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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Athariq Qur'ani Fajri - 5024231031

2025

1 Langkah-Langkah Praktikum

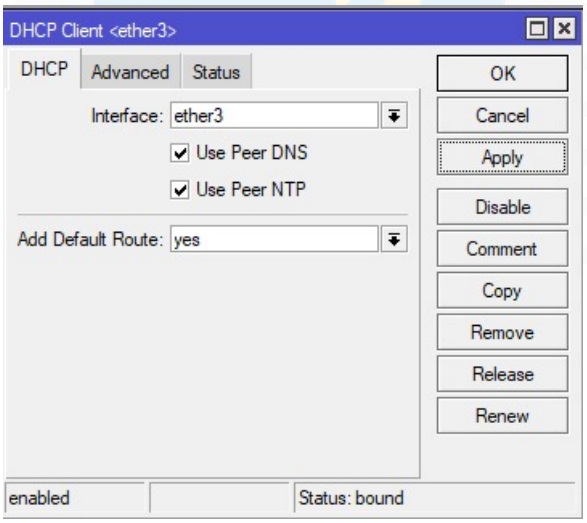
1.1 Implementasi Pemblokiran ICMP dan Konten Website

Perangkat dan Kebutuhan

1. 3 buah kabel UTP yang telah melalui proses crimping
2. 2 unit Router Mikrotik
3. 2 unit Laptop/PC

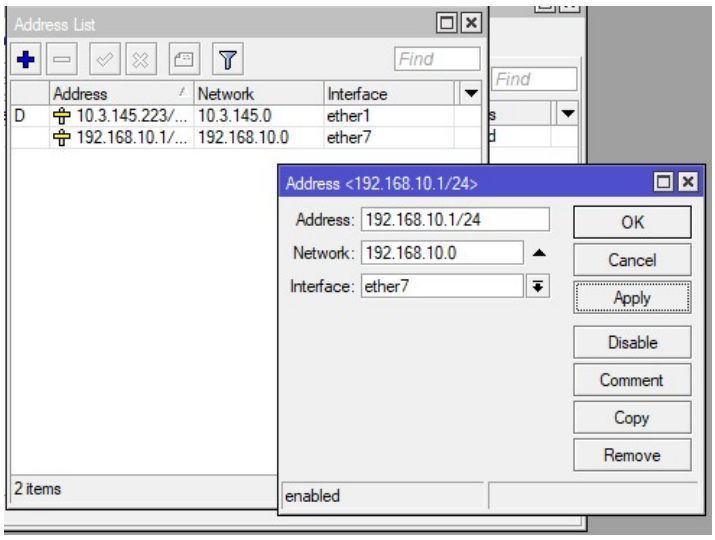
Tahapan Konfigurasi Pemblokiran ICMP dan Konten

1. Lakukan persiapan alat seperti router, laptop, dan kabel UTP yang telah dicrimping dengan baik.
2. Hubungkan laptop dan router menggunakan kabel UTP, kemudian jalankan aplikasi Winbox di masing-masing laptop.
3. Akses router melalui Winbox menggunakan alamat MAC atau IP default yang tersedia.
4. Aktifkan DHCP Client melalui `IP > DHCP Client`. Klik tombol + dan pilih `ether1` sebagai interface utama.



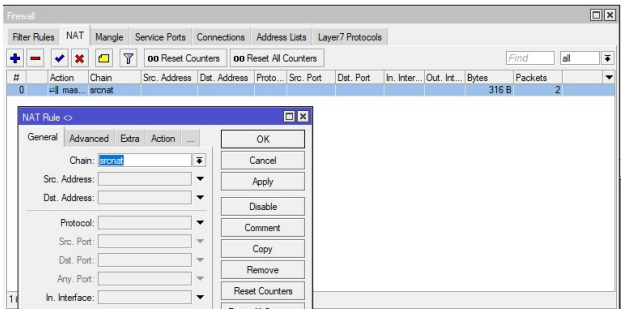
Gambar 1: Aktivasi DHCP Client

5. Konfigurasikan alamat IP untuk interface `ether7` melalui menu `IP > Addresses`. Klik ikon tambah lalu isikan IP `192.168.10.1/24`.

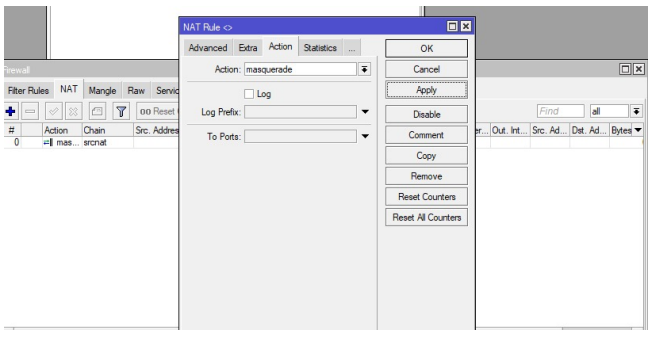


Gambar 2: Penambahan Alamat IP Lokal

6. Atur DHCP Server agar dapat mendistribusikan IP secara otomatis ke perangkat Laptop 2.
7. Buka `IP > Firewall > NAT`, lalu tambahkan rule baru dengan memilih `src-nat` di tab General dan `masquerade` di tab Action.

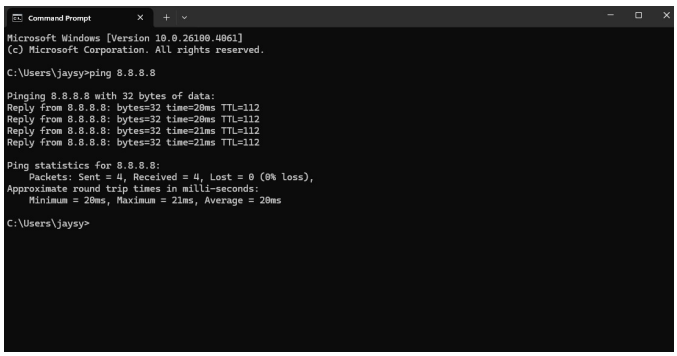


Gambar 3: Konfigurasi NAT - Bagian 1



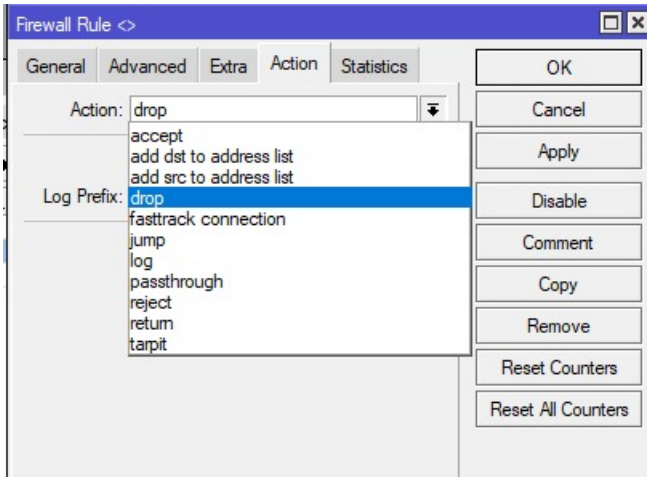
Gambar 4: Konfigurasi NAT - Bagian 2

8. Lakukan pengujian koneksi ke internet dengan melakukan ping ke alamat `8.8.8.8`.



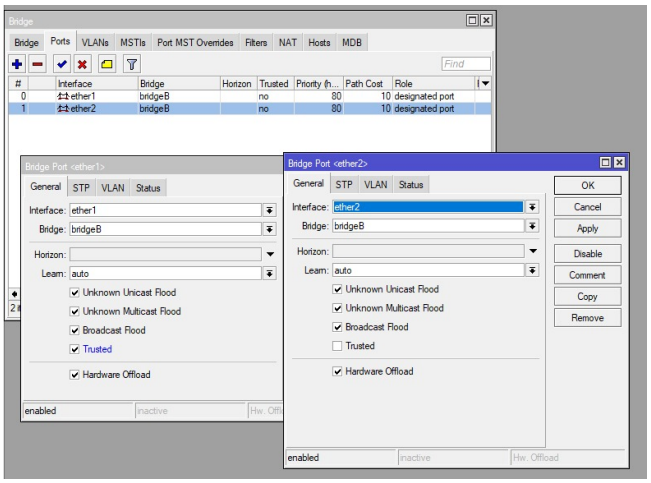
Gambar 5: Pengujian Koneksi dengan Ping

9. Tambahkan aturan firewall melalui `IP > Firewall > Filter Rules` untuk memblokir protokol ICMP dan mengaktifkan pemblokiran konten berdasarkan domain.



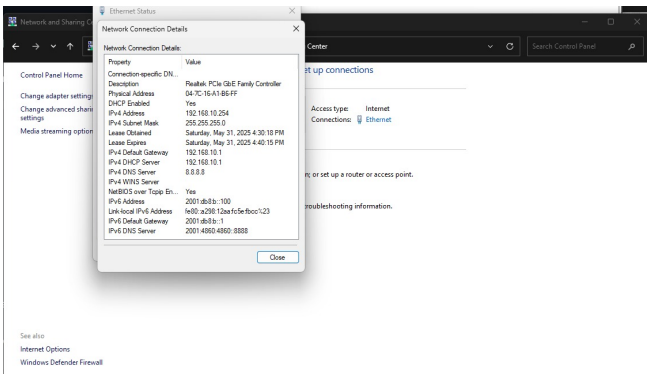
Gambar 6: Rule Firewall untuk Pemblokiran

10. Buat konfigurasi bridge agar router kedua (Router B) dapat difungsikan sebagai hub jaringan.



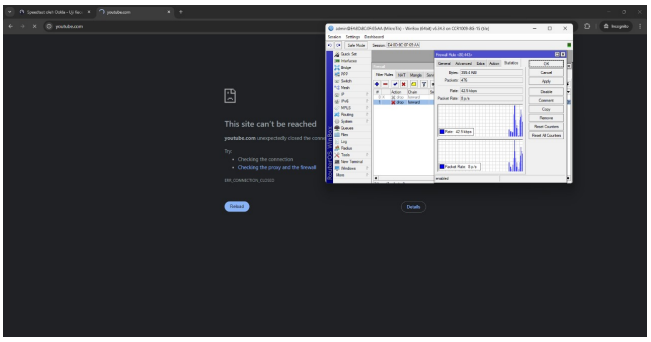
Gambar 7: Konfigurasi Bridge pada Router B

11. Pastikan laptop telah menerima alamat IP secara otomatis dari DHCP Server.



Gambar 8: Cek Pengaturan IP Otomatis

12. Uji implementasi pemblokiran ICMP dan content blocking menggunakan akses jaringan serta pengujian ping ke domain tertentu.



Gambar 9: Hasil Uji Pemblokiran ICMP dan Konten

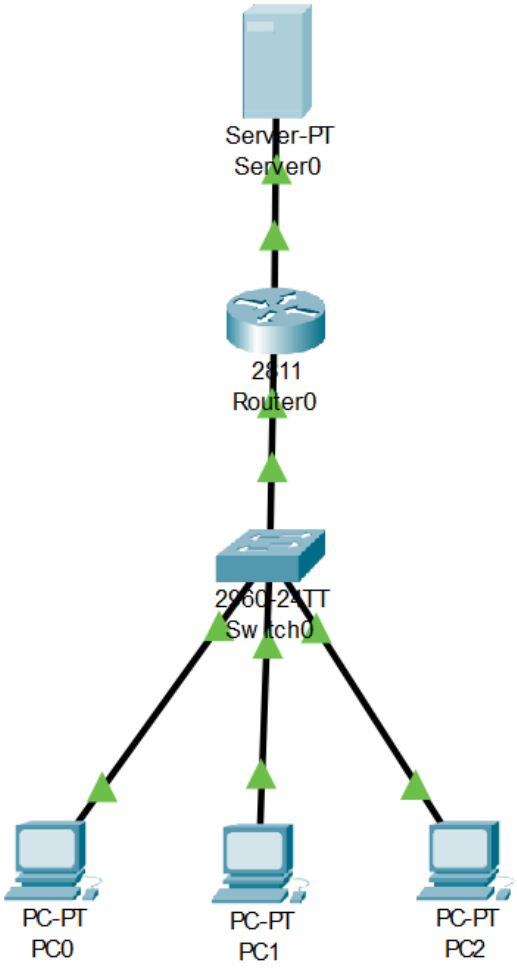
2 Analisis Hasil Praktikum

Percobaan pada sesi kali ini berkaitan dengan implementasi fitur Firewall dan NAT pada perangkat Mikrotik. Seluruh tahapan berhasil dijalankan sebagaimana tercantum dalam panduan modul. Fokus utama praktik adalah pemblokiran akses terhadap konten tertentu dan pembatasan kecepatan internet.

DHCP Client yang diaktifkan pada `ether1` dan DHCP Server pada `ether7` bekerja dengan baik dalam memberikan alamat IP secara otomatis ke perangkat klien. Selain itu, konfigurasi NAT dengan metode `masquerade` berhasil memberikan akses internet bagi perangkat dalam jaringan, yang dibuktikan dengan berhasilnya perintah ping ke `8.8.8.8` selama firewall dinonaktifkan.

Router B dikonfigurasi sebagai *bridge* yang bertindak sebagai hub, memastikan setiap klien tetap terhubung secara konsisten ke jaringan lokal. Pengujian firewall menunjukkan bahwa pemblokiran terhadap protokol ICMP berhasil diterapkan, terlihat dari munculnya pesan RTO (Request Timed Out) saat melakukan ping ketika rule pemblokiran aktif. Untuk fitur content blocking, pengujian awal terhadap situs `speedtest.net` tidak membuahkan hasil, namun saat dilakukan pemfilteran terhadap situs `youtube.com`, sistem berhasil memblokir akses sebagaimana yang diharapkan.

3 Dokumentasi Tugas Modul



Gambar 10: Tangkapan Layar Hasil Pengerjaan Tugas Modul

4 Kesimpulan

Dari seluruh proses konfigurasi dan pengujian yang dilakukan, dapat disimpulkan bahwa praktikum berjalan dengan baik. Fitur-fitur seperti pengaturan DHCP, pemblokiran konten situs web, serta pembatasan kecepatan akses internet menggunakan firewall dan NAT telah diterapkan secara efektif.

Meskipun pada percobaan awal pemblokiran situs `speedtest.net` tidak berhasil, hasil akhir menunjukkan keberhasilan pemblokiran konten ketika diterapkan pada situs `youtube.com`. Hal ini menegaskan bahwa konfigurasi firewall pada Mikrotik mampu membatasi jenis trafik tertentu sesuai dengan aturan yang telah ditentukan oleh administrator jaringan.

5 Lampiran

5.1 Dokumentasi saat praktikum