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

Laporan Akhir
Praktikum Jaringan Komputer

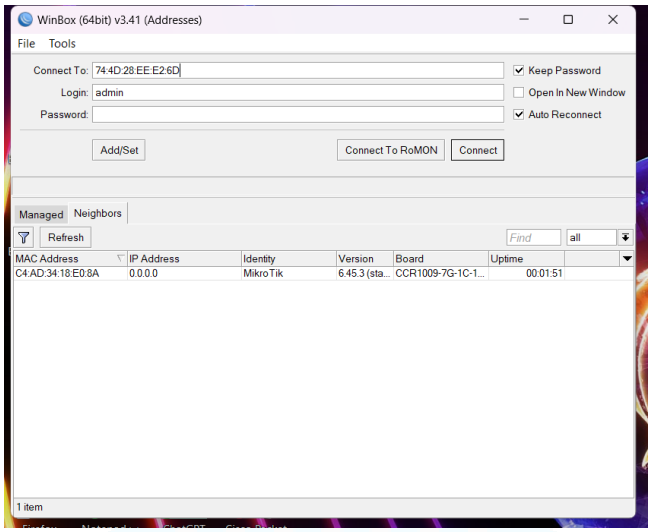
Firewall & NAT

Natania Christin Agustina - 5024231014

2025

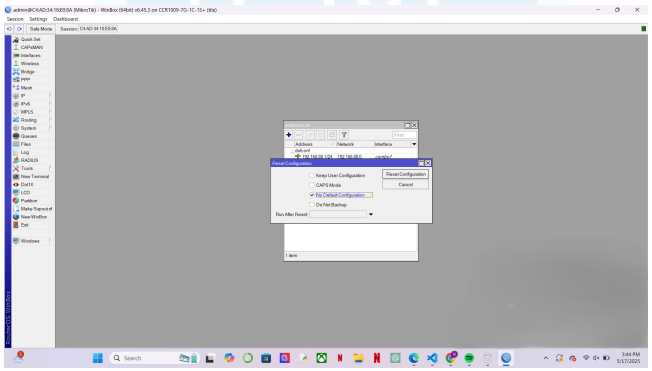
1 Langkah-Langkah Percobaan

- Percobaan Firewall & NAT
  - Nyalakan mikrotik dan hubungkan dengan laptop, login menggunakan winbox.



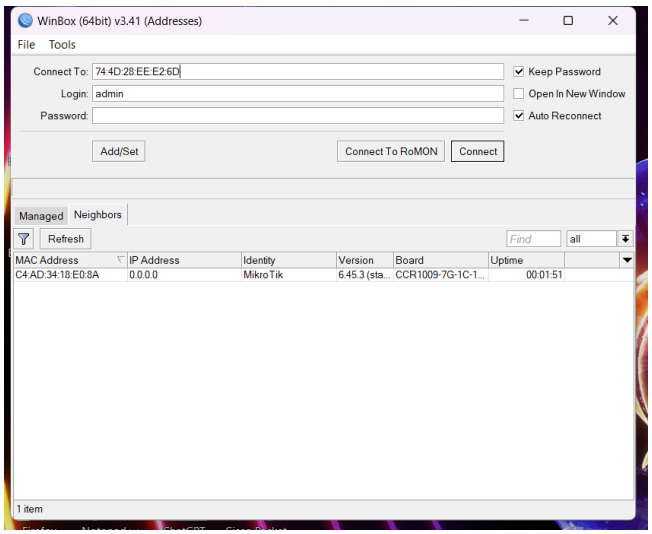
Gambar 1: Masuk Ke Router Menggunakan Winbox

  - Reset mikrotik di pilihan system dan reset configuration, pilih settingan no default configuration kemudian pencet reset konfiguration, tunggu sekitar 3 menit dan mikrotik sudah selesai direset.



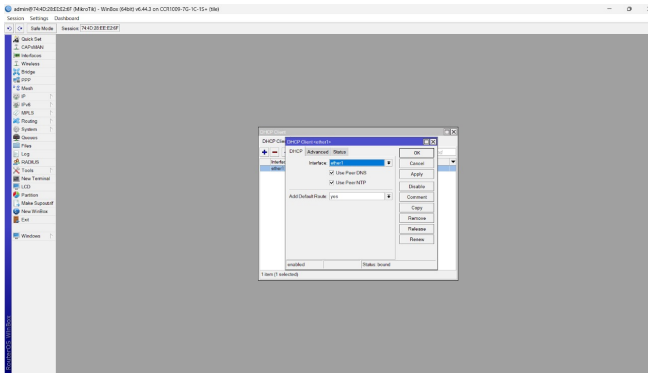
Gambar 2: Reset Router

  - Login lagi ke MikroTik menggunakan Winbox untuk mengakses antarmuka router. Login dapat dilakukan melalui MAC address atau IP default perangkat, dengan menggunakan username "admin" dan tanpa kata sandi jika belum pernah diatur sebelumnya.



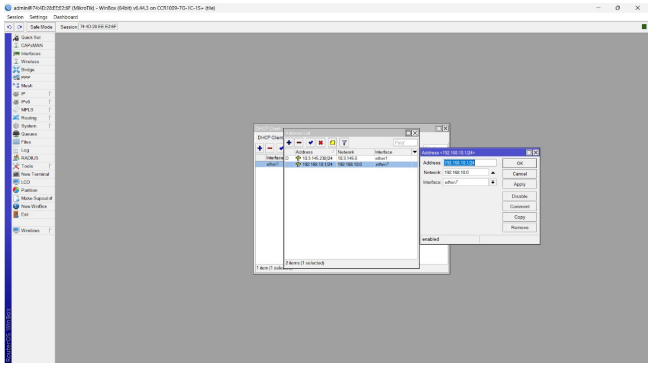
Gambar 3: Masuk Ke Router Menggunakan Winbox

– Kemudian lakukan konfigurasi DHCP Client pada Router A, langkah pertama adalah menyambungkan kabel internet ke interface ether1. Setelah itu, buka aplikasi Winbox dan navigasikan ke menu IP > DHCP Client. Tambahkan konfigurasi baru dengan mengklik ikon "+", lalu pilih interface "ether1" sebagai jalur koneksi yang akan menggunakan DHCP. Setelah selesai, klik tombol "Apply" dan periksa status koneksi. Jika status menunjukkan "bound", berarti Router A telah berhasil memperoleh alamat IP secara otomatis dari server DHCP.



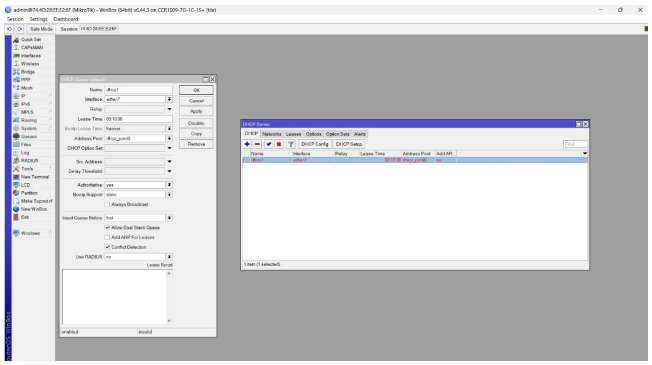
Gambar 4: Konfigurasi DHCP Ether 1

– Selanjutnya, lakukan penambahan alamat IP pada interface ether7 untuk keperluan konektivitas dengan Switch. Buka aplikasi Winbox, lalu navigasikan ke menu IP > Addresses. Tambahkan entri baru dengan mengklik ikon "+", kemudian masukkan alamat IP 192.168.10.1/24 pada kolom Address. Setelah itu, pilih interface "ether7" sebagai jalur yang akan digunakan. Jika sudah, klik tombol "Apply" lalu "OK" untuk menyimpan konfigurasi.



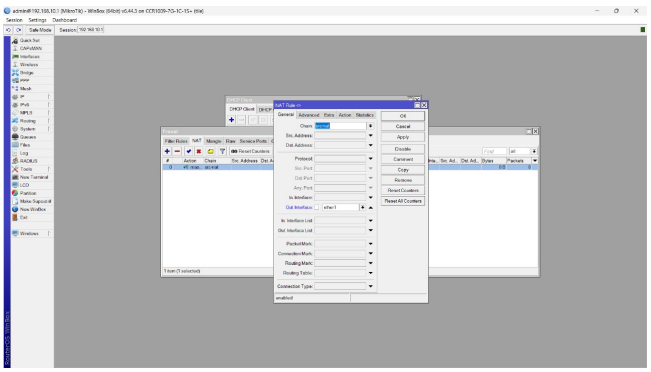
Gambar 5: Konfigurasi IP Address Ether 7

– Setelah itu, lakukan konfigurasi DHCP Server pada Router MikroTik untuk mendistribusikan alamat IP secara otomatis kepada perangkat klien yang terhubung. Buka aplikasi Winbox dan masuk ke menu IP > DHCP Server, lalu klik tombol "DHCP Setup". Pada jendela pertama, pilih interface yang akan digunakan untuk mendistribusikan IP, misalnya "ether7" jika terhubung ke switch atau perangkat klien, lalu klik "Next". Di langkah berikutnya, verifikasi alamat jaringan yang akan digunakan, seperti 192.168.10.0/24, kemudian lanjutkan dengan menekan "Next". Setelah itu, pastikan gateway yang diberikan kepada klien sesuai, misalnya 192.168.10.1, lalu klik "Next". Tentukan rentang alamat IP yang akan dibagikan, misalnya dari 192.168.10.2 hingga 192.168.10.254, kemudian klik "Next". Masukkan alamat DNS server, seperti 8.8.8.8 dan 8.8.4.4, lalu lanjutkan. Pada bagian lease time, atur waktu sewa IP, contohnya 00:10:00 untuk durasi 10 menit, dan klik "Next". Setelah semua tahap selesai, akan muncul pesan "Setup has completed successfully", lalu klik "OK" untuk mengakhiri konfigurasi.

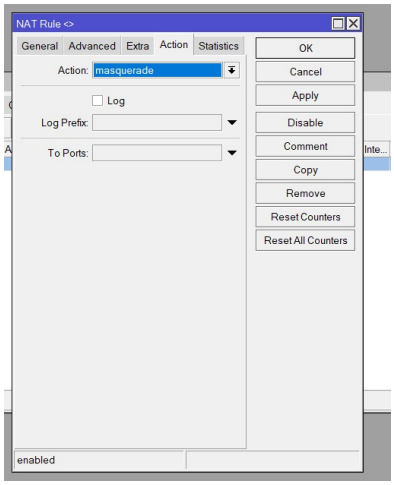


Gambar 6: Konfigurasi DHCP Server

– Langkah berikutnya adalah melakukan konfigurasi NAT (Network Address Translation) agar perangkat klien dapat terhubung ke internet. Buka aplikasi Winbox, lalu masuk ke menu IP > Firewall > NAT. Tambahkan aturan baru dengan mengklik ikon "+", kemudian pada tab "General", atur bagian Chain menjadi "src-nat". Setelah itu, pindah ke tab "Action" dan pilih "masquerade" sebagai jenis tindakan yang akan dilakukan. Jika semua sudah sesuai, klik tombol "Apply" lalu "OK" untuk menyimpan pengaturan. Untuk memastikan NAT telah berfungsi, buka Terminal di Winbox dan lakukan pengujian koneksi internet dengan mengetik perintah ‘ping 8.8.8.8‘, lalu pastikan perangkat mendapatkan balasan (reply).

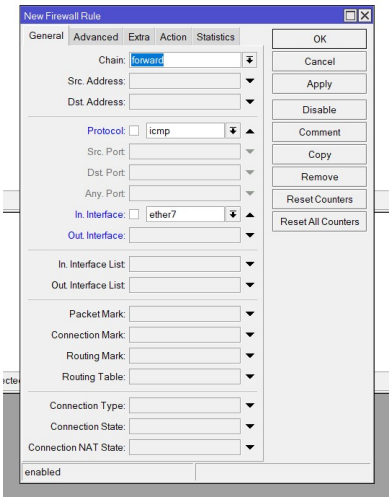


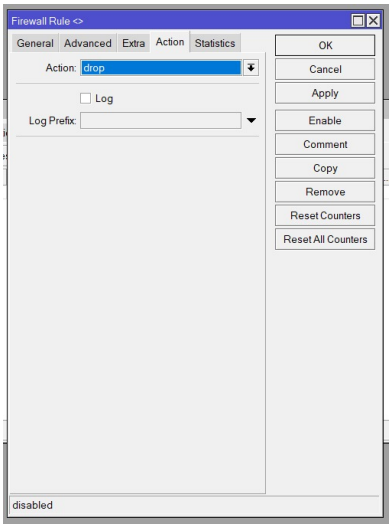
Gambar 7: Konfigurasi NAT



Gambar 8: Konfigurasi Action Pada NAT

– Selanjutnya, lakukan konfigurasi firewall dengan menambahkan aturan filter untuk mengatur lalu lintas jaringan. Buka Winbox dan masuk ke menu IP > Firewall > Filter Rules, kemudian klik ikon "+" untuk menambahkan aturan baru. Untuk memblokir protokol ICMP, pada tab "General" atur Chain menjadi "forward", pilih Protocol "icmp", dan tentukan In. Interface sebagai "ether7". Pada tab "Action", pilih tindakan "drop" untuk memblokir paket tersebut. Selanjutnya, untuk memblokir akses situs web berdasarkan konten, buat aturan baru dengan mengatur Chain pada tab "General" menjadi "forward", Protocol "tcp", Dst. Port "80,443" untuk HTTP dan HTTPS, serta atur In. Interface menjadi "ether7" dan Out. Interface "ether1". Pada tab "Advanced", masukkan kata kunci "speedtest" pada kolom Content untuk memfilter konten tersebut. Terakhir, pada tab "Action" pilih "drop" agar akses dengan konten tersebut diblokir. Simpan pengaturan dengan klik "Apply" dan "OK".

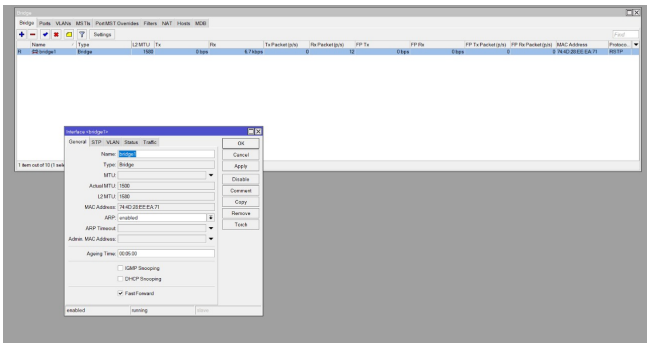




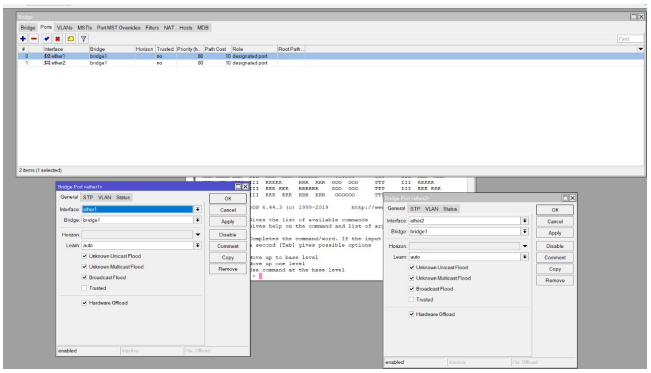
Gambar 9: Konfigurasi Firewall **Gambar 10:** Konfigurasi Firewall

– Lakukan konfigurasi bridge pada Router B untuk mengubah fungsinya menjadi hub. Buka menu Bridge di Winbox, lalu klik ikon "+" untuk membuat bridge baru. Setelah itu, klik "Apply" dan "OK" untuk menyimpan konfigurasi bridge tersebut. Selanjutnya, tambahkan port ke dalam bridge yang telah dibuat dengan membuka menu Bridge > Port. Klik ikon "+",

kemudian pilih interface yang terhubung ke perangkat laptop serta interface yang menghubungkan Router B ke Router A. Dengan pengaturan ini, Router B akan berfungsi sebagai hub yang menghubungkan kedua perangkat tersebut dalam satu jaringan.

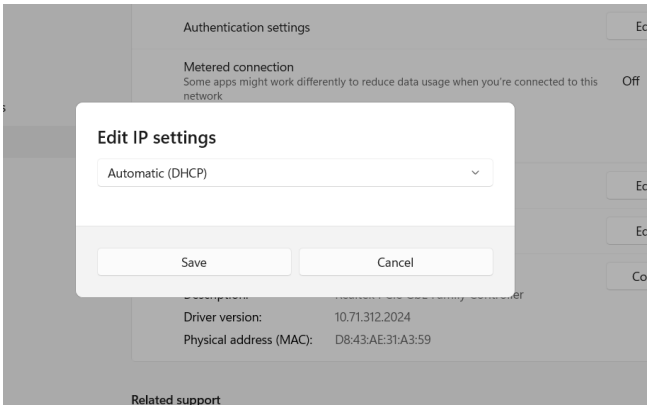


Gambar 11: Konfigurasi Bridge



Gambar 12: Konfigurasi Bridge

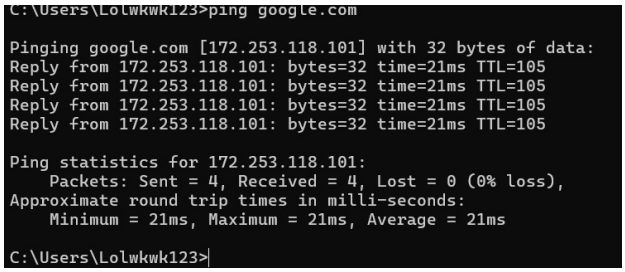
– Pastikan pengaturan alamat IP pada laptop diset secara otomatis menggunakan DHCP agar mendapatkan alamat IP secara dinamis. Untuk melakukannya, buka pengaturan jaringan di sistem operasi laptop melalui menu Settings atau Control Panel, lalu pastikan opsi konfigurasi IP diatur ke DHCP (Automatic). Setelah itu, buka Command Prompt (CMD) dan jalankan perintah ipconfig untuk memeriksa dan memastikan alamat IP telah berhasil diterima oleh laptop dari server DHCP.



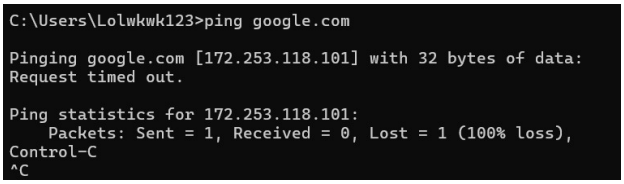
Gambar 13: Konfigurasi Settingan DHCP Laptop

– Lakukan pengujian terhadap konfigurasi yang telah diterapkan untuk memastikan semu-

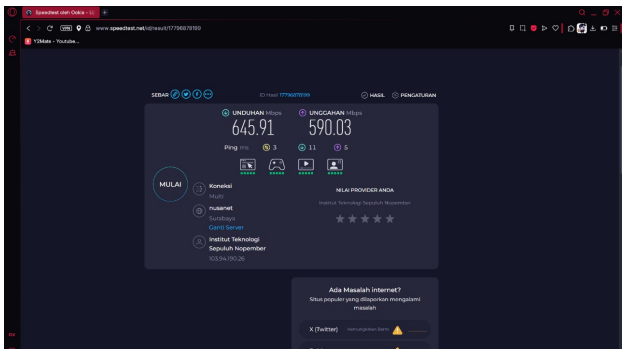
anya berfungsi dengan baik. Untuk pengujian konektivitas menggunakan protokol ICMP, buka Terminal pada laptop dan jalankan perintah ping 8.8.8.8. Saat firewall ICMP aktif, Anda akan mendapatkan respon Request Timed Out (RTO). Untuk menguji lebih lanjut, nonaktifkan aturan firewall ICMP dengan menekan tanda "X" pada aturan terkait di Filter Rules, lalu ulangi perintah ping. Kali ini koneksi seharusnya berhasil dan terhubung. Selanjutnya, untuk pengujian pemblokiran konten, coba akses situs yang mengandung kata kunci "speedtest" seperti www.speedtest.net menggunakan browser. Jika firewall konten aktif, situs tersebut tidak akan dapat diakses atau akan terus memuat tanpa menampilkan isi, menandakan firewall bekerja dengan baik. Kemudian, nonaktifkan aturan firewall konten dengan menekan tanda "X" pada aturan yang sesuai di Filter Rules dan coba akses kembali situs tersebut; sekarang Anda seharusnya dapat mengaksesnya dengan normal.



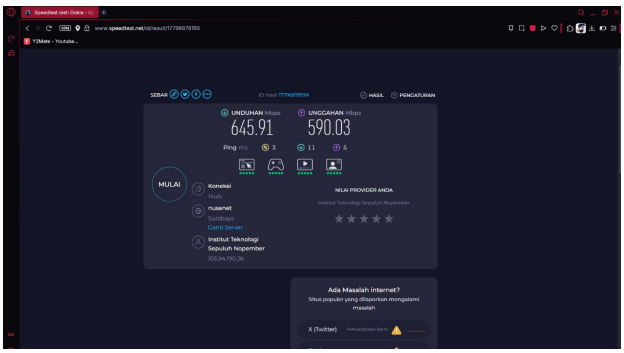
Gambar 14: Hasil Ping Pada CMD Laptop Saat Firewall Mati



Gambar 15: Hasil Ping Pada CMD Laptop Saat Firewall Nyala



Gambar 16: Hasil Pengujian Speedtest Saat Firewall Mati



Gambar 17: Hasil Pengujian Speedtest Saat Firewall Nyala Yang Tetap Tembus

2 Analisis Hasil Percobaan

- Percobaan Firewall & NAT :
  Pada awal percobaan, terdapat kendala saat menyambungkan router ke perangkat laptop dimana router sering keluar dan tidak terdeteksi di Winbox, sehingga perlu beberapa kali percobaan agar koneksi stabil dan router terbaca dengan benar. Setelah berhasil masuk, konfigurasi DHCP Client, DHCP Server, NAT, dan bridge dapat dilakukan sesuai prosedur. NAT dengan metode masquerade berhasil memungkinkan perangkat klien mengakses internet, dibuktikan dengan ping 8.8.8.8 yang mendapatkan balasan. Firewall yang dikonfigurasi untuk memblokir ICMP terbukti efektif, karena saat aturan aktif ping ke 8.8.8.8 menghasilkan Request Timed Out (RTO), dan saat aturan dinonaktifkan ping kembali normal. Namun, pada pengujian pemblokiran akses situs web berdasarkan konten (misalnya situs dengan kata kunci "speedtest"), meskipun aturan firewall telah diaktifkan, akses ke situs tersebut masih berhasil tembus dan dapat dibuka, menunjukkan bahwa filter konten firewall belum bekerja maksimal. Konfigurasi bridge pada Router B berjalan lancar sehingga Router B dapat berfungsi sebagai hub untuk menghubungkan laptop dan Router A. Pengaturan IP otomatis melalui DHCP di laptop juga berhasil, sehingga laptop mendapatkan alamat IP dari server DHCP MikroTik secara dinamis. Secara keseluruhan, konfigurasi firewall dan NAT berjalan sesuai fungsi dasar, namun filter konten membutuhkan penyesuaian lebih lanjut agar dapat memblokir akses situs secara efektif.

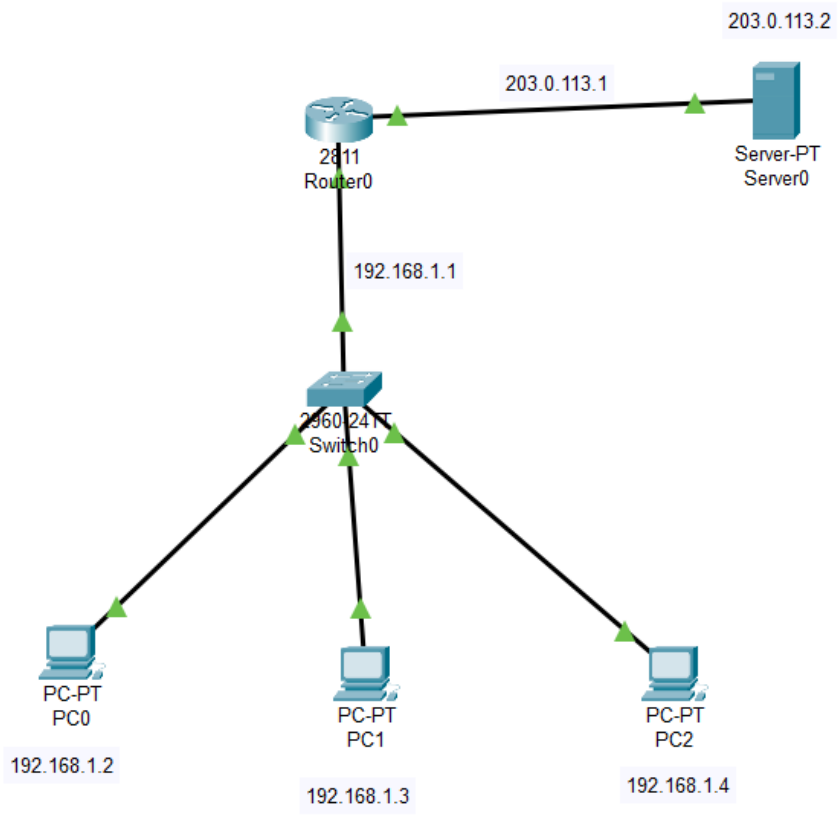
3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:

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

   Jawaban :

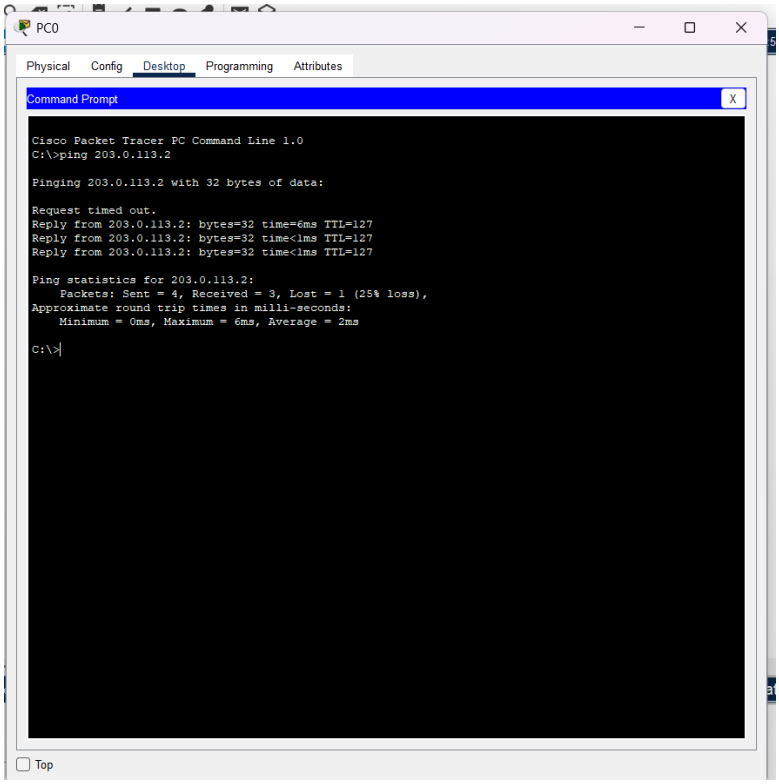
   - Topologi :



Gambar 18: Topologi Sederhana Cisco Packet Tracer

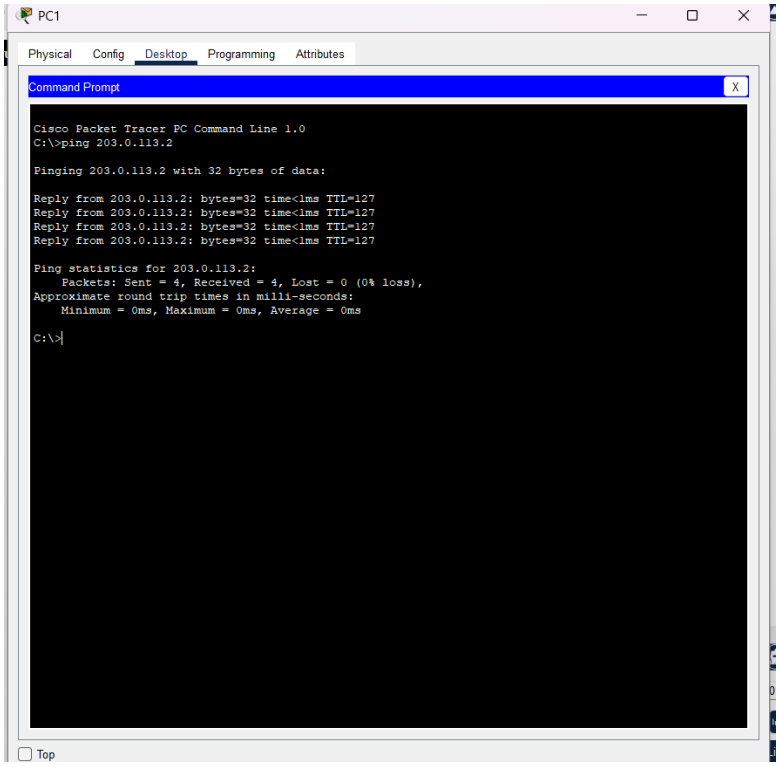
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
   Jawaban :

   - Hasil Ping PC0 ke Server :



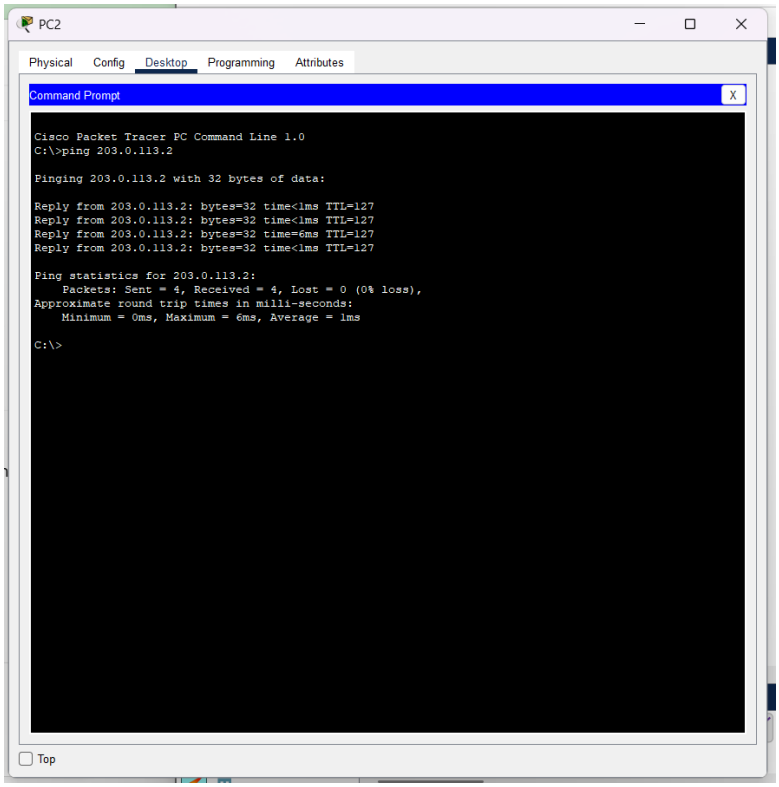
Gambar 19: Hasil Ping PC0 ke Server

- Hasil Ping PC1 ke Server :



Gambar 20: Hasil Ping PC1 ke Server

- Hasil Ping PC2 ke Server :



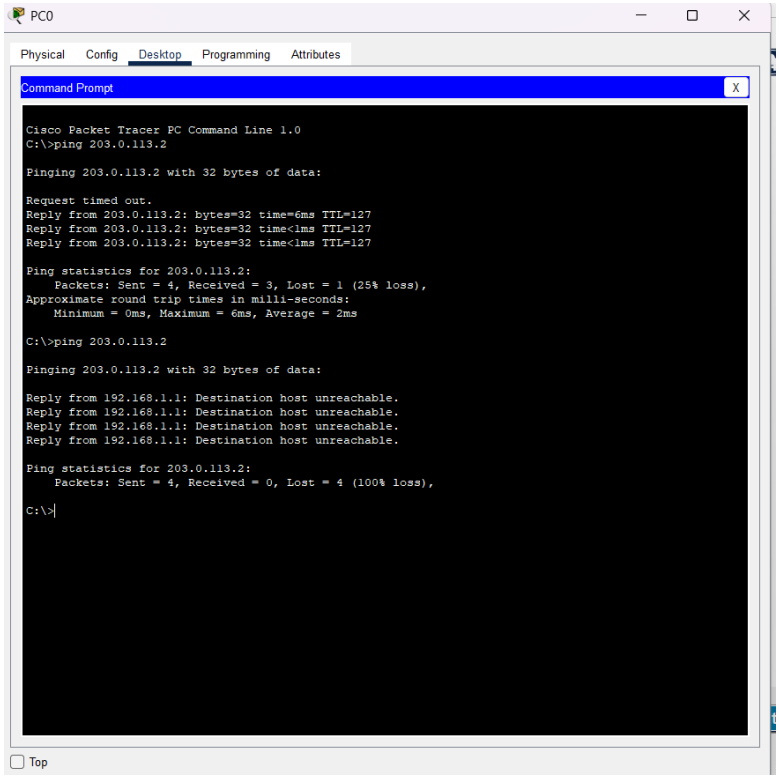
Gambar 21: Hasil Ping PC2 ke Server

3. Konfigurasi Firewall (ACL):

   - Izinkan hanya PC1 yang dapat mengakses Server.
   - Blokir PC1 dan PC3 dari mengakses Server.
   - Semua PC harus tetap bisa saling terhubung di LAN.

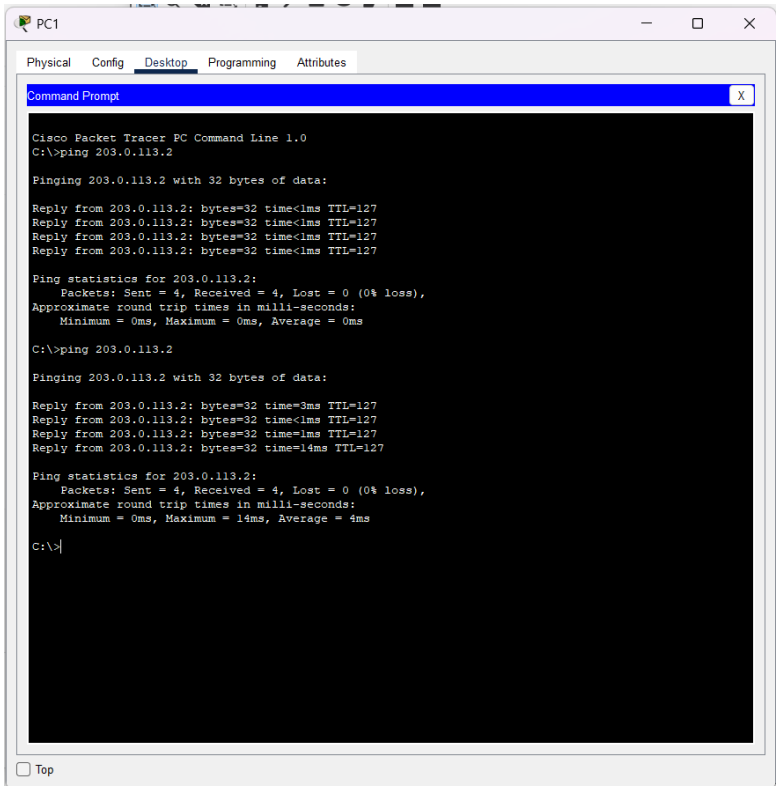
   Uji koneksi menggunakan ping dan dokumentasikan hasilnya.
   Jawaban :

   - Hasil Ping PC0 ke Server :



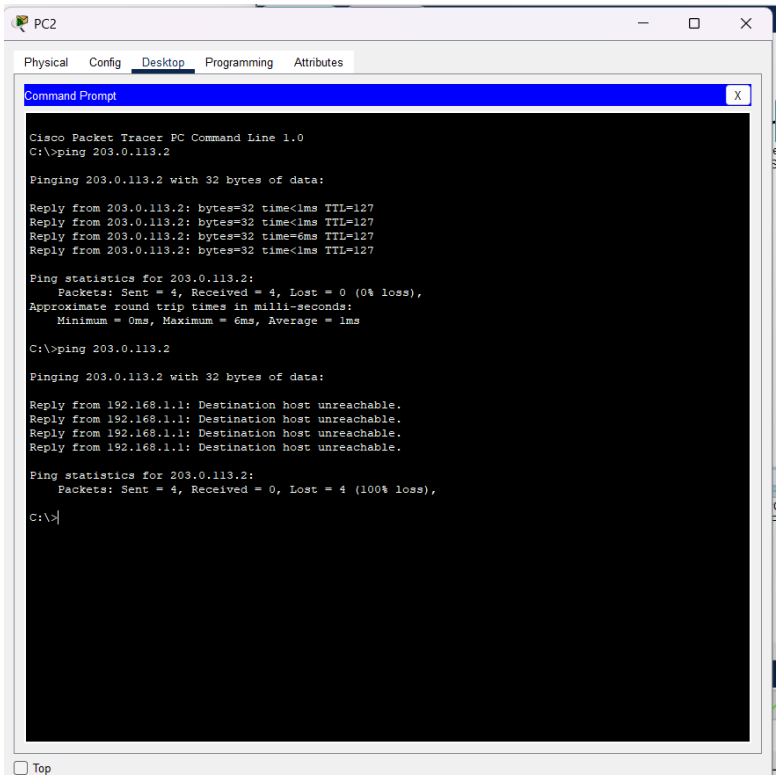
Gambar 22: Hasil Ping PC0 ke Server

- Hasil Ping PC1 ke Server :



Gambar 23: Hasil Ping PC1 ke Server

- Hasil Ping PC2 ke Server :



Gambar 24: Hasil Ping PC2 ke Server

4 Kesimpulan

Pada praktikum ini, konfigurasi NAT dan firewall menggunakan MikroTik berhasil dilakukan dengan cukup baik. Proses dimulai dengan reset router, pemberian IP address, serta pengaktifan DHCP Client dan Server untuk mengelola distribusi alamat IP secara otomatis. Konfigurasi NAT dengan metode masquerade berhasil memungkinkan perangkat klien terhubung ke internet. Pada tahap pengujian konektivitas menggunakan perintah ping firewall berhasil memblokir ICMP sesuai konfigurasi, yang ditunjukkan dengan munculnya Request Timed Out saat aturan aktif, dan reply saat aturan dinonaktifkan. Namun, pada percobaan pemblokiran konten berbasis kata kunci (seperti "speedtest"), meskipun aturan telah ditambahkan pada filter rules, akses terhadap situs web target masih dapat dilakukan, menandakan bahwa filter berbasis konten belum bekerja optimal. Praktikum ini juga sempat mengalami kendala teknis saat awal konfigurasi, yaitu router yang terhubung ke laptop tidak terbaca dengan stabil di Winbox karena perangkat sering terputus (disconnect) sendiri, namun hal tersebut dapat diatasi. Secara keseluruhan, praktikum ini memberikan pemahaman penting terkait penerapan NAT dan firewall di jaringan MikroTik, mulai dari dasar pengelolaan IP hingga pembatasan akses lalu lintas. Praktikum ini menekankan pentingnya ketelitian dalam setiap konfigurasi serta pemahaman lebih dalam mengenai logika filtering lalu lintas untuk menjamin keamanan dan efektivitas jaringan.

5 Lampiran

5.1 Dokumentasi saat Praktikum

- Dokumentasi saat Praktikum

(a) Dokumentasi Selesai Praktikum