



**Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember**

Laporan Akhir Praktikum Jaringan Komputer

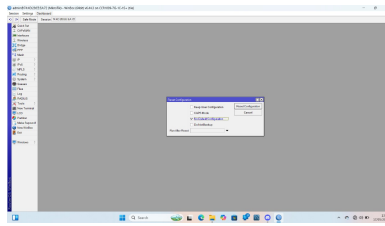
Firewall & NAT

Nadhif Basyara - 502423147

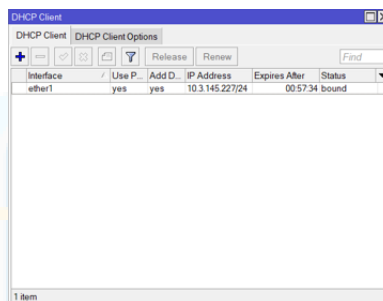
2025

1 Langkah-Langkah Percobaan

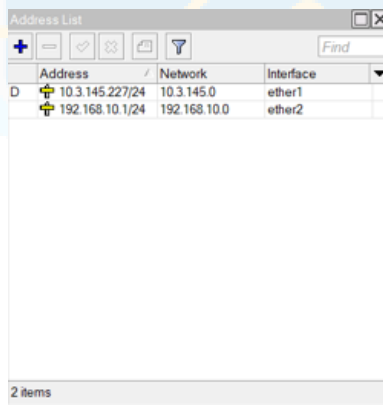
- Langkah pertama yang dilakukan adalah reset router ke kondisi awal agar konfigurasi bersih dan tanpa konflik



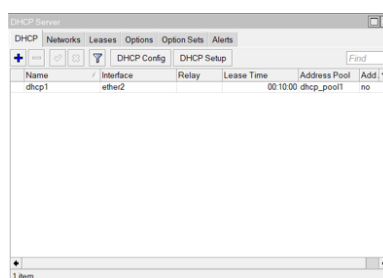
- Setelah tereset login ke router lagi menggunakan winbox
- Sambungkan kabel internet ke ether1, lalu buka IP > DHCP Client, tambahkan entri baru untuk interface ether1, klik Apply, dan pastikan statusnya bound.



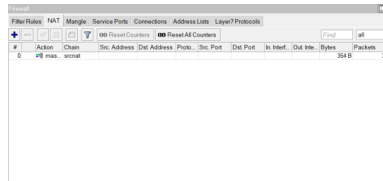
- Tambahkan IP 192.168.10.1/24 ke ether2 via IP > Addresses, lalu klik Apply dan OK.



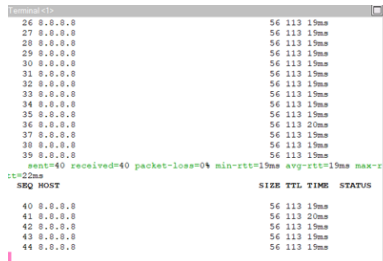
- Konfigurasi DHCP Server di MikroTik



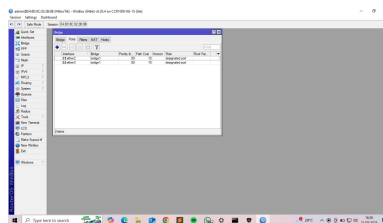
- Setelah itu lakukan konfigurasi NAT



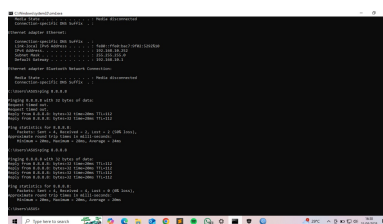
- Lalu tes ping 8.8.8.8



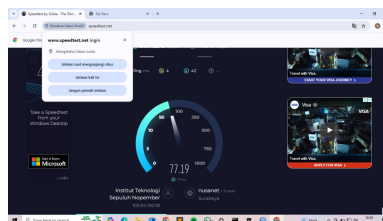
- Selanjutnya lakukan konfigurasi firewall
- Lalu lakukan konfigurasi bridge



- Setelah itu lakukan pengujian konektivitas (ICMP)



- Terakhir lakukan pengujian pemblokiran konten (Browse)

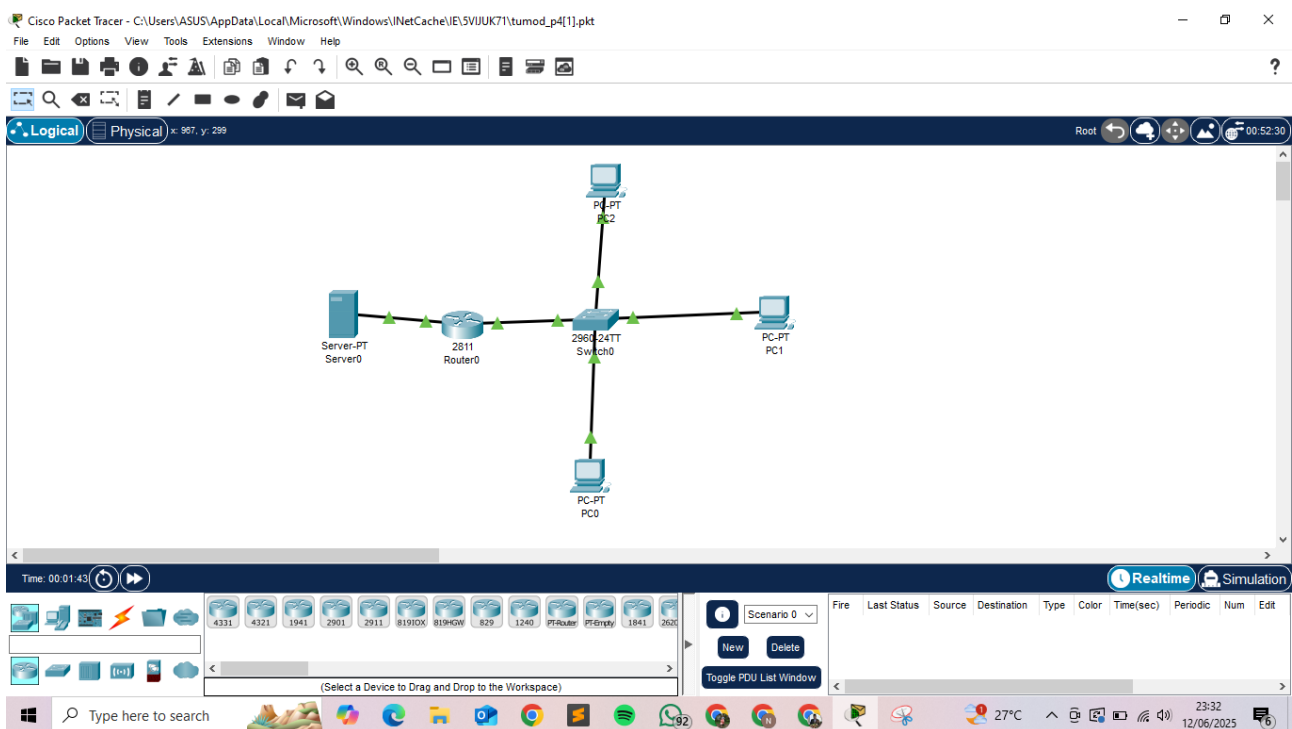


2 Analisis Hasil Percobaan

Pada percobaan ini, dilakukan serangkaian konfigurasi jaringan menggunakan perangkat Mikro-Tik, mulai dari pengaturan DHCP Client hingga konfigurasi NAT, firewall, dan bridge. Setelah router

di-reset ke kondisi awal, DHCP Client pada interface ether1 berhasil mendapatkan alamat IP dari penyedia layanan internet, menandakan koneksi eksternal telah aktif. Selanjutnya, penambahan IP pada ether2 dan konfigurasi DHCP Server memungkinkan perangkat klien menerima IP secara otomatis, memperlancar manajemen jaringan lokal. Pengujian konektivitas menggunakan perintah ping ke DNS Google (8.8.8.8) menunjukkan bahwa akses internet berjalan dengan baik. Konfigurasi NAT dengan metode masquerade berfungsi untuk membagi koneksi internet dari satu IP publik ke seluruh perangkat di jaringan lokal. Di sisi lain, konfigurasi firewall berhasil mengatur dan membatasi lalu lintas data, termasuk pemblokiran akses ke konten tertentu. Terakhir, penggunaan bridge untuk menggabungkan beberapa interface berhasil menciptakan satu domain jaringan yang memungkinkan komunikasi antar perangkat tanpa perlu routing tambahan. Semua pengujian berjalan lancar tanpa kendala, menandakan konfigurasi berhasil dilakukan dengan baik dan sistem jaringan berfungsi sesuai yang diharapkan.

3 Hasil Tugas Modul



4 Kesimpulan

Berdasarkan seluruh rangkaian percobaan yang telah dilakukan, dapat disimpulkan bahwa konfigurasi jaringan menggunakan perangkat MikroTik memberikan fleksibilitas tinggi dalam membangun sistem jaringan yang handal, efisien, dan aman. Melalui tahapan-tahapan konfigurasi seperti DHCP Client, IP Addressing, DHCP Server, NAT, firewall, dan bridging, perangkat MikroTik mampu menjalankan fungsinya sebagai pengelola utama lalu lintas data dalam jaringan. Konfigurasi DHCP Client pada interface yang terhubung ke internet memungkinkan router memperoleh IP secara otomatis dari penyedia layanan, sehingga mempermudah integrasi jaringan internal dengan jaringan global. Pe-

nambahan IP Address dan pengaturan DHCP Server memastikan distribusi alamat IP ke klien berjalan otomatis dan konsisten, mendukung kemudahan manajemen perangkat dalam jaringan lokal. Implementasi NAT dengan teknik masquerade sangat penting untuk memungkinkan perangkat-perangkat dalam jaringan internal mengakses internet menggunakan satu alamat IP publik, sekaligus menjaga keamanan dan efisiensi penggunaan IP. Konfigurasi firewall yang diterapkan juga terbukti efektif dalam mengontrol dan membatasi akses data sesuai kebijakan yang telah ditentukan, seperti pemblokiran akses ke situs atau konten tertentu.