มหาวิทยาลัยแม่ฟ้าหลวง
MAE FAH LUANG UNIVERSITY

1504205 Computer Networks and Communication

Project Report

BY

6631502023	**ARKAR PYAE PHYO**
6631502028	**SWAN HTET**
6631502055	**AUNG MYINT MYAT**

3 May 2025

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to all those who supported us throughout the completion of this project on *Computer Network and Communications*.

First, we would like to thank our professor, Teeravisit Laohapensaeng, for their invaluable guidance, constructive feedback, and continuous encouragement. Their expertise in the field enhanced our understanding of key concepts and helped shape the direction of this project.

We are also grateful to our university, Mae Fah Luang University, for providing the necessary facilities and resources to conduct research and practical experiments. Special thanks to the School of Applied Digital and Technological for offering a comprehensive curriculum that deepened our interest in networking systems.

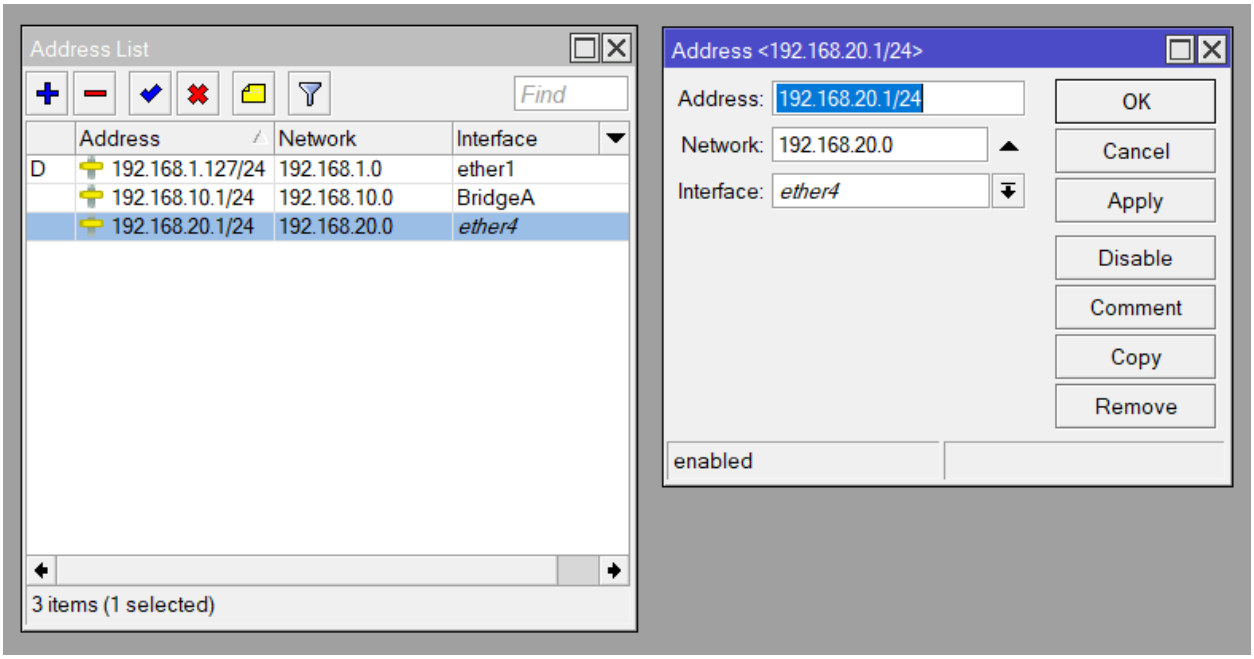
We would also like to thank our classmates and friends for their helpful discussions and collaboration, which contributed to a better learning experience.

Thank you all.

Tables of Contents

Create Network

1.1 Creating the Network B



In this step, a new IP configuration is added to interface ether4.

Address: 192.168.20.1/24

Network: 192.168.20.0

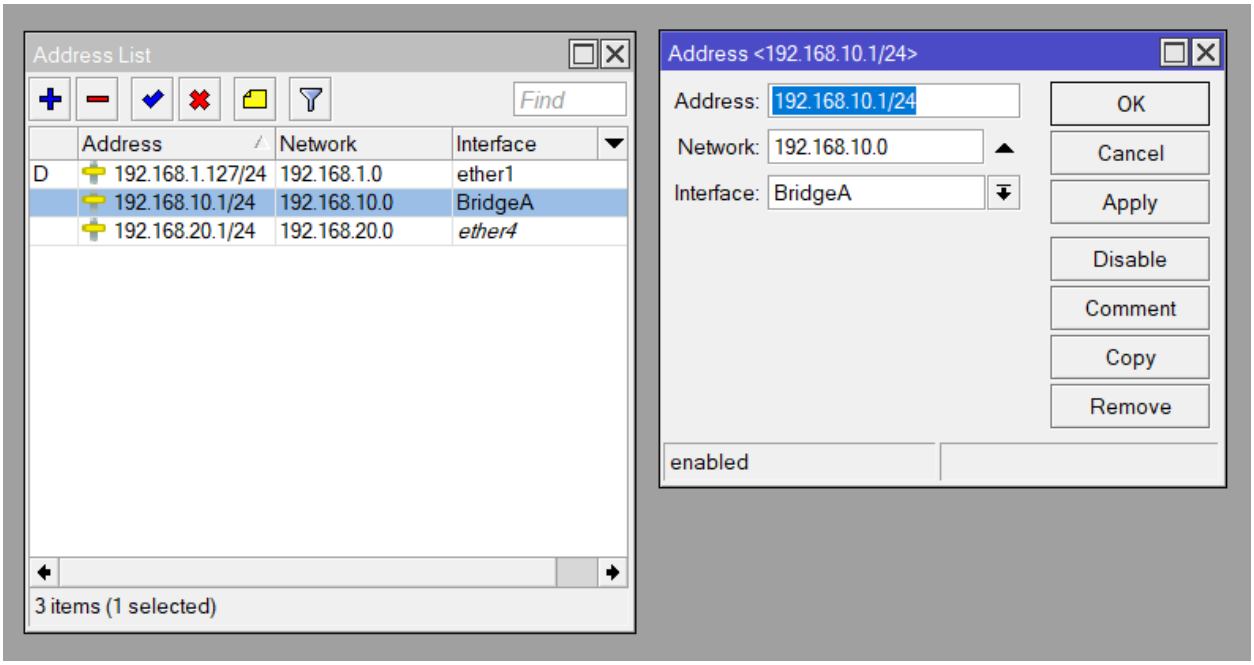
Interface: ether4

This configuration sets up a new subnet (Network B) on the ether4 interface. The IP address 192.168.20.1 is assigned to the router's interface and is commonly used as the default gateway for other devices within the 192.168.20.0/24 network. The 192.168.20.0 is the network address, representing the entire subnet and not an individual host.

This setup enables communication within the 192.168.20.0/24 subnet, where devices can use the 192.168.20.1 address as their gateway to route traffic outside the local network.

Configure IP Address

1.2 Configuring the IP Address for Network A



An IP address has been assigned to the router interface BridgeA for Network A.

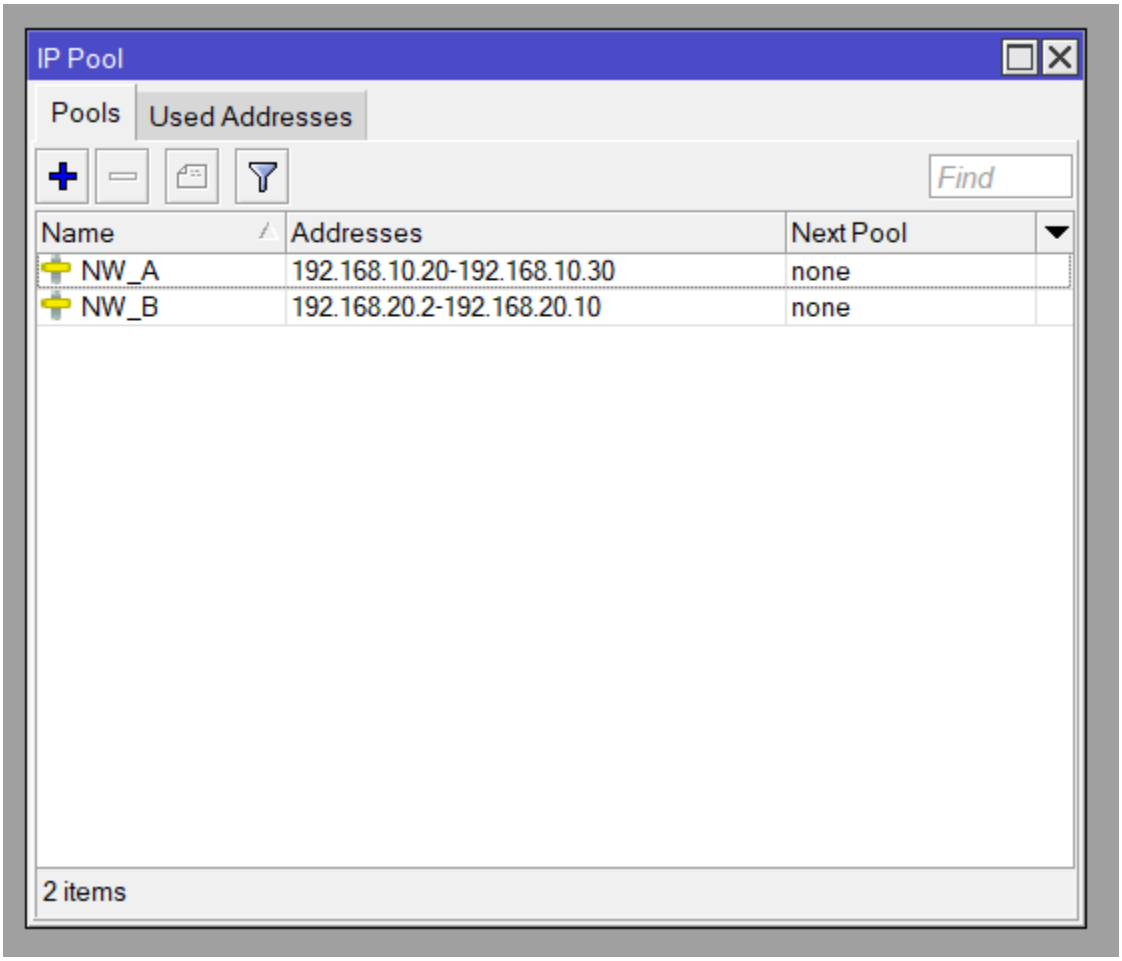
Address: 192.168.10.1/24

Network: 192.168.10.0

Interface: BridgeA

This configuration places the interface BridgeA within the subnet 192.168.10.0/24, making 192.168.10.1 the default gateway for devices in Network A.

1.3 Configuring the IP Pools



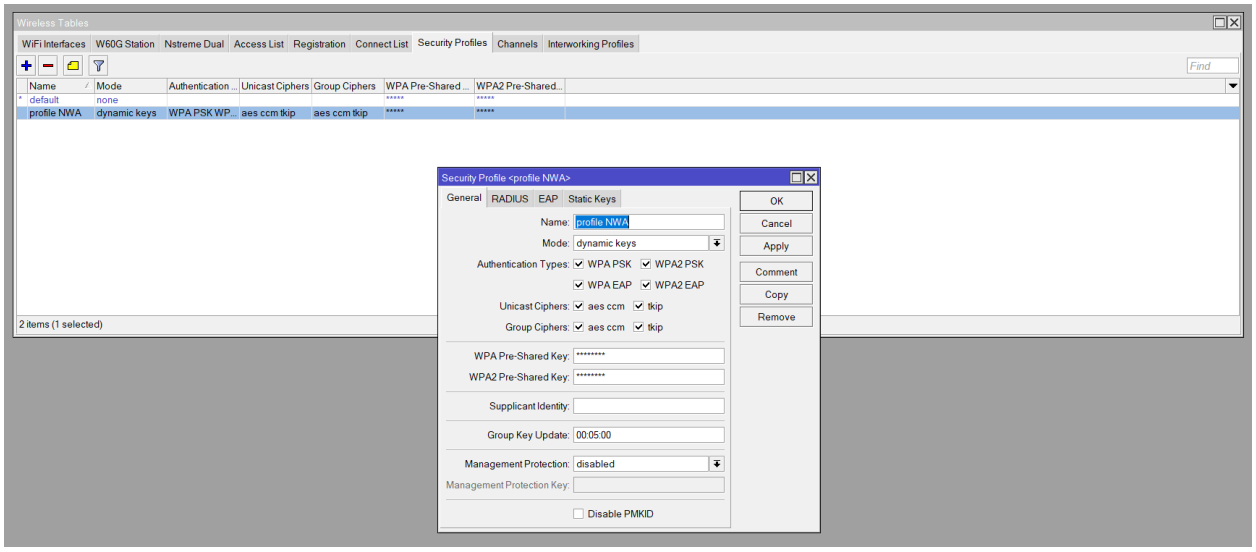
NW_A: Allocates IP addresses within the subnet 192.168.10.0/24. This range is reserved for clients connected to Network A.

NW_B: Allocates IP addresses within the subnet 192.168.20.0/24. This range is reserved for clients connected to Network B.

Each pool is defined with a starting and ending IP address. These addresses are assigned to devices dynamically when they request network access via DHCP. The Next Pool field is set to none, indicating that no overflow or chaining of pools is configured.

Create Wireless Security Profile

2.1 Creating a Wireless Security Profile (NWA)

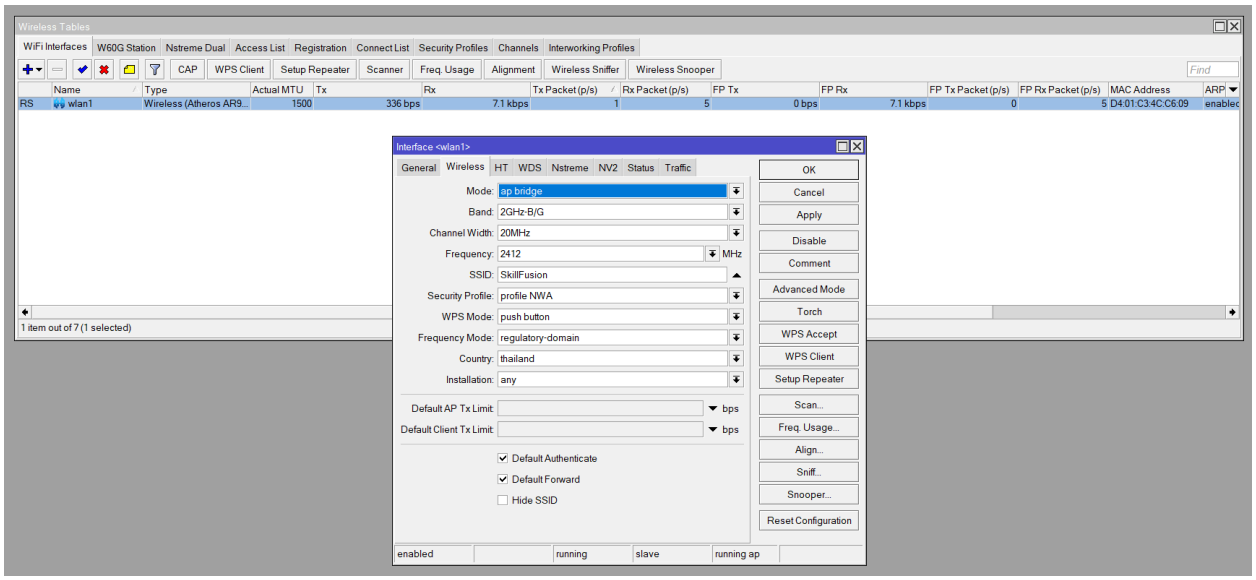


A new wireless security profile named profile NWA was created to secure the wireless network for Network A. This profile uses dynamic encryption keys and supports both WPA and WPA2 authentication protocols.

This profile ensures secure wireless communication using modern encryption standards (AES-CCM) while supporting both WPA and WPA2 for compatibility. It is applied to the wireless interface associated with Network A.

Configure Wireless Access Point

2.2 Configuring Wireless Access Point (wlan1)



The wireless interface wlan1 has been configured to act as an Access Point (AP) for Network A, enabling wireless clients to connect to the network using secure credentials.

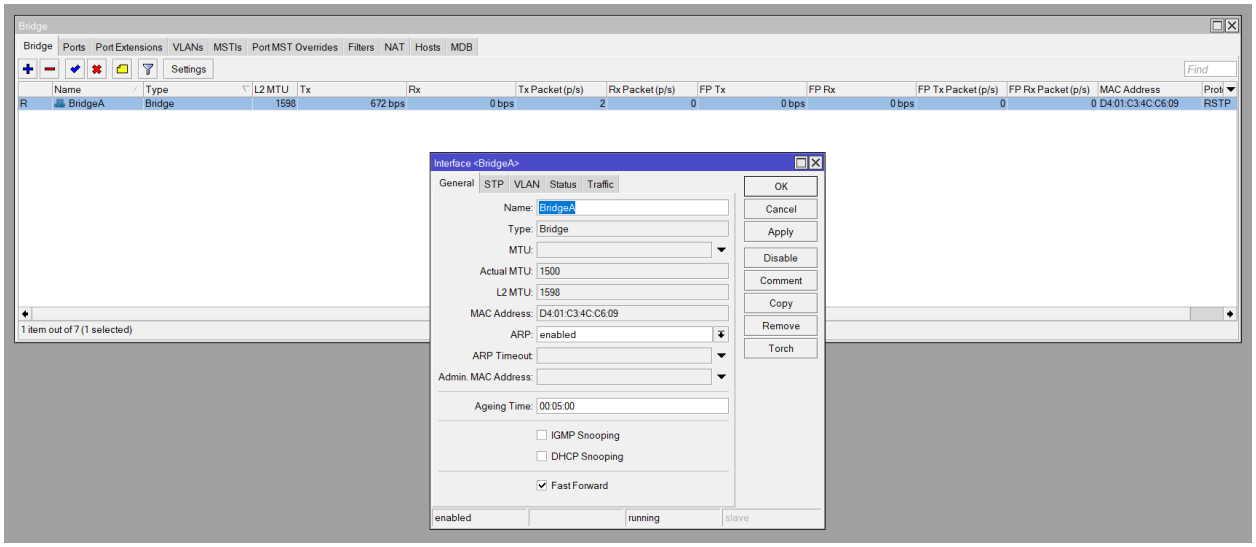
This configuration sets up the wireless network SkillFusion, secured with the previously created profile: profile NWA. Clients connecting to this SSID will receive IP addresses from the corresponding DHCP pool and communicate securely over the network.

Wi-Fi SSID: SkillFusion

Password: 98765432

Create Bridge Interface

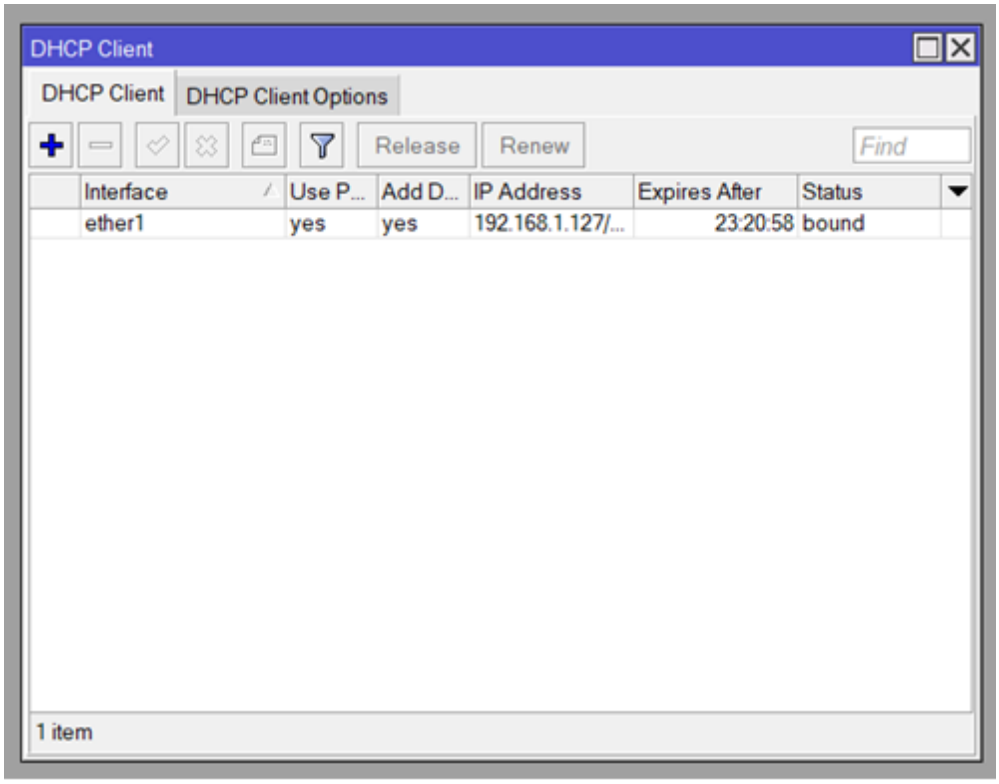
2.3 Creating Bridge Interface (BridgeA)



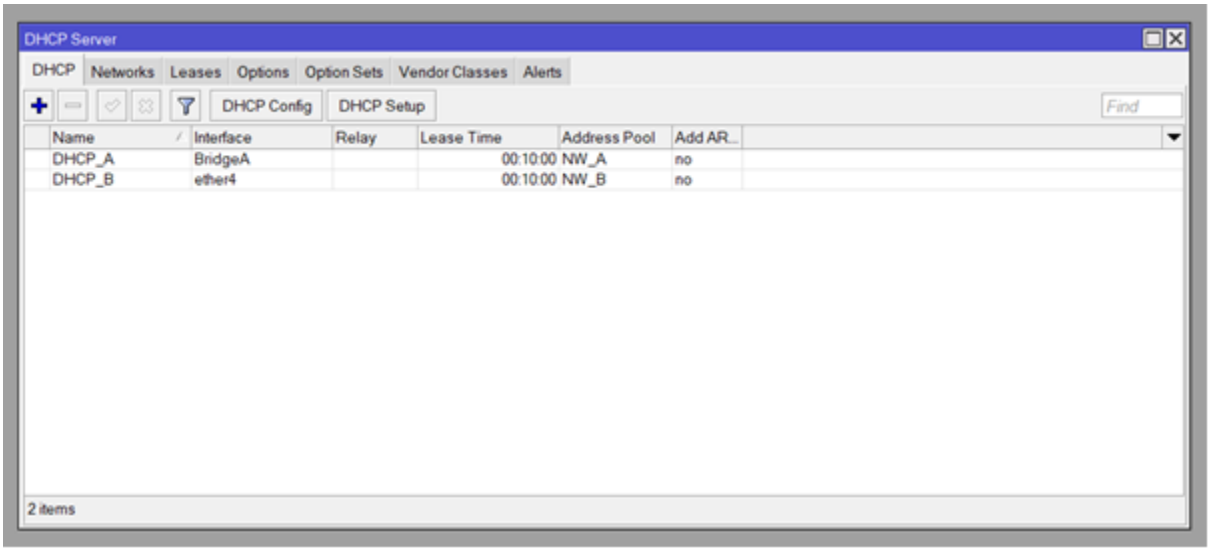
A bridge interface named BridgeA was configured to combine physical interfaces into a single Layer 2 domain. This setup is essential for enabling wired and wireless clients to communicate as part of the same local network (Network A).

The bridge interface allows both wireless (e.g., wlan1) and wired (e.g., ether2, ether3, etc.) interfaces to operate within the same broadcast domain. This is commonly used to facilitate communication and DHCP management for devices in the same subnet.

3.1 Setup DHCP Client

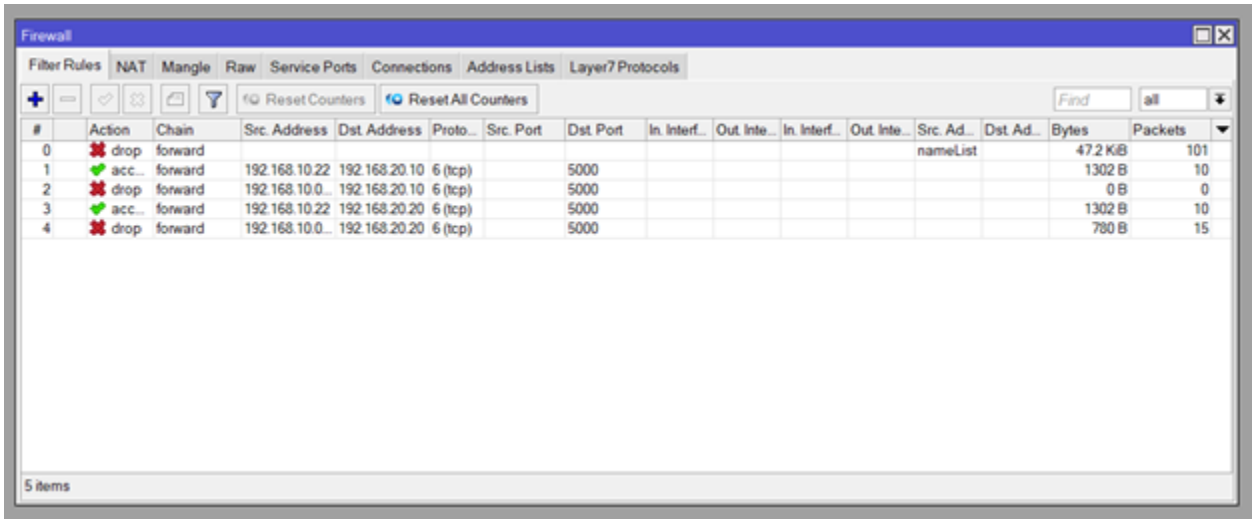


3.2 Setup DHCP Server



Firewall Configuration

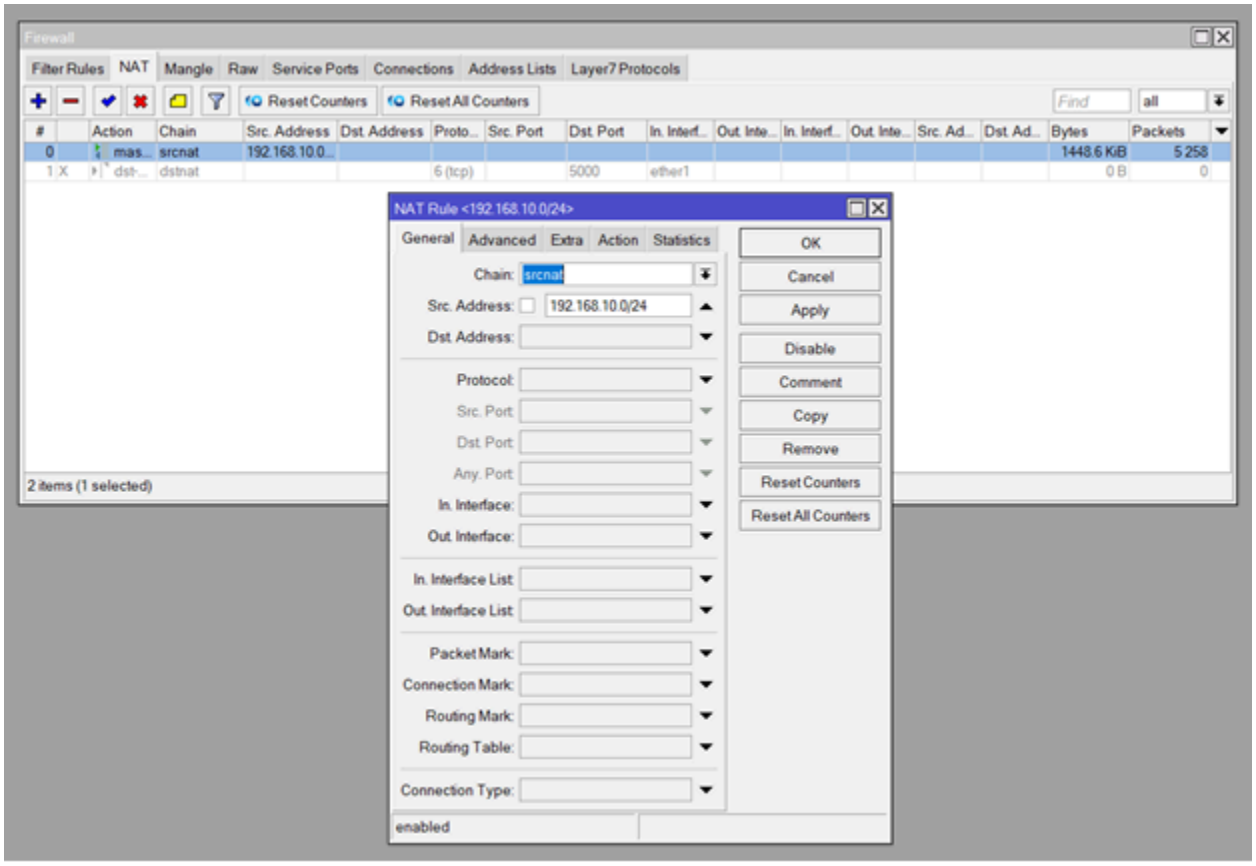
4.1 Firewall Filter Rules Configuration



Firewall filter rules were implemented to control communication between devices in Network A (192.168.10.0/24) and Network B (192.168.20.0/24). These rules are specifically applied to TCP port 5000, which is assumed to be used by a particular service or application. Give Access Supervisor (192.168.10.22) to Machine A (192.168.20.10) and B (192.168.20.20).

This setup ensures fine-grained control over inter-network traffic, enforcing access restrictions while allowing trusted exceptions. We used port 5000 because it conflicts with port 80 in XAMPP Server.

4.2 NAT Configuration



To allow devices on the 192.168.10.0/24 subnet to access external networks (such as the internet), a Source NAT (srcnat) rule using masquerade was implemented.

Chain: srcnat – this chain is used for packets leaving the router.

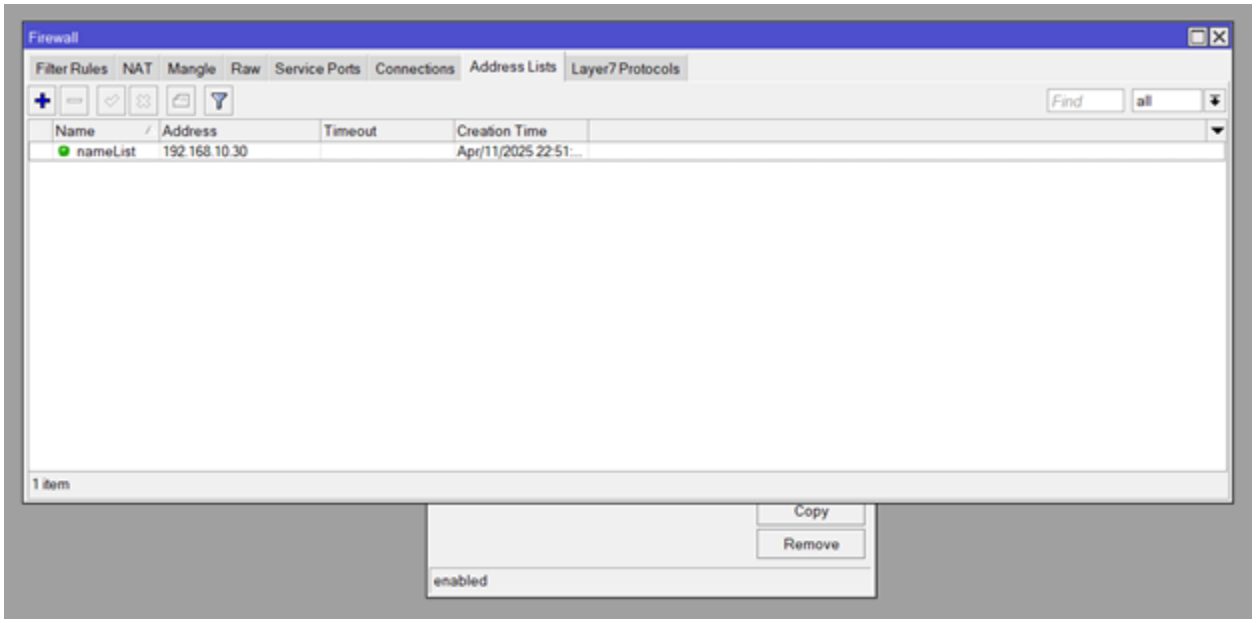
Src. Address: 192.168.10.0/24 – only traffic originating from this subnet is affected.

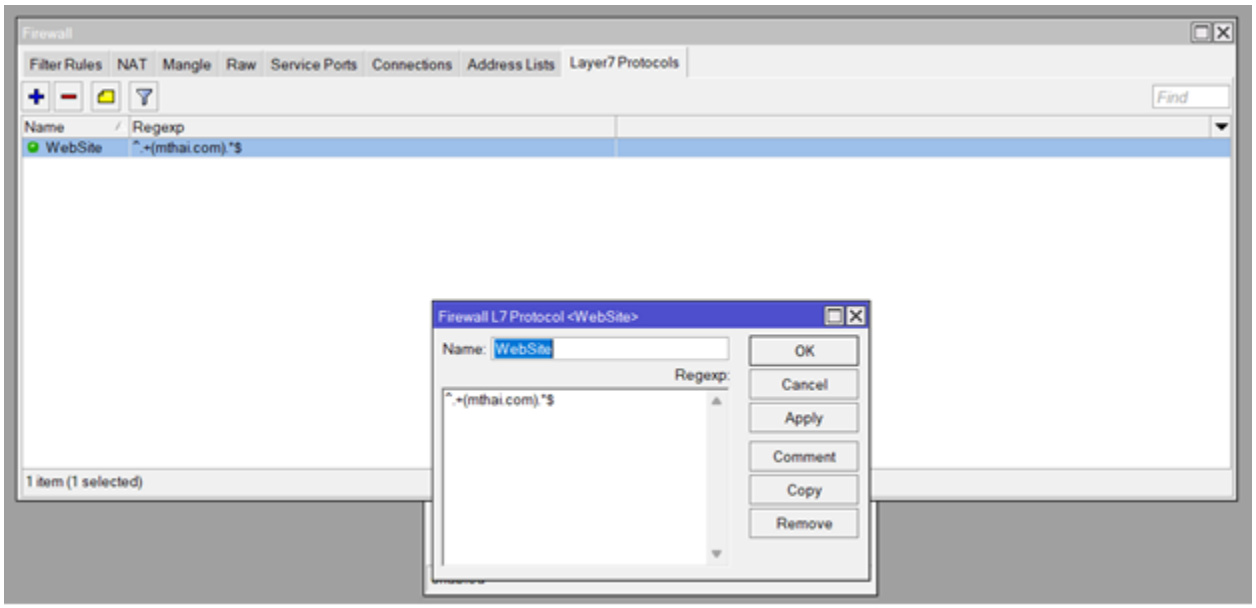
Out. Interface: ether1 – NAT is applied to traffic exiting via this WAN interface.

Action: masquerade – dynamically replaces the source IP with the router's own IP on ether1.

This rule is critical for enabling internet access from private IP ranges, ensuring return traffic is routed properly.

4.3 Firewall Layer7 Protocol

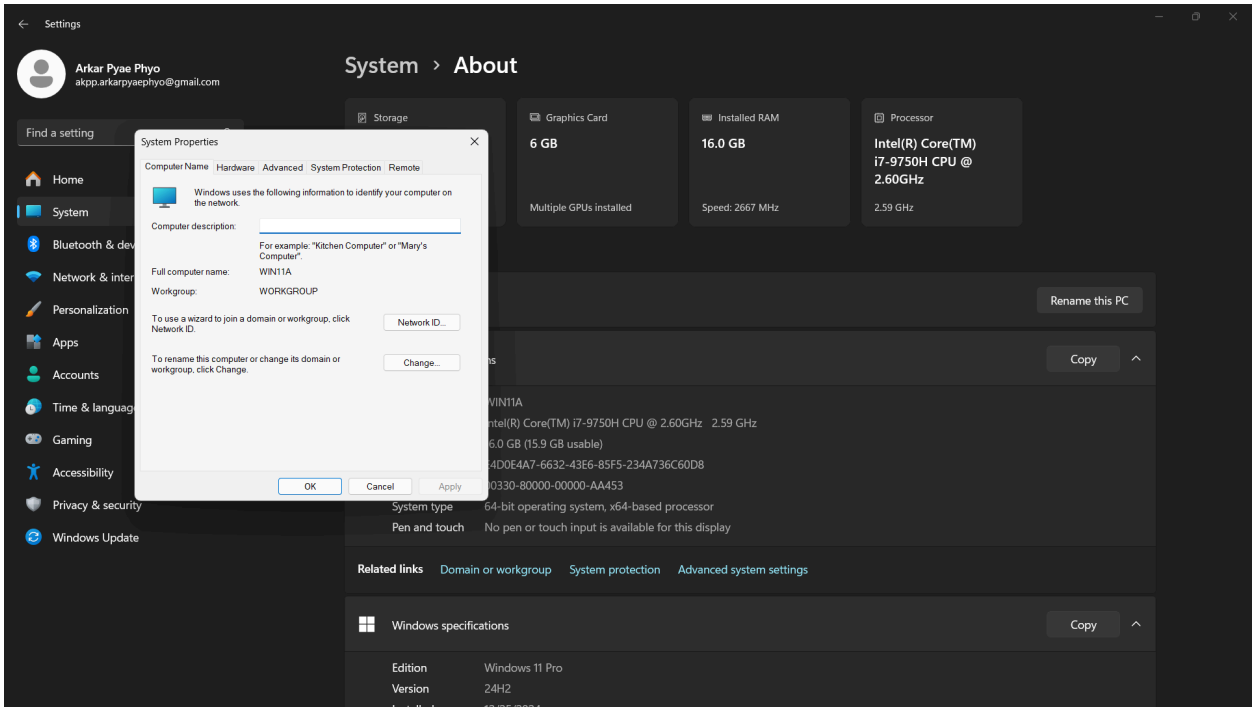




Block IP 192.168.10.30 to mthai.com

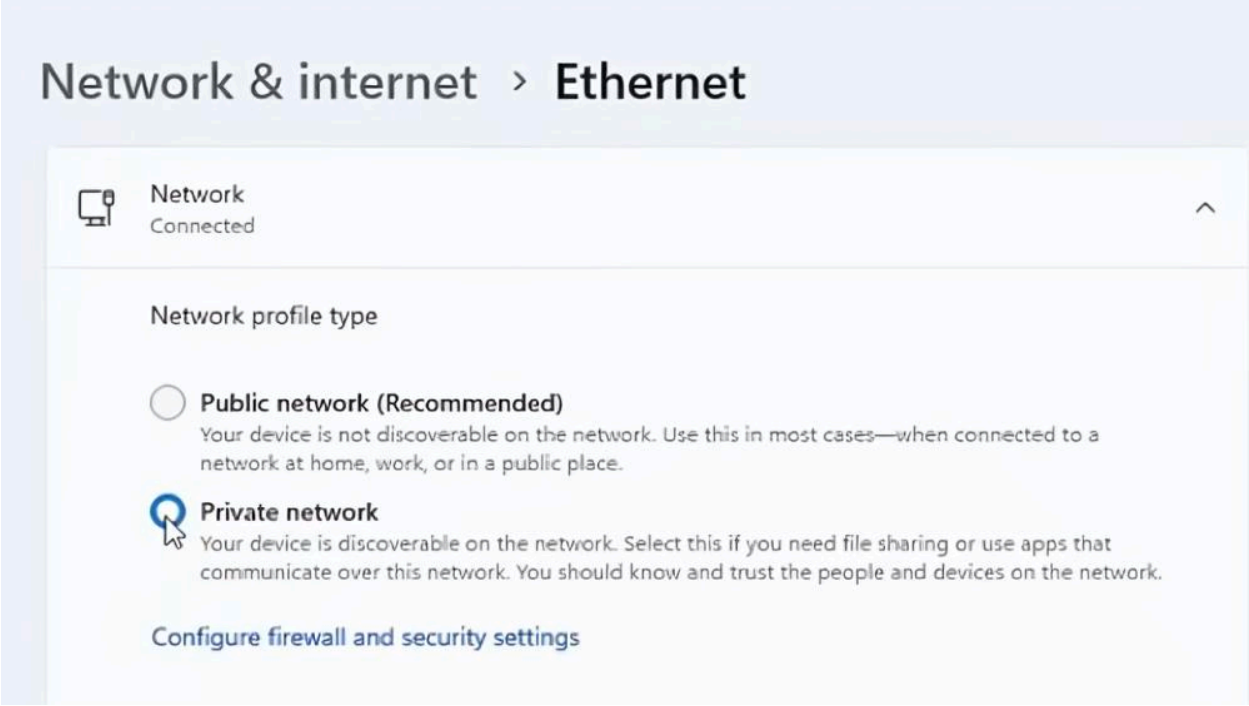
Configure the computer hosting the Company Introduction Web Page to share a folder

1. Renaming the Computer



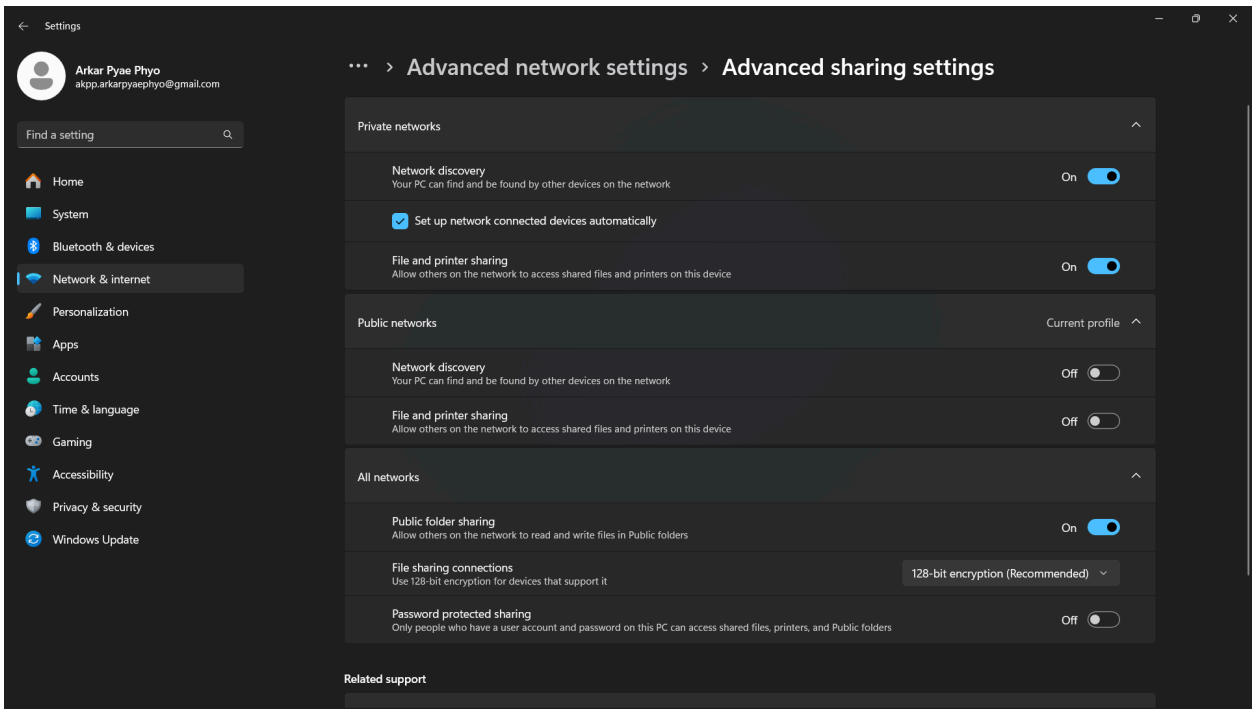
To identify the file server on the network, the computer name was changed via System Properties. The name was updated from the default to a more descriptive one (e.g.,WIN11A) to simplify network access. The system was restarted to apply the changes.

2. Setting Network Profile to Private



The network profile was changed from Public to Private under *Settings* > *Network & Internet* > *Ethernet*. This allows the device to be discoverable on the network, enabling file sharing and communication with other trusted devices within the local network.

3. Configuring Advanced Sharing Settings

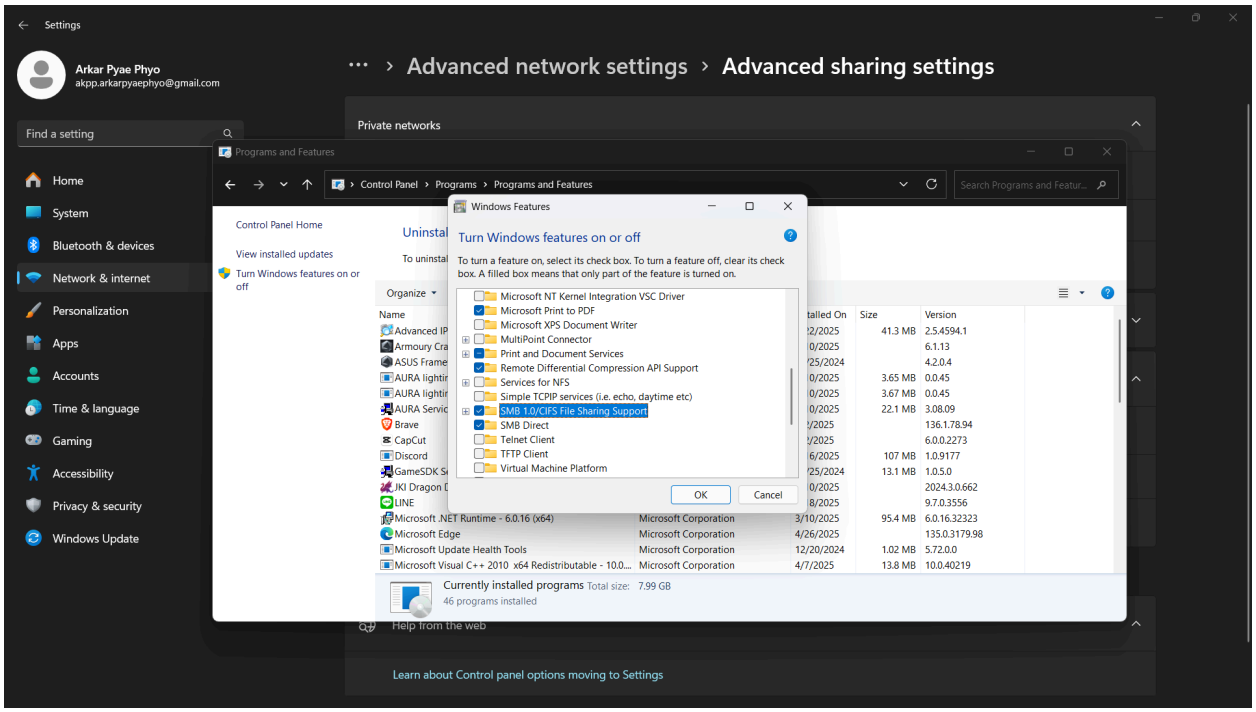


Under Advanced sharing settings, the following options were enabled for the Private network profile:

- **Network discovery**
- **File and printer sharing**

Additionally, under All networks, Public folder sharing was turned on, and Password protected sharing was disabled to allow open access to shared folders without requiring user credentials.

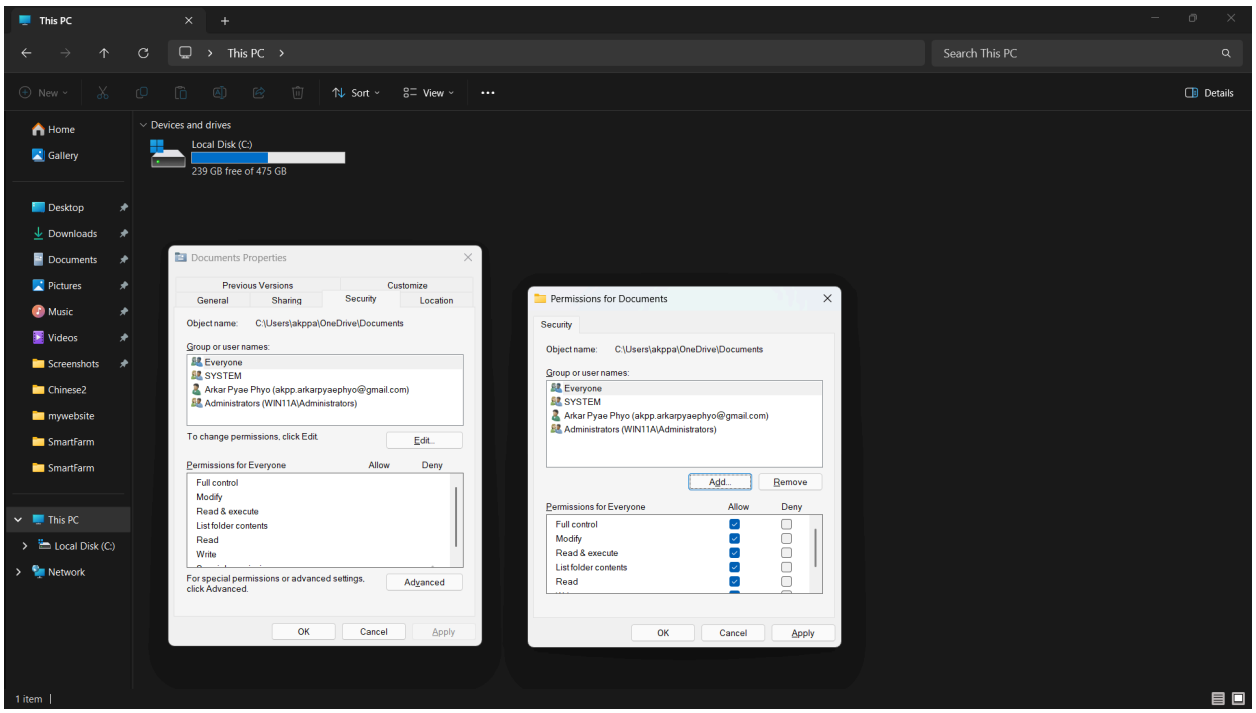
4. Enabling SMB 1.0/CIFS File Sharing Support



In Control Panel > Programs and Features > Turn Windows features on or off, the SMB 1.0/CIFS File Sharing Support feature was enabled.

This legacy protocol is required to allow older or non-Windows devices (like some routers or embedded systems) to access shared files on the network.

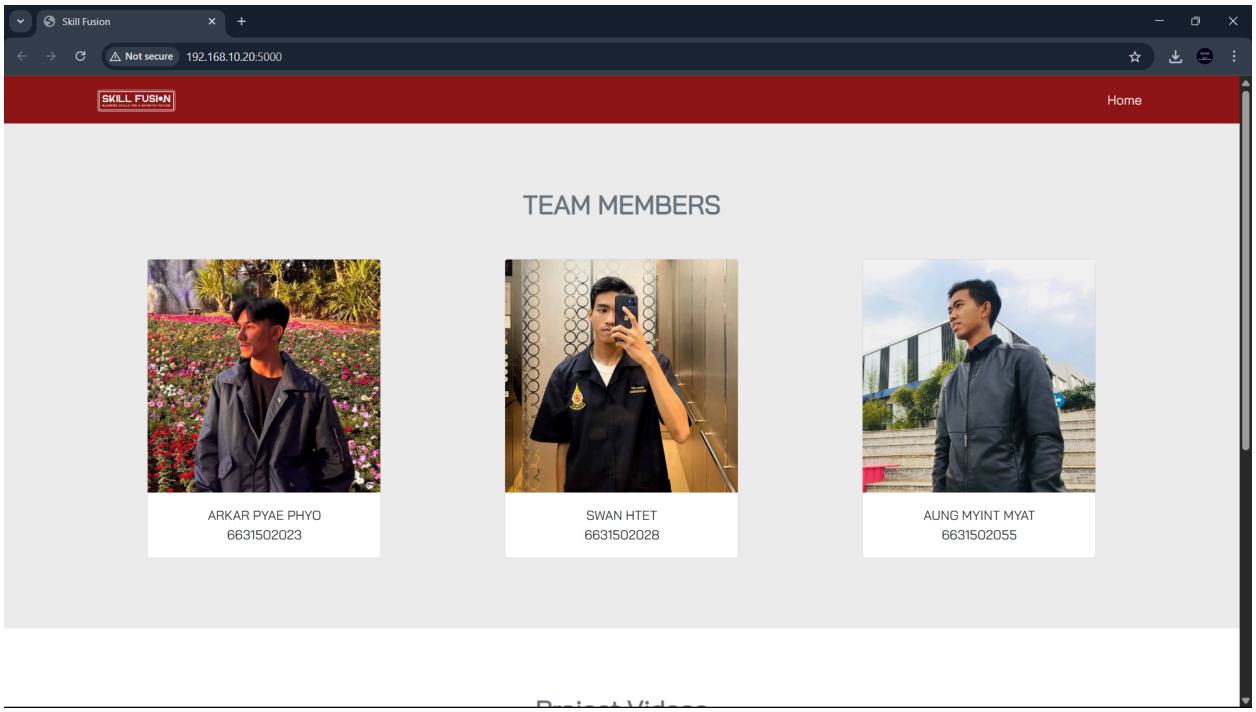
5. Setting Folder Permissions for Sharing



Permissions for the Documents folder were modified. The Everyone group was added and granted full control, allowing all users on the network to access, read, write, and modify files within the shared folder.

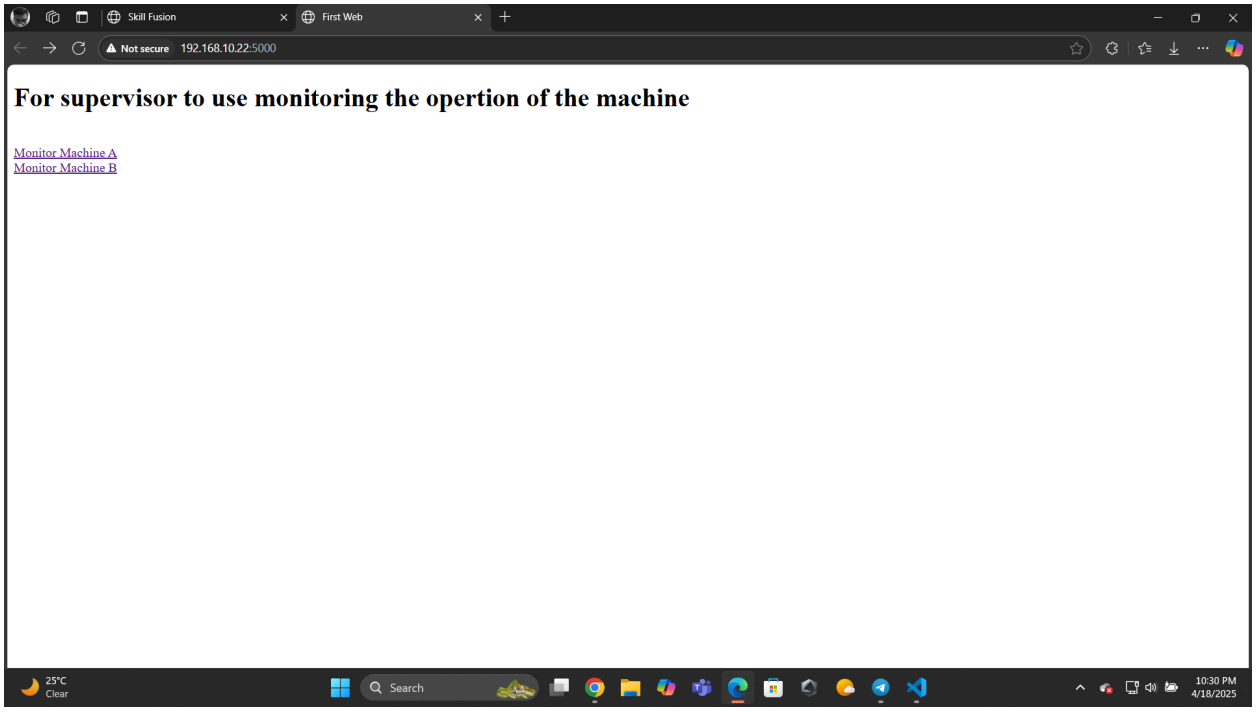
RESULT

Test access to the company's website from an external user



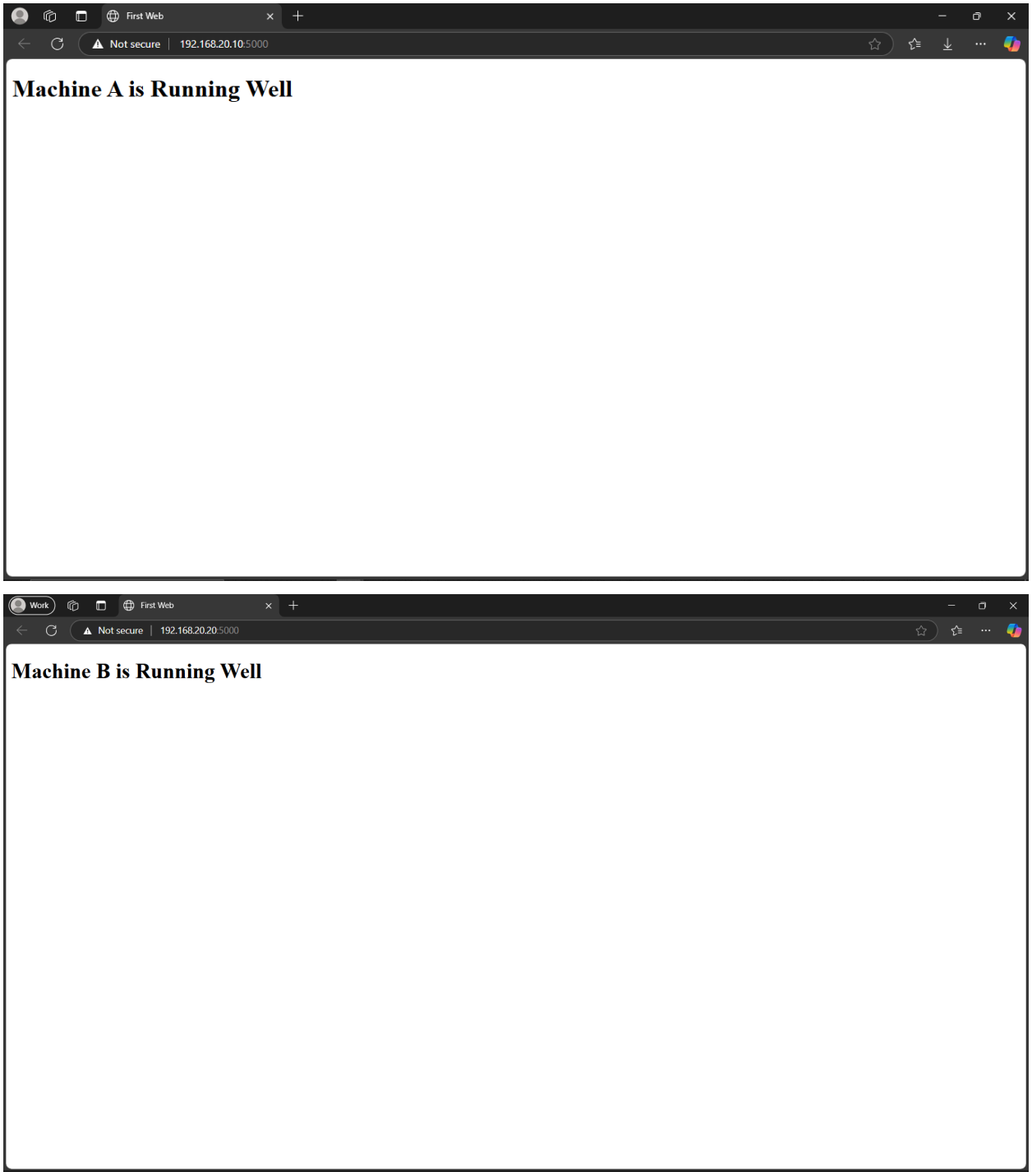
Company Information Website

Test connectivity between the supervisor’s computer and machine A



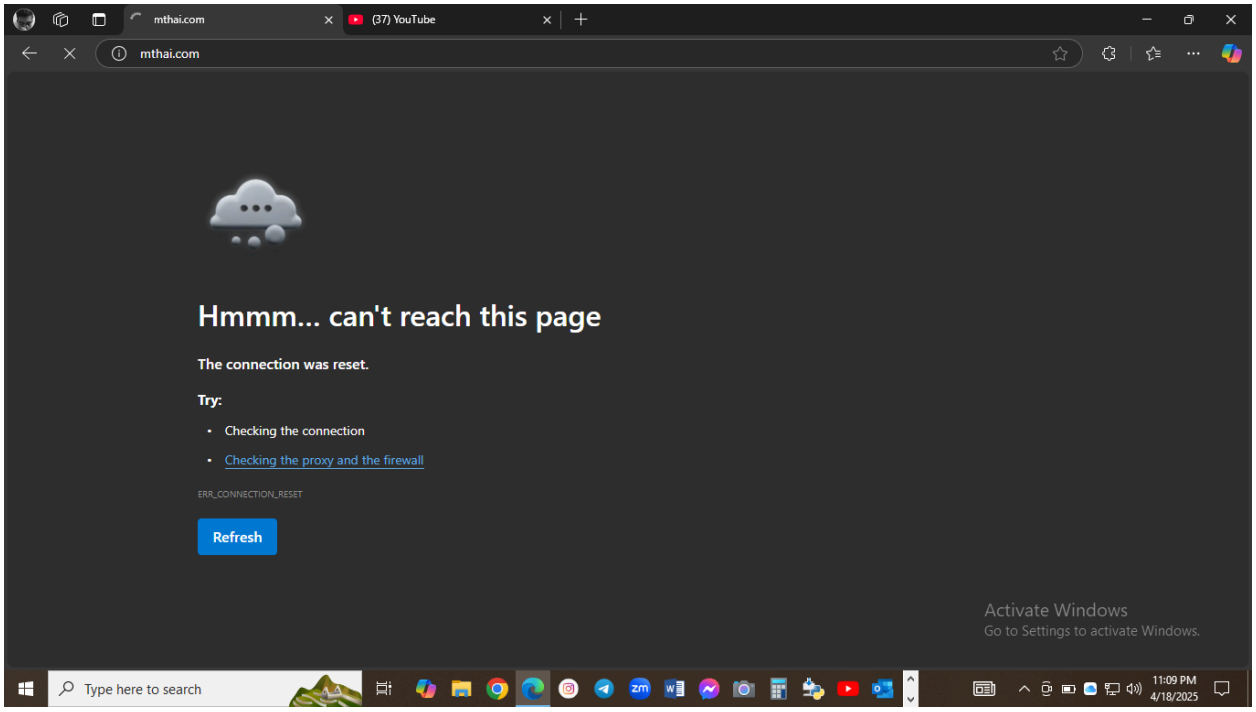
Supervisor Monitoring Website

Test connectivity between the other computer in the network A and a machine A



Machine Operation Simulation Website

Test Blocking the Website



Blocking the Website Access

Test Sharing a File

Steps to Access Shared Folder from Another PC

- Change the network type to Private in Ethernet settings.
- Go to Advanced Sharing Settings in the Control Panel.
- Enable SMB 1.0/CIFS File Sharing Support in Windows Features.

Set permissions and share the folder (e.g., `Documents`) on the host machine.

On another device, open File Explorer and type `\\win11a` in the address bar to view shared folders.