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

Laporan Akhir
Praktikum Jaringan Komputer

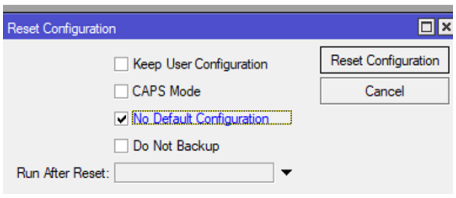
Firewall & NAT

Hilmy Abid Syafi Abiyyu - 5024231029

2025

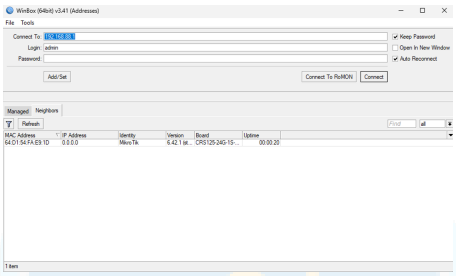
1 Langkah-Langkah Percobaan

- Modul ini dimulai dengan melakukan reset configuration pada router



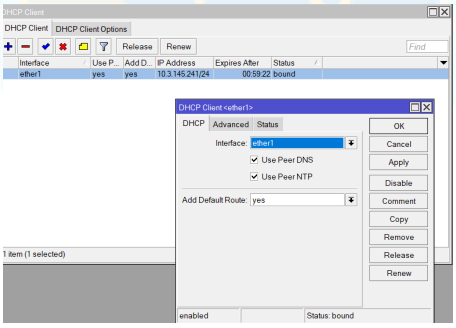
Gambar 1: Reset Configuration

- Kemudian login ke Router menggunakan WinBox



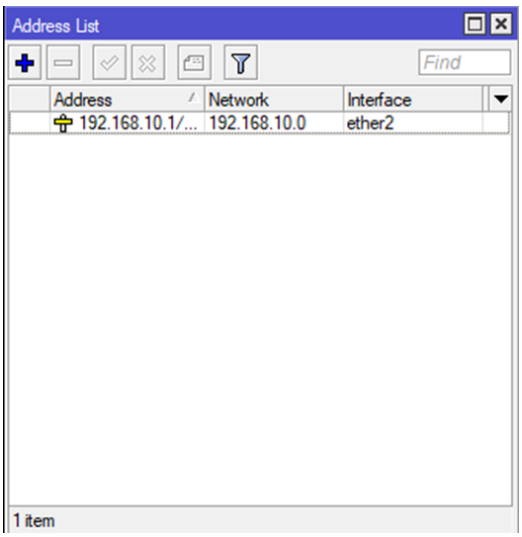
Gambar 2: Login ke Router dengan WinBox

- Lakukan konfigurasi DHCP Client pada Router A (Ether 1) dengan menyambungkan kabel internet ke ether1 pada Router A. Kemudian klik menu IP lalu DHCP Client lalu + kemudian pilih ether1 sebagai interface dan klik Apply serta pastikan status koneksi bound



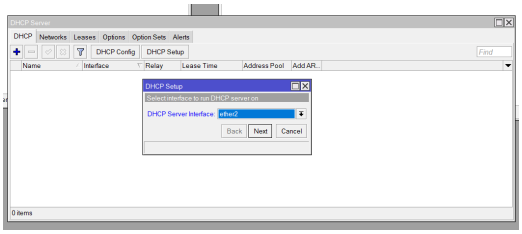
Gambar 3: Konfigurasi DHCP Client pada Router A

- Menambahkan IP Address pada ether2 untuk Switch dengan ke menu IP lalu addresses lalu + dan memasukkan address 192.168.10.1/24 interface ether2 apply lalu ok

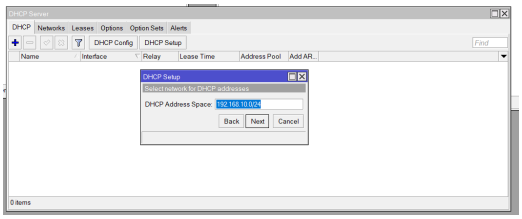


Gambar 4: Penambahan Alamat IP pada Ether2

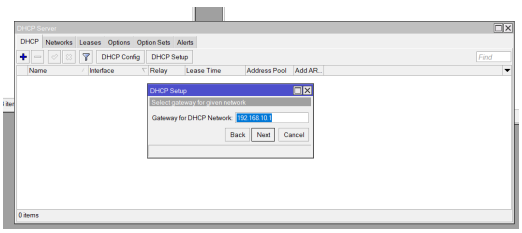
- Lakukan konfigurasi DHCP Server untuk mendistribusikan IP address kepada perangkat klien yang terhubung secara otomatis pada menu IP lalu DHCP server lalu DHCP Setup, pada interface pilih ether7, pada address space 192.168.10.0/24, pada gateway 192.168.10.1 pada addresses to give out 192.168.10.2-192.168.10.254, dns server 8.8.8.8, lease time 00:10:00, lalu klik OK



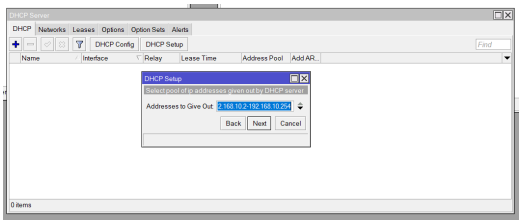
Gambar 5: Konfigurasi DHCP Server Interface



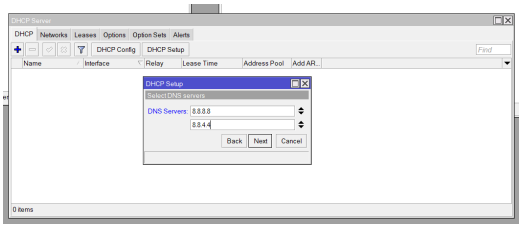
Gambar 6: Konfigurasi DHCP Address Space



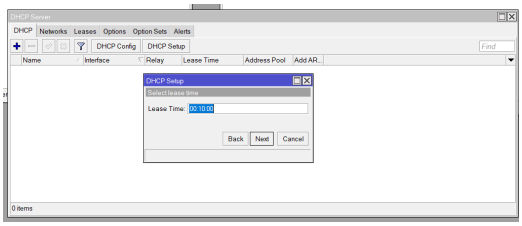
Gambar 7: Konfigurasi Gateway for DHCP Network



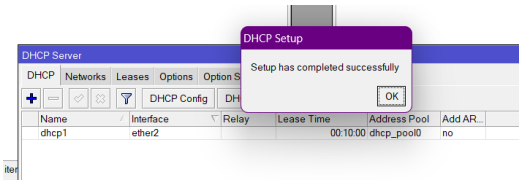
Gambar 8: Konfigurasi Address to Give Out



Gambar 9: Konfigurasi DNS Servers

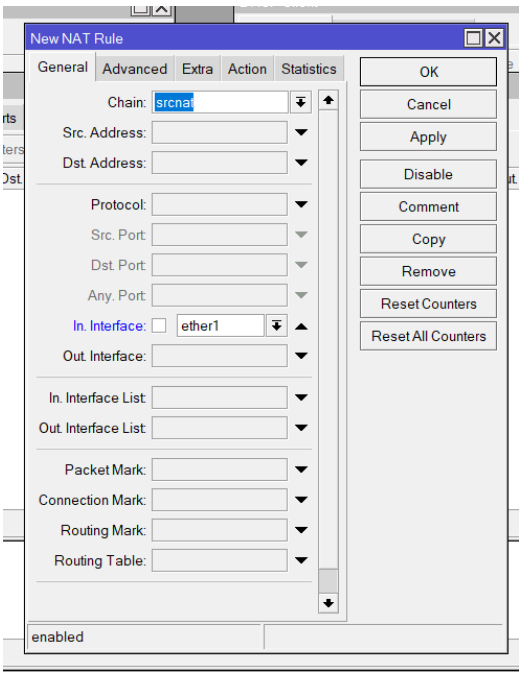


Gambar 10: Konfigurasi Lease Time

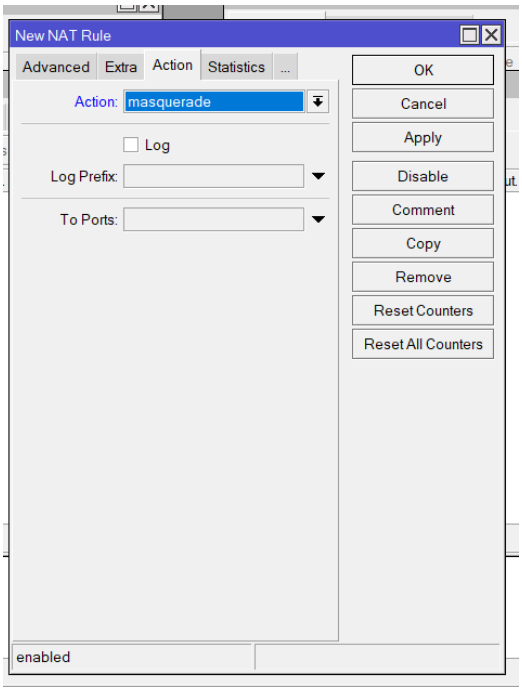


Gambar 11: Setup Successfull

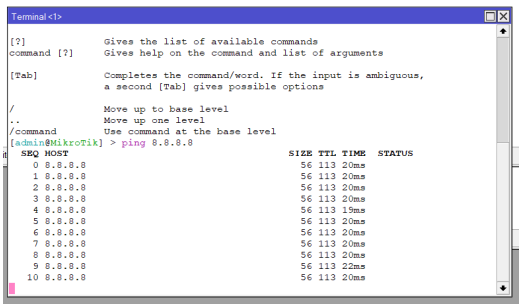
- Lakukan konfigurasi Network Address Translation (NAT) pada menu IP lalu Firewall lalu NAT, klik +, tab General Chain src-nat, tabb Action masquerade, klik apply lalu ok



Gambar 12: Konfigurasi Chain

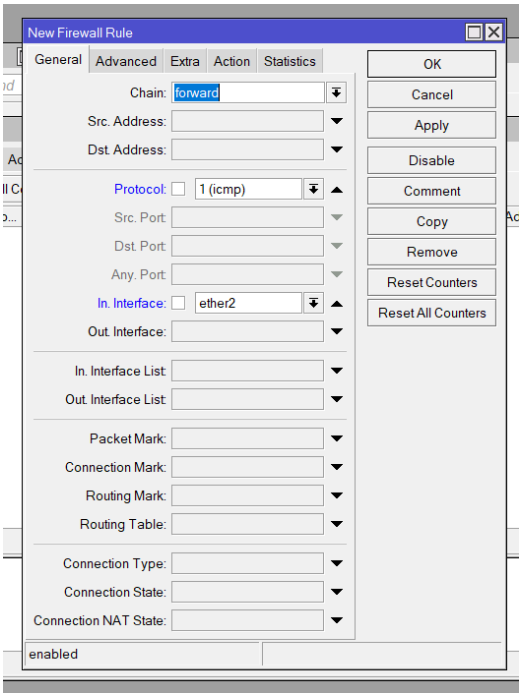


Gambar 13: Konfigurasi Action

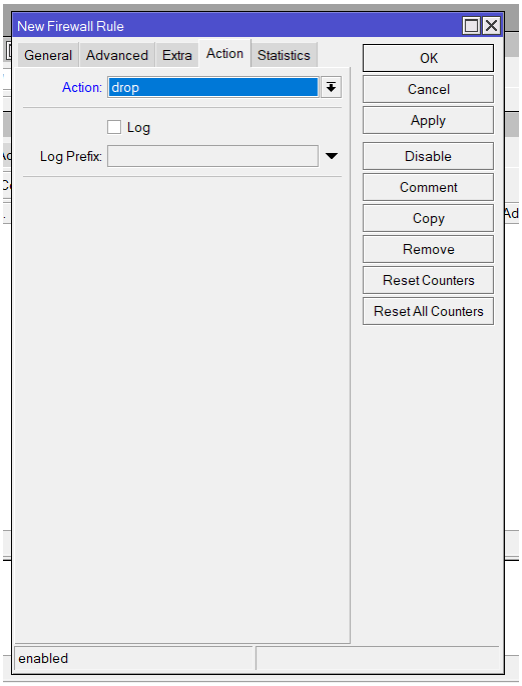


Gambar 14: Uji ping 8.8.8.8

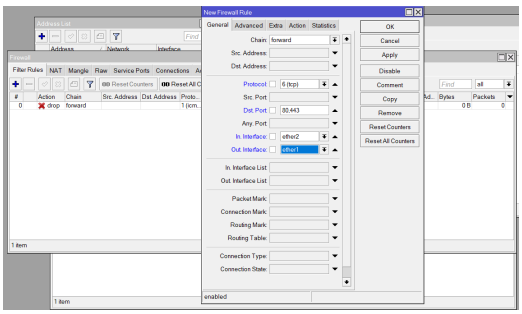
- Lakukan konfigurasi firewall dengan menambahkan aturan filter pada menu IP lalu firewall lalu filter rule, klik +. Untuk pemblokiran Internet Control Message Protocol (ICMP) pada tab general atur chain forward, protocol icmp, In. Interface ether2 action drop. Pemblokiran Akses Situs Web berdasarkan konten pada tab general chain forward, protocol tcp, Dst. Port 80,443, In. Interface ether7, out Interface ether1, tab advanced content speedtest, tab action action drop



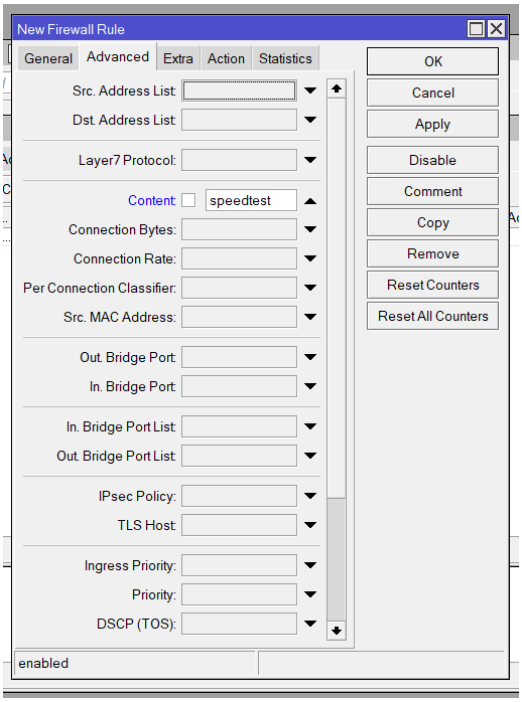
Gambar 15: Konfigurasi Filter Rules



Gambar 16: Konfigurasi Pemblokiran ICMP

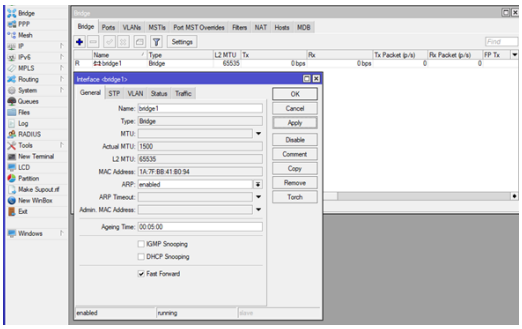


Gambar 17: Konfigurasi Pemblokiran Akses Situs Web Content Blocking

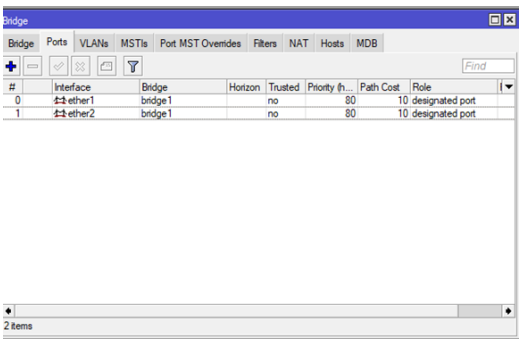


Gambar 18: Konfigurasi Pemblokiran Akses Situs Web Content Blocking

- Lakukan konfigurasi bridge pada router B untuk menjadi hub dengan akses menu Bridge lalu + lalu apply. Tambahkan port ke dalam bridge dengan akses menu bridge lalu port lalu + lalu pilih interface yang terhubung ke perangkat laptop lalu pilih interface terhubung ke router A

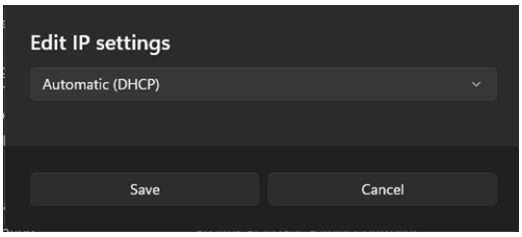


Gambar 19: Konfigurasi General Interface bridge1



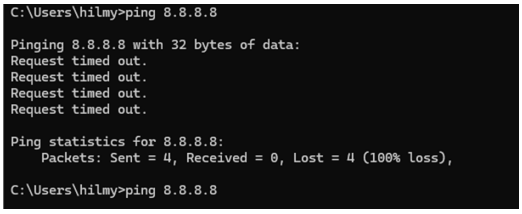
Gambar 20: Konfigurasi Port bridge1

- Lakukan konfigurasi IP Address pada laptop dengan mengaturnya menjadi DHCP pada settings atau control panel.

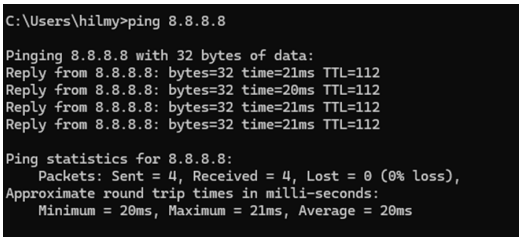


Gambar 21: Konfigurasi IP Address pada Laptop

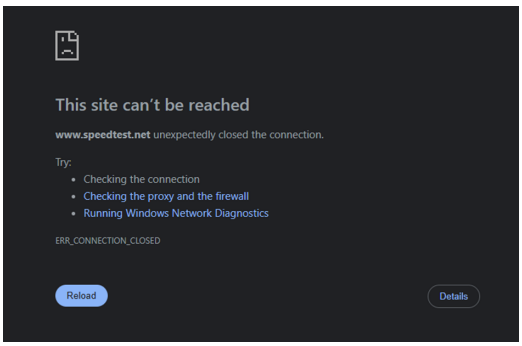
- Lakukan pengujian konfigurasi untuk memverifikasi fungsionalitasnya. Uji ICMP dengan buka terminal pada laptop, ping 8.8.8.8. Ketika firewall aktif responnya akan Request Timed Out (RTO). Ketika firewall nonaktif (X) pada Filter Rules maka akan berhasil. Pengujiaan Pemblokiran Konten dengan mencoba akses situs web dengan kata kunci speedtest. Ketika firewall aktif, situs web tidak dapat diakses. Ketika firewall nonaktif (X) pada Filter Rules maka web bisa diakses dengan normal



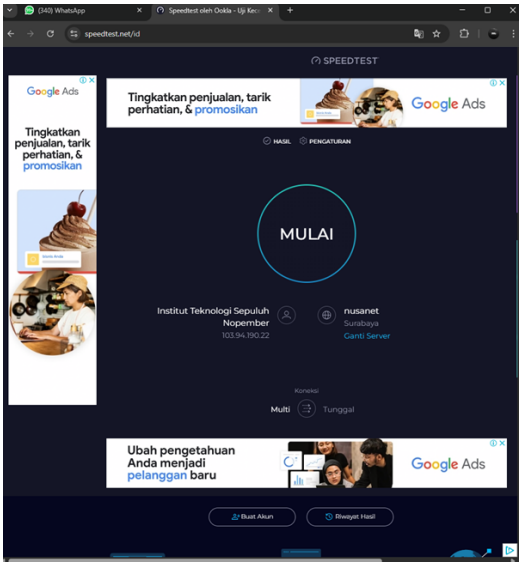
Gambar 22: Uji Coba Konfigurasi: ping 8.8.8.8 (Firewall Aktif)



Gambar 23: Uji Coba Konfigurasi: ping 8.8.8.8 (Firewall Non Aktif



Gambar 24: Cek Website Speedtest (Firewall Aktif)



Gambar 25: Cek Website Speedtest (Firewall Nonaktif)

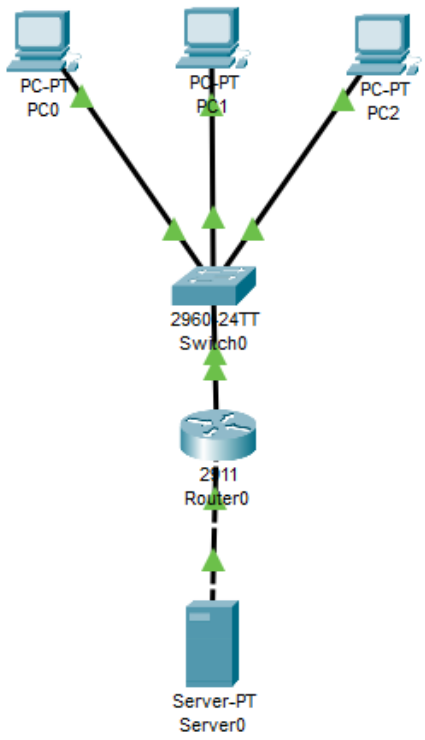
2 Analisis Hasil Percobaan

Konfigurasi jaringan dilakukan untuk memahami fungsi DHCP, NAT, dan firewall pada perangkat MikroTik. Konfigurasi DHCP Client pada Router A berhasil membuat router memperoleh IP dari penyedia layanan internet dan konfigurasi DHCP Server memungkinkan perangkat klien mendapatkan IP secara otomatis melalui ether2. Konfigurasi NAT dengan metode masquerade berhasil membuat perangkat dalam jaringan lokal mengakses internet menggunakan IP publik dari router. Pengujian menggunakan ping 8.8.8.8 menunjukkan bahwa koneksi berhasil dilakukan setelah NAT diaktifkan. Pada bagian firewall, dilakukan pengujian pemblokiran protokol ICMP dan pemblokiran akses situs berdasarkan kata kunci tertentu seperti "speedtest". Hasilnya menunjukkan bahwa saat firewall diaktifkan, koneksi ICMP dan akses ke situs berhasil diblokir, dan dapat kembali normal saat firewall dinonaktifkan. Selain itu, konfigurasi bridge pada Router B juga berhasil dilakukan dengan baik, yang memungkinkan komunikasi antar perangkat dalam jaringan LAN melalui penggabungan beberapa interface ke dalam satu bridge.

3 Hasil Tugas Modul

1. Simulasikan jaringan wireless antara tiga gedung:

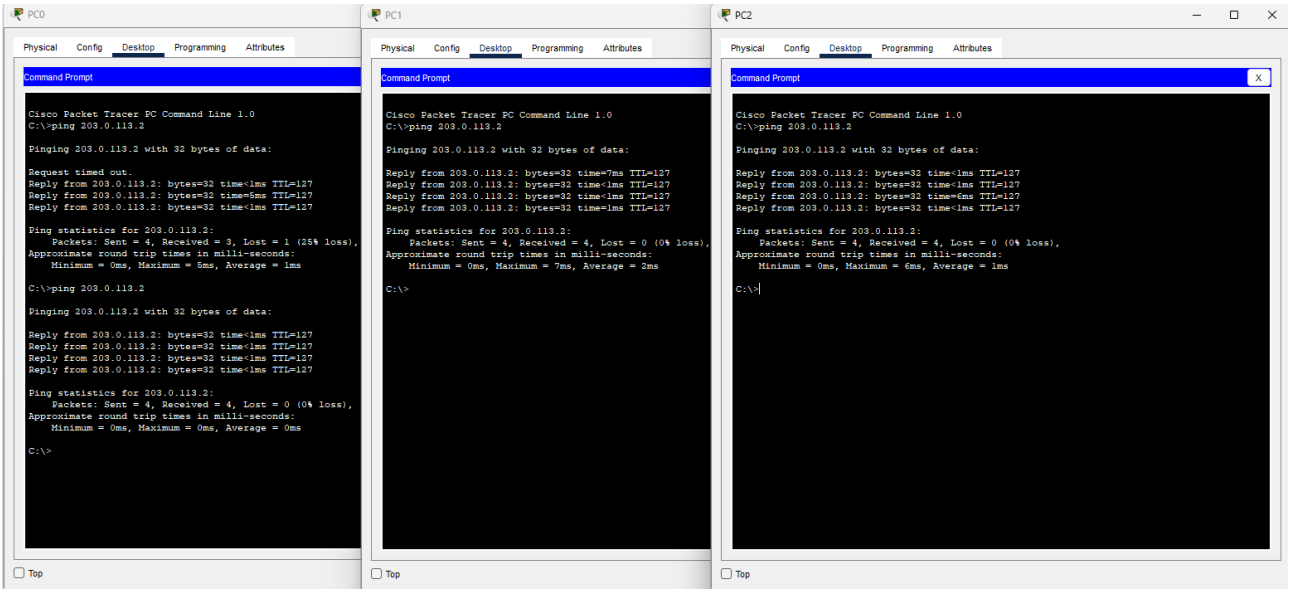
- 1 Router
- 1 Switch
- 3 PC (LAN)
- 1 Server (Internet/Public)



Gambar 26: Topologi Jaringan

2. Konfigurasi NAT:

- Buat agar semua PC bisa mengakses Server menggunakan IP publik Router

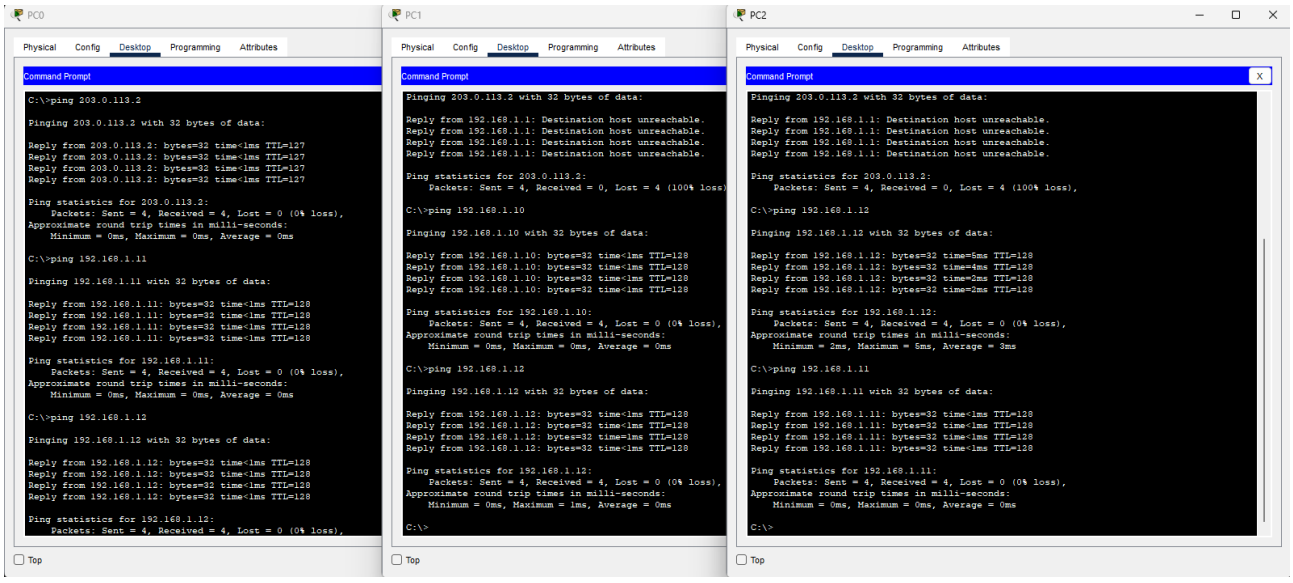


Gambar 27: Semua PC Akses Router

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.



Gambar 28: Tugas Modul Poin No. 3

4 Kesimpulan

Konfigurasi DHCP, NAT, firewall, dan ACL memberikan kontrol penuh terhadap pengelolaan alamat IP, akses internet, serta keamanan dan batasan akses dalam jaringan. Dari hasil praktikum yang telah

dilakukan membuktikan bagaimana teknik-teknik tersebut diimplementasikan secara efektif dalam skenario nyata, baik melalui MikroTik maupun simulasi Cisco Packet Tracer.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 29: Dokumentasi Praktikum