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

Laporan Akhir
Praktikum Jaringan Komputer

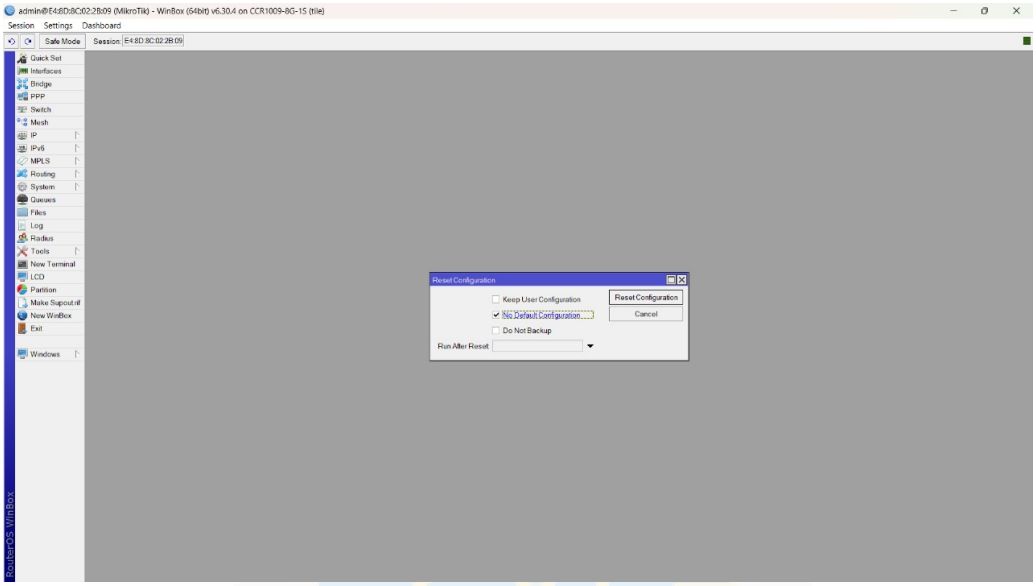
Firewall dan NAT

Bintang Arya Mahendra - 5024231058

2025

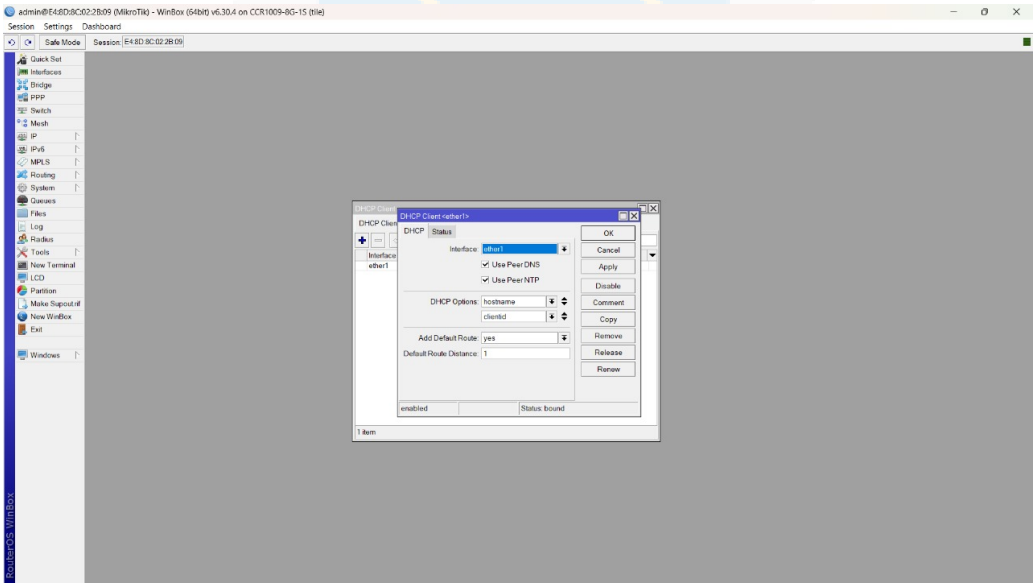
1 Langkah-Langkah Percobaan

Praktikum dimulai dengan menyiapkan topologi jaringan menggunakan dua laptop yang terhubung dengan dua unit router melalui kabel ethernet. Tahap awal yang dilakukan adalah melakukan factory reset pada kedua router untuk memastikan konfigurasi bersih.



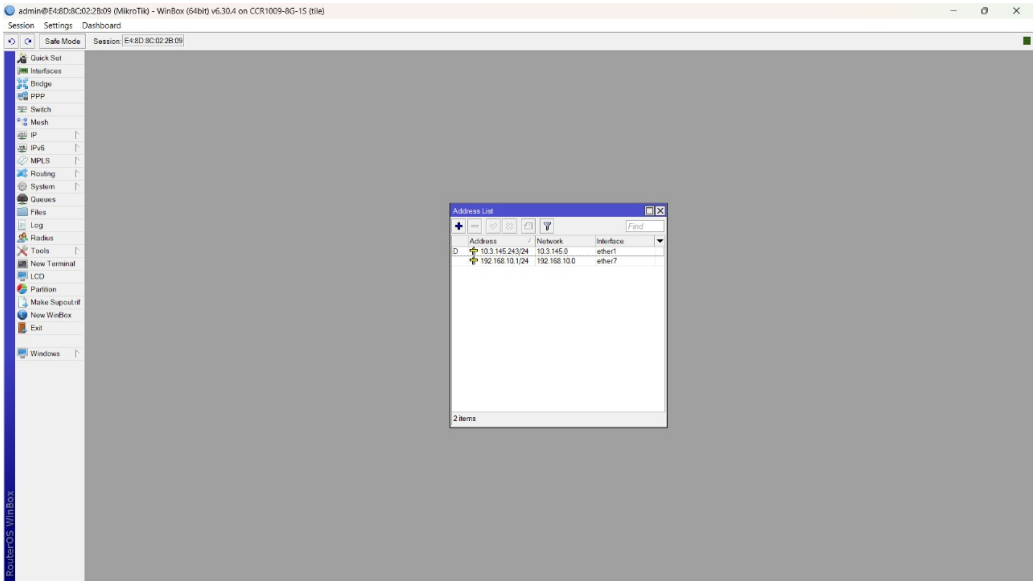
Gambar 1: Proses Reset Konfigurasi Router

Setelah proses reset selesai, kabel internet dihubungkan ke port ether1 pada Router A. Selanjutnya dilakukan konfigurasi DHCP Client melalui menu IP → DHCP Client. Dengan mengklik tombol tambah (+), interface ether1 dipilih sebagai interface utama, kemudian pengaturan diterapkan dengan memastikan status koneksi menunjukkan "bound".



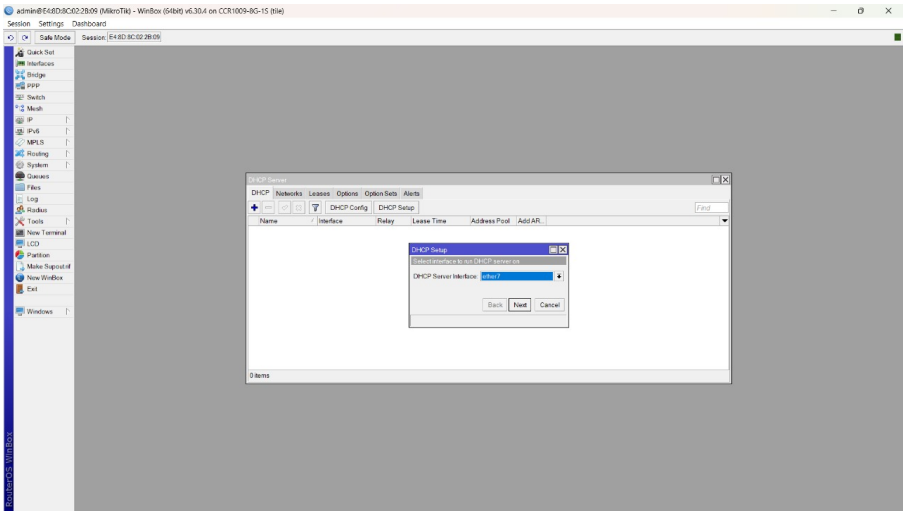
Gambar 2: Pengaturan DHCP Client pada Router A

Langkah berikutnya adalah menambahkan alamat IP pada interface ether7 yang berfungsi sebagai penghubung dengan Switch atau Router B. Melalui menu IP → Addresses, alamat 192.168.10.1/24 ditambahkan dengan memilih interface ether7.

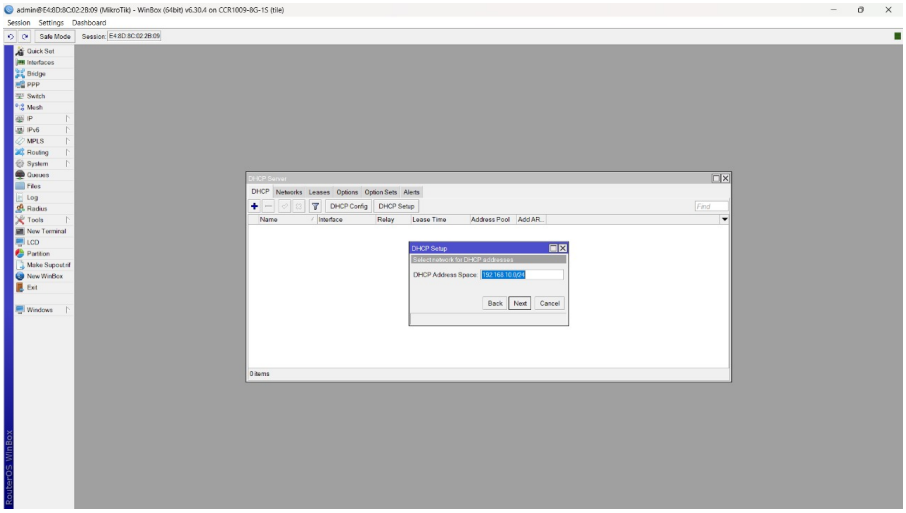


Gambar 3: Konfigurasi Alamat IP pada Interface Ether7

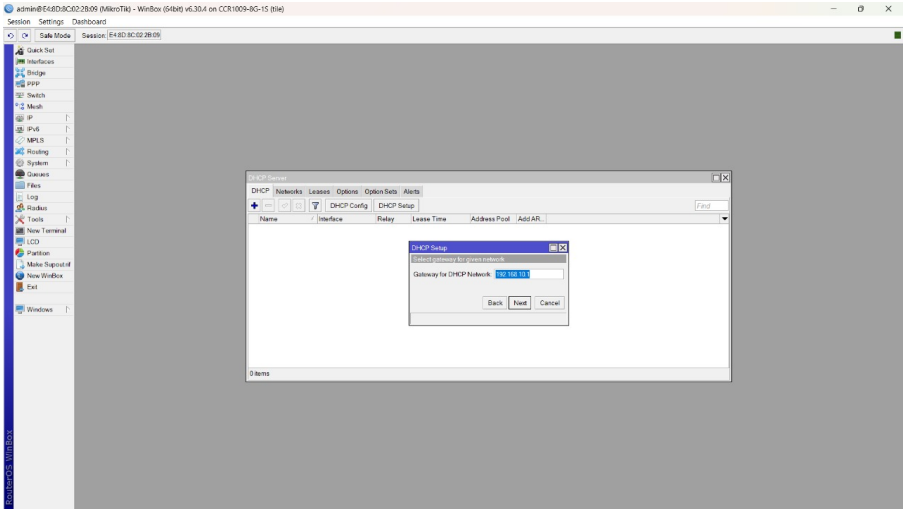
Konfigurasi DHCP Server dilakukan melalui menu IP → DHCP Server dengan menggunakan wizard "DHCP Setup". Berikut adalah tahapan konfigurasi yang dilakukan:



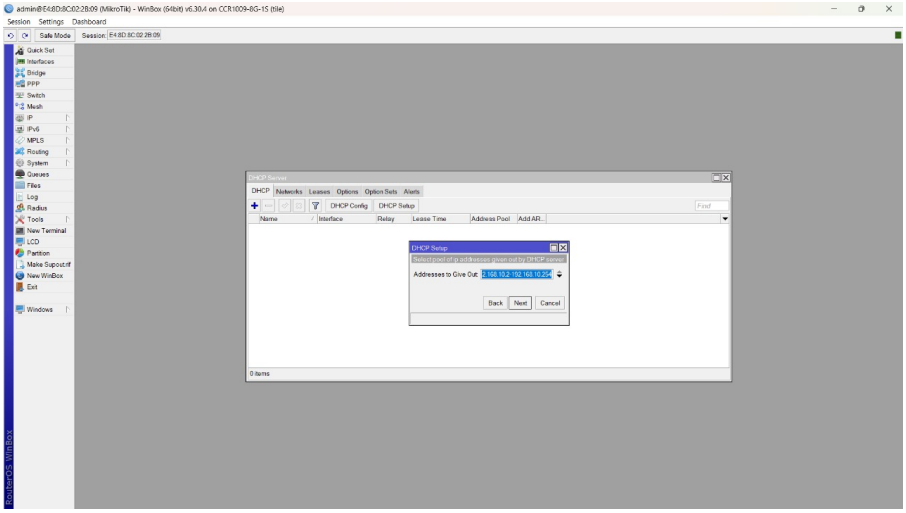
Gambar 4: Pemilihan Interface untuk DHCP Server



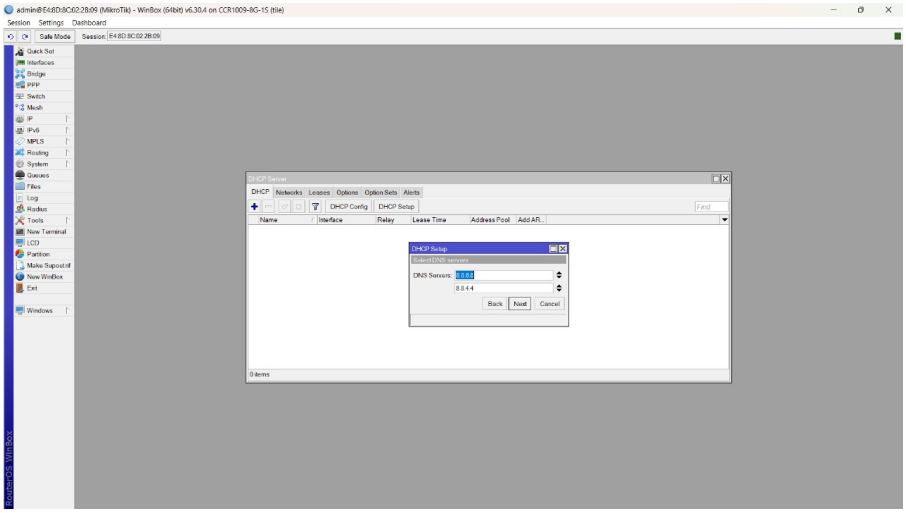
Gambar 5: Pengaturan Address Space



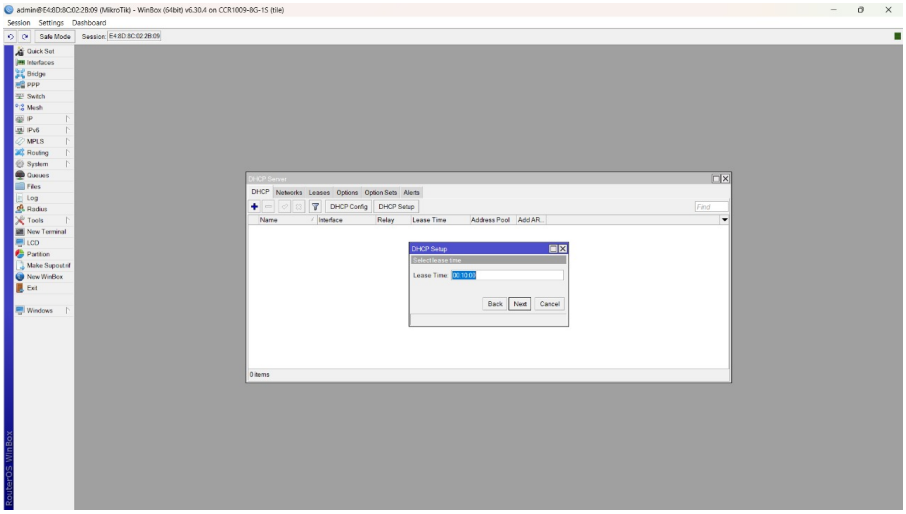
Gambar 6: Konfigurasi Gateway



Gambar 7: Pengaturan Range Alamat IP

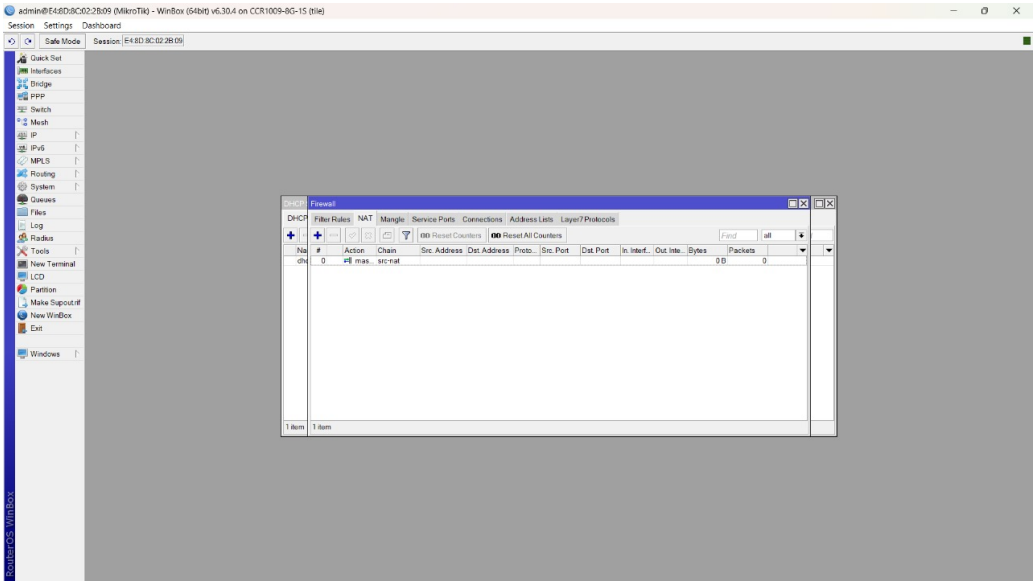


Gambar 8: Konfigurasi DNS Server



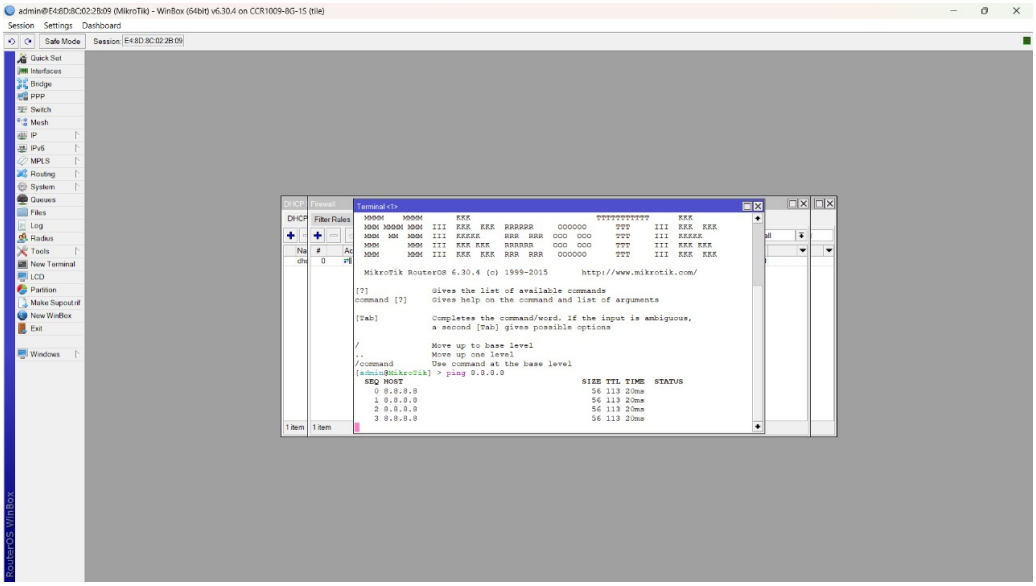
Gambar 9: Pengaturan Lease Time

Implementasi Network Address Translation (NAT) dilakukan melalui menu IP → Firewall → NAT. Rule baru ditambahkan dengan pengaturan chain "srcnat" pada tab General dan action "masquerade" pada tab Action.



Gambar 10: Implementasi NAT Masquerade

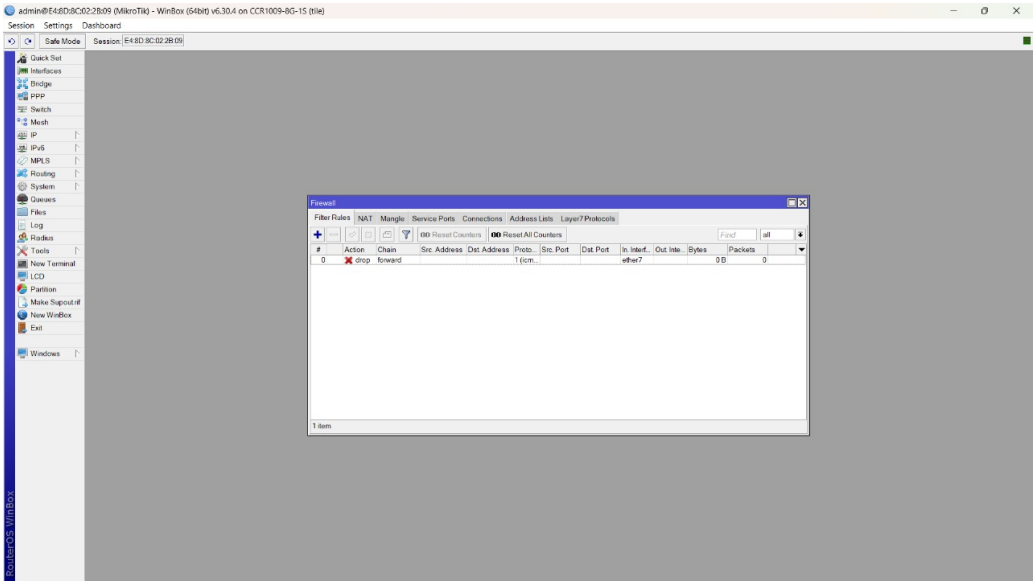
Untuk memverifikasi konektivitas internet, dilakukan pengujian ping ke alamat DNS Google (8.8.8.8) melalui terminal.



Gambar 11: Verifikasi Konektivitas Internet

Konfigurasi firewall untuk pemblokiran protokol ICMP dilakukan melalui menu IP → Firewall → Filter Rules dengan pengaturan sebagai berikut:

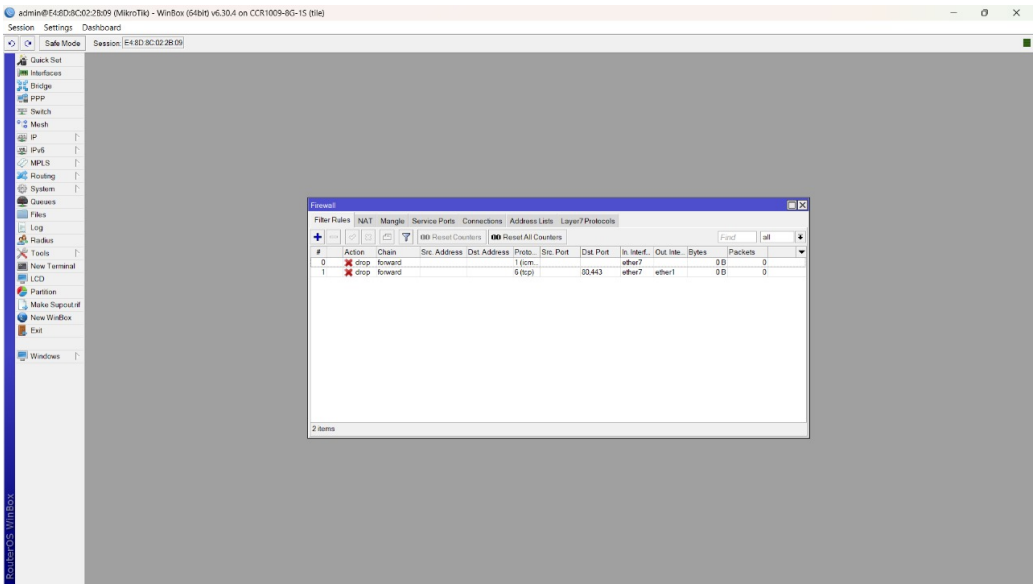
- Chain diatur ke "forward"
- Protocol diatur ke "icmp"
- Input Interface diatur ke "ether7"
- Action diatur ke "drop"



Gambar 12: Konfigurasi Pemblokiran ICMP

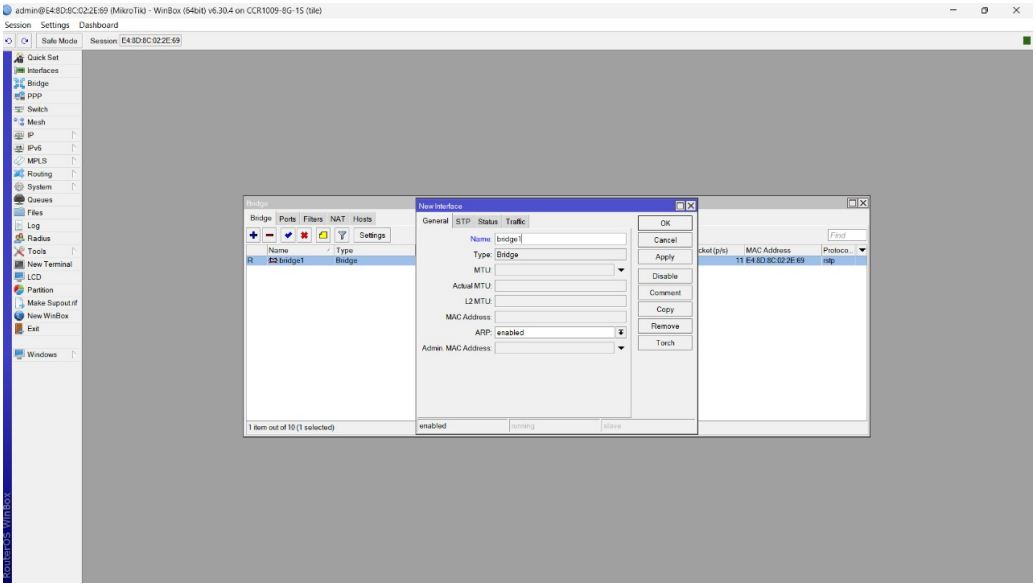
Untuk implementasi content filtering atau pemblokiran konten web, konfigurasi dilakukan dengan pengaturan:

- Chain: "forward"
- Protocol: "tcp"
- Destination Port: "80,443"
- Input Interface: "ether7"
- Output Interface: "ether1"
- Content: "speedtest"
- Action: "drop"



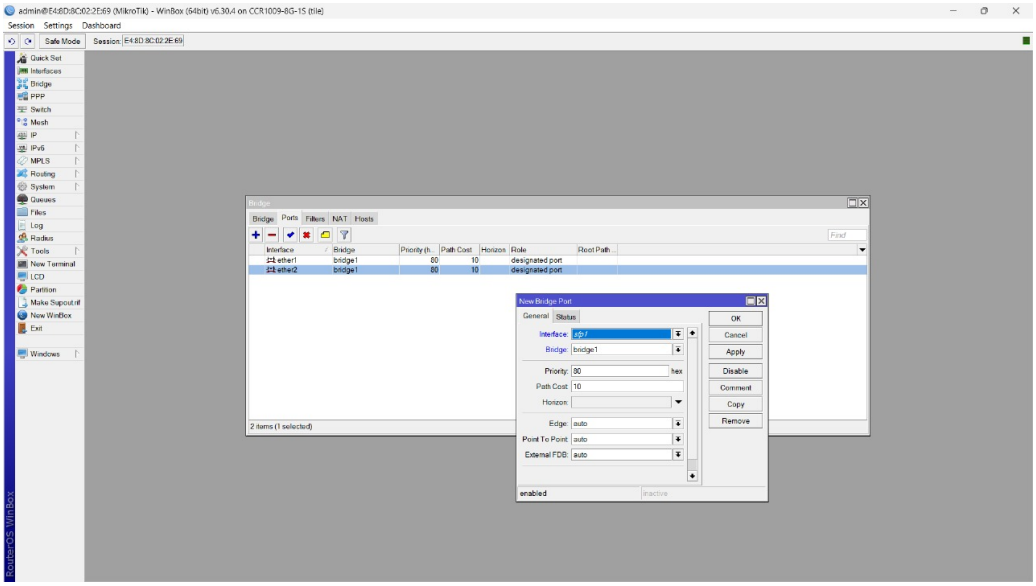
Gambar 13: Implementasi Content Filtering

Pada Router B yang berfungsi sebagai hub, dilakukan konfigurasi bridge melalui menu Bridge dengan menambahkan bridge baru.



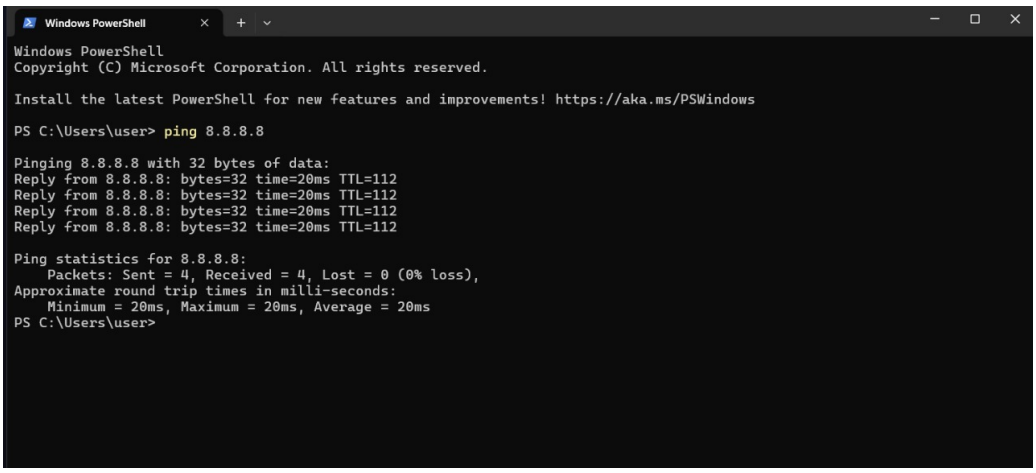
Gambar 14: Konfigurasi Bridge pada Router B

Port-port yang terhubung ke laptop dan Router A ditambahkan ke dalam bridge melalui menu Bridge → Ports.



Gambar 15: Penambahan Port ke Bridge

Setelah konfigurasi IP pada laptop selesai, dilakukan pengujian konektivitas ICMP dengan melakukan ping ke 8.8.8.8 melalui command prompt.



Gambar 16: Pengujian Pemblokiran ICMP

Hasil menunjukkan "Request Timed Out" yang mengindikasikan bahwa firewall telah berhasil memblokir traffic ICMP. Pengujian content filtering dilakukan dengan mencoba mengakses situs yang mengandung kata "speedtest".

Gambar 17: Pengujian Content Filtering

2 Analisis Hasil Percobaan

Implementasi seluruh tahapan konfigurasi telah berhasil dilaksanakan sesuai dengan prosedur yang ditetapkan. Setelah pengaturan DHCP, NAT, dan firewall selesai, perangkat klien dapat memperoleh alamat IP secara otomatis dan terhubung ke internet dengan lancar.

Ketika rule firewall untuk memblokir ICMP diaktifkan, hasil ping ke alamat 8.8.8.8 menampilkan pesan "Request Timed Out", yang menunjukkan bahwa rule firewall berfungsi dengan optimal. Demikian pula saat mencoba mengakses website yang mengandung konten "speedtest", halaman gagal dimuat sesuai dengan rule content blocking yang telah dikonfigurasi.

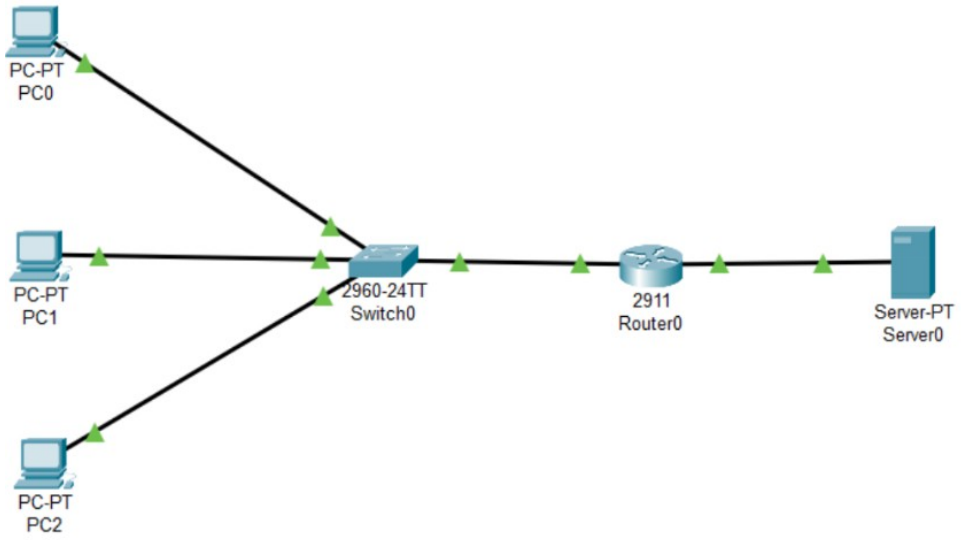
Berdasarkan hasil pengujian tersebut, dapat disimpulkan bahwa implementasi firewall efektif untuk membatasi jenis traffic tertentu sesuai dengan kebutuhan keamanan jaringan. Meskipun sempat mengalami kendala dalam pemilihan interface dan urutan langkah implementasi, namun setelah dilakukan troubleshooting yang teliti, seluruh fitur dapat berfungsi sesuai dengan spesifikasi yang diharapkan.

3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan :

   -1 Router -1 Switch -3 PC (LAN) -1 Server (Internet/Public)

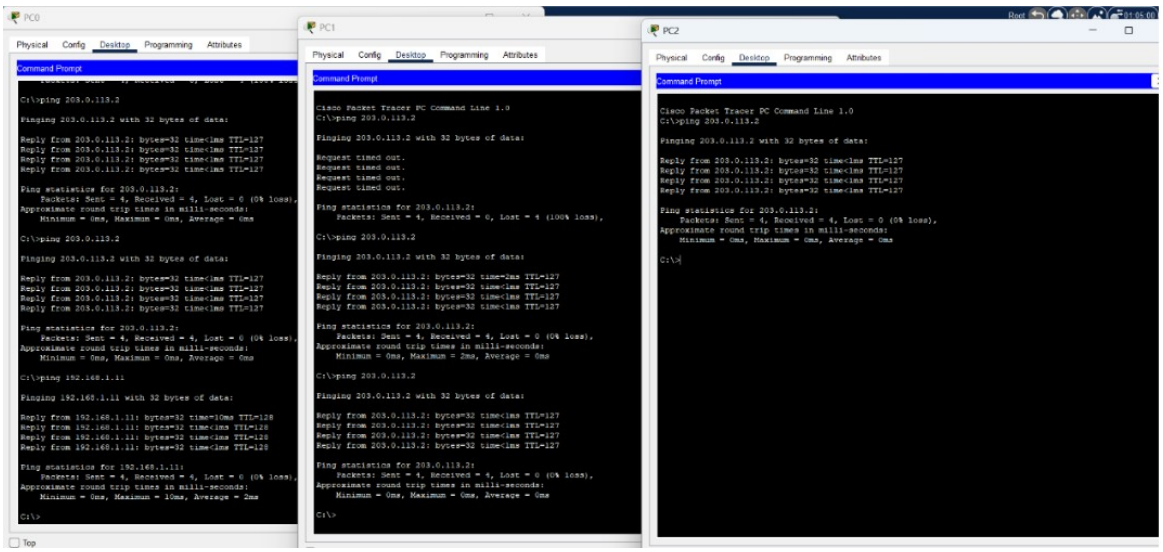
   Jawaban :



Gambar 18: Topologi Sederhana Cisco Packet Tracer

2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.

   Jawaban :

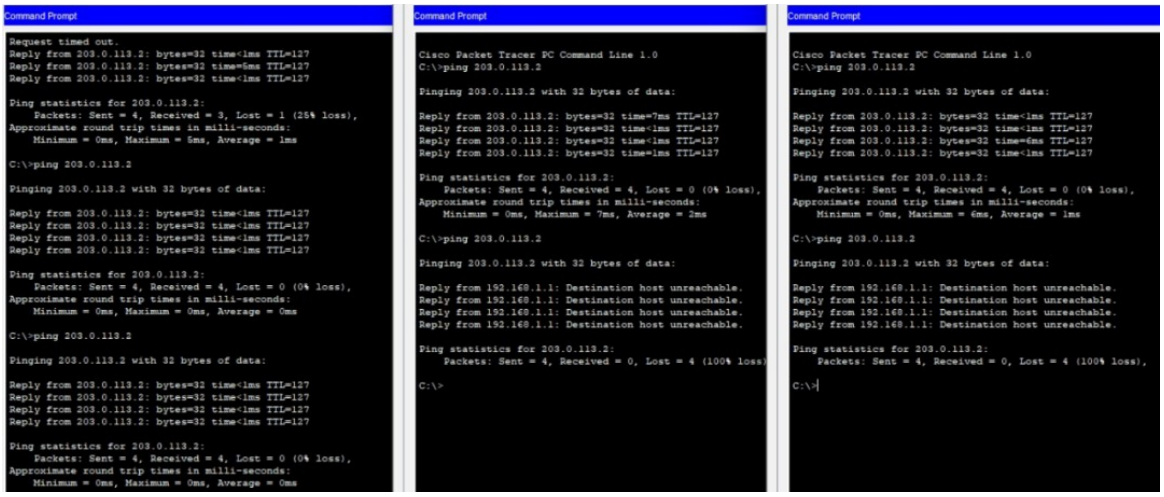


Gambar 19: Semua PC Terhubung ke Server

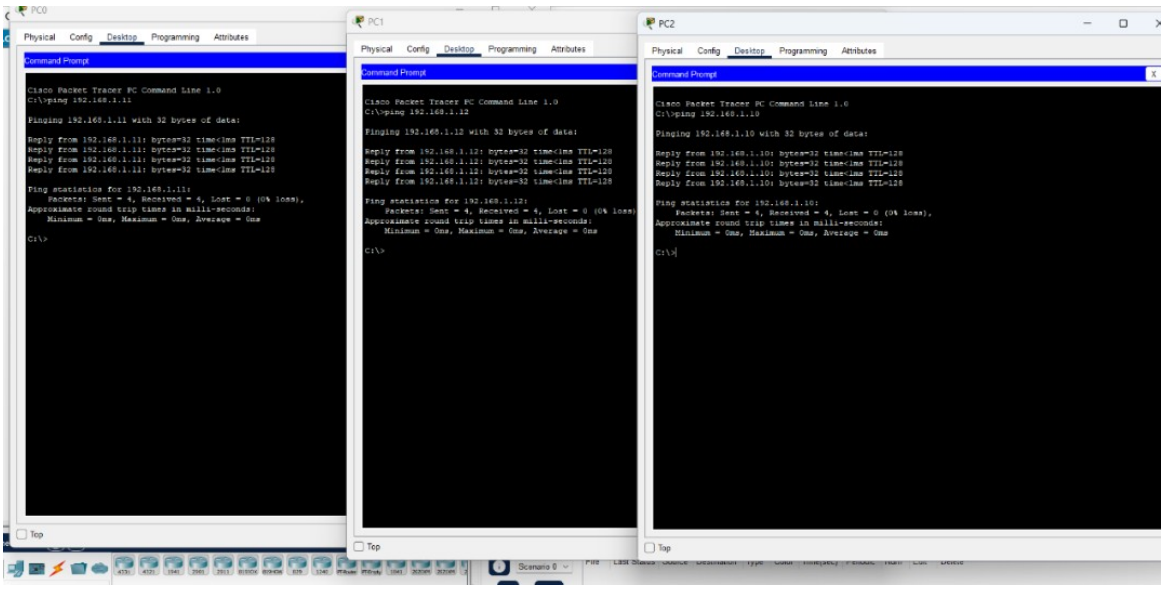
3. Konfigurasi Firewall (ACL) :

   PC1 yang hanya dapat mengakses Server. Blokir PC2 PC3 dari mengakses Server. Semua PC harus tetap saling terhubung di LAN.

Jawaban : Disini untuk PC1 = PC0 dan PC3 = PC2.



Gambar 20: Hanya PC0 yang Dapat Mengakses Server



Gambar 21: Semua PC Saling Terhubung dalam LAN

4 Kesimpulan

Melalui praktikum ini, kami berhasil memahami mekanisme kerja NAT dan firewall pada perangkat MikroTik RouterOS. Network Address Translation memungkinkan perangkat dalam jaringan lokal untuk mengakses internet melalui single public IP address, sementara firewall berfungsi sebagai sistem kontrol akses untuk mengatur lalu lintas data, termasuk kemampuan memblokir ping dan akses ke website tertentu.

Seluruh scenario pengujian menunjukkan hasil yang konsisten dengan teori yang telah dipelajari. Praktikum ini memberikan pemahaman mendalam tentang bagaimana konfigurasi sederhana dapat memberikan dampak signifikan terhadap keamanan dan kontrol jaringan.

Praktikum ini juga menekankan pentingnya ketelitian dan systematic approach dalam melakukan konfigurasi jaringan, karena kesalahan minor dapat menyebabkan disfungsi pada keseluruhan sistem jaringan. Pengalaman hands-on ini memperkuat pemahaman teoritis dengan implementasi praktis yang dapat diterapkan dalam skenario jaringan yang sesungguhnya.

5 Lampiran

5.1 Dokumentasi Praktikum