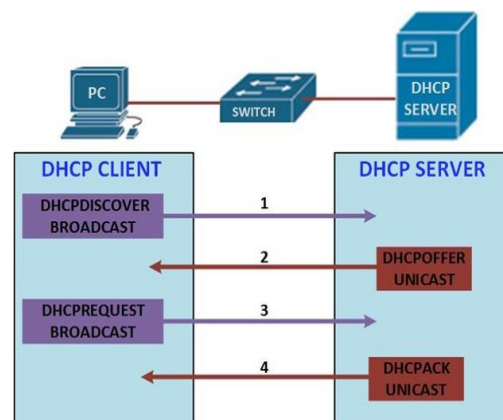


Figure 2.2 Dynamic Host Configuration Protocol (DHCP)

2.4 Domain Name System (DNS)

The Domain Name System (DNS) is a fundamental technology that underpins the modern internet. Before its development, early networks like ARPANET used a centralized system called HOSTS.TXT to map hostnames to IP addresses. This approach became increasingly unmanageable as the network expanded. In 1983, Paul Mockapetris introduced DNS to address these limitations. DNS is a distributed and hierarchical system that allows users to access websites using human-readable domain names instead of numerical IP addresses. It operates through a network of servers that work together to resolve domain names into IP addresses, enabling seamless navigation of the internet.

DNS's design was a response to the growing complexity of the internet. The HOSTS.TXT file, initially maintained by Stanford University, required manual updates and distribution across the network, which became impractical as the number of connected devices increased. Mockapetris's implementation of DNS automated this process, allowing for a scalable and efficient system. The introduction of DNS marked a significant milestone in the evolution of the internet, providing a robust infrastructure that supports the vast and dynamic nature of today's online world.



Figure 2.3 Domain Name System (DNS)

2.5 Group Policy Objects (GPOs)

Group Policy Objects (GPOs) are essential tools for managing and configuring settings across multiple Windows computers within an Active Directory environment. They enable system administrators to enforce security policies, control user behavior, and streamline administrative tasks across the network. A GPO is a virtual collection of policy settings that define how a computer or user account behaves within the Windows Server environment. These settings can include configurations for security,

software installation, scripts, and folder redirection. Administrators can create and manage GPOs using tools like the Group Policy Management Console (GPMC) or the Local Group Policy Editor for local settings. Each GPO has a unique identifier and follows the hierarchical structure of Active Directory for policy evaluation.

The design of GPOs addresses the growing complexity of managing numerous computers and users in large organizations. Before GPOs, administrators had to configure each system individually, which was time-consuming and error-prone. With GPOs, administrators can apply settings to groups of users or computers, ensuring consistency and compliance across the organization. GPOs are processed in a specific order: local GPO, site GPO, domain GPO, and organizational unit (OU) GPO, with each level overriding the previous one if there are conflicting settings. This hierarchical processing allows for flexible and granular control over policy application. Additionally, GPOs can be filtered using security groups to apply policies based on specific criteria, further enhancing their versatility in managing diverse environments.

2.6 Unmanaged Switch

The D-Link DGS-105GL is a 5-port Gigabit Ethernet switch designed to provide high-speed and reliable network connectivity for small offices, home offices, and other small network environments. It allows multiple devices, such as computers, printers, and network-attached storage (NAS), to communicate efficiently over a local area network (LAN). Each of the five ports supports 10/100/1000 Mbps speeds with auto-negotiation, enabling seamless integration with devices of varying network speeds. This feature ensures that each connected device can operate at its optimal speed without manual configuration.

As an unmanaged switch, the DGS-105GL requires no advanced setup, making it ideal for plug-and-play deployment. It employs store-and-forward switching technology, which checks data packets for errors before forwarding them to the correct destination, improving the reliability and integrity of network communications. The switch supports Full Duplex operation for faster bidirectional data transfer and IEEE 802.3x flow control, which prevents data loss during periods of network congestion. Its metal casing and fanless design provide durability and silent operation, while energy-efficient features reduce power consumption. Overall,

the DGS-105GL offers a cost-effective, high-performance solution for connecting multiple devices in small-scale network environments.

Figure 2.4
Switch



Unmanaged

2.7 Cat6 Cable

Ethernet

A Category 6 (Cat 6) Ethernet cable is a type of twisted-pair copper cable specifically designed to carry high-speed network data while minimizing interference and maintaining signal integrity. Like all twisted-pair cables, it contains four pairs of copper wires twisted together, but in Cat 6 each pair is twisted more tightly and with a slightly different twist rate. This precise twisting design significantly reduces crosstalk, which occurs when signals from one pair interfere with signals from another pair. Because electromagnetic noise affects both wires equally, it is effectively canceled out at the receiving end, ensuring more reliable and error-free data transmission.

Compared to older standards such as Category 5e (Cat 5e), Cat 6 is manufactured with stricter specifications. While Cat 5e supports frequencies up to 100 MHz, Cat 6 can handle frequencies up to 250 MHz, which allows for faster and more consistent data transfer. The cable uses pure copper conductors, ensuring optimal conductivity, and often incorporates additional design features like internal plastic separators (splines) or shielding to further isolate each twisted pair. These enhancements reduce electromagnetic interference, making Cat 6 well-suited for dense cable environments such as offices, server rooms, and data centers.

In practical applications, Cat 6 cables can reliably transmit Gigabit Ethernet (1 Gbps) over distances of up to 100 meters. For 10 Gigabit Ethernet (10 Gbps) connections, they perform effectively over shorter distances, typically up to 55 meters, depending on environmental factors and installation quality. This makes Cat 6 ideal for modern networks that require high bandwidth and low latency, including corporate networks, educational institutions, and high-performance home setups. Overall, Cat 6 Ethernet cables provide a cost-effective, reliable, and future-ready solution for networking. Their combination of reduced crosstalk, higher frequency

capacity, and enhanced construction ensures they remain a preferred choice for both current and next-generation network deployments.



Figure 2.5 Cat6 Ethernet Cable

CHAPTER 3

SYSTEM DESIGN

3.1 Network Diagram

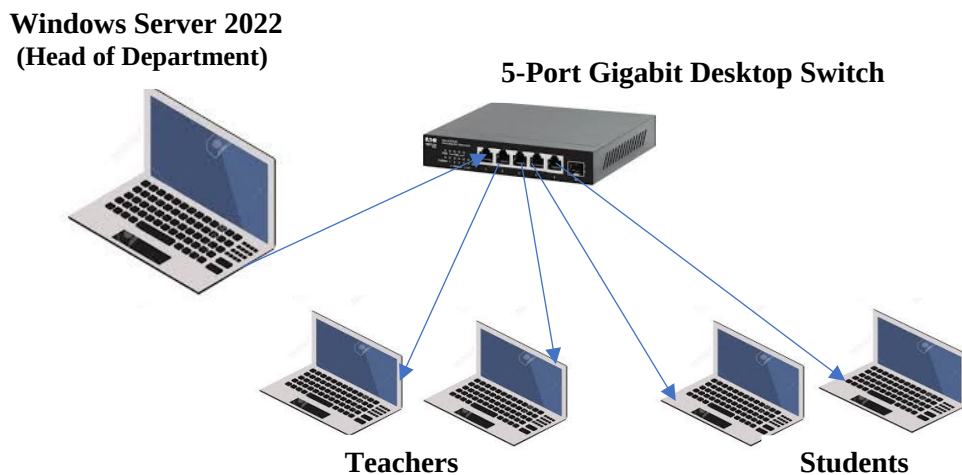


Figure 3.1 Network Diagram

Figure 3.1 shows a small computer network that uses a star shape design (star topology). In this setup, every device connects to one main device in the middle, which is a 5-port Gigabit Desktop Switch. The switch works like a hub, making sure data goes to the right computer.

In this network, there are three important devices: a computer with Windows Server 2022, teacher's laptop, and student's laptop. The server is very important because it provides services like user login, file sharing, and security for the laptops. The teacher and student laptops can use these services and also share information with each other through the switch.

This star-shaped network is popular because it is easy to manage, reliable, and can be expanded easily. Also, if one computer stops working, the rest of the network will still work fine. Another advantage of this design is that it provides better performance, since each device has its own dedicated connection to the switch. Troubleshooting problems is also simpler, as network issues can be quickly located by checking individual connections. In educational or office environments, this setup is highly effective because it supports centralized management, resource sharing, and network monitoring. Furthermore, future upgrades such as adding more laptops or replacing the switch with a larger one can be done without disrupting the existing connections, making this topology both flexible and practical.

3.2 Block Diagram of System

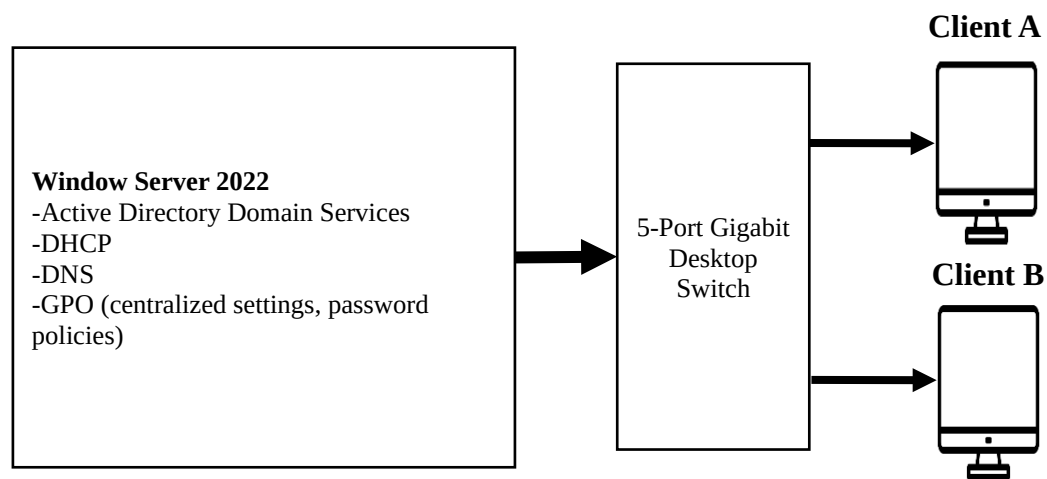


Figure 3.2 Block Diagram of System

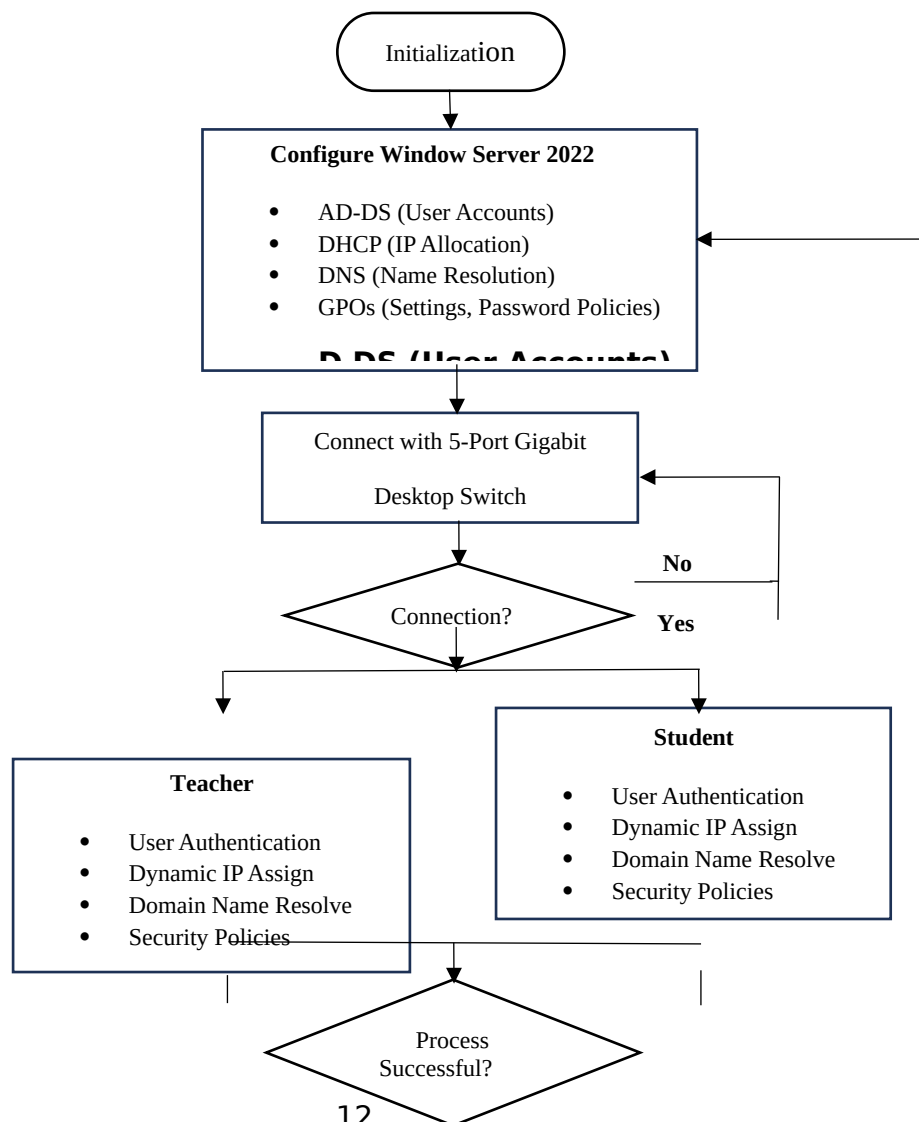
This network setup demonstrates a client-server environment managed through Windows Server 2022's core services. The server acts as the control hub, running several critical services: Active Directory authenticates users and devices, DHCP automatically assigns network addresses, DNS translates domain names, and Group Policy enforces security rules across all connected devices. These integrated services work together to create a secure, manageable network environment.

The physical connection between components is handled by a 5-port Gigabit switch, which efficiently routes traffic between the server and two client computers (Client A and Client B). This switch enables high-speed communication while allowing the server to centrally manage network resources. The entire system exemplifies a basic but complete domain network, where the server maintains control over user access, device settings, and network configuration, while clients receive

these managed services through their switch connection. This architecture is particularly effective for small business networks needing centralized administration.

Windows Server 2022 delivers scalability and flexibility, enabling a small network to grow into a large enterprise environment as organizational needs evolve. Its features, including file and storage management along with built-in security tools, strengthen the client-server model. Centralized management simplifies administrative tasks, allowing IT staff to create and manage user accounts, apply updates, and enforce security policies from a single location. The star topology enhances network reliability by isolating failures, ensuring that if one client disconnects or encounters issues, the rest of the network remains operational. This configuration also supports future expansion, making it easy to add additional clients or servers. Overall, a domain-based network using Windows Server 2022 offers an ideal combination of control, performance, and security for small to medium-sized organizations.

3.3 Flowchart of System



No

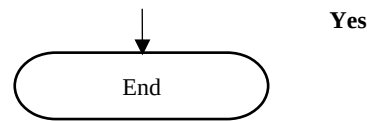


Figure 3.3 Flowchart of System

Figure 3.3 illustrates the step-by-step operation of the campus network management system, providing a clear overview of how the server and connected devices interact. The process begins with the Initialization stage, during which the system is powered on and essential preliminary checks are performed to ensure that all hardware components and software services are ready for operation. Once the system has been initialized, Windows Server 2022 is configured with a set of essential services required for efficient network management. These services include Active Directory Domain Services (AD DS) for creating and managing user accounts, Dynamic Host Configuration Protocol (DHCP) for automatically assigning IP addresses to client devices, Domain Name System (DNS) for translating domain names into IP addresses, and Group Policy Objects (GPOs) for applying system settings and enforcing security policies such as password complexity, software restriction, and desktop configurations.

After the server configuration is complete, it is connected to a 5-Port Gigabit Desktop Switch, which enables reliable communication between the server and all network devices. The system then performs a network connection verification to ensure all devices can communicate properly. If the connection fails, the workflow loops back to recheck and reconfigure the setup until connectivity is successfully established. Once the network connection is verified, two types of users Teachers and Students are allowed to access the system. Both groups follow a similar workflow, which includes authentication through AD DS, obtaining dynamic IP addresses from DHCP, resolving domain names via DNS, and complying with security rules defined by the server.

The system then verifies whether all processes have been completed successfully. If any issues are detected, the workflow returns to the network

verification step to address and resolve the problems. If successful, the system reaches the End stage, marking the completion of the workflow.

This flowchart emphasizes efficiency, reliability, and security in a small client-server environment. AD DS allows administrators to centrally manage user accounts, organize users into groups, and enforce consistent permissions. DHCP reduces manual configuration errors by automatically providing IP addresses, while DNS ensures smooth communication by converting human-readable names into IP addresses. GPOs maintain consistent security and operational policies across all devices.

The network verification process, combined with the loop-back mechanism, significantly enhances system reliability by detecting and resolving connectivity issues before they affect operations. Moreover, the network's scalable and flexible design allows smooth integration of new users and devices, while centralized control ensures strong security, efficient management, and optimized performance across the entire campus network.

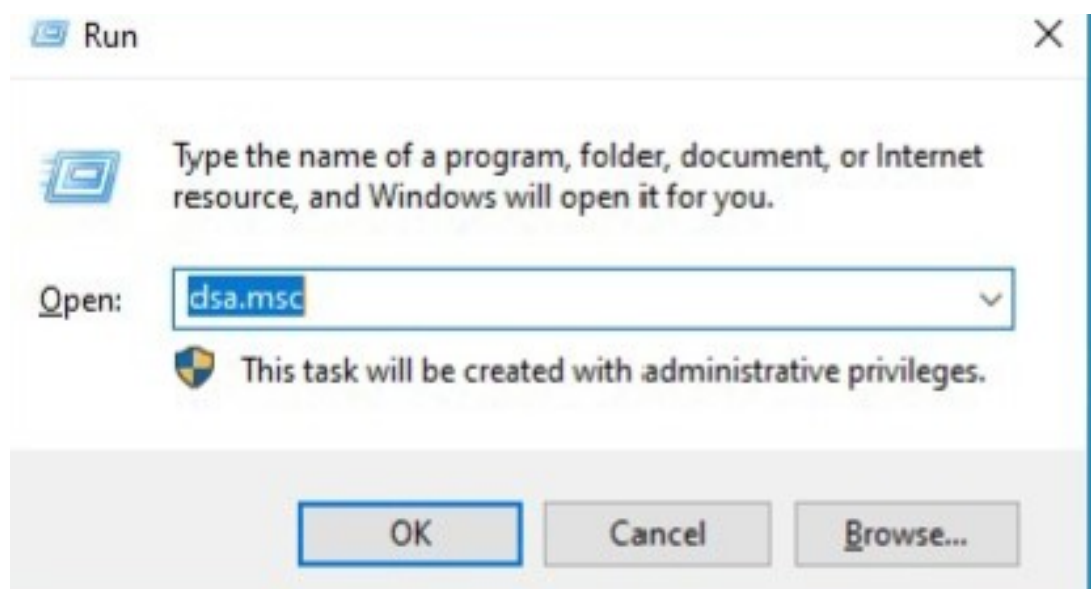
CHAPTER 4

IMPLEMENTATION

4.1 Server Configuration

4.1.1 Active Directory Domain Services (AD DS) Configuration

After successfully completing the domain setup, the next step is to log in to the newly created ucsh.edu.mm domain using the designated administrator account. This ensures that you have the necessary privileges to manage and configure the domain environment. Once logged in, you can begin managing users, groups, and organizational units. To access the management console, press Windows + R on your keyboard to open the Run dialog box, then type `dsa.msc` and press Enter. This action will launch Active Directory Users and Computers (ADUC), a central tool used for



domain administration and account management tasks. Opening Active Directory Users and Computers (dsa.msc) is shown in figure 4.1.

Figure 4.1 Opening Active Directory Users and Computers (dsa.msc)

As shown in figure 4.2, in the Active Directory Users and Computers (ADUC) console, expand the domain tree to view available options. Right-click the domain name ucsh.edu.mm, select New, and then choose Organizational Unit from the context menu. A dialog box will appear, prompting you to enter a name for the new OU. Type FCST as the name to represent the department or organizational group. Next, check the option Protect container from accidental deletion to prevent unintentional removal of the OU. After completing these steps, click OK to confirm and successfully create the FCST Organizational Unit within the domain structure.

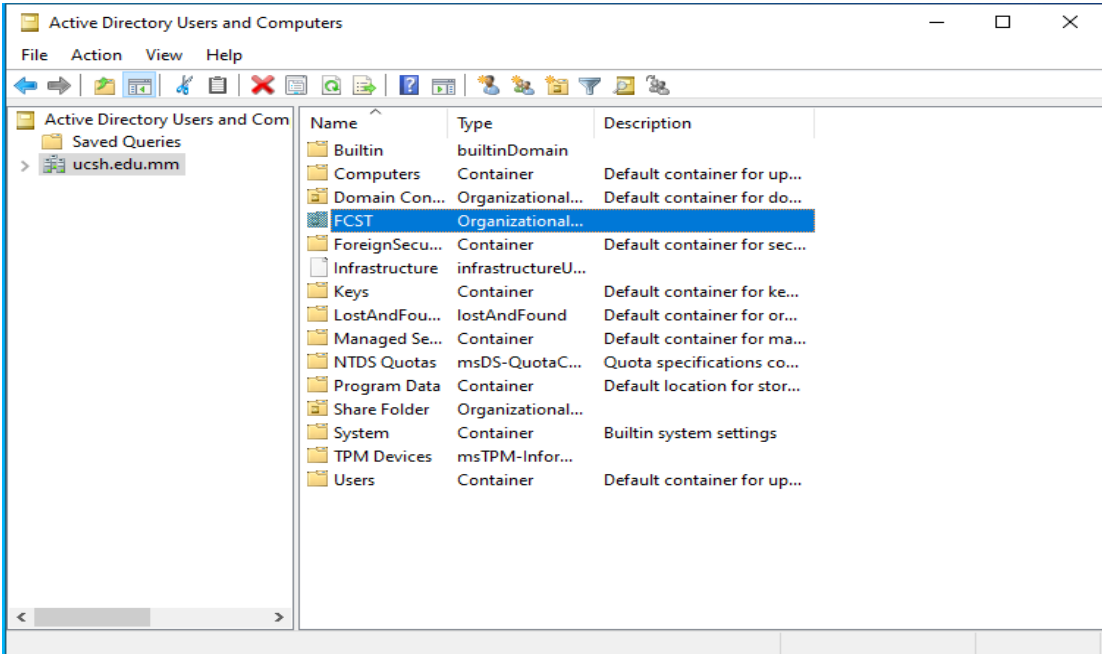


Figure 4.2 Organizational Units View

After creating the FCST Organizational Unit (OU), as shown in Figure 4.3, the next step is to organize user accounts by adding two sub-OUs. Open Active Directory Users and Computers (ADUC), expand the ucsh.edu.mm domain, and locate the FCST OU. Right-click it, select New, then choose Organizational Unit. Create the first sub-OU named Admins for administrative accounts and the second sub-OU named Students for student accounts. This structure improves account management, enforces consistent policies, reduces administrative errors, and ensures efficient organization of users across the domain.

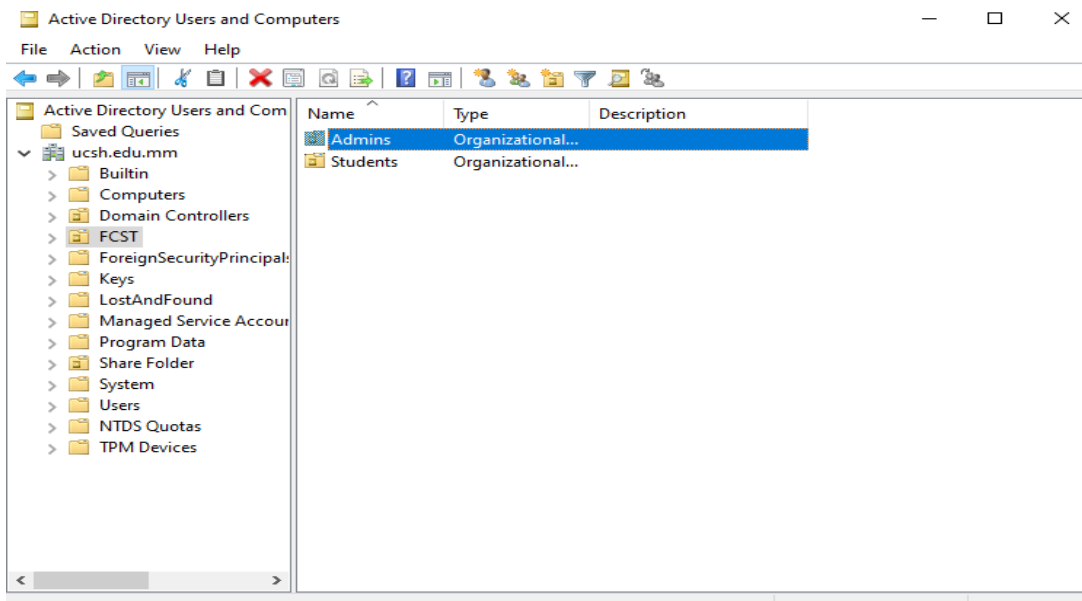


Figure 4.3 Admins and Students OUs under FCST

Created four user accounts in the Admin OU to manage administrative tasks and provide proper control over the domain environment. Figure 4.4 shows created user accounts within the Admins.

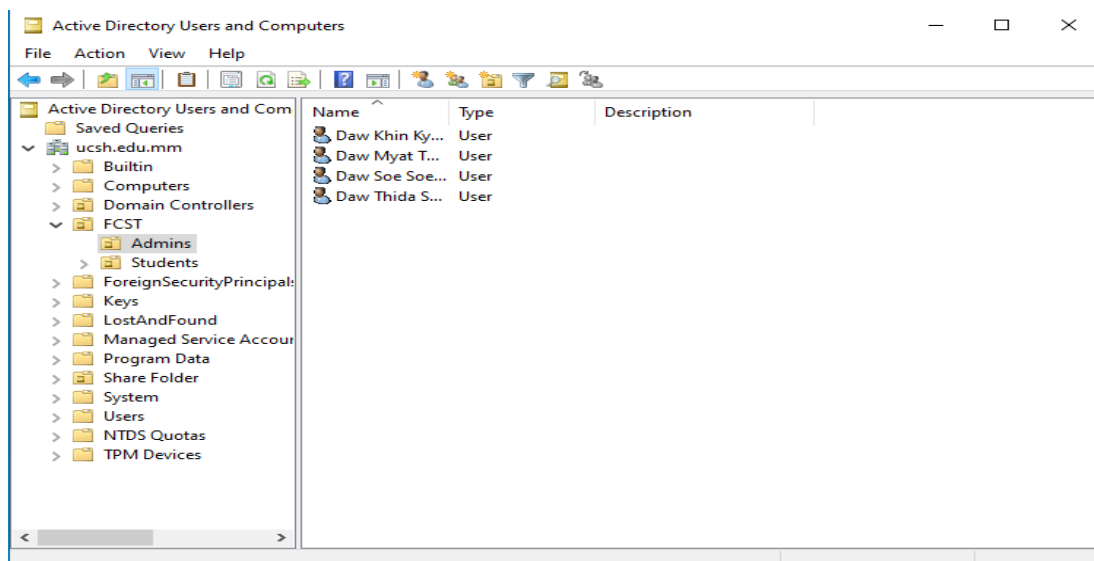


Figure 4.4 User Accounts within the Admins

As displayed in figure 4.5, created a separate Students OU in order to organize student accounts more systematically. Inside the Students OU, created individual OUs for better classification, and under each of those OUs, Created one user account. This structure helps in maintaining a clear hierarchy, making it easier to manage permissions, policies, and security settings for both administrators and students.

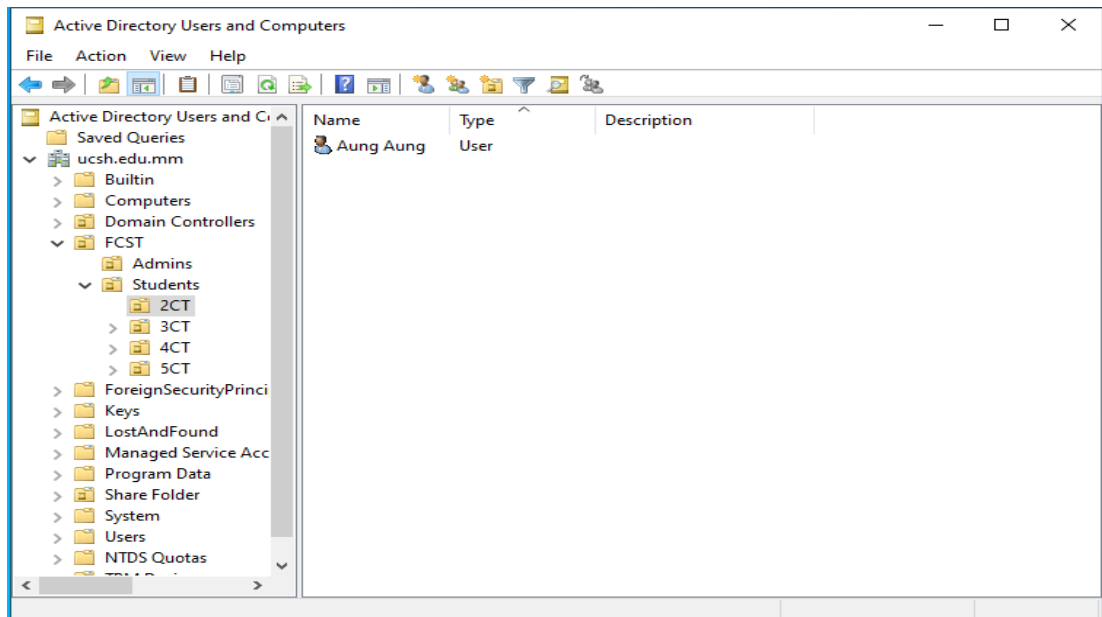


Figure 4.5 User Accounts within the Students

4.1.2 DHCP Configuration

Configured the DHCP Server role by first opening Server Manager and selecting Add Roles and Features.

Chose the Role-based or feature-based installation option and selected my server from the available list.

In the roles section, checked DHCP Server and clicked Next, then followed the prompts to complete the installation.

Once the installation was finished, clicked Complete DHCP configuration to launch the post-installation wizard, which finalized the setup and prepared the server to operate within the network. After that, created a scope is shown in figure 4.6.

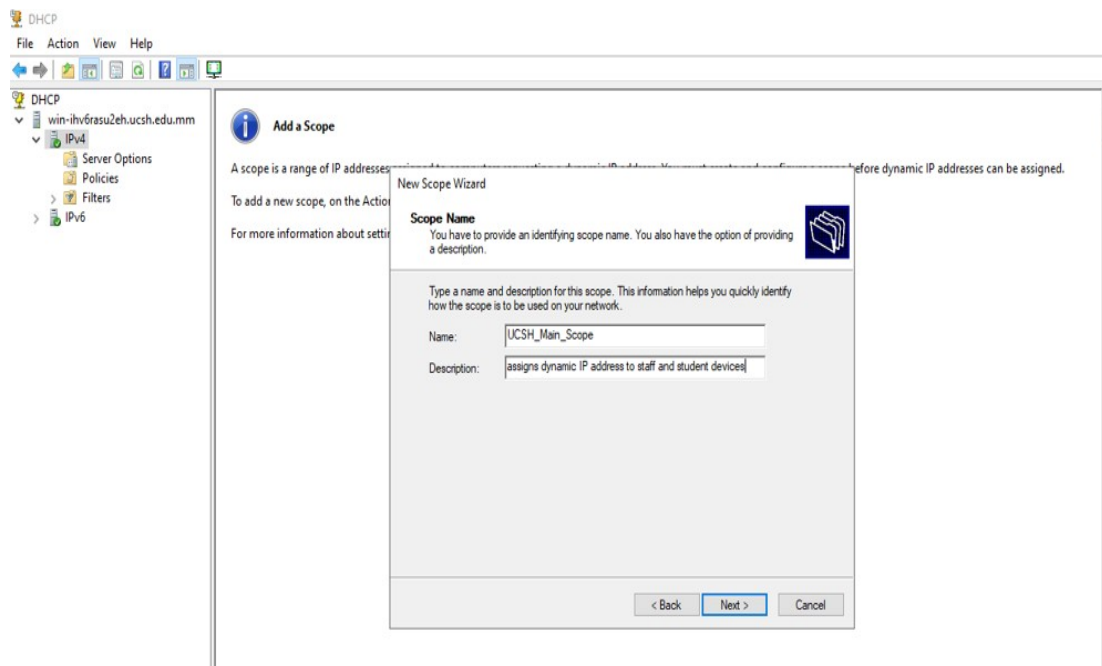


Figure 4.6 Creating DHCP Scope

Next, authorized the DHCP server in Active Directory Domain Services so that it could assign IP addresses within the domain securely.

During the post-installation process, provided my domain administrator credentials, which registered the DHCP server in Active Directory.

This authorization step ensured that the server was trusted by the domain and allowed it to begin issuing IP leases to client devices automatically the 192.168.1.0 scope for my network.

In DHCP Manager, right-clicked IPv4 and then select New Scope, named it LAN-192.168.1.0/24, and set the start and end IP addresses from 192.168.1.100 to 192.168.1.200 with a subnet mask of 255.255.255.0.

Configure DHCP IP address range is displayed in figure 4.7.

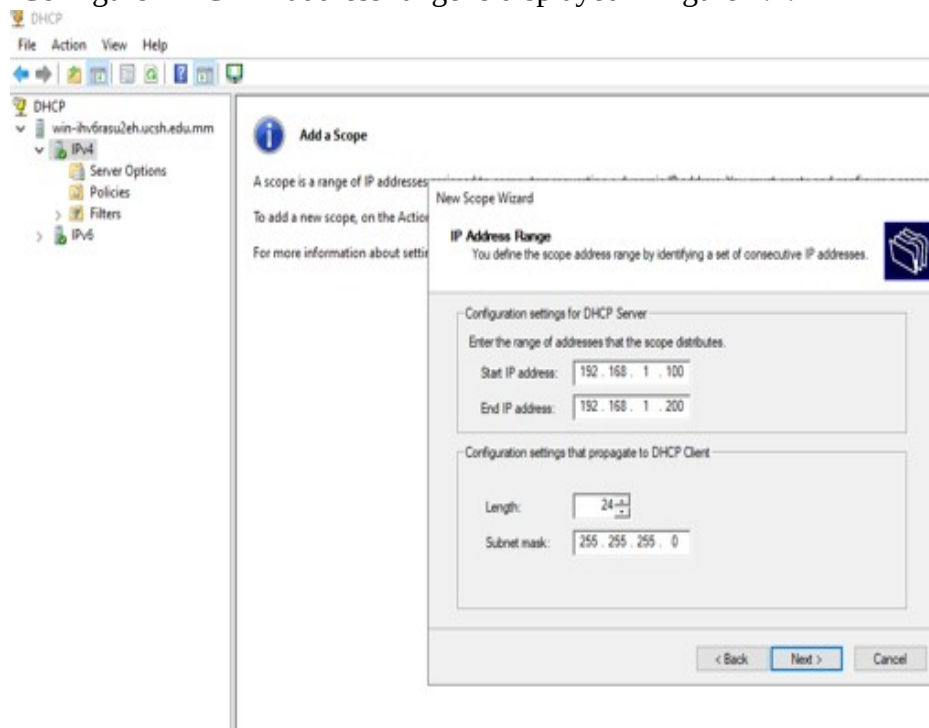


Figure 4.7 IP Address Range in DHCP Scope

Added an exclusion range from 192.168.1.150 to 192.168.1.160 for static devices to prevent conflicts and set the lease duration to 8 days. Exclusive IP configuration step is shown in figure 4.8.

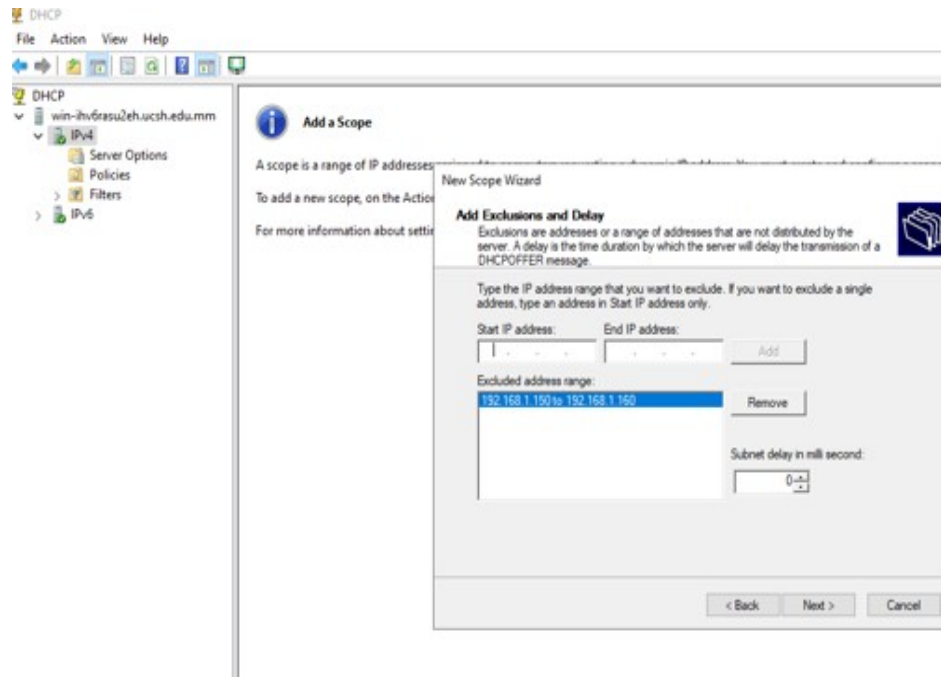


Figure 4.8 Exclusive IP

Activated the scope by right-clicking it and selecting Activate, confirming that the DHCP server is ready to assign IP addresses within the configured range while respecting the exclusion list. Active Scope is shown in figure 4.9, and then DHCP Scope configuration is finished.

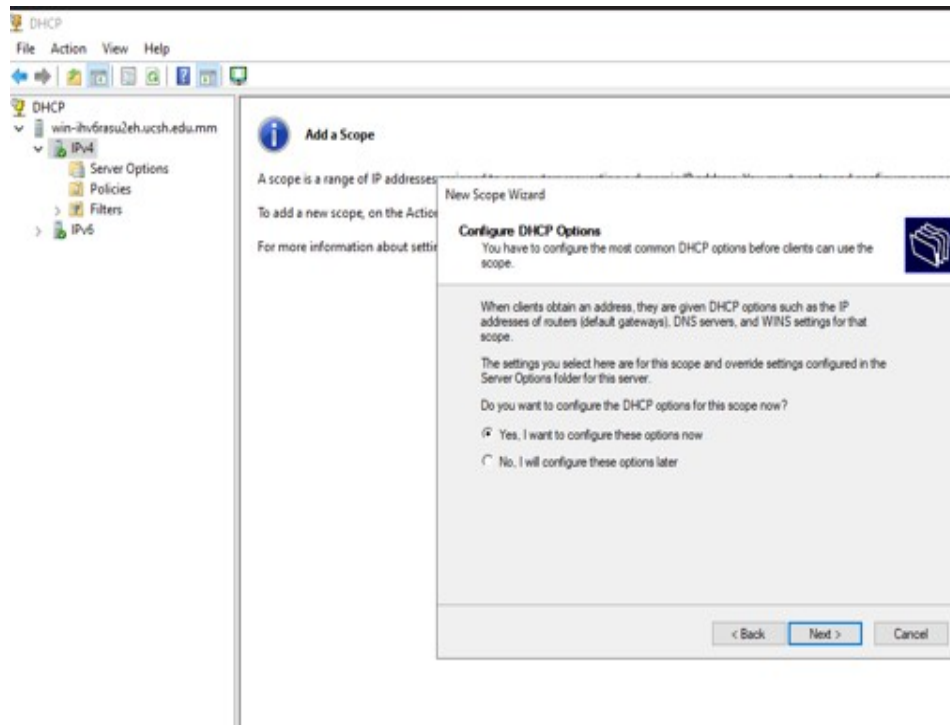


Figure 4.9 Active Scope

Verified that the DHCP service was running by pressing Win + R, typing services.msc, and locating DHCP Server. Made sure the service was set to Automatic and was Running. Finally, tested a client in the 192.168.1.0/24 network by releasing and renewing its IP configuration to confirm that it successfully received an IP from DHCP server.

4.1.3 DNS Configuration

Installed the DNS Server role by opening Server Manager, selecting Add Roles and Features, and choosing Role-based or feature-based installation. Selected my server and checked DNS Server, then proceeded with the installation. After it completed, verified that the DNS service was installed and running. Opened DNS Manager through Server Manager, then selected Tools, and then DNS. This console allowed me to manage all DNS settings for my domain ucsh.edu.mm.

Created a Forward Lookup Zone for ucsh.edu.mm. Right-clicked Forward Lookup Zones, then selected New Zone, chose Primary Zone, and stored it in Active Directory for replication. Named the zone ucsh.edu.mm. Then, added an AAA (A) record with the fully qualified domain name ucsh.edu.mm and IP address 192.168.1.20. This ensures that the hostname resolves correctly to the server's IP address. Creating Host in DNS Forward Lookup Zone is shown in figure 4.10.

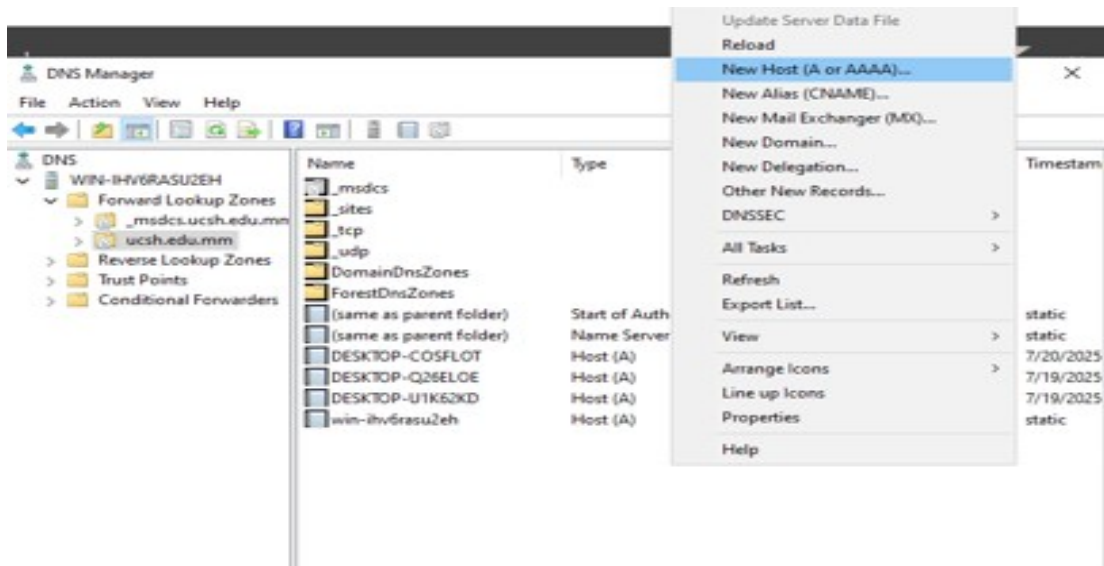


Figure 4.10 Creating Host in DNS Forward Lookup Zone

After that matching name and IP is shown in figure 4.11.

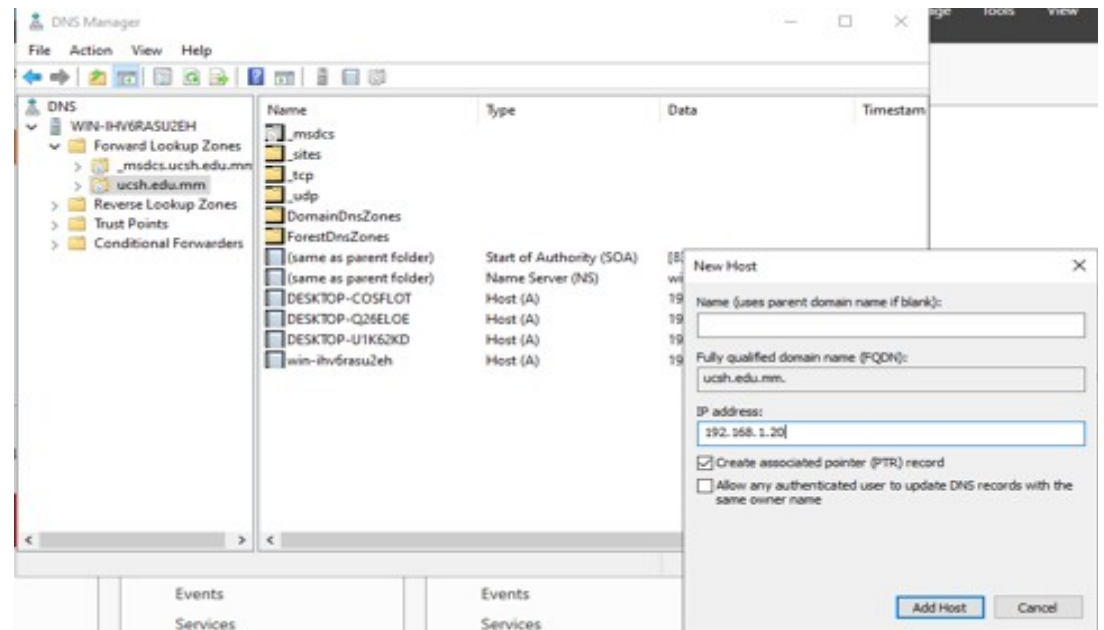


Figure 4.11 Matching Name and IP

As shown in figure 4.12, a Reverse Lookup Zone was created to allow IP addresses to resolve back to hostnames. This was done by right-clicking Reverse Lookup Zones and selecting New Zone. A Primary Zone was created and stored in Active Directory, with the network ID set to 192.168.1. Finally, a PTR record was added so that 192.168.1.20 correctly resolved back to the hostname ucsh.edu.mm.

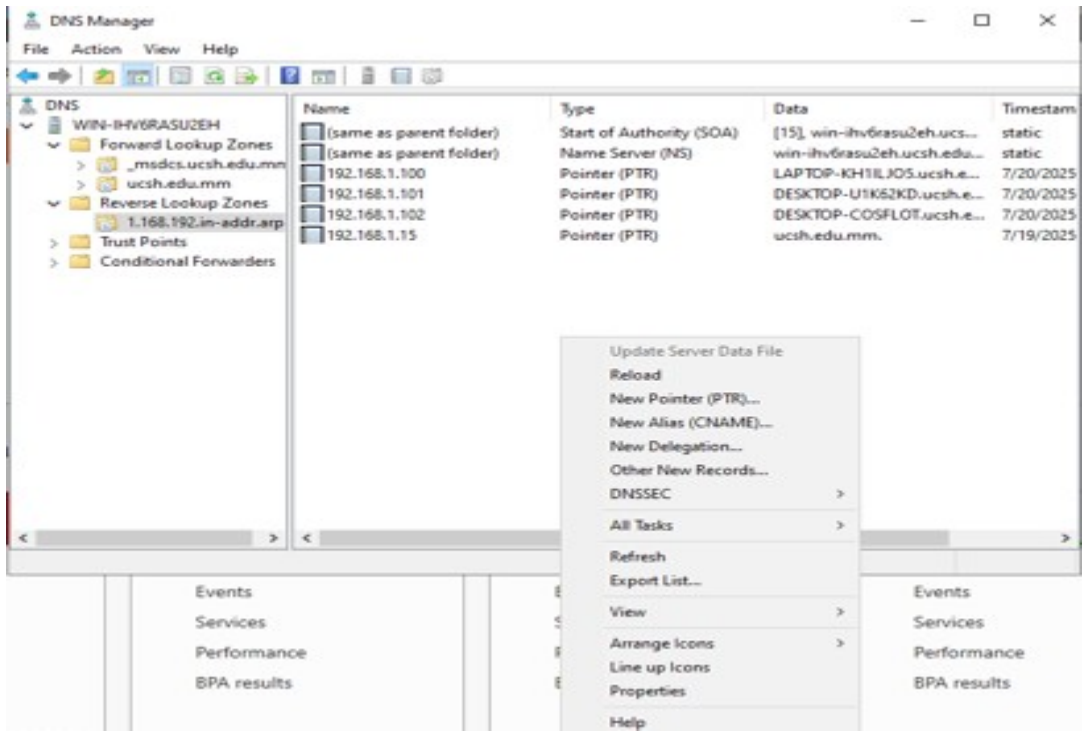


Figure 4.12 Creating PTR in DNS Reverse Lookup Zone

Figure 4.13 shows matching the IP and Name for DNS Reverse Lookup Zone.

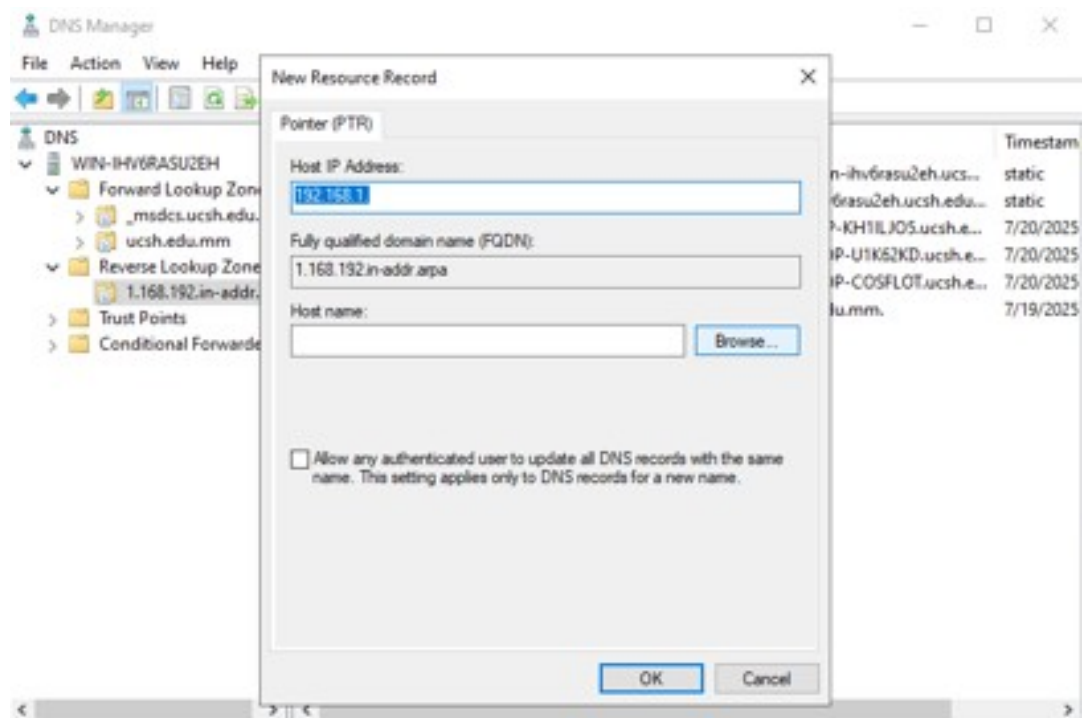


Figure 4.13 Matching IP and Name

4.1.4 Password Policy with Group Policy Object (GPO) Configuration

Configured the password policy for the domain using a Group Policy Object in Active Directory to manage user authentication security. First, opened the Group Policy Management Console and either created a new GPO or edited an existing one linked to the domain. Default domain policy is displayed in figure 4.14.

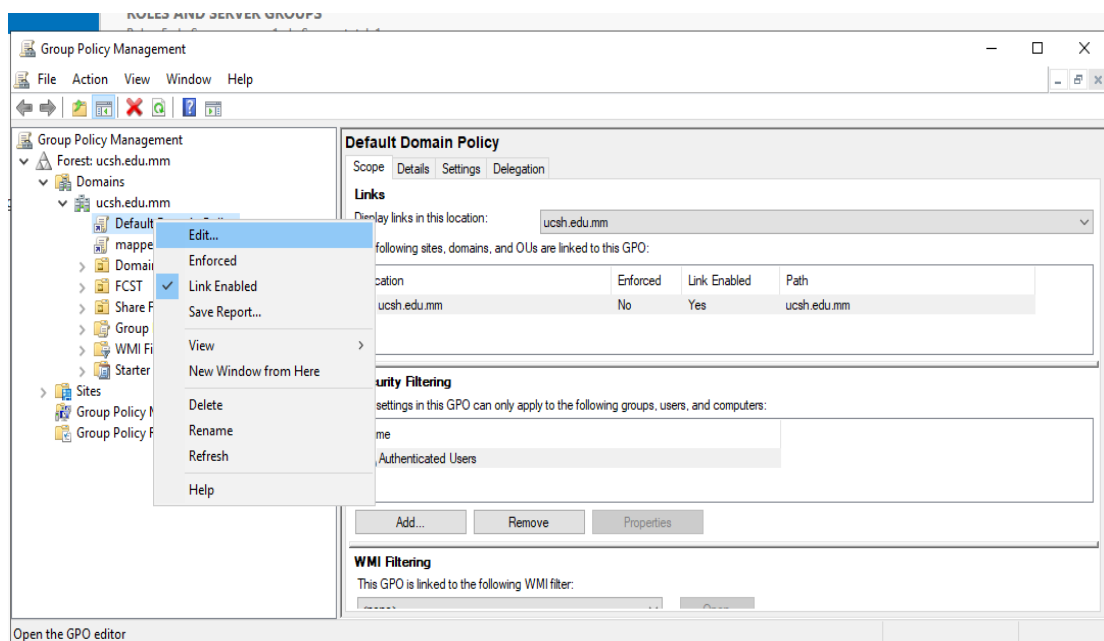


Figure 4.14 Default Domain Policy

Within the Group Policy Object (GPO), Carefully navigated through several configuration levels to apply important security settings for user accounts. Starting from Computer Configuration, proceeded to Policies, then expanded Windows Settings, followed by Security Settings.

From there, selected Account Policies and finally accessed the Password Policy option. In this section, specifically configured the minimum password length requirement, setting it to eight characters. By enforcing this policy, every user in the domain is required to create a password that contains at least eight characters.

This configuration helps establish a fundamental layer of account security by preventing the use of weak, extremely short, and easily guessable passwords, which are highly vulnerable to attacks.

Enforcing such a policy ensures stronger password practices across the entire network, thereby reducing security risks and promoting better compliance with organizational standards. These settings are illustrated in figure 4.15.

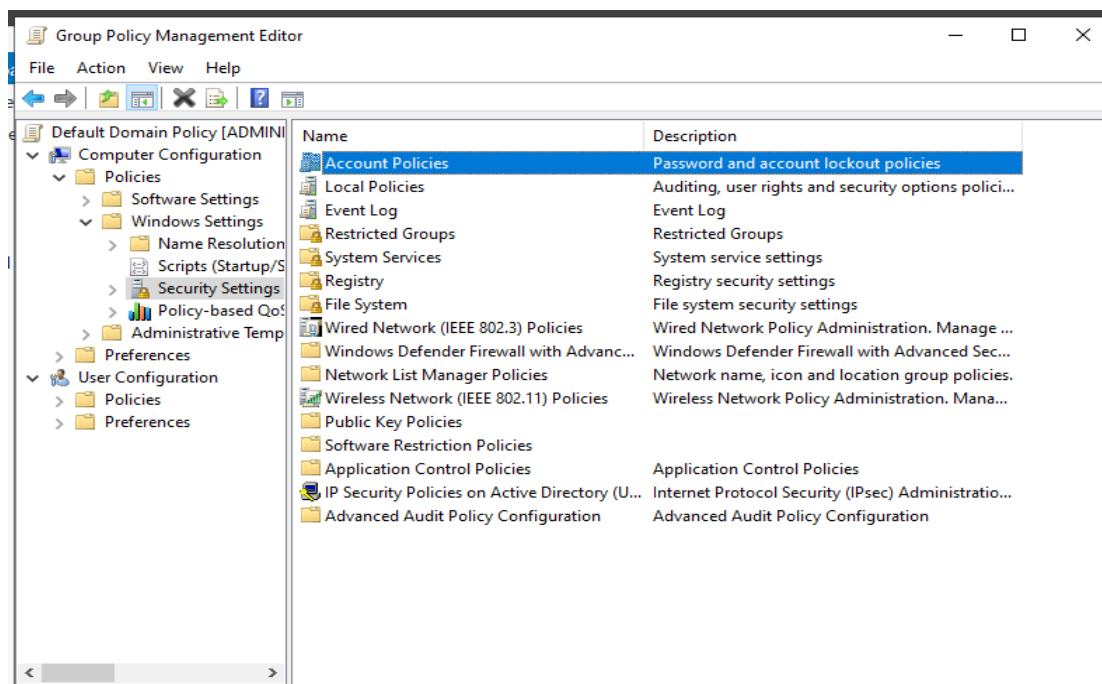


Figure 4.15 Security Settings and Account Policies

Password complexity requirements were disabled to simplify password creation while still enforcing the minimum length policy. The GPO was then linked to the appropriate Organizational Units, ensuring it applied to all relevant accounts.

Finally, the `gpupdate /force` command was executed on client computers to immediately enforce consistent password management. Password Policies is shown in figure 4.16.

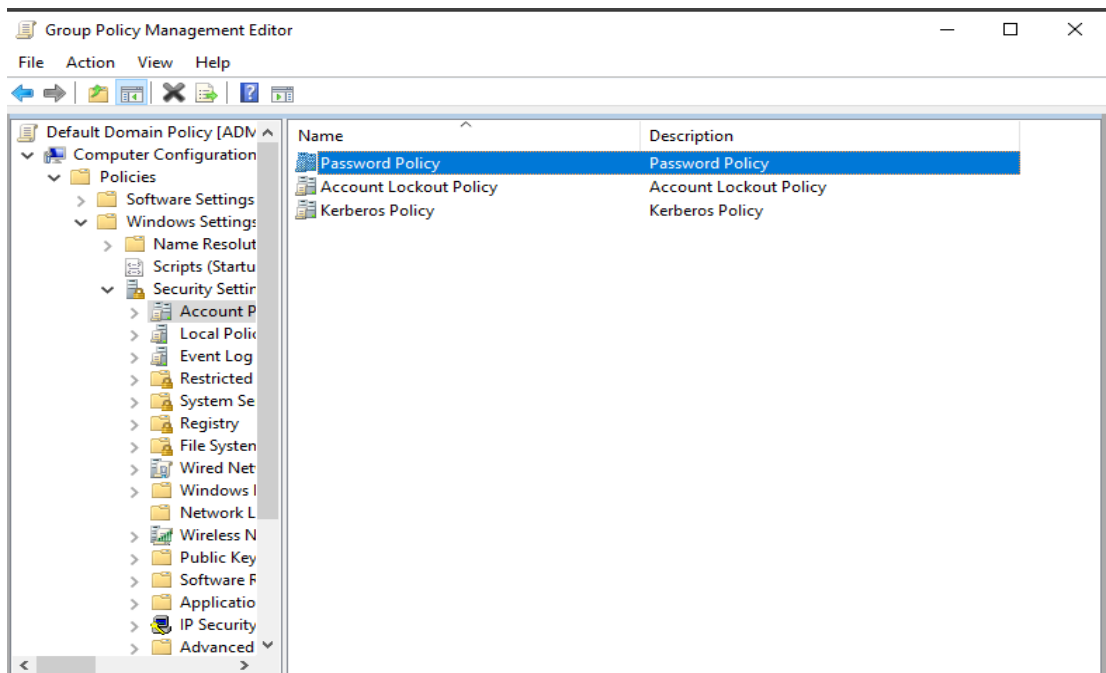


Figure 4.16 Password Policies

4.2 Client Configuration

4.2.1 Dynamic IPv4 Configuration Via DHCP

As shown in figure 4.17, configured the IPv4 settings for my network adapter by opening `ncpa.cpl`, which displays all network connections on the computer.

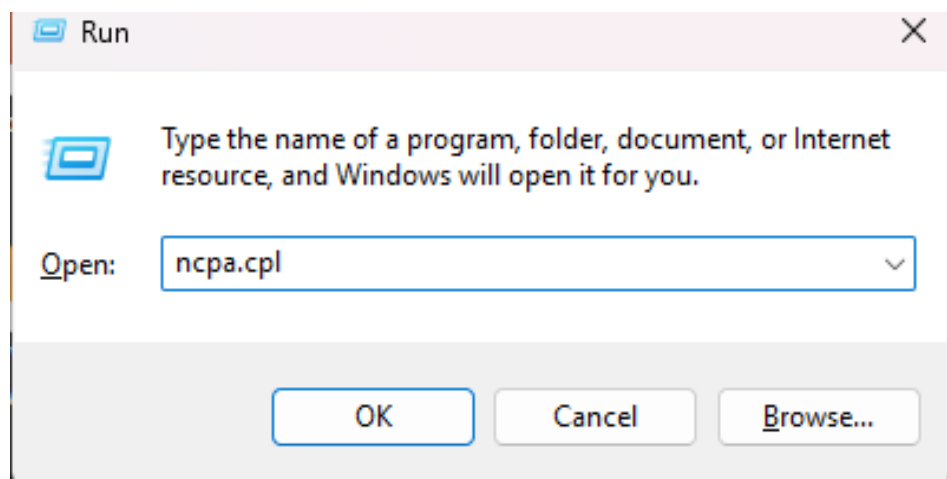


Figure 4.17 CMD to Open Network Connection

Right-clicked on the network adapter wanted to configure and selected Properties. In the properties window, selected Internet Protocol Version 4 (TCP/IPv4) and clicked on Properties is displayed in figure 4.18.

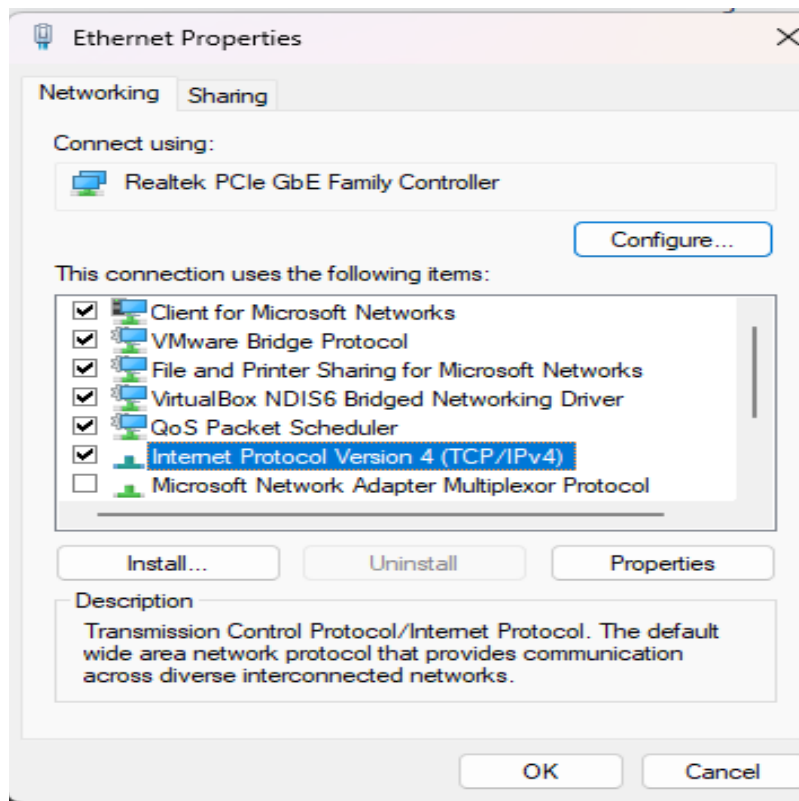


Figure 4.18 Internet Protocol Version 4

As shown in figure 4.19, the IPv4 properties, chose Obtain an IP address automatically and Obtain DNS server address automatically. This configuration, called Dynamic IPv4 configuration via DHCP, allows the network adapter to automatically receive an IP address, subnet mask, default gateway, and DNS server information from the DHCP server. By doing this, ensured that my device can connect to the network without manually entering any network details. This method is commonly used in networks where IP addresses are centrally managed, preventing conflicts and simplifying network administration. This configuration is the opposite of static IPv4 settings, where all the network parameters are manually assigned.

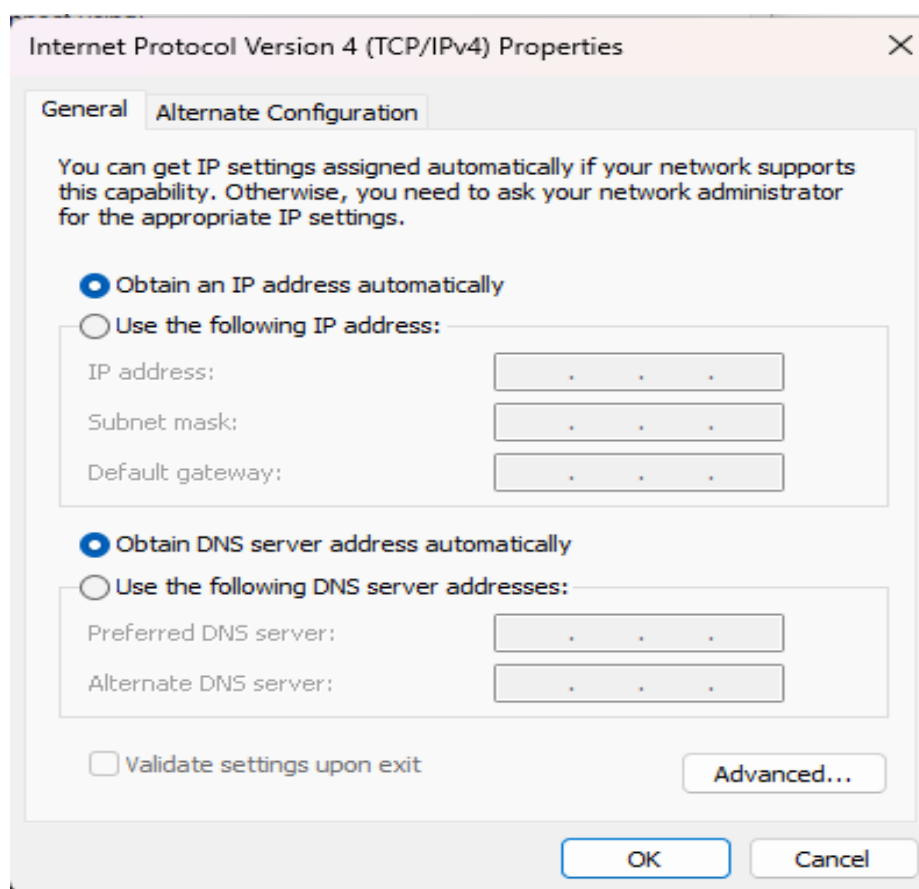


Figure 4.19 Setting to Get DHCP

4.2.2 Domain Membership Configuration

To join the Active Directory domain, I opened sysdm.cpl, which launched the System Properties window. In System Properties, I selected the Computer Name tab and clicked Change to modify the computer's membership. This allowed me to enter the domain name and provide the necessary credentials, enabling the computer to

become a member of the domain. Figures 4.20 and 4.21 show the System Properties configuration for this process.

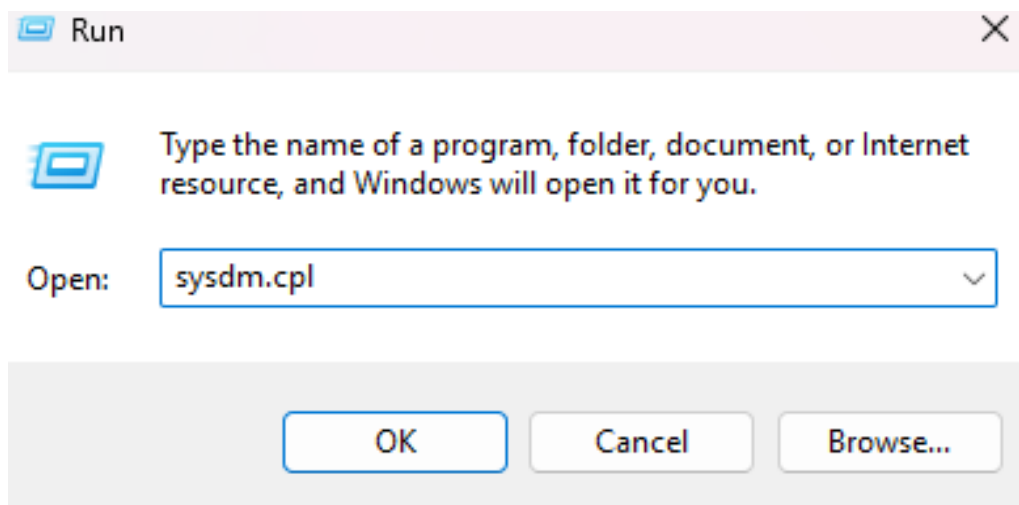


Figure 4.20 CMD to Open System Properties

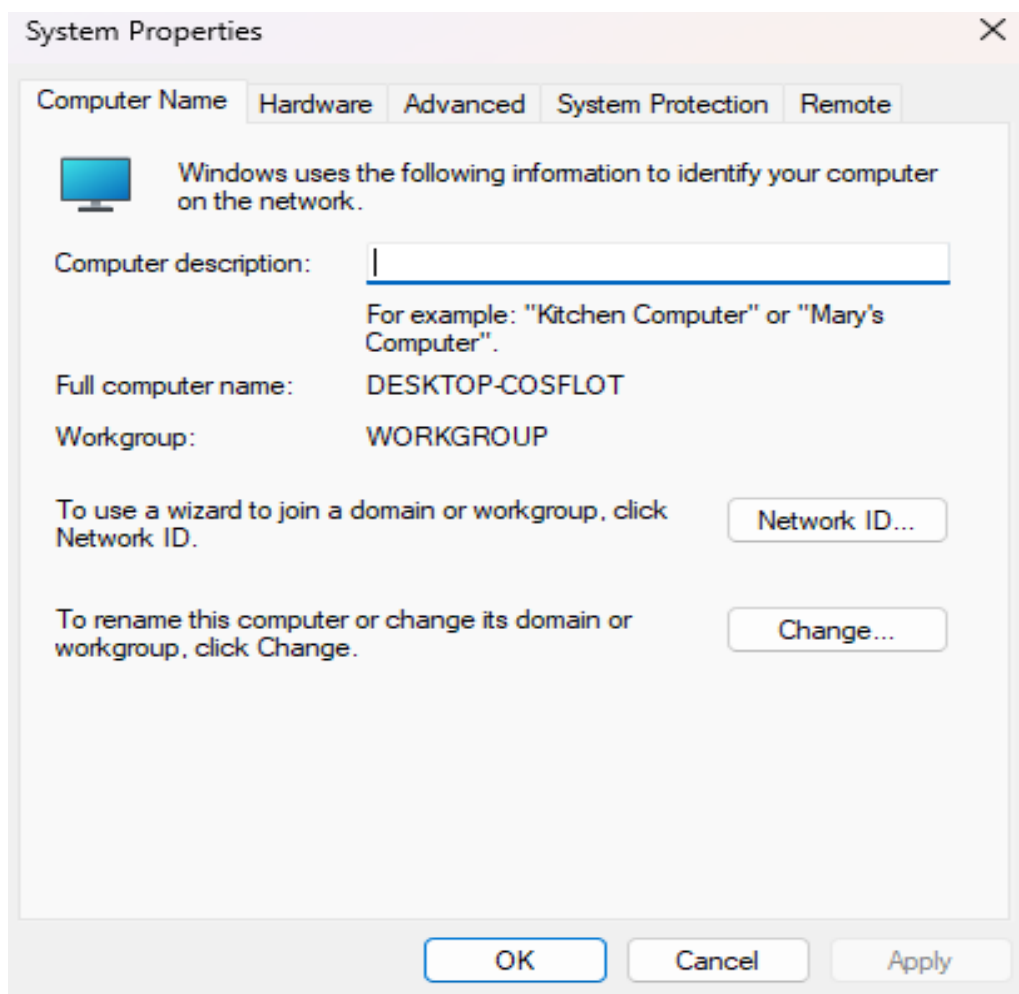


Figure 4.21 System Properties

In the settings window, entered the domain name ucsh.edu.mm to connect the computer to the Active Directory Domain Services (AD DS) environment. After entering the domain name, provided the credentials of a user account that has permission to add computers to the domain. Once the credentials were verified and accepted, the computer was successfully joined to the domain. This configuration allows the computer to authenticate users using Active Directory accounts, apply Group Policy settings automatically, and access network resources such as shared folders, printers, and applications managed within the domain.

By joining the domain, all users and computers on the network can be centrally managed, which enhances security, simplifies administrative tasks, and ensures consistent application of policies across the network.

After completing the domain join, restarted the computer to finalize the process and enable domain user logins.

This setup is essential for integrating the computer into a managed network environment and allows it to fully participate in the centralized management provided by Active Directory. Change Domain Name setting is shown in figure 4.22.

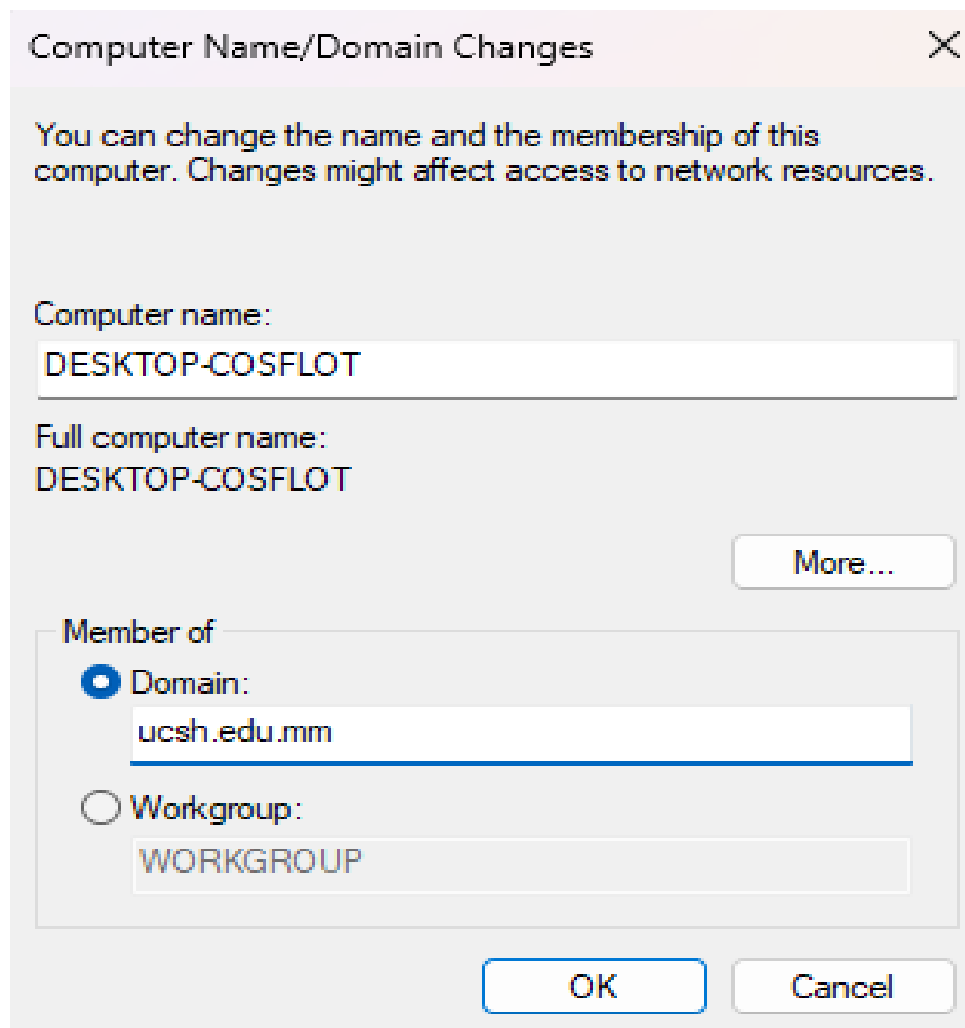


Figure 4.22 Change Domain Name

4.3 Implementation Result

4.3.1 Implementation of Active Directory Domain Services (AD DS)

After successfully configuring Active Directory Domain Services (AD-DS), the users that were created under the designated Organizational Unit (OU) were able to log in to domain-joined computers without any issues.

This demonstrates that the domain environment is functioning correctly and that centralized authentication is properly established. By joining client machines to the domain, the login process no longer depends on local accounts but instead uses domain credentials managed within AD-DS.

This provides stronger security, easier administration, and consistent user access across the network. It also ensures that policies applied through Group Policy Objects (GPOs) are enforced on all domain users.

Overall, the AD-DS configuration proved successful, as users created in the OU could access the system with their assigned accounts in a secure and centralized manner. The login of Admin account and Student account on a domain-computer are shown in figure 4.23 and figure 4.24.

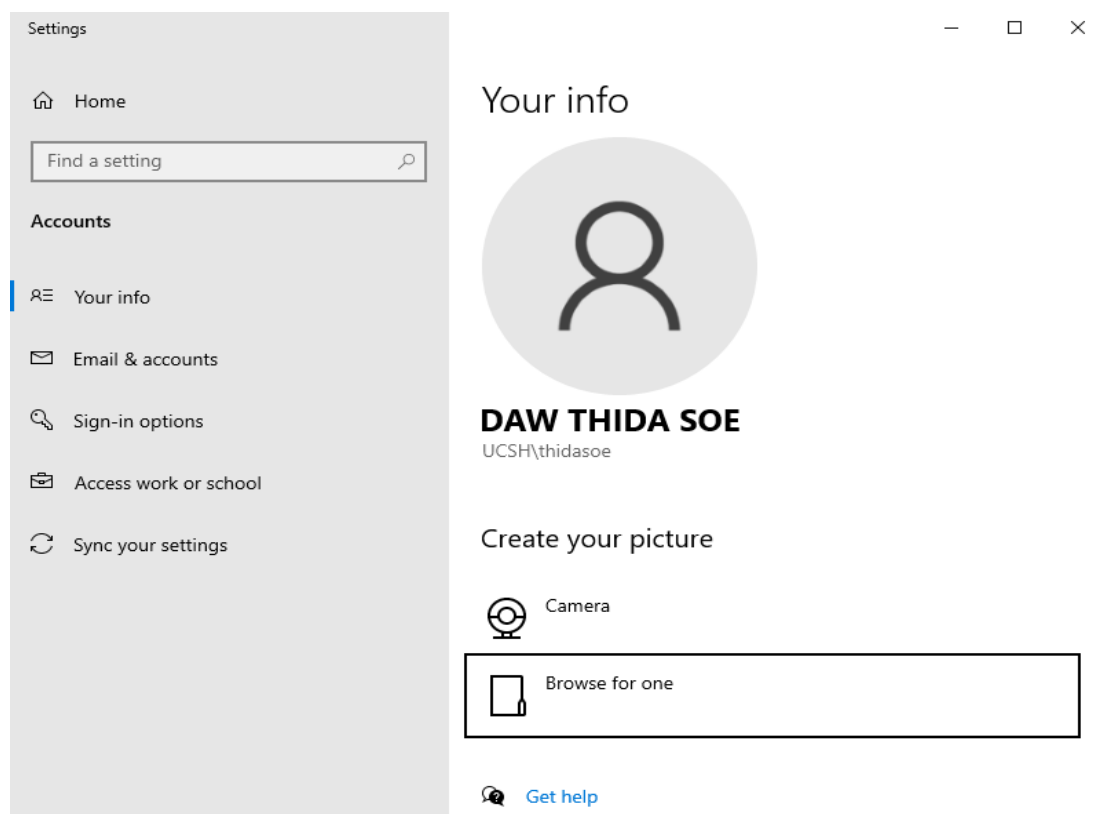


Figure 4.23 Admin Account

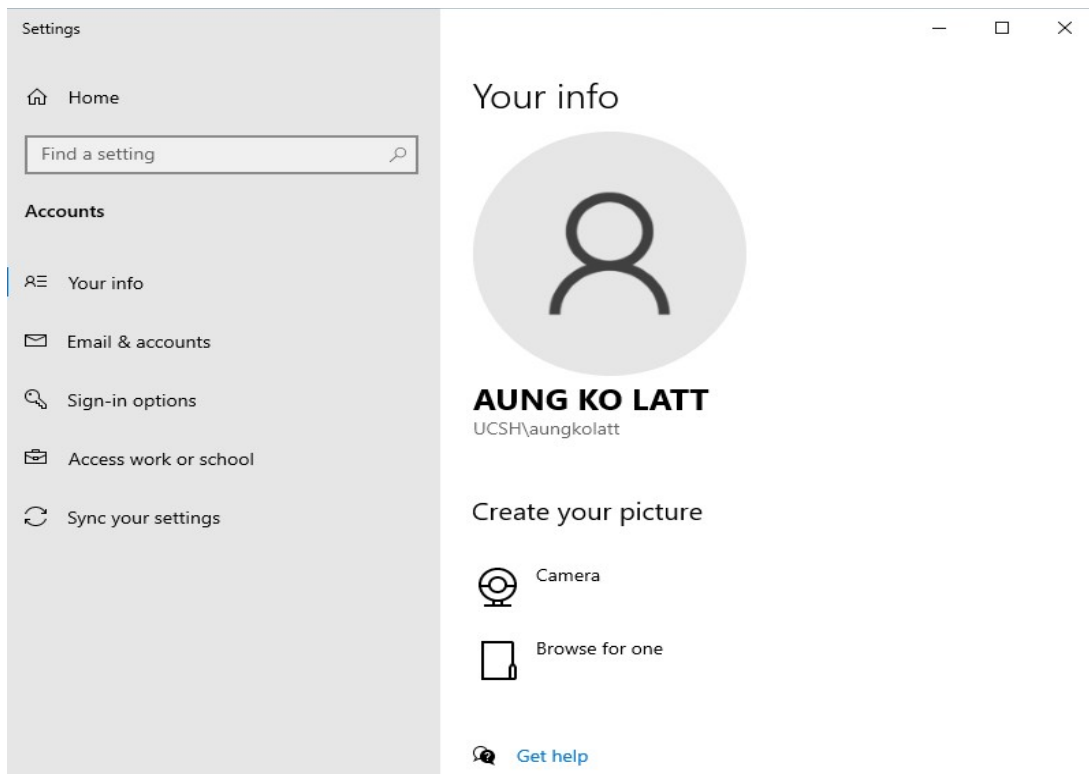


Figure 4.24 Student Account

4.3.2 Implementation Service of DHCP

After completing the DHCP configuration for the 192.168.1.0/24 network, the DHCP scope was successfully activated and thoroughly verified to ensure proper functionality. The configured IP address range, from 192.168.1.100 to 192.168.1.200, was correctly applied, while the exclusion range of 192.168.1.150 to 192.168.1.160 was reserved for devices requiring static IP addresses. This setup prevents IP conflicts by ensuring that critical devices retain their assigned addresses while dynamic addresses are issued to other clients.

The DHCP Server service was confirmed to be running in Automatic mode, guaranteeing that the server remains continuously available to assign IP addresses. To test the configuration, client machines on the network were instructed to release and renew their IP addresses. Both clients successfully received addresses from the DHCP pool, with the first client obtaining 192.168.1.101 and the second client receiving 192.168.1.102.

These results confirm that the DHCP server is functioning as expected, efficiently and automatically distributing IP addresses within the defined range, honoring the exclusion list, and managing lease durations. Figure 4.25 shows verification of IP assignment from the DHCP server.

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : ucsh.edu.mm
Link-local IPv6 Address . . . . . : fe80::83b3:ed0:4e94:668f%9
IPv4 Address. . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Figure 4.25 Check IP from DHCP

4.3.3 Implementation Service of DNS

After installing and configuring the DNS Server role, the DNS service was verified to be running properly on the server, ensuring that it was operational and ready to handle name resolution requests. A Forward Lookup Zone for ucsh.edu.mm was created and configured to be stored in Active Directory, allowing replication across domain controllers for consistency. Within this zone, an A (AAA) record was added, mapping the fully qualified domain name ucsh.edu.mm to the IP address 192.168.1.20, ensuring accurate hostname resolution. To test the configuration, a ping command was executed using the domain name ucsh.edu.mm, which successfully responded, confirming that the DNS server correctly resolves hostnames to IP addresses. This configuration allows domain-joined client machines to locate and connect to the server without issues, validating that the DNS setup is fully functional. Figure 4.26 illustrates the domain connectivity check.

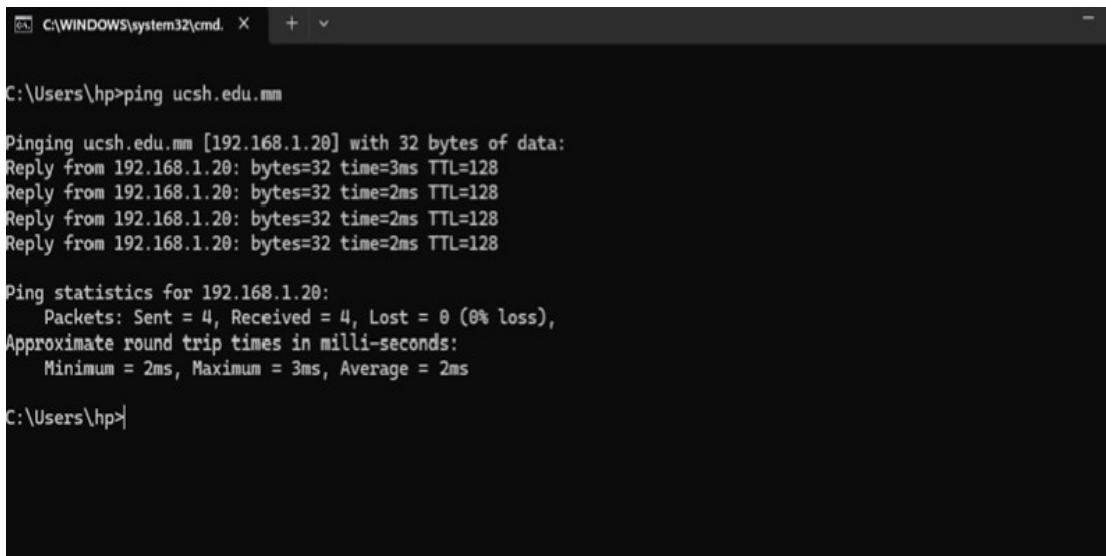
A screenshot of a Windows Command Prompt window. The title bar shows 'C:\WINDOWS\system32\cmd.' and standard window controls. The command prompt shows the user 'hp' at 'C:\Users\hp>' typing 'ping ucsh.edu.mm'. The output shows four successful replies from 192.168.1.20 with 32 bytes of data, response times of 3ms, 2ms, 2ms, and 2ms, and a TTL of 128. Ping statistics for 192.168.1.20 show 4 packets sent, 4 received, 0 lost (0% loss), and approximate round trip times of 2ms minimum, 3ms maximum, and 2ms average. The prompt ends with 'C:\Users\hp>|'.

Figure 4.26 Check Domain Connectivity

CHAPTER 5

CONCLUSION

The Campus LAN Management System is designed to provide a comprehensive and efficient solution for connecting and managing all computers, servers, and other network devices within universities and educational institutions. By implementing Windows Server 2022 as the central server platform, along with Active Directory Domain Services (AD DS), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS), the system allows administrators to effectively manage user accounts, control IP address allocation, ensure proper name resolution, and regulate access to shared resources across the network. In addition to these core services, the use of Group Policy Objects (GPOs) and advanced management tools enables the enforcement of security policies, monitoring of network performance, and optimization of overall network efficiency. This approach ensures that the campus network remains secure, reliable, and well-organized while minimizing administrative workload and reducing potential errors in network management. The system also supports scalability, allowing institutions to expand their network infrastructure as needed without compromising performance or security. By integrating automated management and centralized control, the Campus LAN Management System provides both students and staff with consistent access to network resources and services, enhancing productivity and collaboration. Overall, this system represents a critical framework for building a secure, high-performance, and well-managed network

environment in educational campuses, enabling efficient communication, resource sharing, and IT administration across all connected devices.

5.1 Advantages of the Project

The Campus LAN Management System provides administrators with a centralized platform to efficiently manage all network devices, servers, and client machines across the campus. By consolidating control in a single interface, the system simplifies administrative tasks, minimizes human errors, and significantly reduces the time required for routine maintenance. It also facilitates the seamless sharing of essential resources such as printers, storage devices, and internet connections, ensuring stable and consistent network performance while improving overall productivity. Beyond operational efficiency, the system enhances security by continuously monitoring user activities, network traffic, and device status in real time. Potential threats, including unauthorized access attempts, malware, or suspicious behavior, can be identified and addressed swiftly. Administrators can centrally enforce security policies, configure firewalls, and deploy updates, maintaining a secure and compliant network environment. Overall, the system ensures that campus users experience a reliable, secure, and high-performing network infrastructure at all times.

5.2 Limitation and Future Work

The Campus LAN Management System offers a centralized and efficient approach to managing network infrastructure, allowing administrators to control servers, client machines, and network devices from a single interface. However, despite its many advantages, the system has certain limitations that need to be considered. Its overall performance is highly dependent on the proper functioning of both hardware and software components. Any device failure, software malfunction, or misconfiguration can significantly affect network stability and efficiency. Furthermore, expanding the network or integrating additional devices often requires careful configuration and the expertise of skilled IT personnel, which can increase administrative workload and complexity.

Looking toward future improvements, the system could benefit from the integration of advanced features such as automated security threat detection and real-time alerts, which would help identify and respond to potential risks more quickly. Cloud-based monitoring and management capabilities could also allow administrators

to manage the network remotely, enhancing flexibility and accessibility. Additionally, providing support for larger and more complex networks, strengthening user access controls, and regularly updating security policies would improve both reliability and protection. Implementing these enhancements would ensure a robust, secure, and high-performing campus network for all users.

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", 5STARCook, 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.

