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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

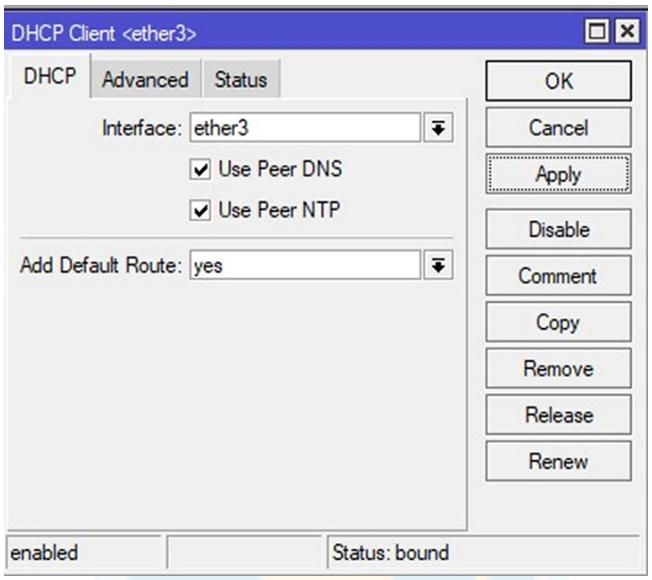
Arhya Hafidz Hafidin - 5024231042

2025

1 Langkah-Langkah Percobaan

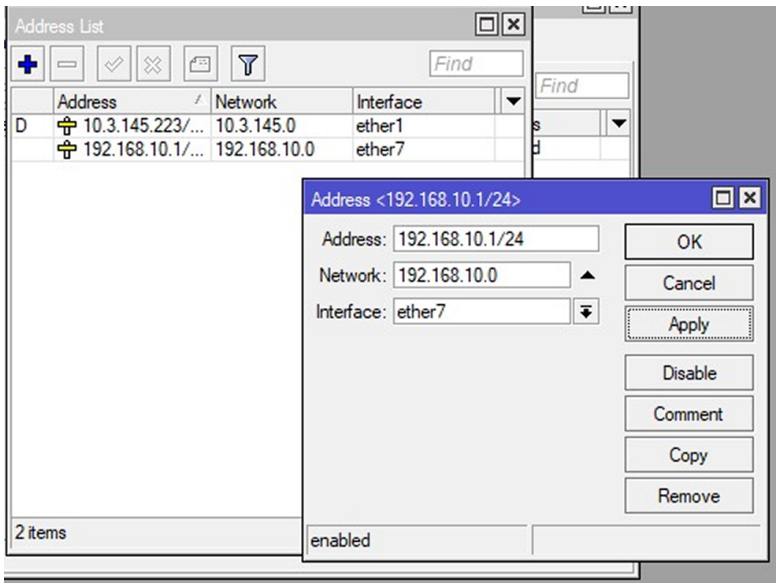
Implementasi Pemblokiran ICMP dan Konten Website

1. Siapkan perangkat yang diperlukan, seperti router, laptop, dan kabel UTP yang telah dikonektor dengan benar.
2. Sambungkan laptop ke router menggunakan kabel UTP, lalu jalankan aplikasi Winbox pada masing-masing laptop.
3. Akses router melalui Winbox dengan menggunakan alamat MAC atau IP default yang tersedia.
4. Aktifkan fitur DHCP Client melalui menu IP > DHCP Client, kemudian klik tanda tambah (+) dan pilih ether1 sebagai interface utama.



Gambar 1: Aktivasi DHCP Client

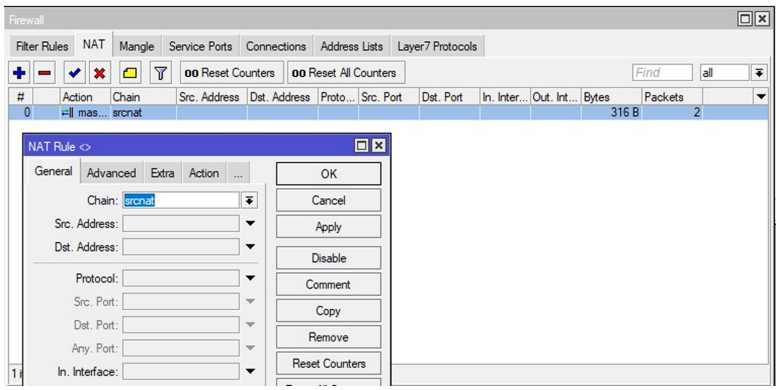
5. Atur alamat IP untuk interface ether7 melalui menu IP > Addresses dengan menambahkan IP 192.168.10.1/24.



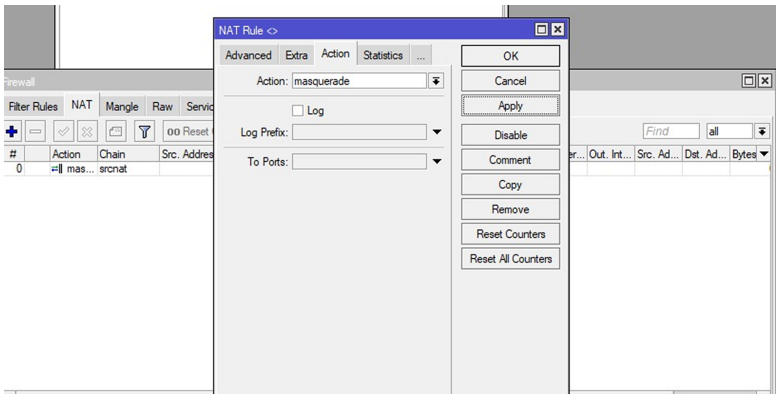
Gambar 2: Penambahan Alamat IP Lokal

6. Konfigurasikan DHCP Server agar dapat mendistribusikan alamat IP secara otomatis ke perangkat Laptop 2.

7. Tambahkan aturan NAT melalui menu IP > Firewall > NAT. Pada tab General pilih src-nat, dan pada tab Action pilih *masquerade*.

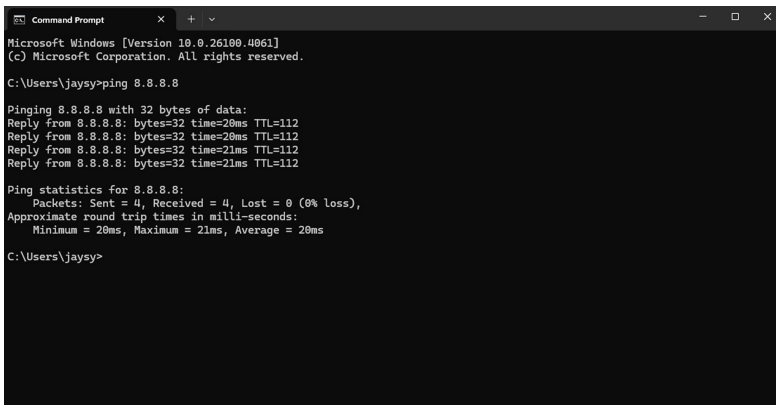


Gambar 3: Konfigurasi NAT - Bagian 1



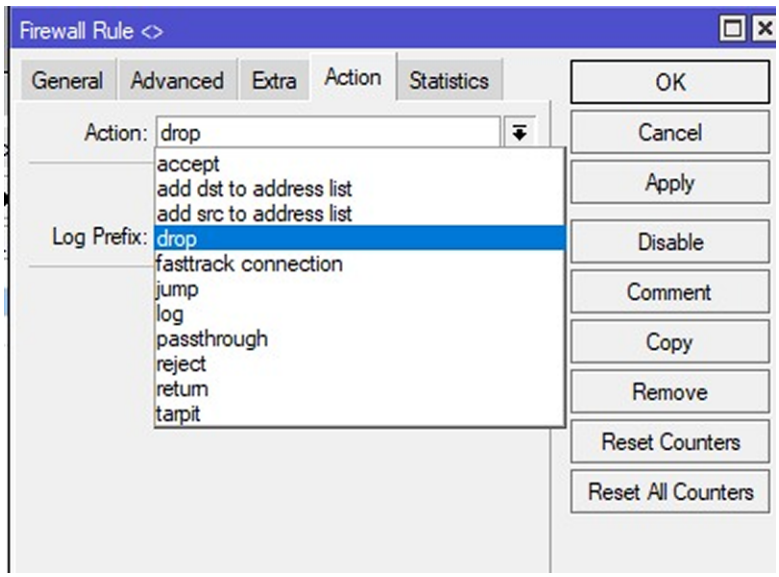
Gambar 4: Konfigurasi NAT - Bagian 2

8. Lakukan uji koneksi ke internet dengan menjalankan perintah ping ke alamat 8.8.8.8.



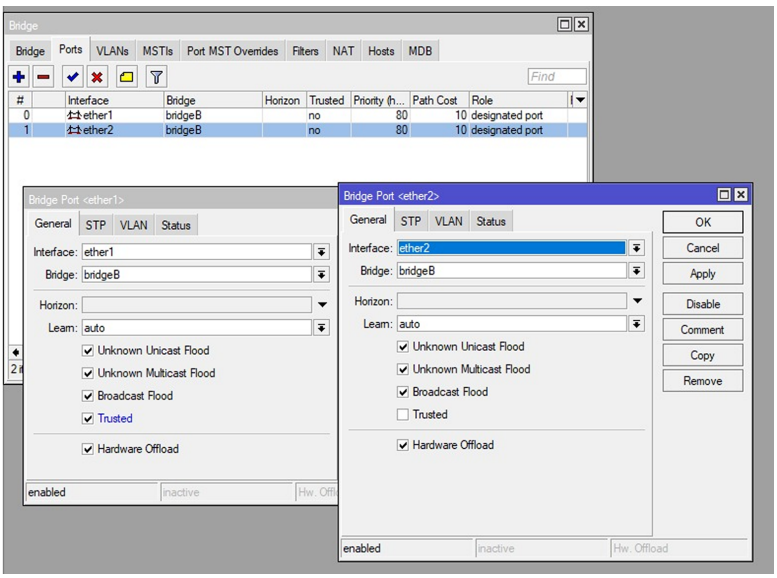
Gambar 5: Pengujian Koneksi dengan Ping

9. Buat filter firewall melalui menu IP > Firewall > Filter Rules untuk memblokir protokol ICMP dan mengaktifkan pemblokiran berdasarkan domain.



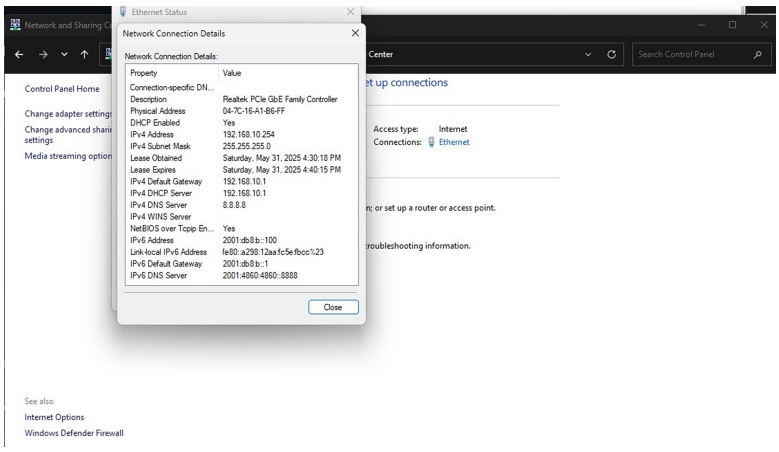
Gambar 6: Rule Firewall untuk Pemblokiran

10. Konfigurasikan bridge agar router kedua (Router B) dapat berfungsi sebagai hub jaringan.



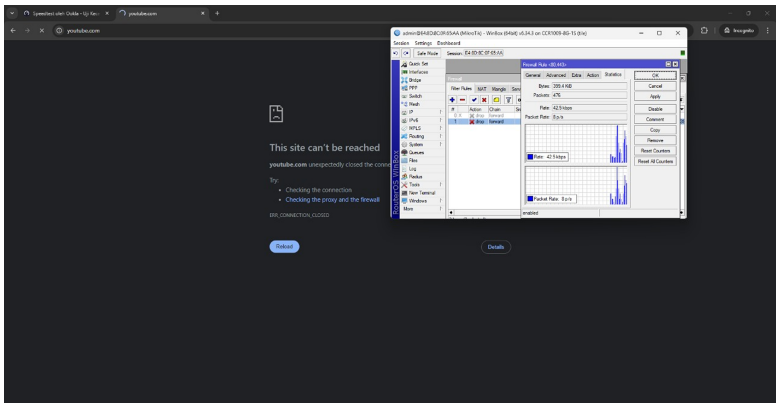
Gambar 7: Konfigurasi Bridge pada Router B

11. Pastikan Laptop telah memperoleh alamat IP secara otomatis dari DHCP Server.



Gambar 8: Cek Pengaturan IP Otomatis

12. Uji fungsi pemblokiran ICMP dan konten dengan mencoba akses jaringan serta ping ke domain tertentu.



Gambar 9: Hasil Uji Pemblokiran ICMP dan Konten

2 Analisis Hasil Percobaan

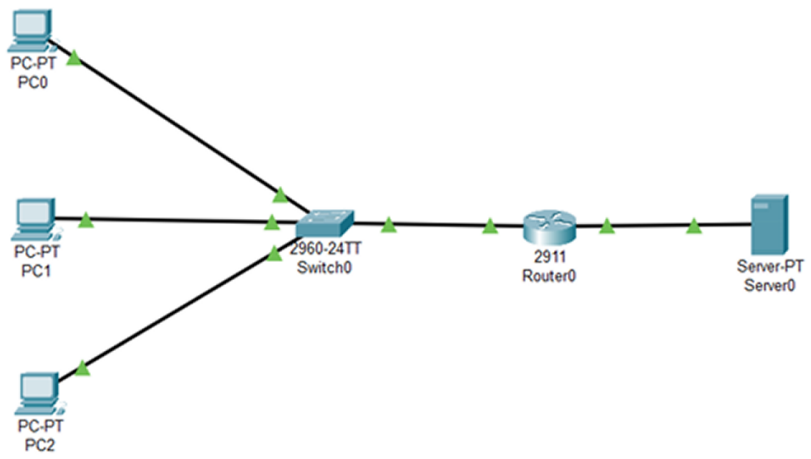
Pada percobaan kali ini membahas penerapan fitur Firewall dan NAT di perangkat Mikrotik. Semua langkah bisa dijalankan dengan lancar sesuai panduan yang ada di modul. Fokus utamanya ada di pemblokiran akses ke konten tertentu dan pembatasan kecepatan internet.

DHCP Client yang dipasang di ether1 dan DHCP Server di ether7 bisa bekerja dengan baik untuk memberikan IP otomatis ke perangkat klien. Selain itu, konfigurasi NAT memakai metode masquerade juga berhasil memberikan akses internet ke perangkat di jaringan. Hal ini dibuktikan lewat uji coba ping ke 8.8.8.8 yang sukses, asalkan firewall-nya belum diaktifkan.

Router B dikonfigurasi jadi bridge supaya bisa bertindak sebagai hub. Dengan begitu, tiap perangkat klien bisa tetap terhubung ke jaringan lokal tanpa masalah.

Pada bagian pengujian firewall, terbukti kalau aturan pemblokiran ICMP jalan dengan baik. Soalnya ketika coba ping sambil aturan aktif, muncul pesan Request Timed Out. Untuk fitur pemblokiran konten, awalnya di coba blokir speedtest.net tapi belum berhasil. Tapi ketika dialihin ke youtube.com, sistem berhasil ngeblok akses seperti yang diharapkan.

3 Hasil Tugas Modul



Gambar 10: Hasil Tugas Modul

4 Kesimpulan

Berdasarkan seluruh tahapan konfigurasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa praktikum berhasil dilaksanakan dengan baik. Berbagai fitur seperti pengaturan DHCP, pemblokiran akses ke situs tertentu, serta pembatasan kecepatan koneksi melalui firewall dan NAT telah berhasil diterapkan secara optimal.

Walaupun pada awalnya pemblokiran terhadap situs speedtest.net belum memberikan hasil yang diharapkan, pada akhirnya pemblokiran terhadap youtube.com berjalan dengan sukses. Hal ini membuktikan bahwa konfigurasi firewall di perangkat Mikrotik mampu membatasi jenis lalu lintas jaringan tertentu sesuai kebijakan yang telah ditetapkan oleh administrator.

5 Lampiran

Gambar 11: Dokumentasi Kelompok