Campus Local Area Network Management System

Min Htet Moe Yan, Ye Htet
Student, 5th Year, B.C.Tech.
University of Computer Studies, Hinthada

Supervised by
Daw Thida Soe
Faculty of Computer Systems and Technologies
University of Computer Studies, Hinthada

Abstract: Local Area Networks (LANs) are frequently constructed in small and medium-sized enterprises with primarily switch-based technology. In the project, Microsoft Windows Server (2022) is used as the core management platform to design and implement a LAN Network Management System for University of Computer Studies (Hinthada). Multiple server roles are integrated into the system, such as Internet Information Services (IIS) for web hosting, file sharing services for collaborative data access, Domain Name System (DNS) for name resolution, Dynamic Host Configuration Protocol (DHCP) for automated IP address allocation, Active Directory Domain Services (AD DS) for centralized authentication and directory management, Group Policy Objects (GPO) for centralized policy enforcement, and Remote Desktop Services (RDS) for remote administration. A PowerShell script was used to conduct tasks and examine both active and inactive devices inside the DHCP scope in order to improve network monitoring. Only switch was used as the connecting medium during the implementation, which took place in a test LAN environment. The effects exhibited greater administrative control, reduced time spent on manual configuration, reliable and secure network connectivity, effective user and resource management. This project provides an adaptable and affordable solution to organizations who require robust LAN administration.

Keywords: Microsoft Windows Server, LAN management system, Active Directory Domain Services**,** Dynamic Host Configuration Protocol**,** Domain Name System, Group Policy Objects, Internet Information Services, Remote Desktop Services, PowerShell.

INTRODUCTION

The Local Area Network (LAN) is the foundation for resource management, data sharing, and communication in contemporary businesses. In order to guarantee high availability, security, and effective operation, effective LAN administration is necessary. The implementation of a switch-based LAN infrastructure that is fully controlled by Microsoft Windows Server is the primary objective of this project. To ensure centralized control and smooth communication, essential services include AD DS, DHCP, DNS, GPO, IIS web server, file sharing, remote desktop, and PowerShell are implemented. The system reduces manual configuration, improves security, enhances network performance, and provides an affordable solution by integrating these services. The ultimate goal of the project is to establish a LAN environment that is dependable, adaptable, and easy to manage in order to meet the academic and administrative needs of the educational institution.

Accepted Date: 30.9.2025
www.ucsh.edu.mm

PROBLEM

In many networks, poor network management causes the overall performance of the system to become slow and unpredictable. Without adequate management, issues including poor performance, intellectual property disagreements, and resource abuse may arise. Unauthorized access and security risks are also frequent problems. Users may experience unsecured file sharing, hostname resolution issues, and a lack of authentication. User administration becomes challenging in the absence of centralized policies. These issues can be successfully resolved by utilizing services like AD DS, DHCP, DNS, GPO, IIS, file sharing, remote desktop, and PowerShell. Better performance, dependability, security, efficiency, and centralized network management are thus guaranteed by the project.

APPROACH

The project begins with setting up a Windows Server and installing all required services. Each service is configured to meet the specific needs of the LAN environment. User accounts, policies, and permissions are created in AD DS and GPO for secure management. Network testing is conducted to ensure proper IP allocation, domain resolution, file access, and web hosting. Finally, the system is monitored and fine-tuned for performance, security, and reliability.

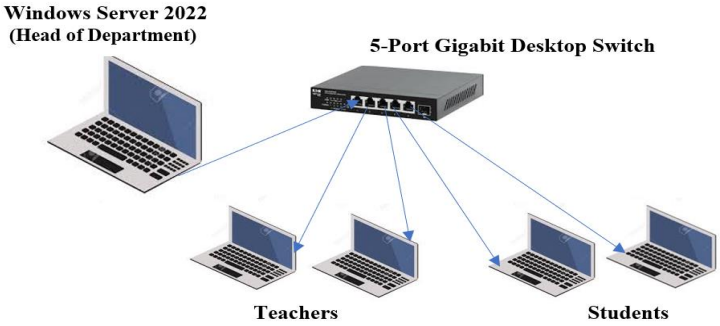


Figure 1: Network Diagram of System

Figure 1 shows a small computer network that uses a star shape design (star topology). The switch works like a hub, making sure data goes to the right computer. All client PCs are connected to the switch and access services through the server.

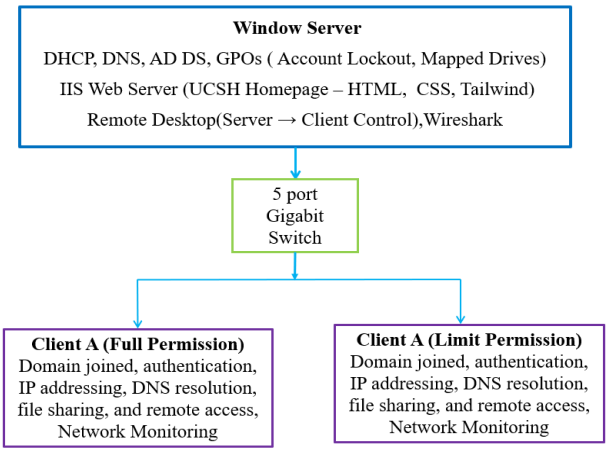


Figure 2: Functional Block Diagram of System

Accepted Date: 30.9.2025

The functional block diagram is shown in Figure 2. The server provides essential services such as authentication, IP addressing, DNS resolution, file sharing, create home page of the UCSH organization, remote access and employs Wireshark for monitoring network activity.

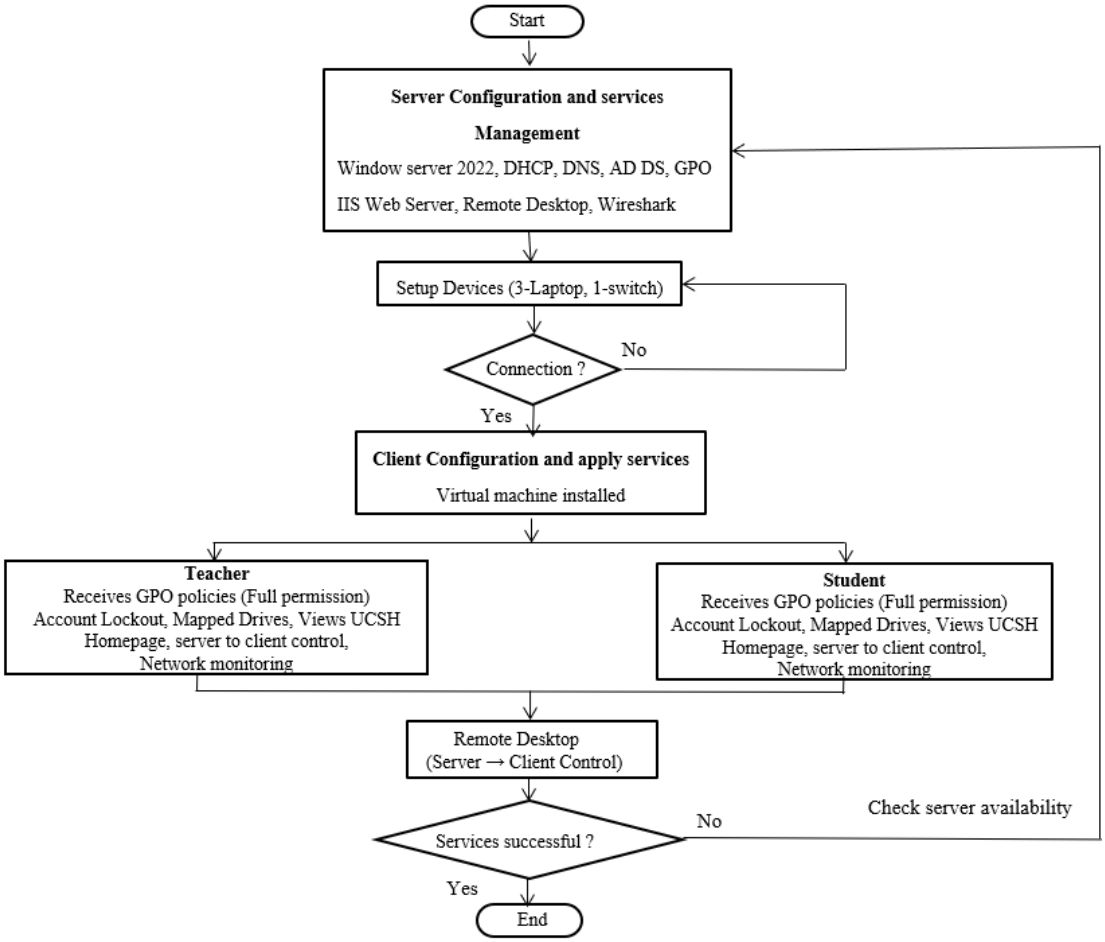


Figure 3: Flowchart of System

Figure 3 presents a flowchart of the server-client network setup process. It begins with installing and configuring Windows Server 2022 for security and centralized management. Physical devices, including three laptops and a 5-port Gigabit Switch, are then connected and tested for connectivity. Client computers are configured with role-based access—teachers having full rights and students limited access. Finally, Remote Desktop is enabled, ensuring centralized control and reliable performance.

RESULTS

The LAN network was designed using a single switch and Windows Server services to provide centralized management. AD DS was implemented for user authentication, while DHCP and DNS ensured automatic IP allocation and name resolution. GPO was applied for policy management, and IIS enabled web hosting within the network. File sharing and Remote Desktop services provided efficient resource access and remote connectivity. The implementation results showed improved network performance, secure access control, and reliable service delivery for all users.

Accepted Date: 30.9.2025
www.ucsh.edu.mm

The IIS Web Server was configured on the Windows Server, the hosted website became accessible across the LAN using the DNS name instead of the IP address. A DNS record was created to map IP address of the server to the domain name ucsh.edu.mm. Client computers on the LAN could successfully access the site by typing this DNS name into their browsers. This confirmed that the IIS setup, DNS resolution, and network connectivity were working properly. The webpage displayed on multiple client machines, proving that the site was available to all authorized users in the campus network. This implementation is illustrated in Figure 4.

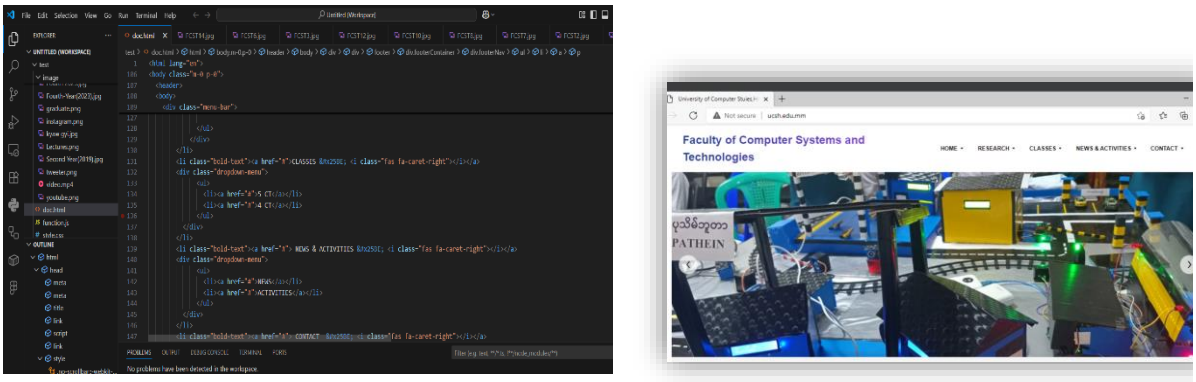


Figure 4: Hosting Home Page

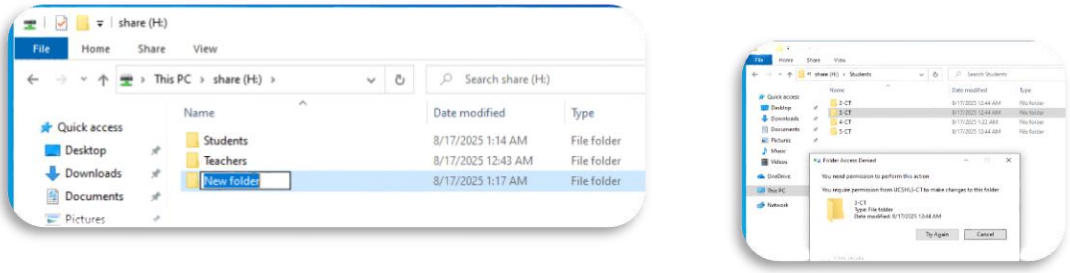


Figure 5: File Sharing with Teachers and Students Account on a Client PC

Displayed in the Figure 5, Teachers accounts had full control over all shared folders and files, allowing them to manage, update, and maintain the system freely. Students accounts were limited by NTFS and GPOs to access only their assignment. Unauthorized access attempts by students were blocked with an “access denied” message. This implementation confirmed the successful application of role-based file sharing. Administrative data stayed secure while students accessed their resources reliably.

Figure 6: Mapping Drives in Network Location

Figure 7: Implementing Lock Account

Accepted Date: 30.9.2025

When domain users log in, GPO automatically maps network drives based on their group membership. The mapped drives appear in File Explorer with the designated drive letter set in GPO. This allows users to access their shared folders instantly without manual mapping. The logout policy clears cached data and credentials to enhance security. Overall, GPO ensures smooth drive mapping and strict logout enforcement for all users. The result of the policy is shown in Figure 6.

Illustrated in the Figure 7, the Account Lockout Policy was implemented to enhance security by limiting repeated failed login attempts. If a user enters the wrong password three times, their account is locked for 30 minutes. Administrators can manually unlock the account through Active Directory if immediate access is needed. This policy enhances security, prevents unauthorized access, and encourages proper password management.

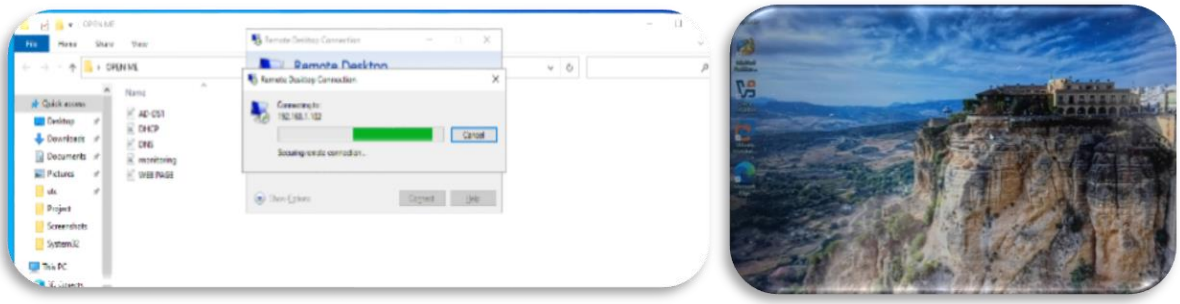


Figure 8: Remote Desktop from Server to Client

The DHCP monitoring process can be automated using a PowerShell script. It retrieves active leases with Get-DhcpServerv4Lease and tests connectivity using Test-Connection**.** Devices that respond are marked **True**, while non-responsive ones are marked **False**. Further checks on inactive devices can be performed remotely via Remote Desktop Services**.** The remote desktop implementation of server-to-client is shown in Figure 8**.**

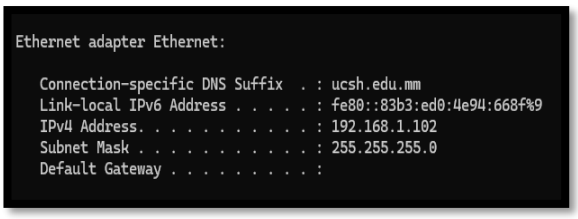
After configuring AD-DS, users created in the Organizational Unit were able to log in to domain-joined computers successfully, confirming centralized authentication. This setup enhances security and simplifies administration by using domain credentials instead of local accounts. It also ensures Group Policy Objects are applied consistently across all users. The login of Admin account and Student account on a domain-computer are shown in Figure 9.

Figure 9: Login of Admin and Student Account on a Domain Computer

Accepted Date: 30.9.2025
www.ucsh.edu.mm

The DHCP server was configured for the **192.168.1.0/24** network. A scope of **192.168.1.100–192.168.1.200** was set with an exclusion of **192.168.1.150–192.168.1.160** for static devices. Client machines successfully released and renewed their IPs. They received addresses **192.168.1.101** and **192.168.1.102** from the pool. Figure 10 shows verification of IP assignment by the DHCP server.

The DNS Server role was installed and verified to be running properly, ensuring it could handle name resolution requests. A Forward Lookup Zone for **ucsh.edu.mm** was created with an A record mapping the domain name to IP address 192.168.1.20. Testing with a ping confirmed successful hostname resolution, proving the DNS setup is fully functional. Figure 11 illustrates the domain connectivity check.



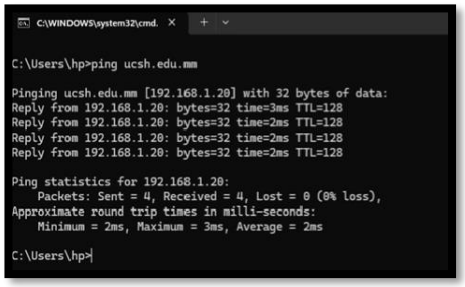


Figure 10: Verification of IP Assignment **Figure 11: Checking the Domain Name Creation**

CONCLUSION

This project showed how to set up a local area network (LAN) with just one switch and Windows Server services. The effective configuration of essential services included AD DS, DHCP, DNS, GPO, IIS, File Sharing, and Remote Desktop. The system offered centralized resource sharing, automated IP management, and secure authentication. Improvements in network performance and dependability made administration simpler for administrators. All things considered, objective of the project establishing a productive and controllable LAN environment was accomplished.

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

[4] Behrouz A. Forouzan,"TCP/IP Protocol Suite", McGraw-Hill International Education, United States, 4th Edition, 2012.

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

Accepted Date: 30.9.2025
www.ucsh.edu.mm

[6] Chengjin Mou, “International Journal of Advanced Network Monitoring and Controls”, Sciendo, Poland, 2023.
[7] Gerardus Blokdyk, “Windows Server A Complete Guide, 2021 Edition”, 5STARCooks, United States, October 15, 2020.
[8] James F. Kurose, Keith W. Ross, “Computer Networking: A Top-Down Approach”, Pearson Education, United States, 8th Edition, 2021.

Accepted Date: 30.9.2025
www.ucsh.edu.mm