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

Laporan Akhir
Praktikum Jaringan Komputer

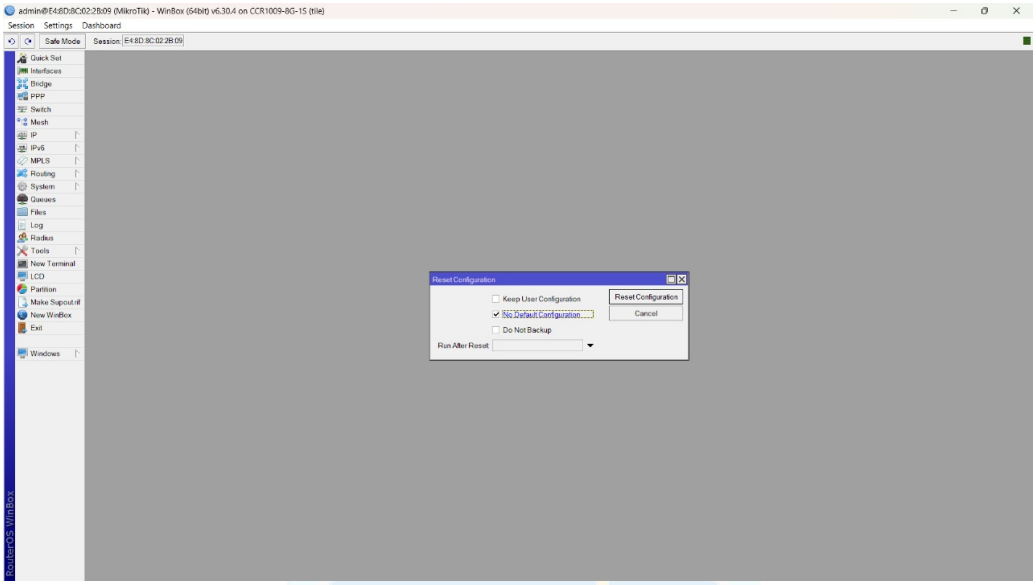
Firewall & NAT

Theo Kawalisa Pinem - 5024231008

2025

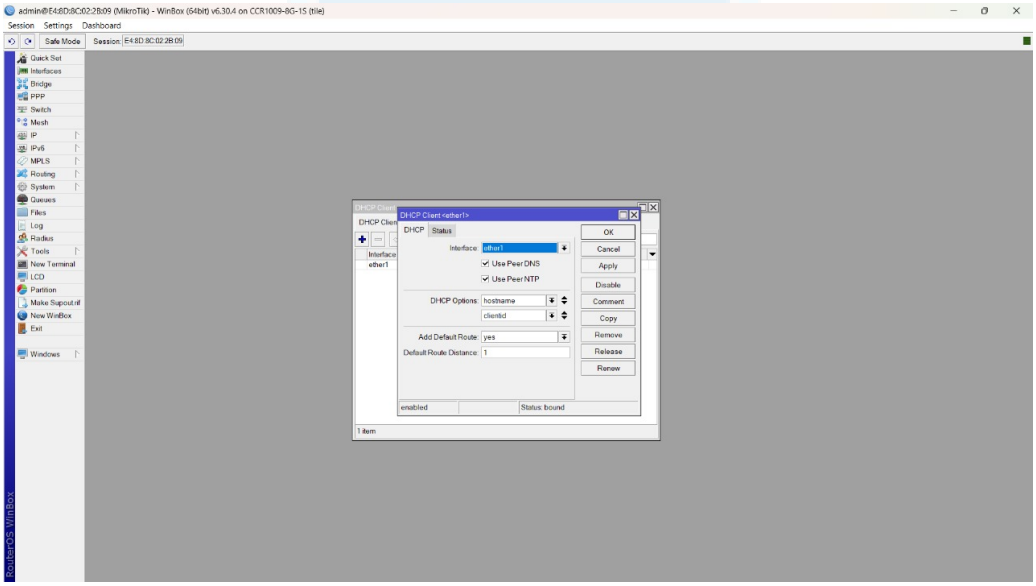
1 Langkah-Langkah Percobaan

Praktikum ini dimulai dengan menghubungkan dua laptop dengan dua router menggunakan kabel LAN, kemudian lakukan login, namun kita melakukan reset dulu terhadap router sebelum digunakan.



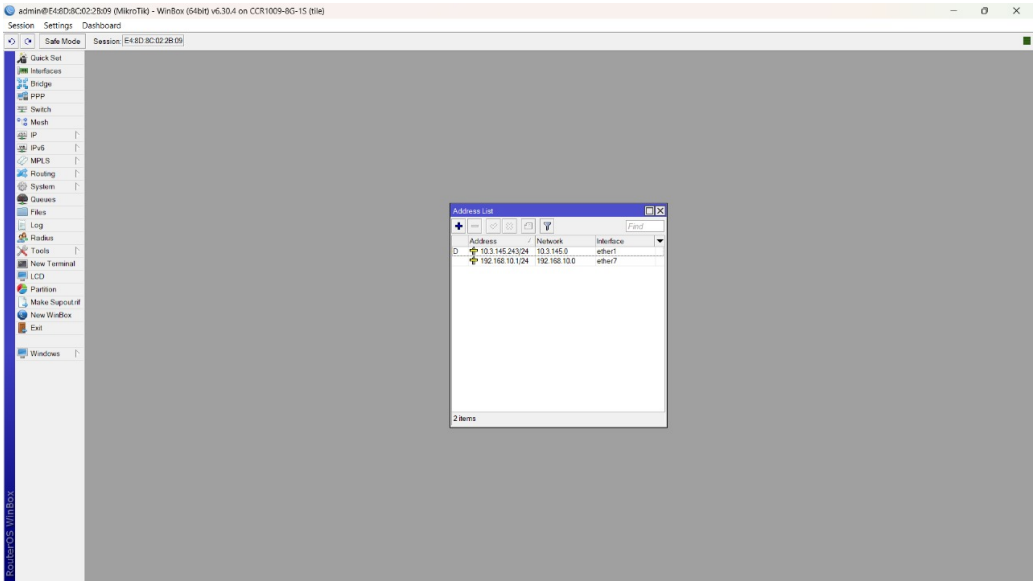
Gambar 1: Reset Konfigurasi Router

Setelah router di reset, sambungkan kabel internet ke ether 1 pada Router A dan lakukan konfigurasi DHCP Client dengan cara mengakses menu IP -> DHCP Client, kemudian klik ikon "+", dan pilih ether1 sebagai interface dan klik "apply" serta pastikan status koneksi sudah dalam "bound".



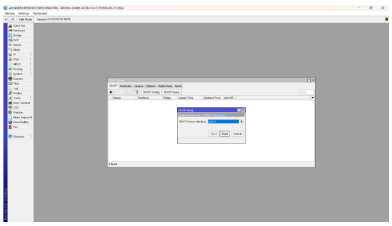
Gambar 2: Konfigurasi DHCP Client pada Router A

Lalu tambahkan alamat IP pada ether7 yang dimana adalah konektivitas dengan Switch atau Router B dengan ke menu IP lalu Addresses, klik ikon "+", masukkan address 192.168.10.1/24, pilih interface ether7 dan klik "apply" kemudian "ok".

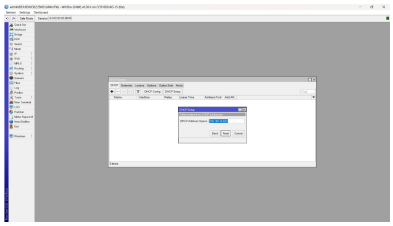


Gambar 3: Penambahan Alamat IP pada Ether 7

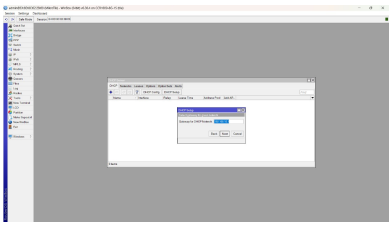
Kemudian lakukan konfigurasi DHCP Server dengan cara mengakses menu IP, lalu DHCP server, klik tombol "DHCP Setup" dan pastikan konfigurasinya sudah sesuai pada gambar - gambar berikut ini.



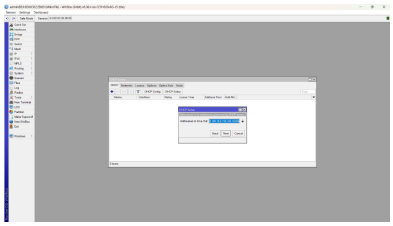
Gambar 4: Konfigurasi Interface



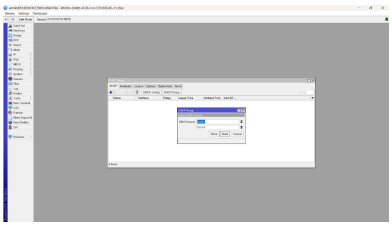
Gambar 5: Konfigurasi Address Space



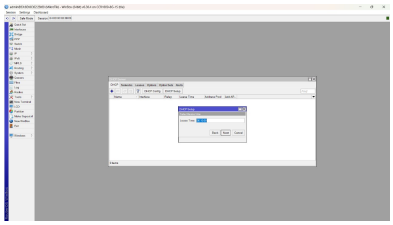
Gambar 6: Konfigurasi Gateway



Gambar 7: Konfigurasi Address to Give Out

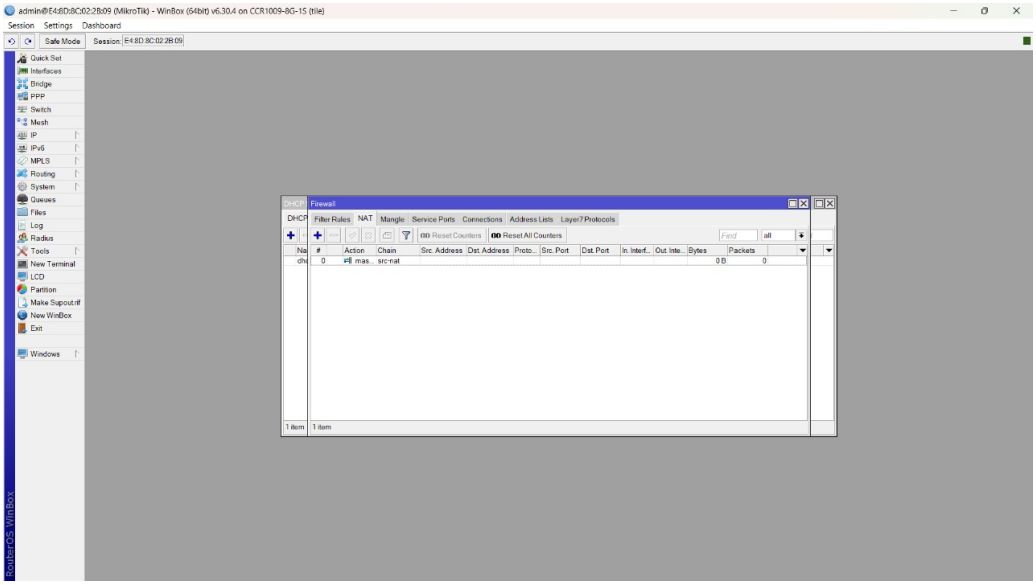


Gambar 8: Konfigurasi DNS



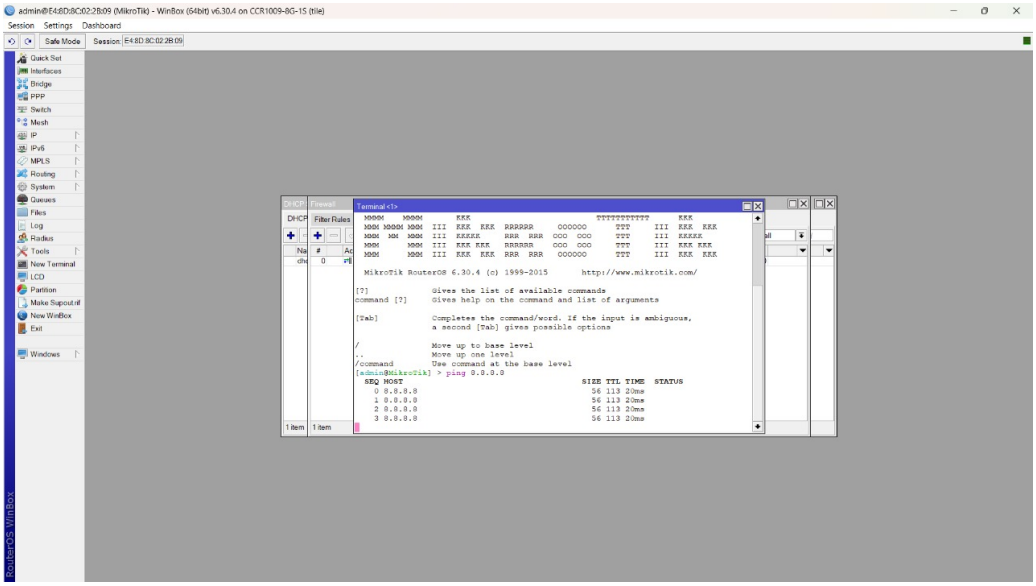
Gambar 9: Konfigurasi Lease Time

Lalu lakukan konfigurasi NAT dengan mengakses menu IP lalu Firewall lalu NAT, klik ikon "+", pada tab "General", atur menjadi "src-nat", pada tab "Action", atur menjadi "masquarade", klik "apply" dan "ok".



Gambar 10: Konfigurasi NAT

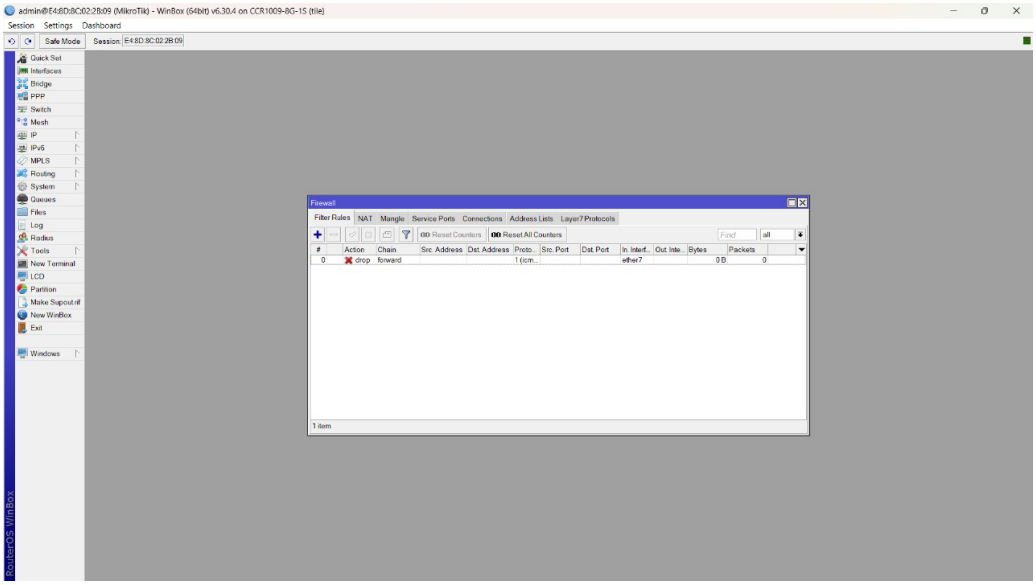
Kemudian lakukan tes koneksi dengan membuka terminal baru dan lakukan pinging dengan ping 8.8.8.8.



Gambar 11: Tes Koneksi

Lalu lakukan konfigurasi firewall dengan mengakses menu IP, lalu firewall, lalu filter rule dan klik ikon "+". Untuk pemblokiran ICMP bisa dilakukan dengan mengatur :

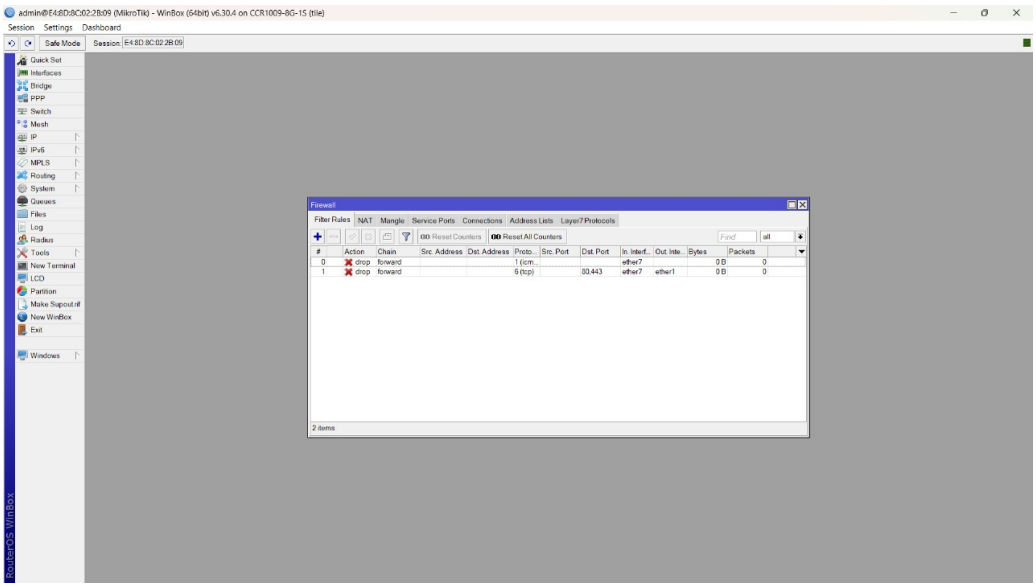
1. Pada tab "General", atur Chain: "forward".
2. Pada tab "General", atur Protocol: "icmp".
3. Pada tab "General", atur In. Interface: "ether7".
4. Pada tab "Action", atur Action: "drop".



Gambar 12: Konfigurasi Pemblokiran ICMP

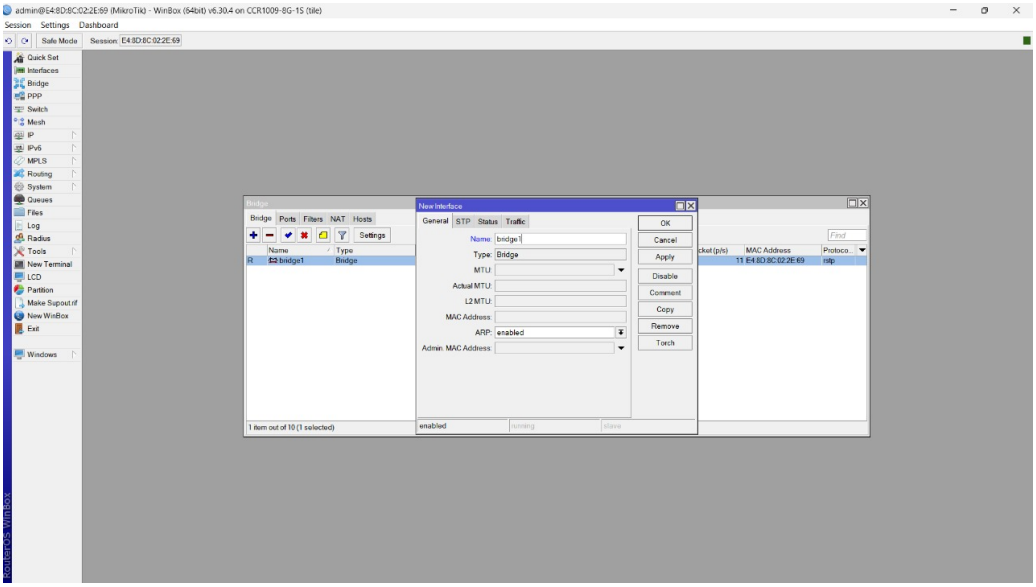
Untuk pemblokiran akses situs web berdasarkan konten atau content blocking bisa dengan mengatur :

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



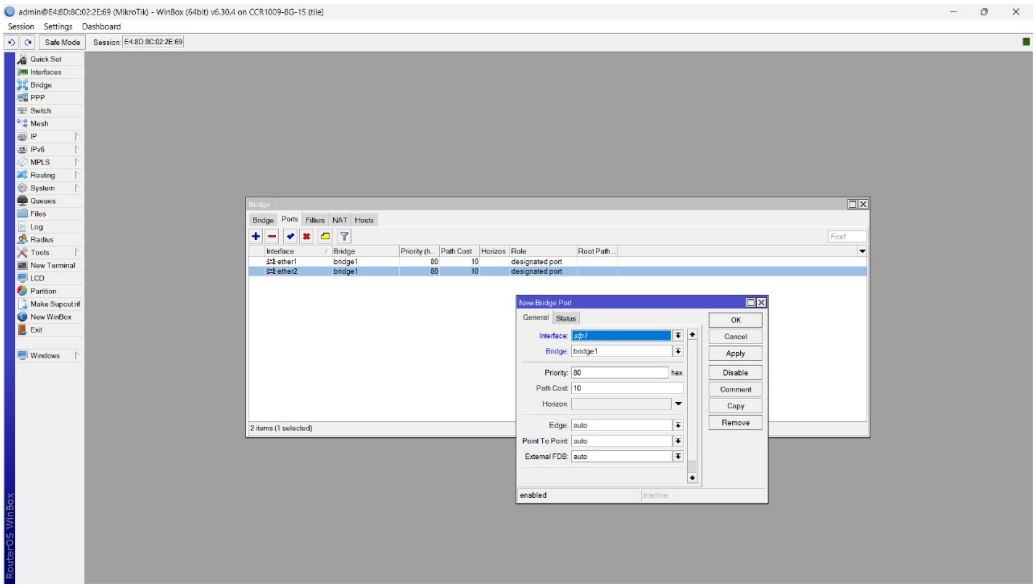
Gambar 13: Konfigurasi Content Blocking

Kemudian lakukan konfigruasi bridge pada Router B (Hub) dengan mengakses menu bridge, klik "+", "apply", dan "ok".



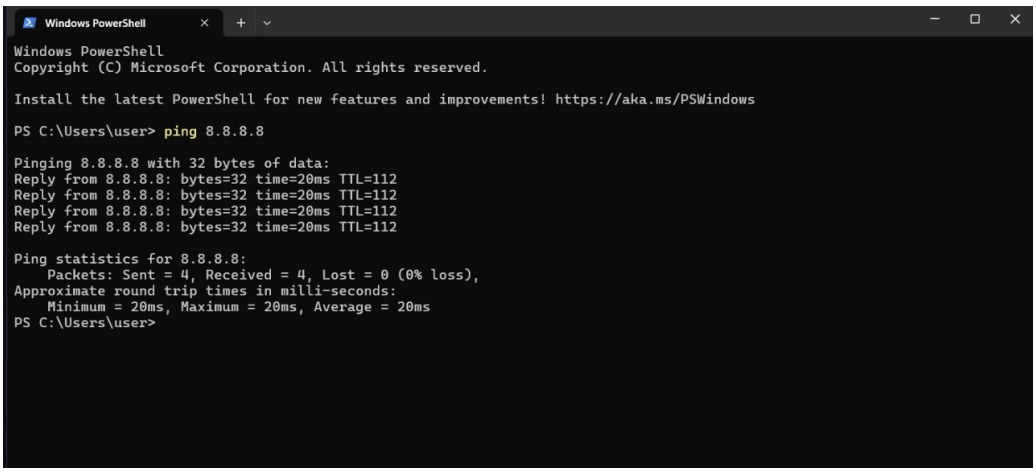
Gambar 14: Konfigurasi Bridge pada Router B

Lalu tambahkan port dalam bridge yang sudah dibuat dengan mengakses menu bridge lalu port, klik "+", pilih interface yang terhubung ke perangkat laptop, dan pilih interface yangn terhubung ke Router A.



Gambar 15: Konfigurasi Port dalam Bridge

Setelah itu, lakukan konfigurasi alamat IP pada laptop dengan IP yang sudah diatur tadi dan lakukan pinging untuk menguji konektivitas ICMP dengan ping 8.8.8.8 pada command prompt.



Gambar 16: Pengujian Konektivitas ICMP

Hasil menunjukkan Request Timed Out (RTO) yang menandakan firewall sudah aktif. Untuk pengujian pemblokiran konten bisa dilakukan dengan melakukan browsing speedtest seperti pada gambar berikut.

Gambar 17: Pengujian Content Blocking

2 Analisis Hasil Percobaan

Selama praktikum, semua tahapan konfigurasi berhasil dijalankan sesuai petunjuk. Setelah dilakukan pengaturan DHCP, NAT, dan firewall, perangkat klien bisa mendapatkan IP secara otomatis dan

terkoneksi ke internet. Pada saat firewall ICMP diaktifkan, hasil ping ke 8.8.8.8 menunjukkan Request Timed Out, yang berarti rule firewall sudah berjalan dengan benar. Begitu juga saat mencoba mengakses situs "speedtest", halaman gagal dimuat, sesuai dengan rule content blocking yang telah dibuat. Dari hasil ini, bisa disimpulkan bahwa konfigurasi firewall dapat digunakan untuk membatasi jenis trafik tertentu. Walaupun sempat terjadi kebingungan pada pemilihan interface dan urutan langkah, namun setelah dicoba ulang dengan teliti, semua fitur dapat berfungsi sebagaimana mestinya.

3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan :

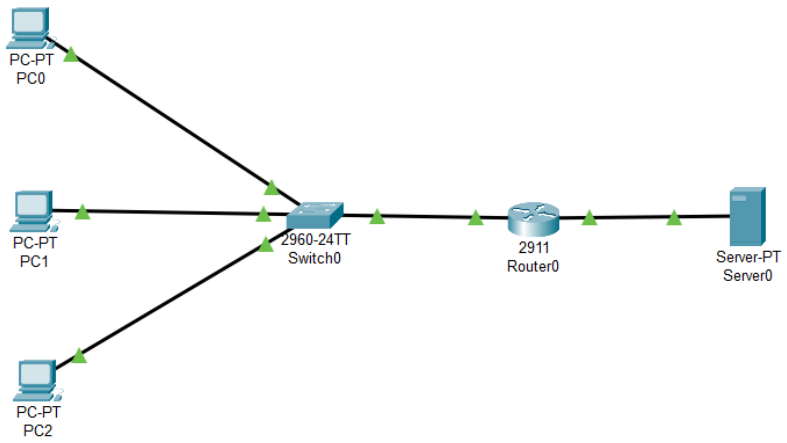
   (a) 1 Router

   (b) 1 Switch

   (c) 3 PC (LAN)

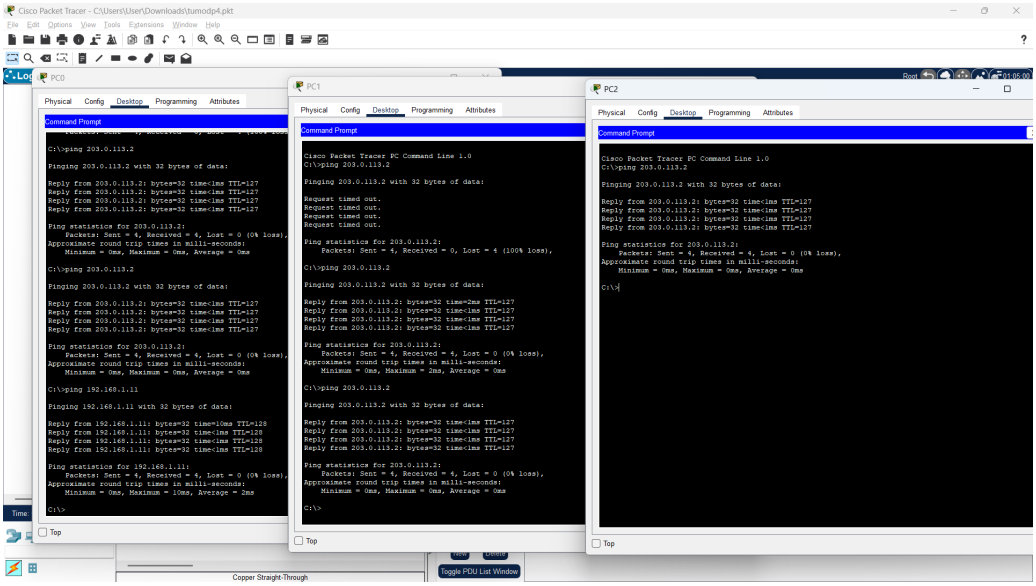
   (d) 1 Server (Internet/Public)

   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: Hasil Ping dari PC0 ke Server

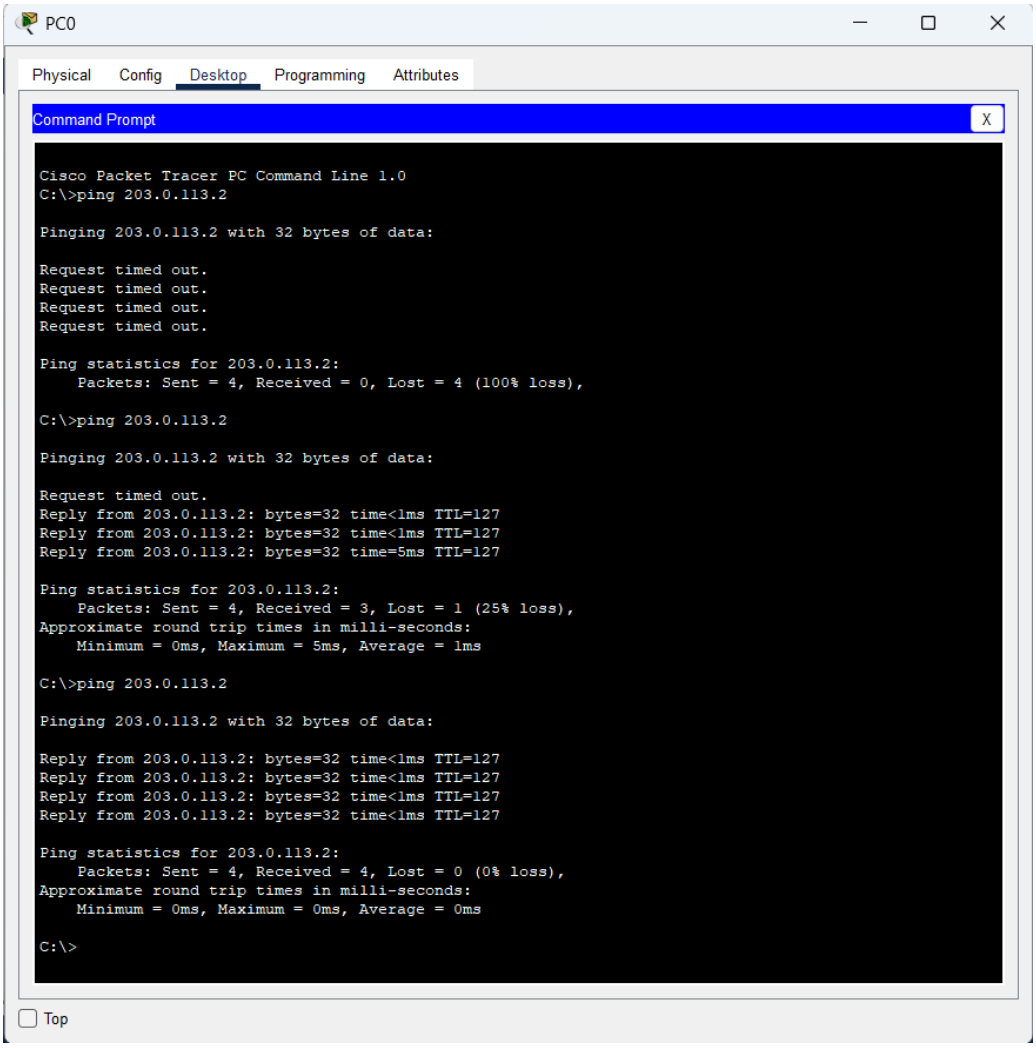
3. Konfigurasi Firewall (ACL) :

   (a) Izinkan hanya PC1 yang dapat mengakses Server.

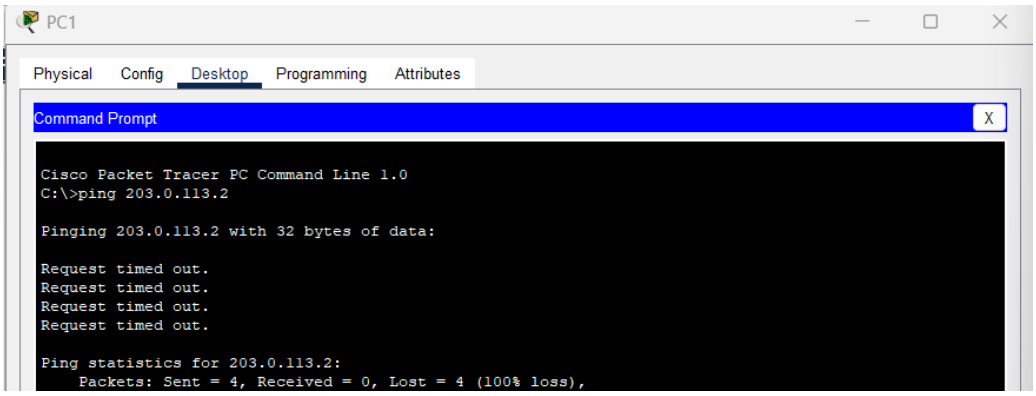
   (b) Blokir PC2 dan PC3 dari mengakses Server.

   (c) Semua PC harus tetap bisa saling terhubung di LAN.

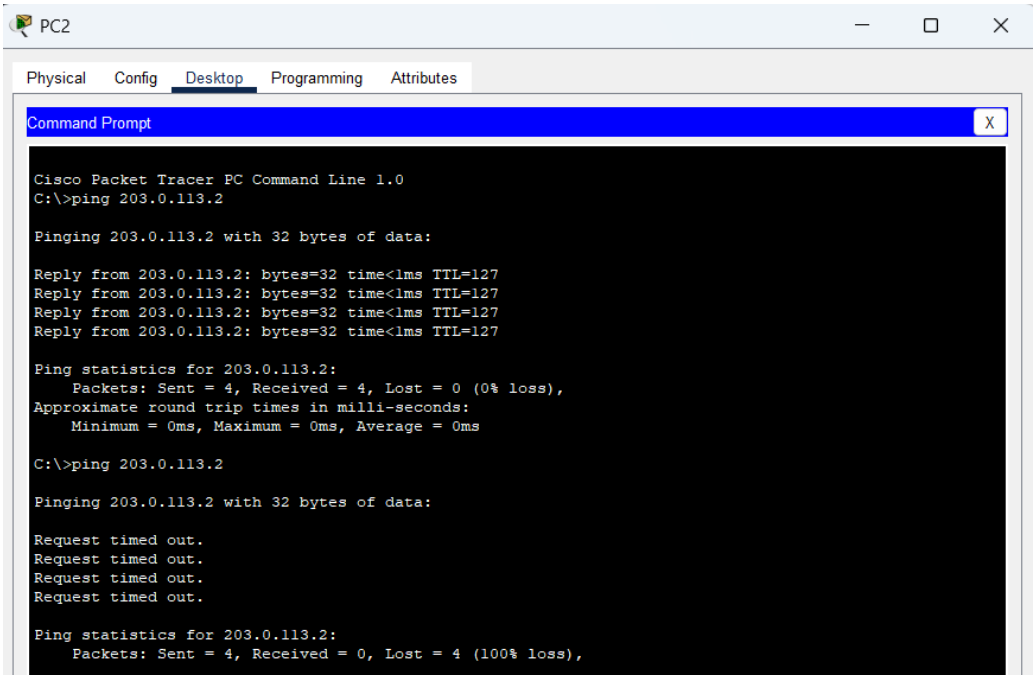
Jawaban : Disini untuk PC1 = PC0 dan PC3 = PC2.



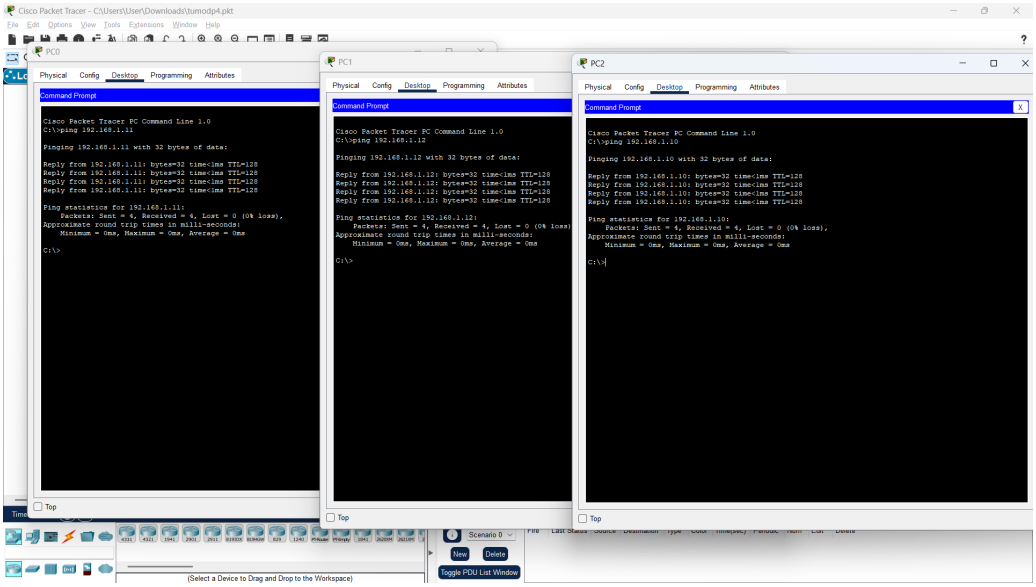
Gambar 20: Hanya PC0 yang Mengakses Server



Gambar 21: PC1 Tidak Bisa Mengakses Server



Gambar 22: PC2 Tidak Bisa Mengakses Server



Gambar 23: Semua PC Saling Terhubung dalam LAN

4 Kesimpulan

Melalui praktikum ini, praktikan dapat mengetahui bagaimana cara kerja NAT dan firewall di MikroTik. NAT memungkinkan perangkat dalam jaringan lokal bisa mengakses internet, sementara firewall digunakan untuk mengatur lalu lintas data, seperti memblokir ping dan akses ke situs tertentu. Semua pengujian menunjukkan hasil yang sesuai dengan teori, dan praktikum ini membantu memperkuat pemahaman tentang bagaimana konfigurasi sederhana bisa memberikan efek besar dalam keamanan dan kontrol jaringan. Praktikum ini juga menekankan pentingnya ketelitian saat konfigurasi, karena kesalahan kecil bisa menyebabkan fungsi jaringan tidak berjalan dengan baik.

5 Lampiran

5.1 Dokumentasi saat praktikum