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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

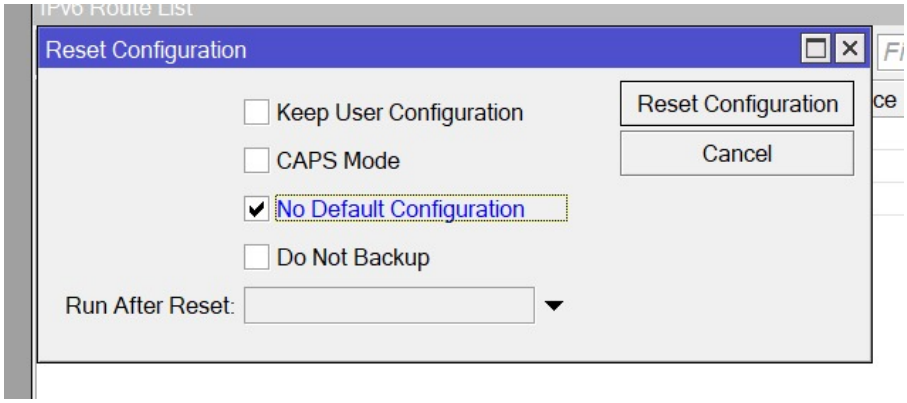
Kenny Joe Neville - 5024231079

2025

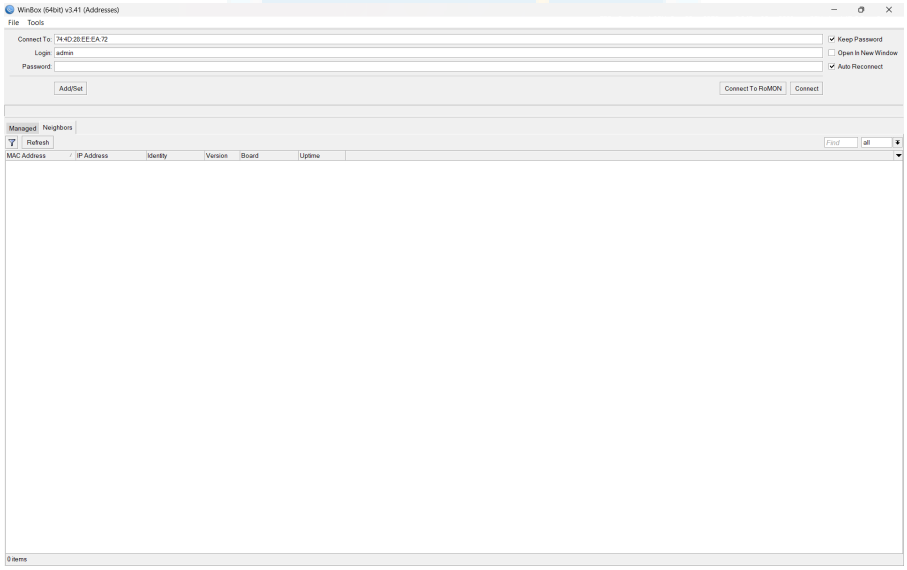
1 Langkah-Langkah Percobaan

1.1 Eksekusi Firewall & NAT

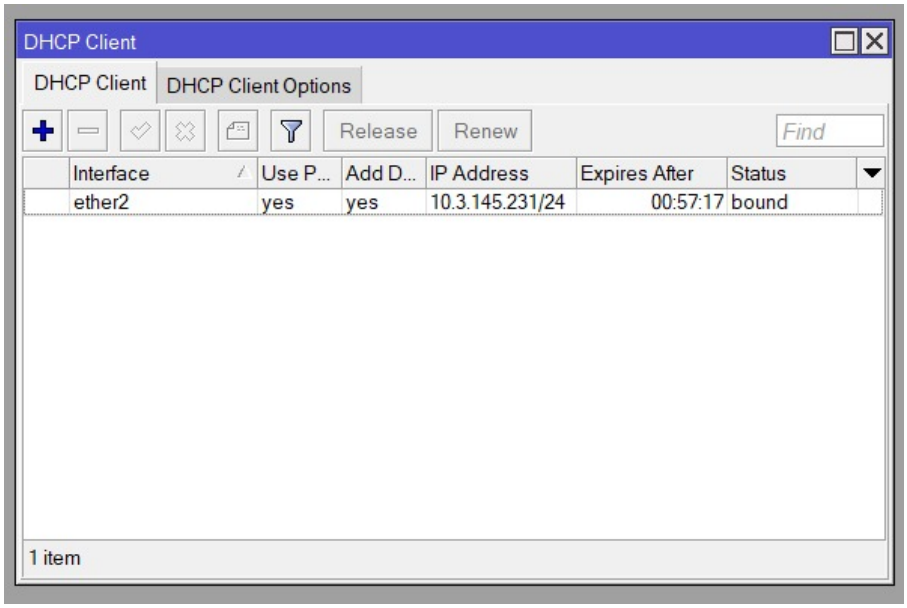
- Reset router terlebih dahulu dengan cara tekan sebuah tool bernama system kemudian pilih reset configuration, Centang bagian No Default Configuration kemudian reset.



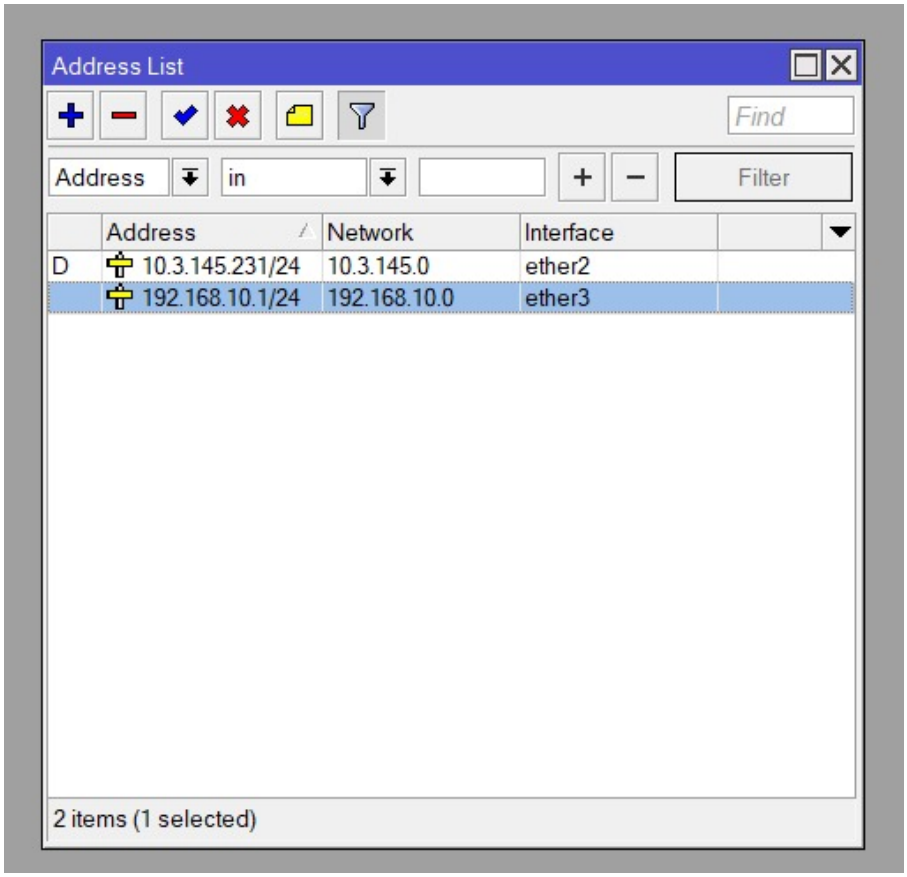
- Login ke router kembali menggunakan winbox untuk mengakses router.



- Buka IP > DHCP Client, klik "+", pilih interface "ether2", lalu klik "Apply" dan pastikan statusnya "bound".

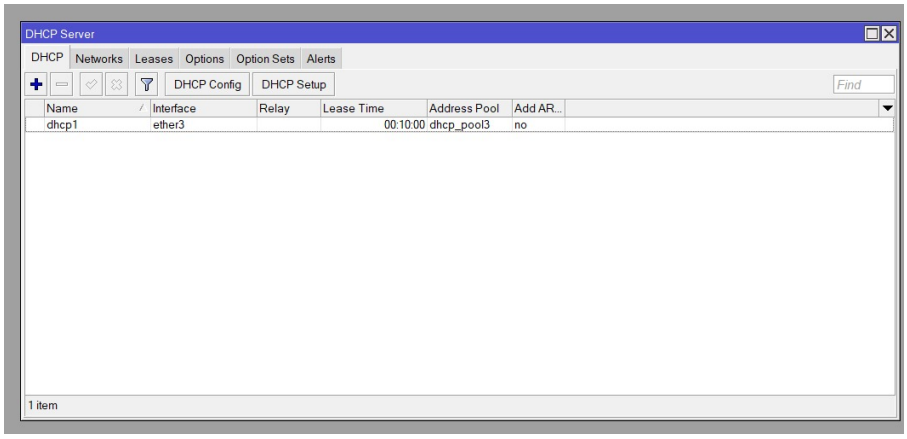


- Buka IP > Addresses, klik "+", isi Address: 192.168.10.1/24, pilih Interface "ether7", lalu klik "Apply" dan "OK

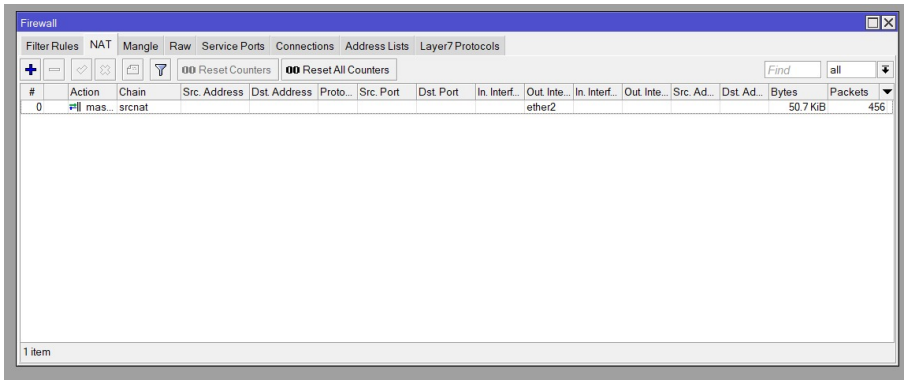


- Untuk mengatur DHCP Server, buka menu IP > DHCP Server dan klik "DHCP Setup". Pilih interface yang akan digunakan, misalnya "ether7", lalu klik Next. Verifikasi address space (contoh: 192.168.10.0/24), gateway (192.168.10.1), dan rentang IP yang akan dibagikan (192.168.10.2–192.168.10.254), kemudian lanjutkan dengan klik Next di setiap langkah. Masukkan DNS Server seperti 8.8.8.8 dan 8.8.4.4, lalu atur lease time sesuai kebutuhan, misalnya 10 menit (00:10:00). Setelah semua langkah selesai, akan muncul pesan "Setup has completed

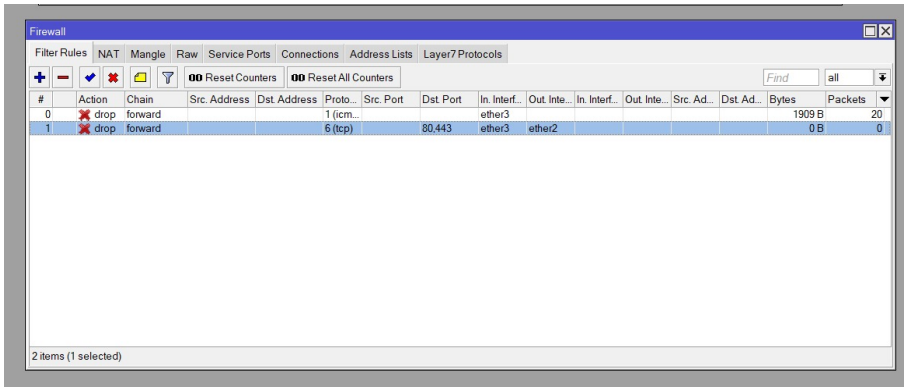
successfully", klik "OK" untuk mengakhiri proses.



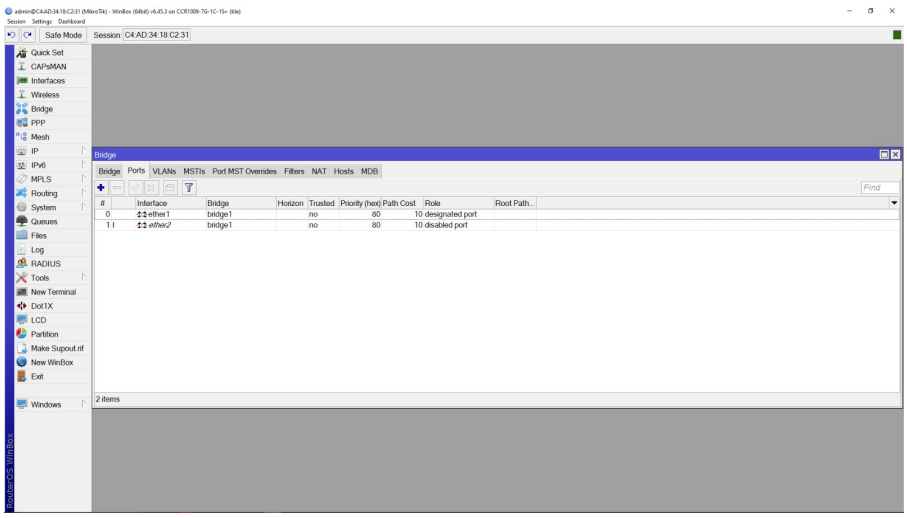
- Buka IP > Firewall > NAT, klik "+", atur Chain ke "src-nat" di tab General, lalu pilih Action "masquerade". Klik "Apply" dan "OK". Untuk uji coba, buka Terminal dan jalankan ping 8.8.8.8, pastikan ada reply.



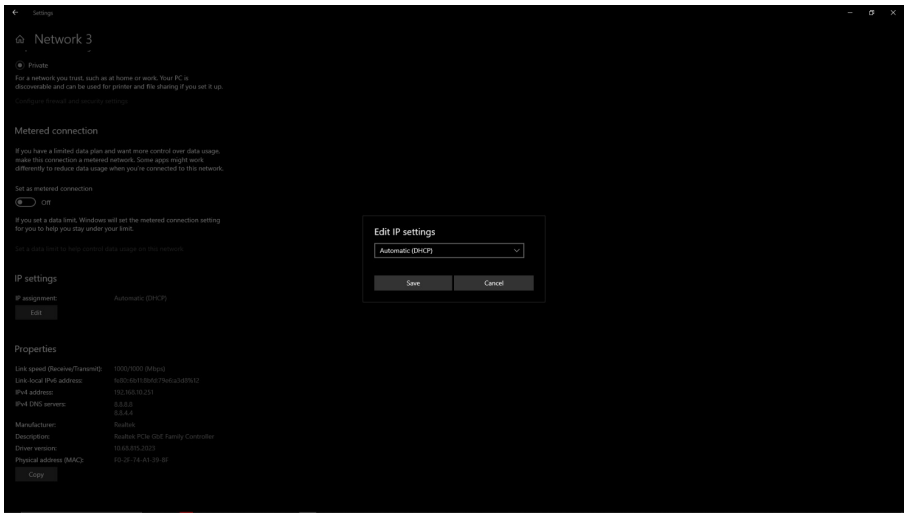
- Buka IP > Firewall > Filter Rule, lalu klik "+" untuk menambah rule baru.
- Di tab General, set Chain ke "forward", Protocol ke "icmp", dan In. Interface ke "ether7". Di tab Action, pilih "drop".

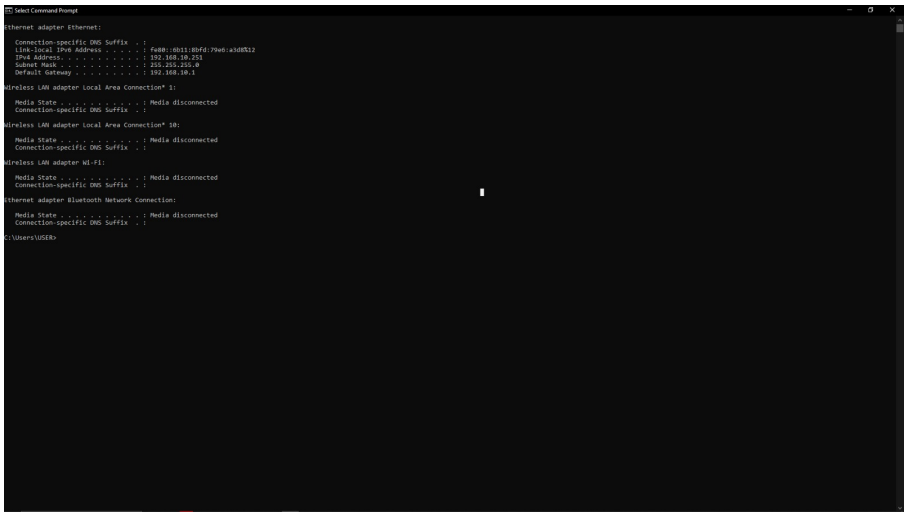


- Buka menu Bridge, klik "+", lalu klik "Apply" dan "OK", untuk membuat bridge baru.
- Buka Bridge > Port, klik "+", lalu tambahkan interface yang terhubung ke laptop dan Router A.

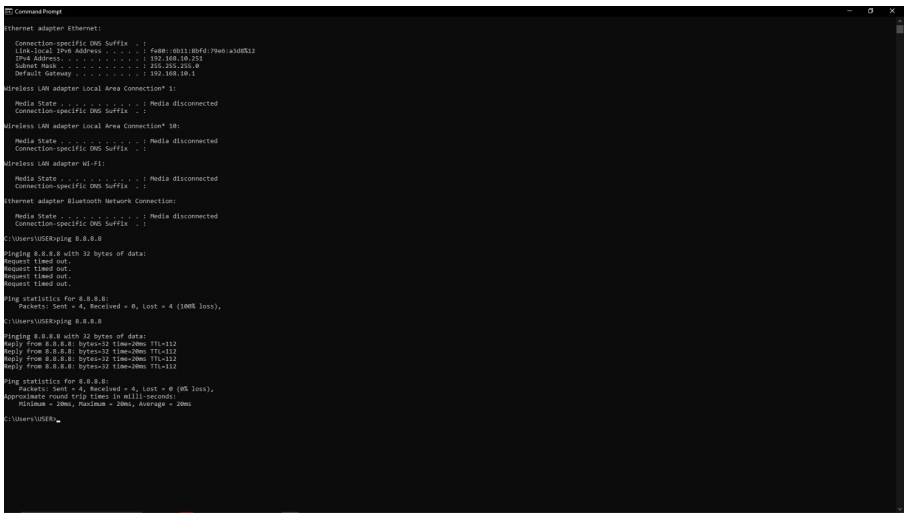


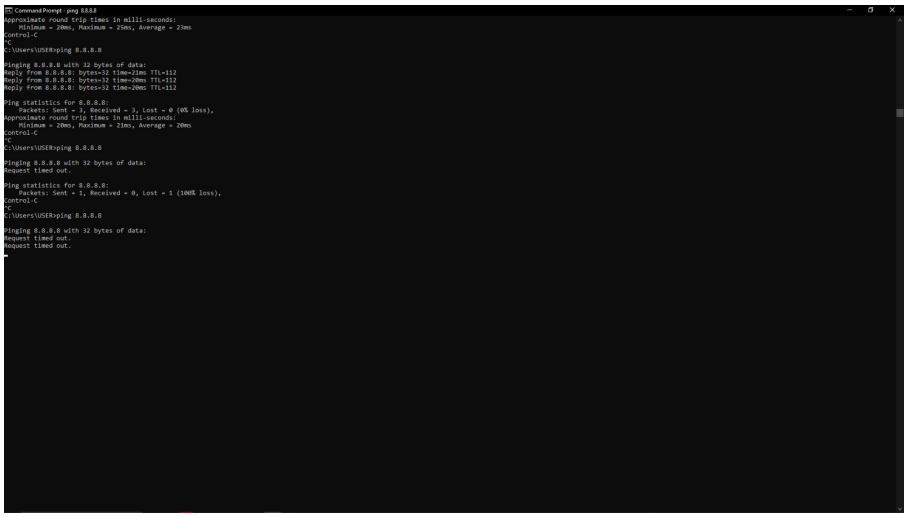
- Di pengaturan jaringan laptop, pastikan mode DHCP aktif. Buka CMD dan ketik ‘ipconfig‘ untuk cek alamat IP yang diterima.



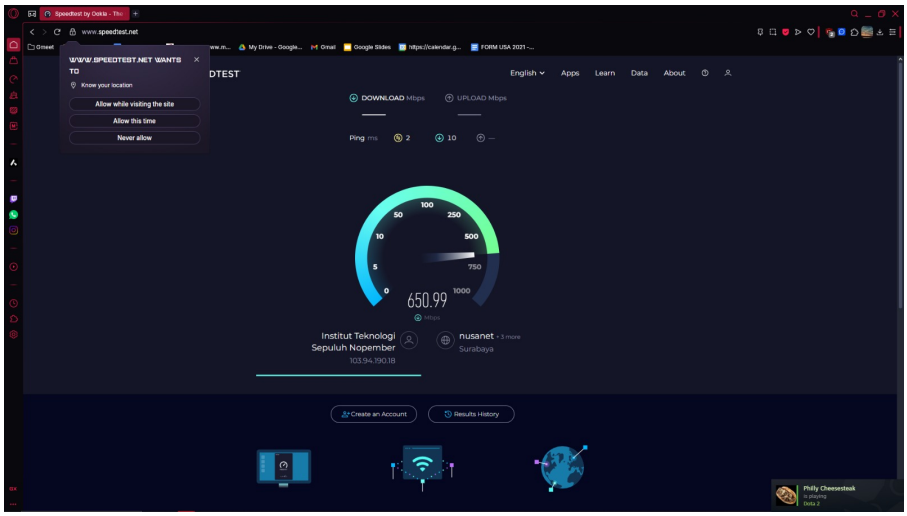


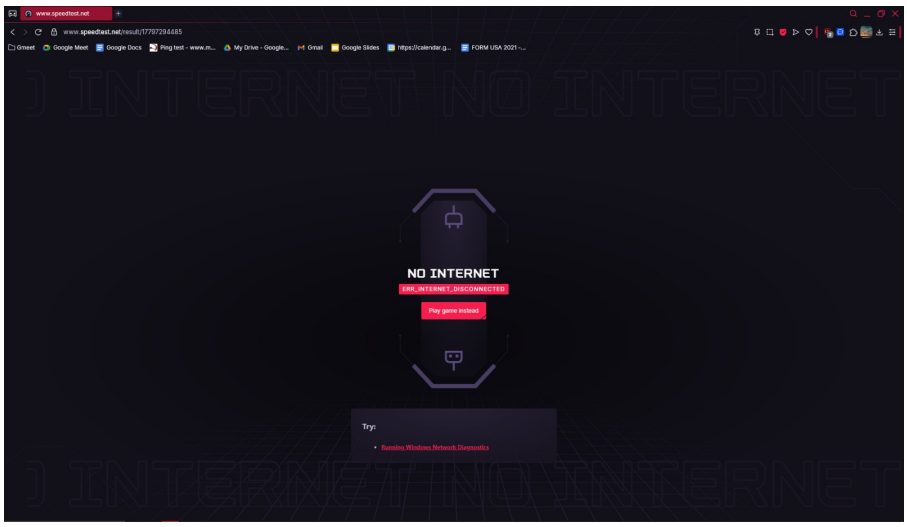
- Buka Terminal laptop dan jalankan ‘ping 8.8.8.8‘. Jika firewall aktif, akan muncul Request Timed Out. Matikan firewall ICMP dengan disable aturan di Filter Rules, lalu ulangi ping, seharusnya berhasil.





- Coba buka situs dengan kata kunci "speedtest" (misal www.speedtest.net). Jika firewall konten aktif, situs tidak akan terbuka. Nonaktifkan aturan firewall di Filter Rules, lalu coba akses lagi, seharusnya situs bisa dibuka normal.





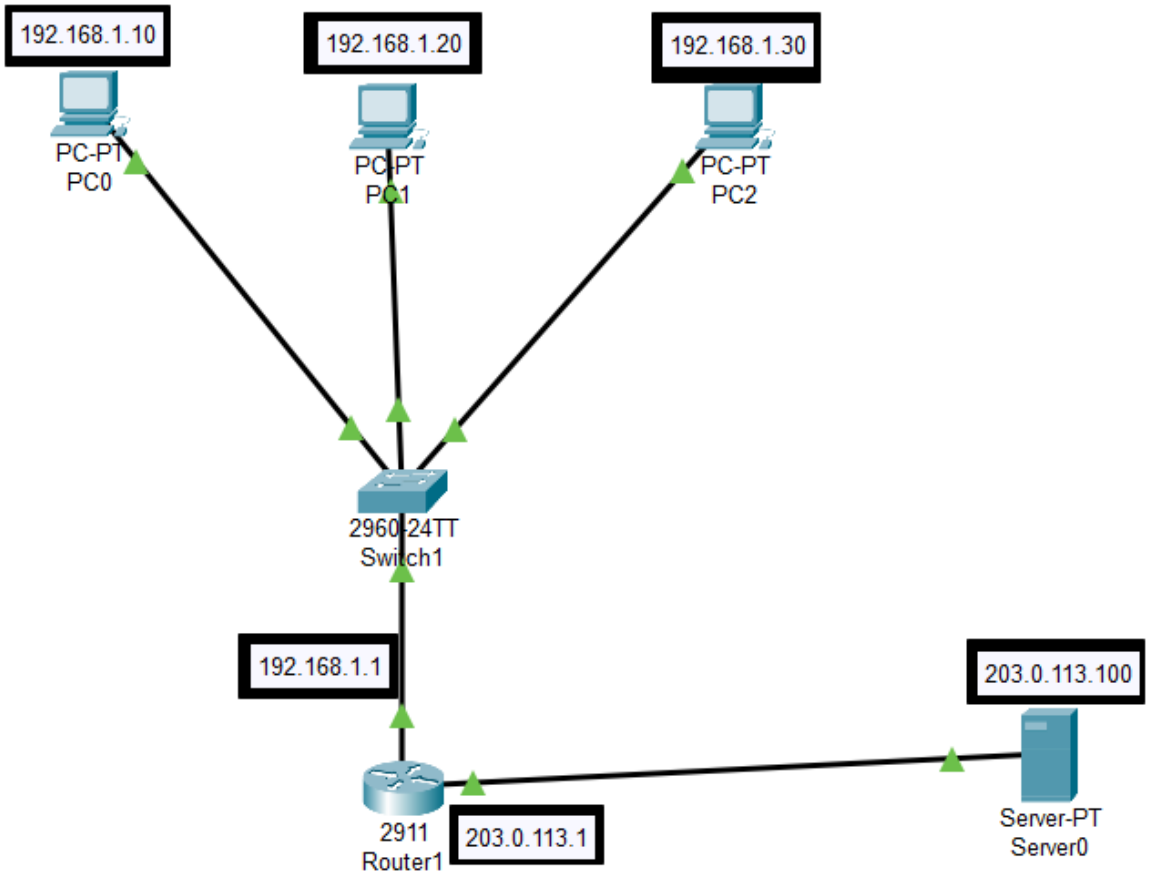
2 Analisis Hasil Percobaan

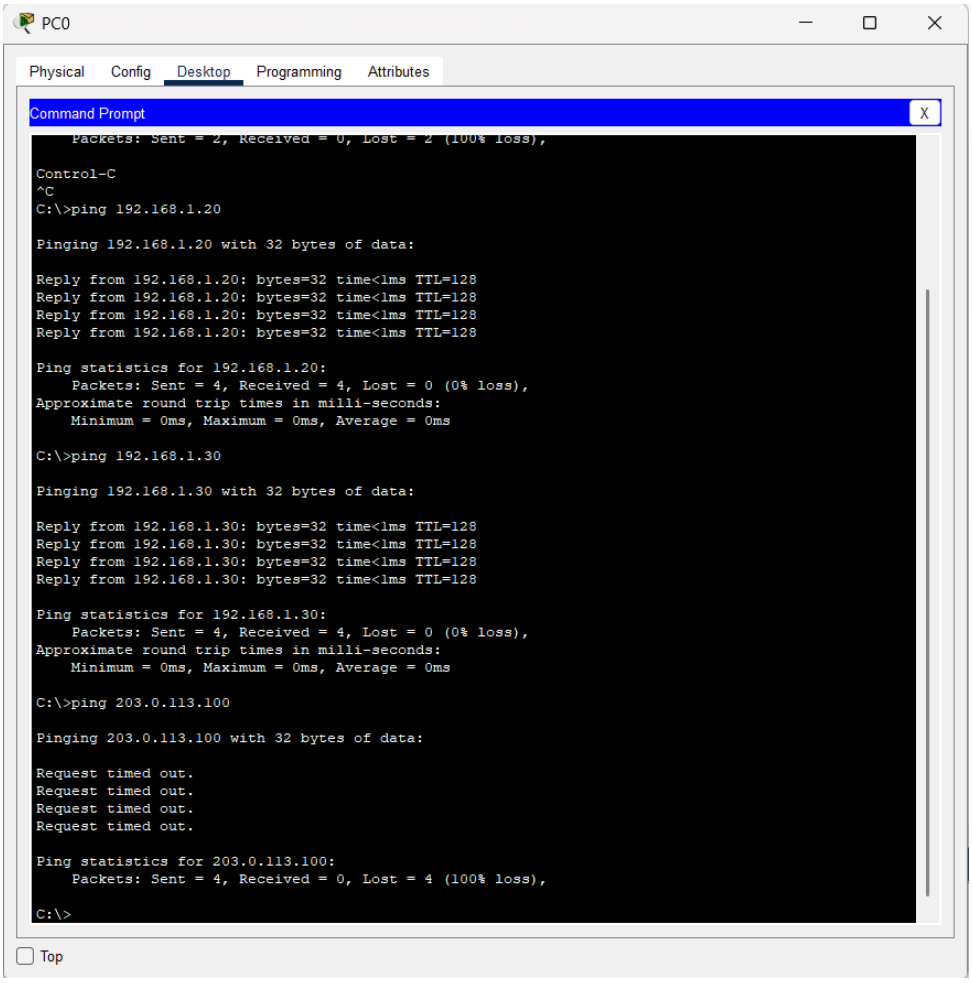
Berdasarkan tahapan praktikum yang telah dilaksanakan, konfigurasi firewall dan NAT pada router Mikrotik berhasil diterapkan sesuai dengan skenario yang dirancang. Implementasi NAT menggunakan metode masquerade mampu memberikan koneksi internet kepada perangkat-perangkat dalam jaringan lokal melalui interface ether2 yang terhubung ke jaringan global. Keberhasilan ini dibuktikan dengan suksesnya perintah ping ke alamat 8.8.8.8 dari terminal router. Kemudian, konfigurasi firewall filter yang bertujuan untuk memblokir protokol ICMP dari interface ether7 juga berjalan dengan baik. Saat aturan firewall tersebut diaktifkan, perangkat yang tersambung melalui ether7 tidak dapat melakukan ping ke internet, seperti terlihat dari munculnya pesan Request Timed Out. Ketika aturan ini dinonaktifkan, koneksi kembali normal dan perintah ping berhasil dijalankan, membuktikan bahwa aturan filter tersebut bekerja sebagaimana mestinya. Selain itu, pengujian terhadap pemblokiran akses berdasarkan kata kunci juga menunjukkan hasil yang positif. Saat aturan firewall untuk konten diaktifkan, akses ke situs seperti (http://www.speedtest.net) terblokir dan situs tidak dapat dimuat. Namun, ketika aturan tersebut dinonaktifkan, situs kembali dapat diakses. Hal ini mengindikasikan bahwa firewall Mikrotik efektif dalam melakukan penyaringan konten berbasis kata kunci.

3 Hasil Tugas Modul

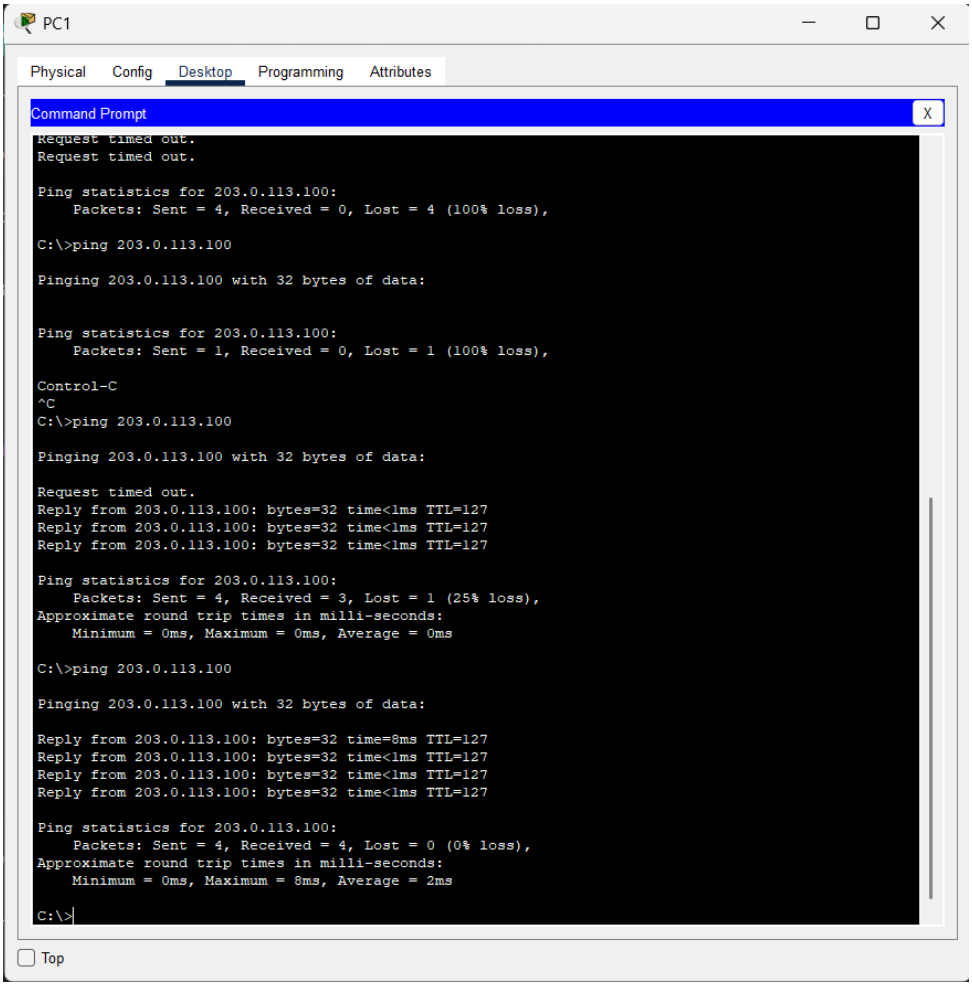
- Buatlah topologi sederhana di Cisco Packet Tracer dengan:
  - 1 Router
  - 1 Switch
  - 3 PC (LAN)
  - 1 Server (Internet/Public)
- Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
- Konfigurasi Firewall (ACL):
  - Izinkan hanya PC1 yang dapat mengakses Server.

– Blokir PC1 dan PC3 dari mengakses Server.
– Semua PC harus tetap bisa saling terhubung di LAN.
– Uji koneksi menggunakan ping dan dokumentasikan hasilnya.

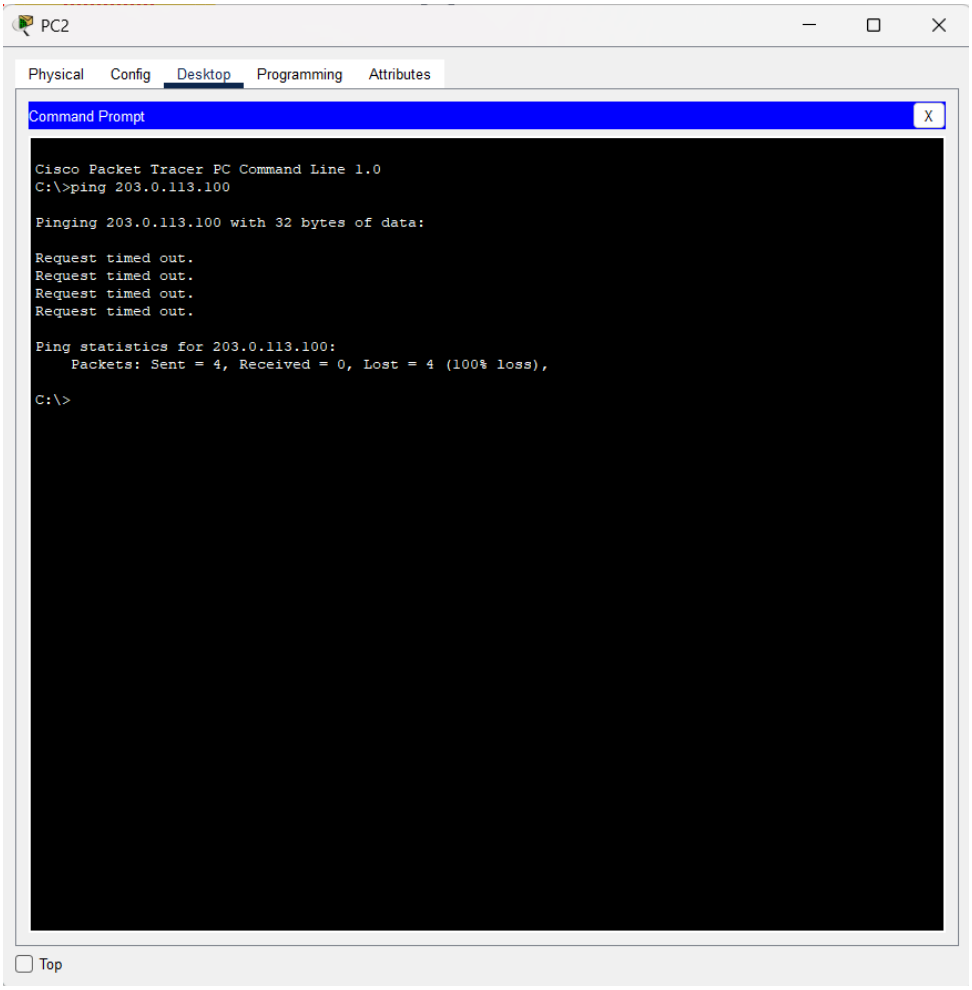



PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\>ping 192.168.1.20
Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.20:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.30
Pinging 192.168.1.30 with 32 bytes of data:
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 203.0.113.100
Pinging 203.0.113.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 203.0.113.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

Gambar 1: PC0


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Request timed out.
Request timed out.
Ping statistics for 203.0.113.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 203.0.113.100
Pinging 203.0.113.100 with 32 bytes of data:
Ping statistics for 203.0.113.100:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\>ping 203.0.113.100
Pinging 203.0.113.100 with 32 bytes of data:
Request timed out.
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Ping statistics for 203.0.113.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 203.0.113.100
Pinging 203.0.113.100 with 32 bytes of data:
Reply from 203.0.113.100: bytes=32 time=8ms TTL=127
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Reply from 203.0.113.100: bytes=32 time<1ms TTL=127
Ping statistics for 203.0.113.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 8ms, Average = 2ms
C:\>
Top

Gambar 2: PC1



Gambar 3: PC2

4 Kesimpulan

Dari praktikum yang telah dilakukan, dapat disimpulkan bahwa pengaturan firewall dan NAT pada router Mikrotik memegang peranan penting dalam pengendalian lalu lintas data sekaligus menjaga keamanan jaringan. Penggunaan NAT dengan teknik masquerade memungkinkan berbagai perangkat dalam jaringan lokal untuk mengakses internet melalui satu alamat IP publik, sehingga lebih efisien dalam pemanfaatan IP. Sementara itu, fitur firewall memberikan kemampuan untuk memfilter koneksi berdasarkan protokol seperti ICMP maupun berdasarkan konten seperti akses ke situs tertentu. Berdasarkan hasil pengujian, aturan-aturan firewall yang diterapkan terbukti efektif dalam membatasi koneksi sesuai konfigurasi, serta dapat dinonaktifkan sewaktu-waktu untuk mengembalikan akses. Selain itu, konfigurasi DHCP dan pengelolaan interface turut memastikan jaringan berjalan stabil dan terorganisir. Secara keseluruhan, praktikum ini memberikan pemahaman yang komprehensif tentang bagaimana fitur-fitur pada Mikrotik dapat digunakan untuk membangun jaringan yang aman, efisien, dan sesuai kebutuhan, serta menekankan pentingnya keterampilan teknis dalam pengelolaan sistem jaringan modern.

5 Lampiran

Gambar 4: Dokumentasi telah melakukan praktikum