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

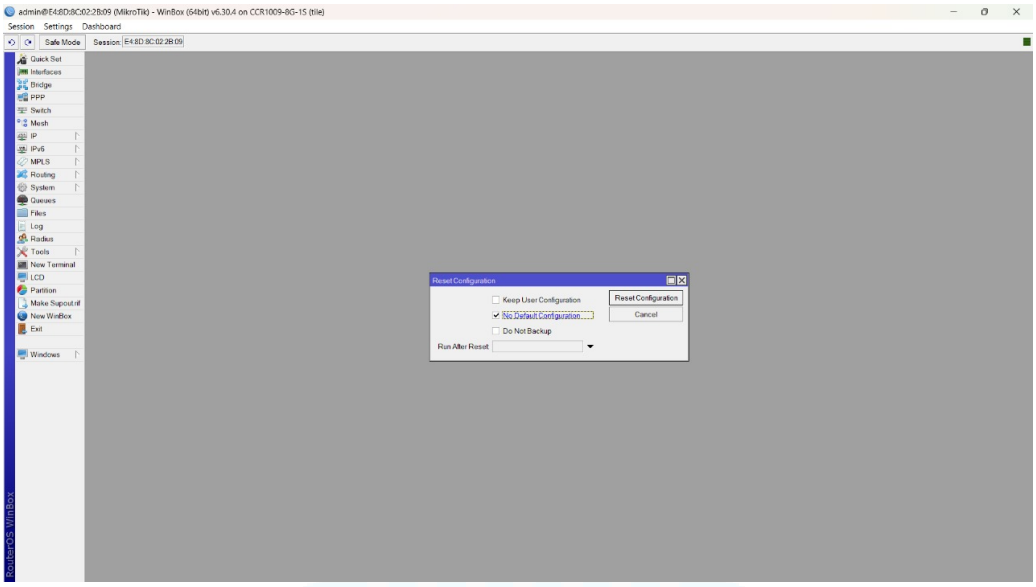
Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Sultan Syafiq Rakan - 5024231009

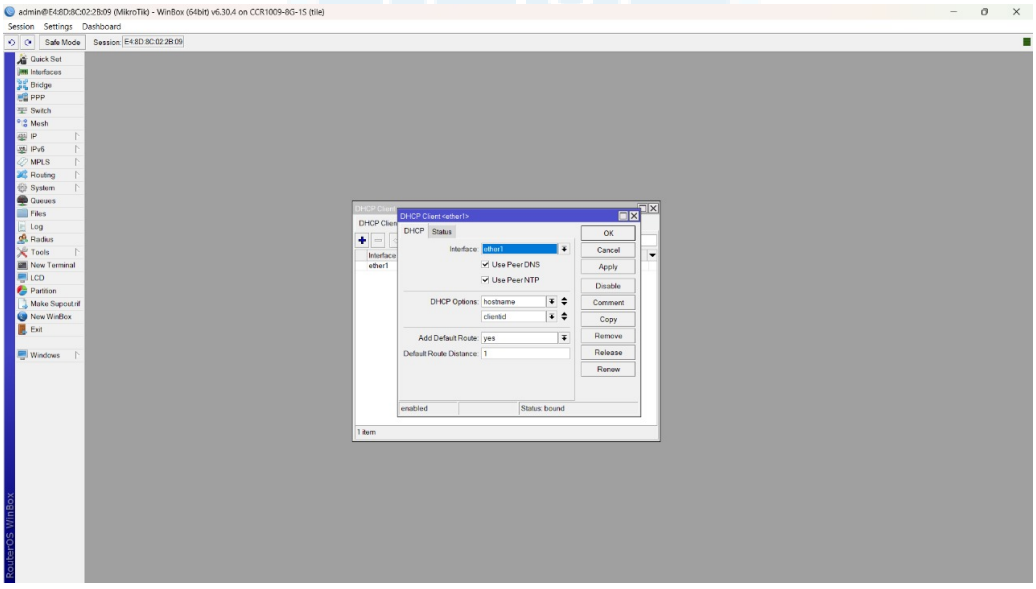
2025

sectionProsedur Percobaan Praktikum ini diawali dengan menghubungkan dua laptop ke dua router menggunakan kabel LAN. Sebelum melakukan konfigurasi, router direset terlebih dahulu untuk menghapus pengaturan sebelumnya, kemudian dilakukan login ke sistem router.



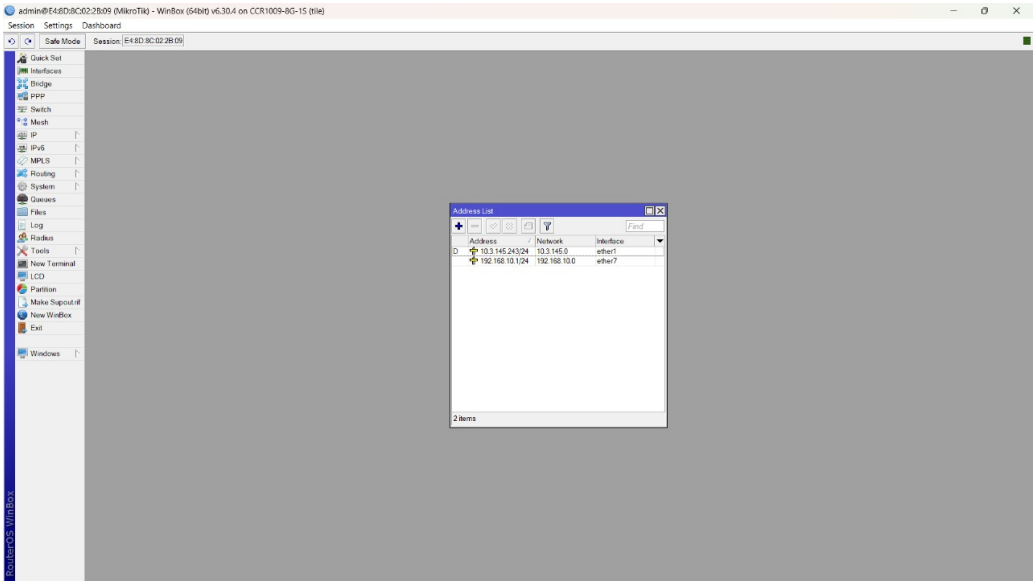
Gambar 1: Proses Reset Router

Setelah reset, sambungkan kabel internet ke port ether1 pada Router A. Konfigurasikan DHCP Client melalui menu IP > DHCP Client, klik tanda "+", pilih ether1 sebagai antarmuka, lalu klik "Apply". Pastikan status koneksi menunjukkan "bound" untuk menandakan router telah menerima IP dari ISP.



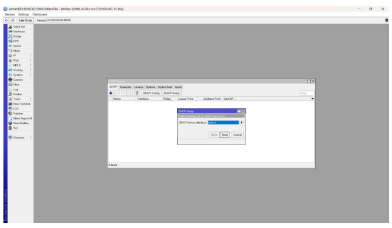
Gambar 2: Pengaturan DHCP Client pada Router A

Selanjutnya, tambahkan alamat IP pada port ether7, yang menghubungkan ke switch atau Router B. Masuk ke menu IP > Addresses, klik tanda "+", masukkan alamat 192.168.10.1/24, pilih antarmuka ether7, lalu klik "Apply" dan "OK".

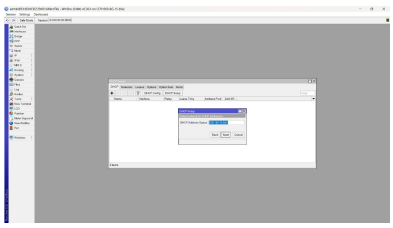


Gambar 3: Penambahan Alamat IP pada Ether7

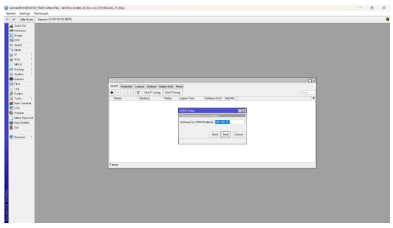
Konfigurasikan DHCP Server melalui menu IP > DHCP Server, klik "DHCP Setup", dan pastikan pengaturan sesuai dengan langkah-langkah berikut, seperti ditunjukkan pada gambar.



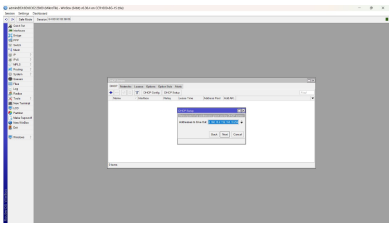
Gambar 4: Pemilihan Antarmuka



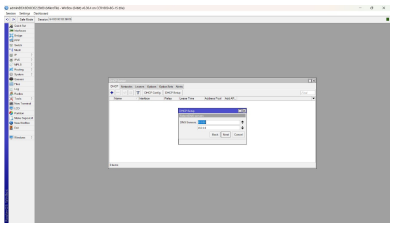
Gambar 5: Pengaturan Ruang Alamat



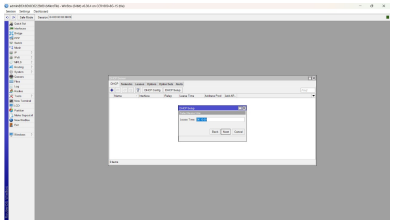
Gambar 6: Pengaturan Gateway



Gambar 7: Rentang Alamat IP

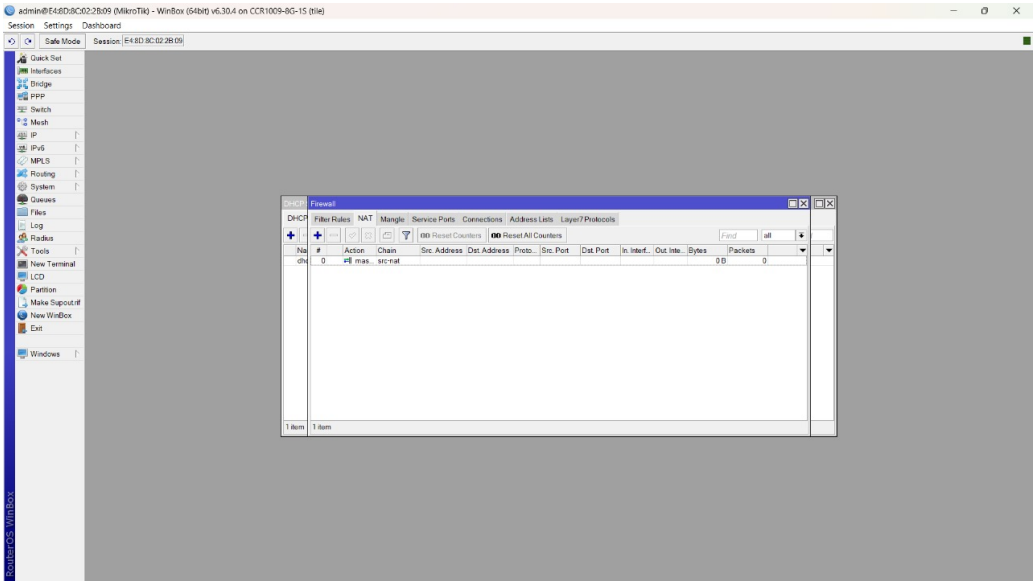


Gambar 8: Pengaturan DNS



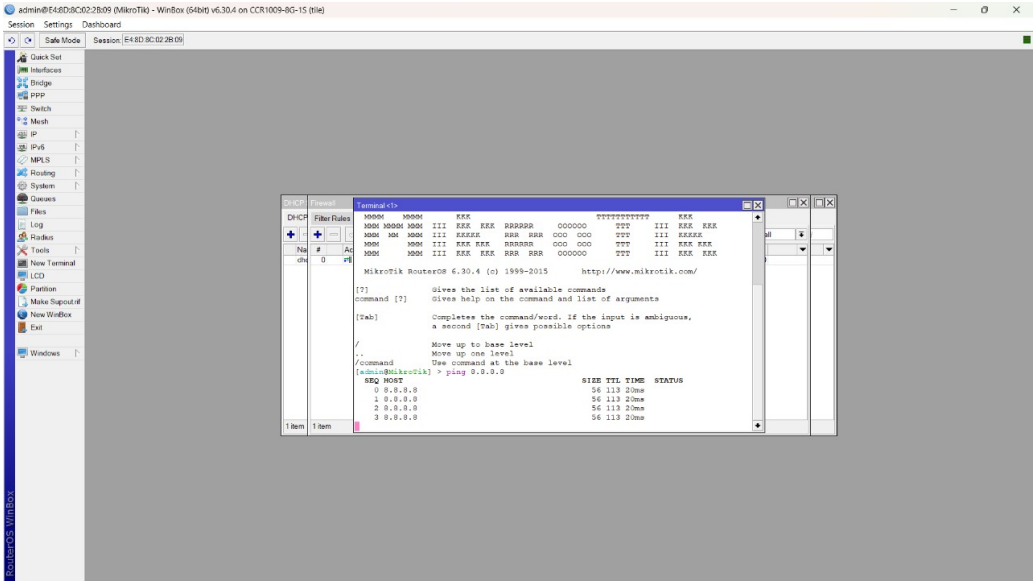
Gambar 9: Waktu Sewa IP

Lanjutkan dengan konfigurasi NAT melalui menu IP > Firewall > NAT. Klik tanda "+", pada tab "General" atur Chain ke "srcnat", pada tab "Action" pilih "masquerade", lalu klik "Apply" dan "OK".



Gambar 10: Pengaturan NAT

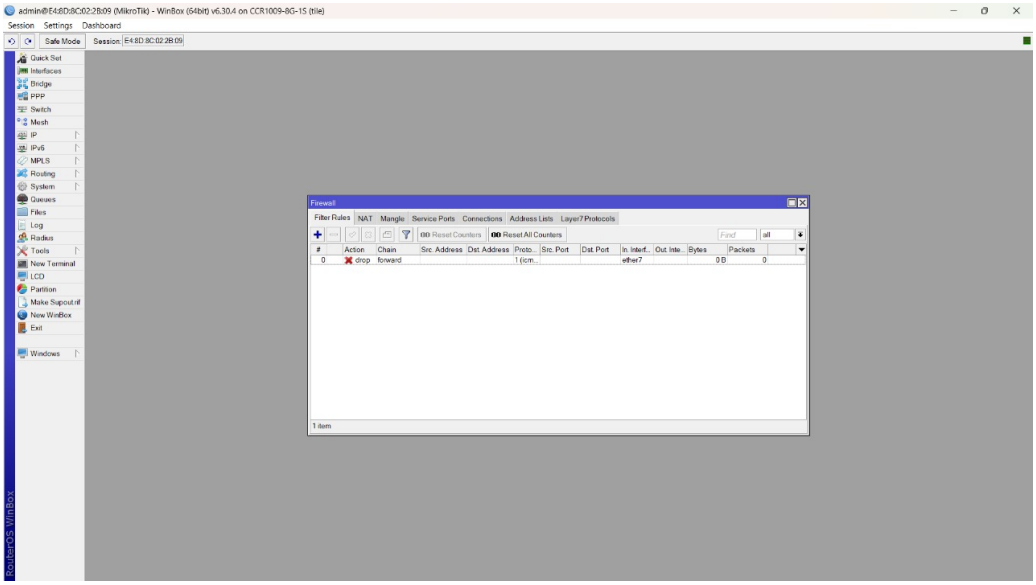
Uji konektivitas dengan membuka terminal baru pada router dan lakukan ping ke alamat 8.8.8.8 untuk memastikan akses internet berfungsi.



Gambar 11: Pengujian Konektivitas Internet

Konfigurasikan firewall untuk memblokir ICMP melalui menu IP > Firewall > Filter Rules, klik tanda "+", dan atur sebagai berikut:

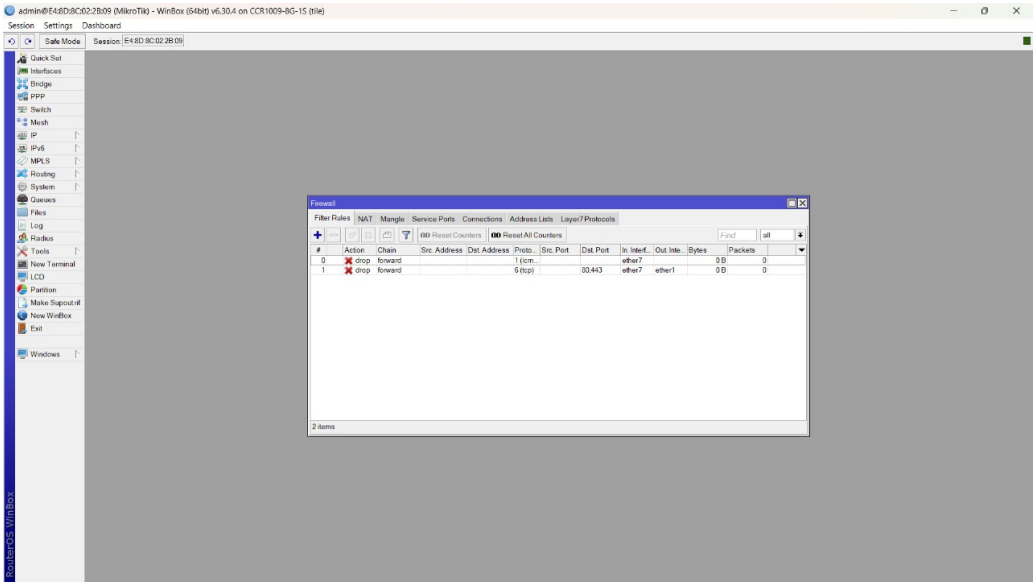
1. Tab "General": Chain = "forward".
2. Tab "General": Protocol = "icmp".
3. Tab "General": In. Interface = "ether7".
4. Tab "Action": Action = "drop".



Gambar 12: Pemblokiran Protokol ICMP

Untuk memblokir akses ke situs web berdasarkan konten, konfigurasikan firewall sebagai berikut:

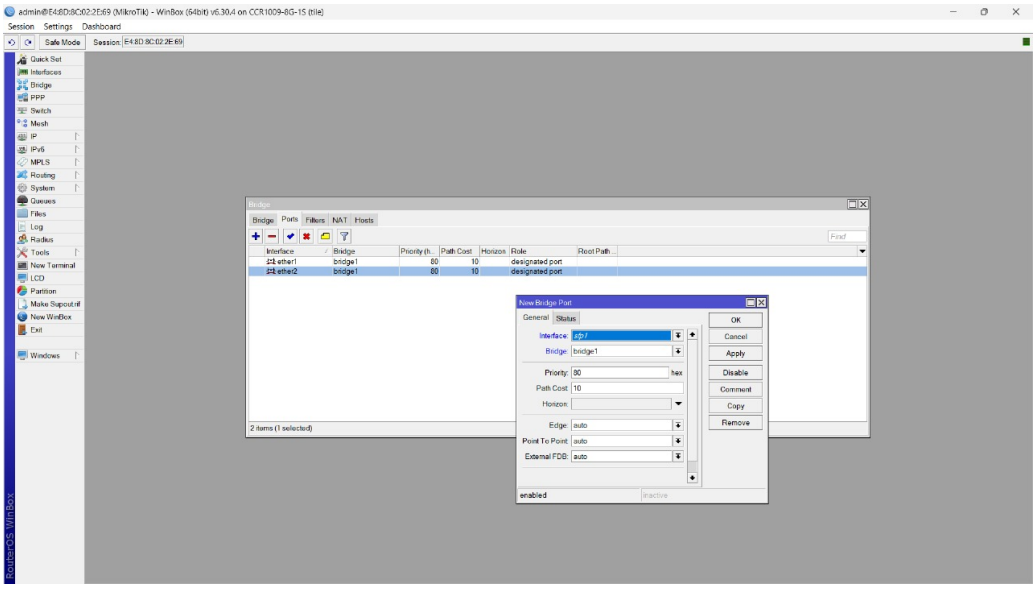
1. Tab "General": Chain = "forward".
2. Tab "General": Protocol = "tcp".
3. Tab "General": Dst. Port = "80,443".
4. Tab "General": In. Interface = "ether7".
5. Tab "General": Out. Interface = "ether1".
6. Tab "Advanced": Content = "speedtest".
7. Tab "Action": Action = "drop".



Gambar 13: Pemblokiran Konten Web

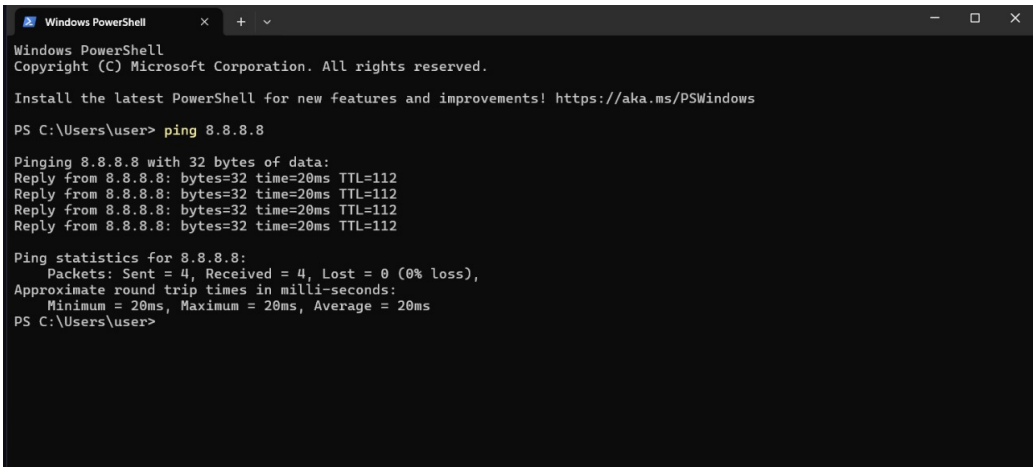
Pada Router B (berfungsi sebagai hub), konfigurasikan bridge melalui menu Bridge, klik tanda "+", lalu klik "Apply" dan "OK".

Tambahkan port ke bridge yang telah dibuat melalui menu Bridge > Ports, klik tanda "+", pilih antarmuka yang terhubung ke laptop dan antarmuka yang terhubung ke Router A, lalu klik "OK".



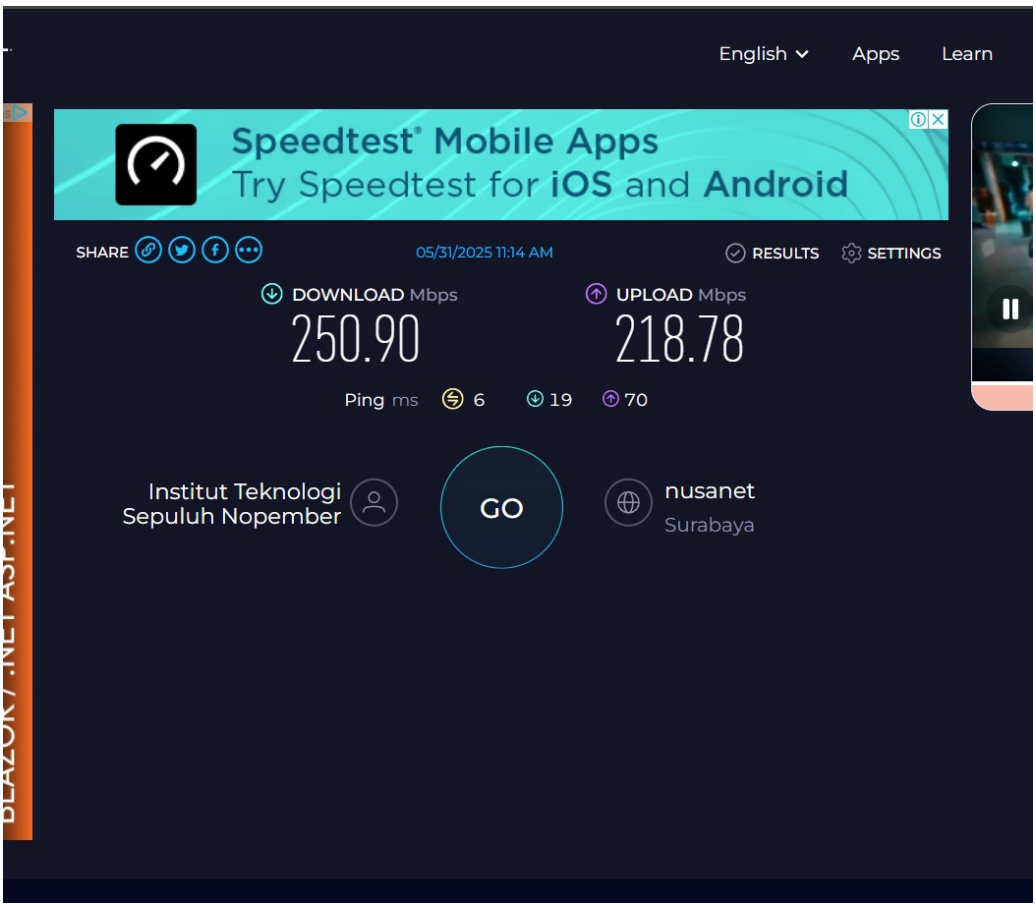
Gambar 14: Penambahan Port pada Bridge

Atur alamat IP pada laptop sesuai dengan rentang IP yang telah dikonfigurasi, lalu uji konektivitas ICMP dengan menjalankan perintah `ping 8.8.8.8` pada Command Prompt laptop.



Gambar 15: Uji Konektivitas ICMP dari Laptop

Hasil pengujian menunjukkan *Request Timed Out*, yang mengindikasikan bahwa aturan firewall untuk ICMP berfungsi. Untuk menguji pemblokiran konten, akses situs seperti speedtest.net melalui peramban pada laptop.



Gambar 16: Uji Pemblokiran Konten Web

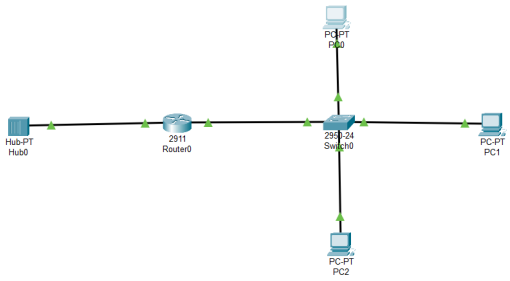
1 Analisis Hasil Percobaan

Selama praktikum, semua langkah konfigurasi berhasil diimplementasikan sesuai panduan. Pengaturan DHCP memungkinkan klien memperoleh alamat IP secara otomatis, sementara NAT memastikan akses ke internet. Ketika aturan firewall untuk ICMP diaktifkan, ping ke 8.8.8.8 menghasilkan *Request Timed Out*, menunjukkan bahwa pemblokiran ICMP berjalan sesuai rencana. Demikian pula, saat mengakses situs speedtest.net, halaman tidak dapat dimuat, sesuai dengan aturan pemblokiran konten. Hasil ini membuktikan bahwa firewall efektif dalam mengontrol lalu lintas jaringan. Meskipun awalnya terdapat kesulitan dalam memilih antarmuka yang tepat, setelah dilakukan pengecekan ulang, semua fungsi berjalan dengan baik.

2 Hasil Tugas Modul

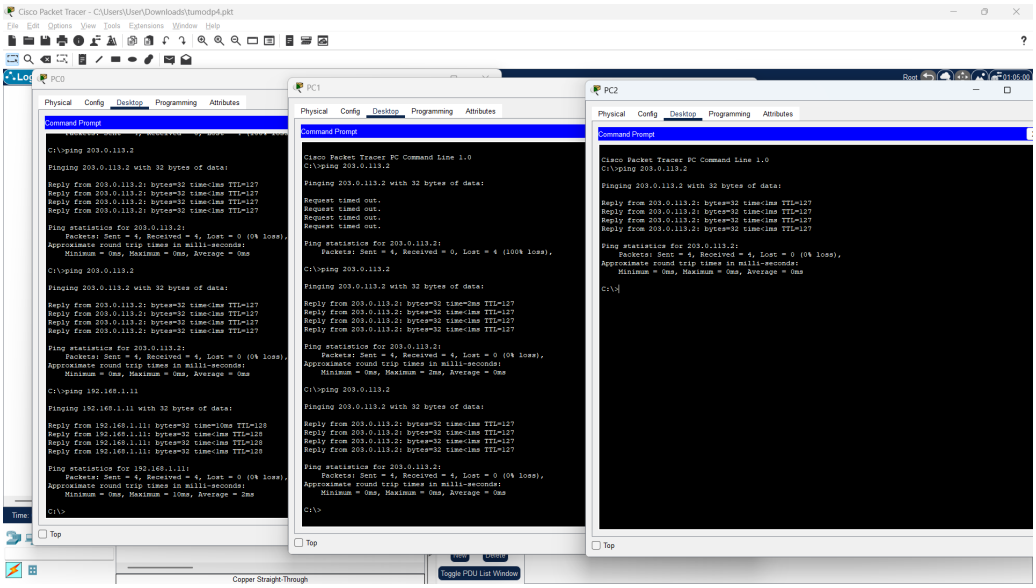
1. Buat topologi sederhana di Cisco Packet Tracer yang terdiri dari:
   (a) 1 Router
   (b) 1 Switch
   (c) 3 PC (LAN)
   (d) 1 Server (Internet/Publik)

   Jawaban:



Gambar 17: Topologi Jaringan

2. Konfigurasikan NAT agar semua PC dapat mengakses server menggunakan alamat IP publik router. **Jawaban:**



Gambar 18: Akses PC ke Server melalui NAT

3. Konfigurasikan firewall (ACL) dengan ketentuan:

   (a) Hanya PC1 yang diizinkan mengakses server.

   (b) PC2 dan PC3 diblokir dari akses ke server.

   (c) Semua PC tetap dapat saling terhubung dalam LAN.

   Jawaban: (Catatan: PC1 = PC0, PC3 = PC2)

3 Kesimpulan

Praktikum ini memberikan wawasan tentang fungsi NAT dan firewall pada perangkat MikroTik. NAT memungkinkan perangkat di jaringan lokal mengakses internet menggunakan satu alamat IP publik, sementara firewall mengatur lalu lintas jaringan, seperti memblokir protokol ICMP atau akses ke situs tertentu. Semua pengujian menghasilkan output sesuai teori, memperkuat pemahaman tentang pengelolaan jaringan yang aman dan efisien. Praktikum ini juga menunjukkan pentingnya ketelitian dalam konfigurasi, karena kesalahan kecil dapat mengganggu fungsi jaringan.

4 Lampiran

Dokumentasi Praktikum

Gambar 19: Dokumentasi