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

Laporan Akhir
Praktikum Jaringan Komputer

Modul Firewall NAT

Susilo Hendri Yudhoyono - 5024231016

2025

1 Langkah-Langkah Percobaan

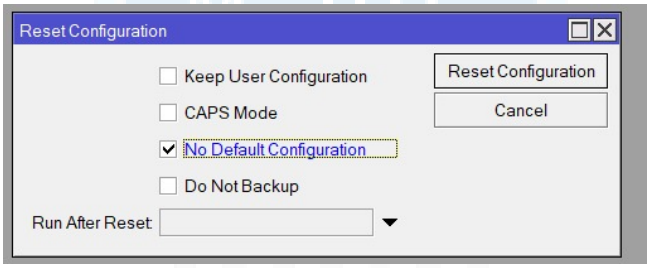
1.1 Alat dan Bahan

Adapun alat dan bahan yang digunakan dalam praktikum ini adalah sebagai berikut:

- Laptop
- Router MikroTik
- Kabel LAN
- LAN to USB adapter

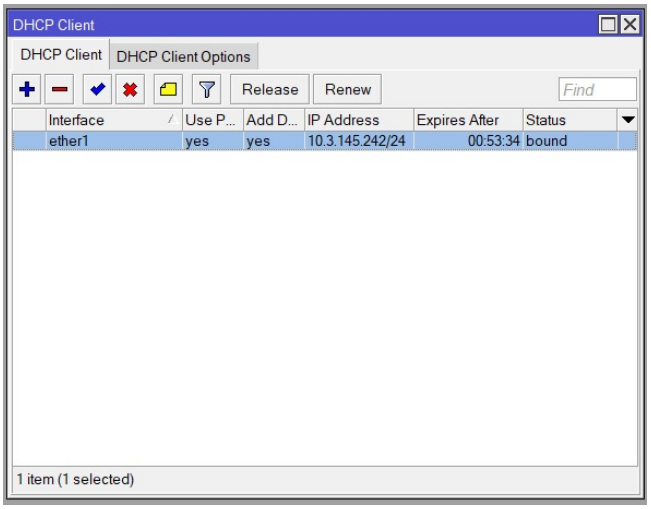
1.2 Langkah-Langkah Percobaan

1. Menyiapkan semua alat yang diperlukan seperti laptop, router MikroTik, kabel LAN, dan LAN to USB adapter.
2. Menghubungkan kabel LAN dari port router MikroTik ke adapter LAN to USB, lalu menyambungkannya ke laptop.
3. Membuka aplikasi Winbox, kemudian masuk menggunakan IP address kosong (default) untuk memulai konfigurasi pada Router 1.
4. Reset router mikrotik terlebih dahulu dengan masuk ke system.



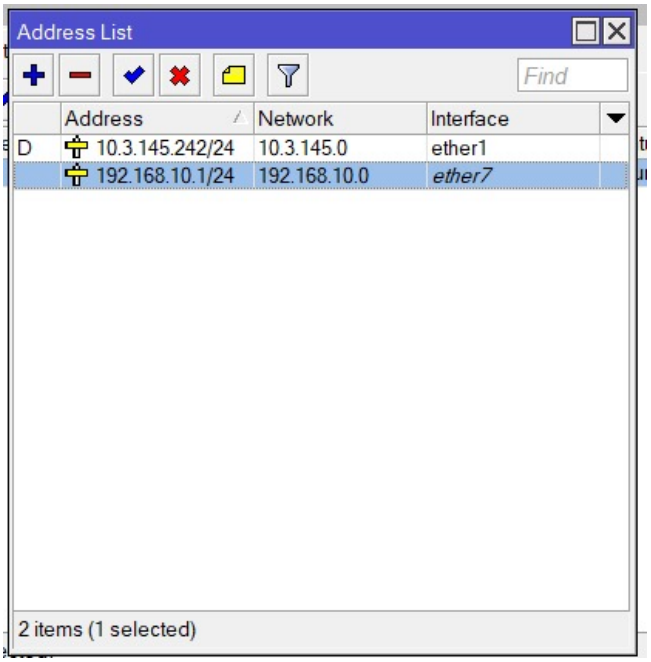
Gambar 1: Reset konfigurasi

5. Tambahkan dhcp client pada ether 1.



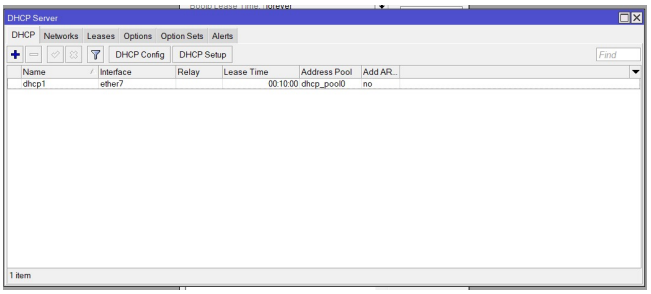
Gambar 2: dhcp client

6. Tambahkan ip address pada ether 7.



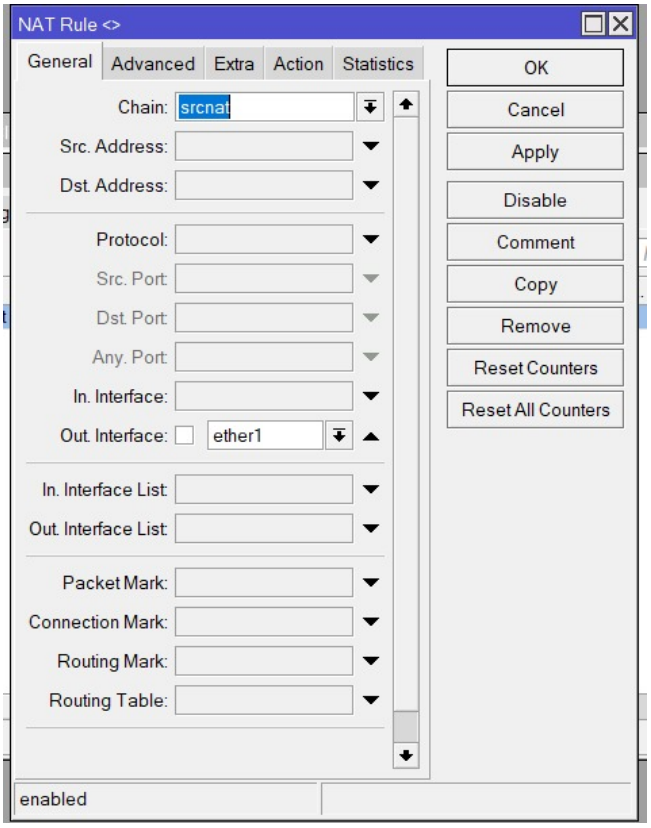
Gambar 3: IP address ether 7

7. Tambahkan dhcp server pada ether 7 agar lan mendapatkan ip secara otomatis.



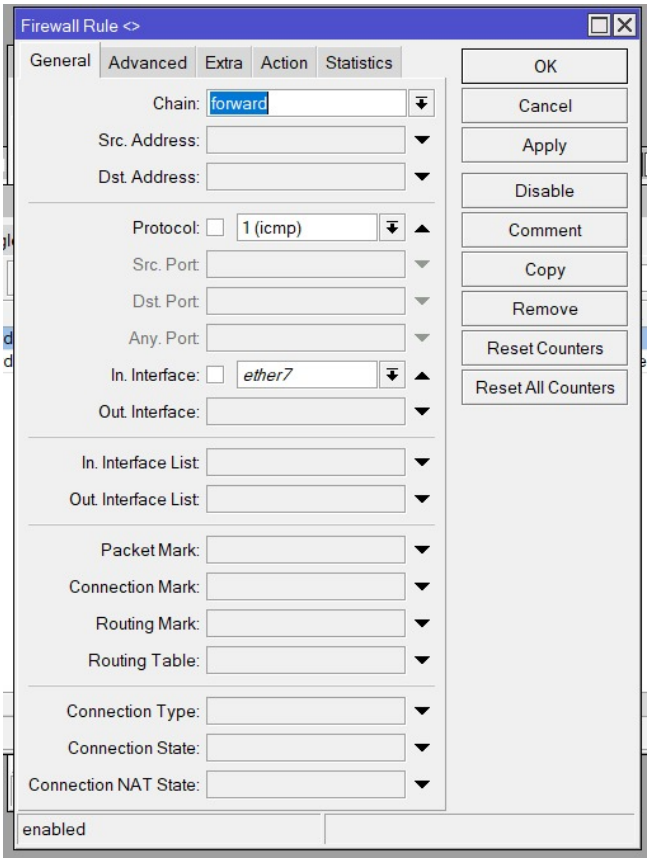
Gambar 4: dhcp server

8. Tambahkan NAT agar client bisa akses internet dengan action masquerade.

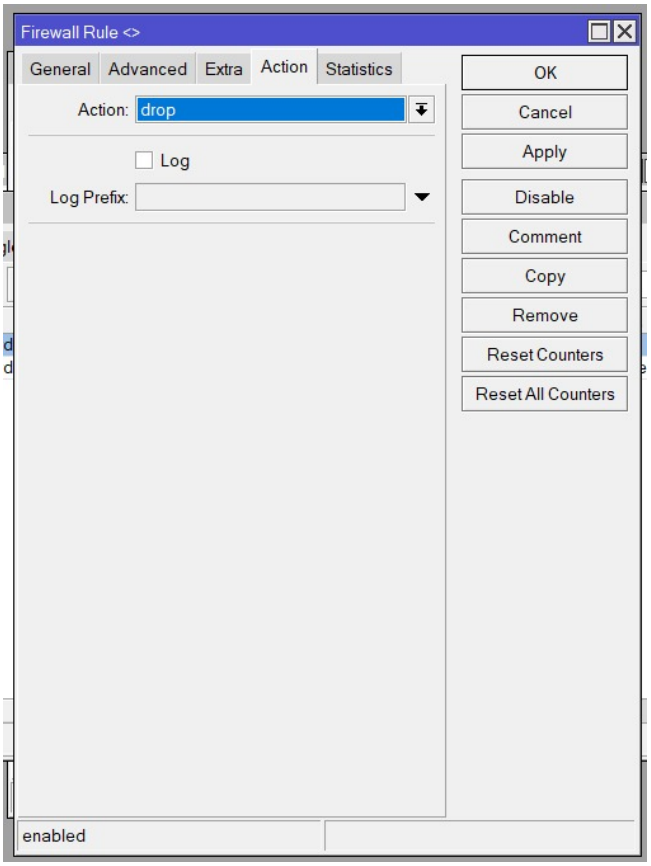


Gambar 5: NAT

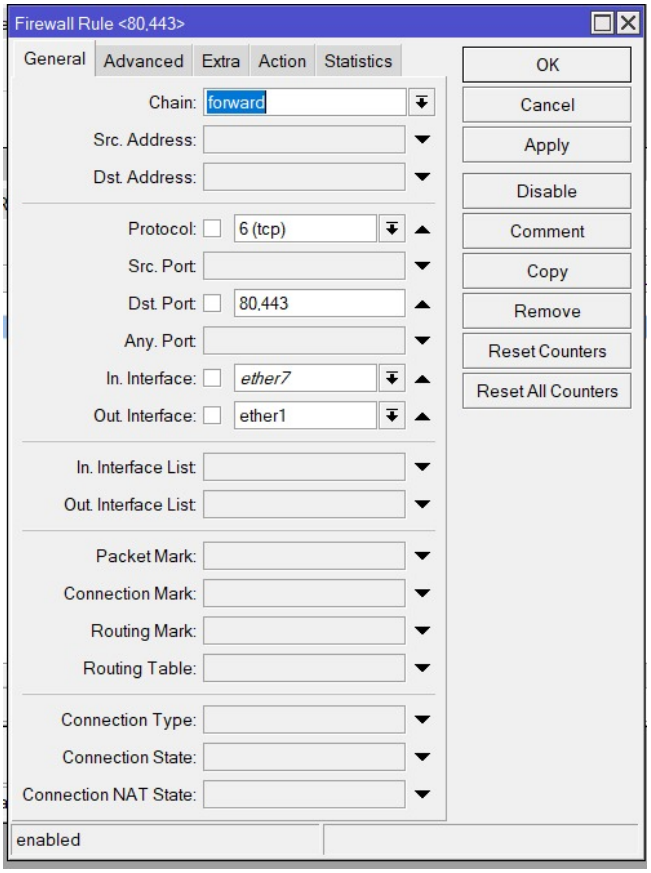
9. Tambahkan konfigurasi Firewall.



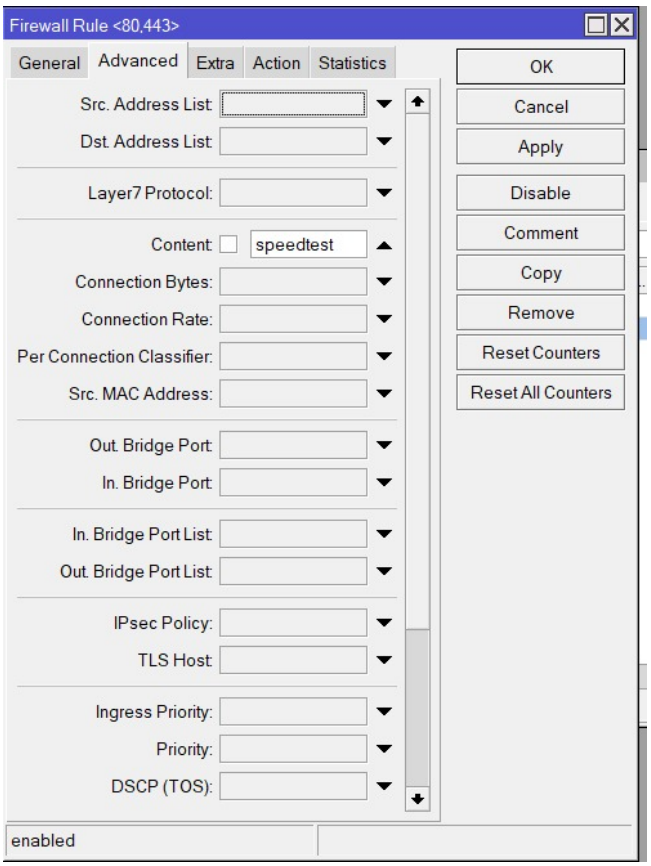
Gambar 6



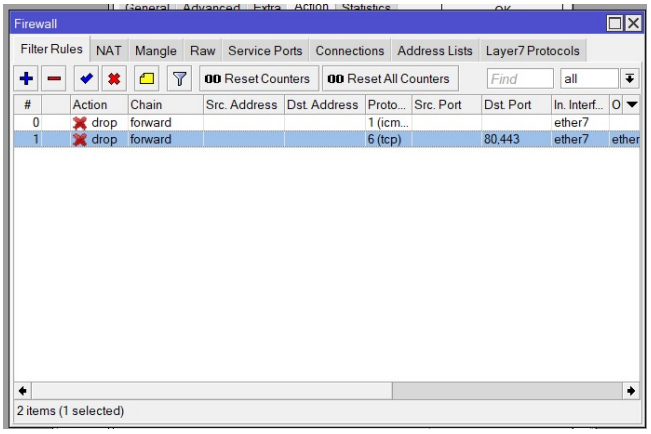
Gambar 7: action drop



Gambar 8

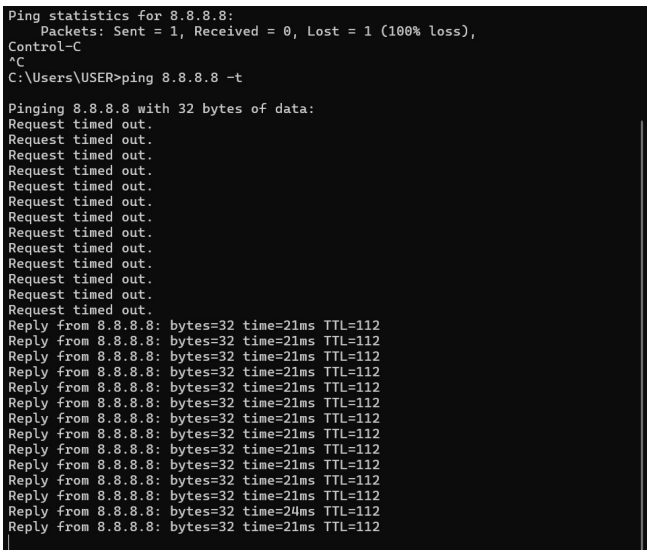


Gambar 9: blokir speedtest



Gambar 10: Enter Caption

10. Akses menu Bridge > Ports, klik ikon "+", lalu tambahkan interface yang terhubung ke laptop dan interface yang terhubung ke Router A ke dalam bridge.
11. Lakukan ping pada 8.8.8.8. Pastikan hasilnya RTO pada saat aktif firewallnya, dan pastikan reply pada saat firewall tidak aktif.

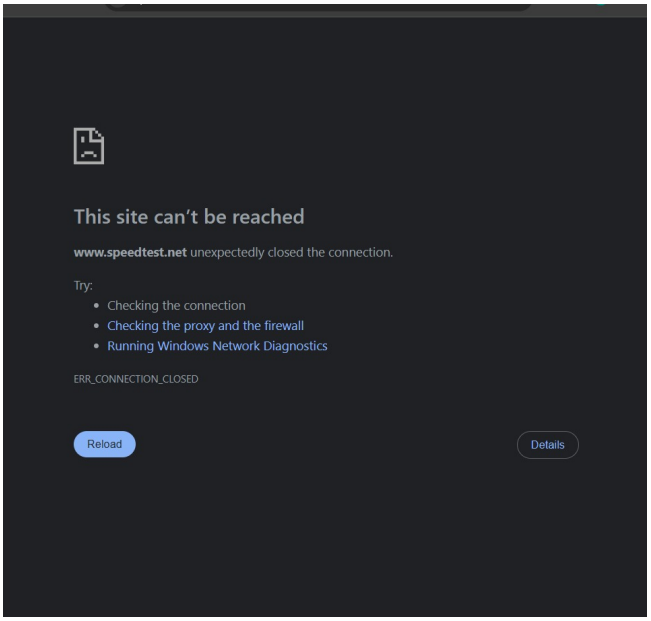


```
Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\USER>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
```

Gambar 11: hasil ping

12. Akses web yang diblokir tadi yaitu speedtest, pastikan hasilnya tidak dapat diakses.



This site can't be reached

www.speedtest.net unexpectedly closed the connection.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_CLOSED

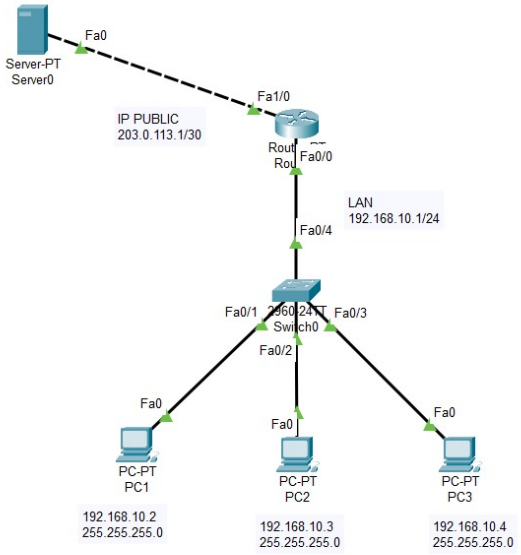
Gambar 12: hasil akses web

2 Analisis Hasil Percobaan

Pada percobaan ini, dilakukan konfigurasi jaringan untuk mengatur konektivitas dan pembatasan akses dari jaringan lokal (LAN) ke internet. Pertama, NAT (Network Address Translation) diaktifkan agar perangkat-perangkat di LAN dapat mengakses internet dengan mengubah IP privat menjadi IP publik. Selanjutnya, konfigurasi firewall diterapkan untuk memblokir akses ke DNS Google (8.8.8.8) dan situs web Speedtest. Hal ini bertujuan untuk membatasi akses pengguna terhadap layanan tertentu, baik untuk alasan keamanan maupun pengelolaan bandwidth. Selain itu, DHCP Client diaktifkan pada interface ether1 yang terhubung ke ISP agar router dapat memperoleh IP publik secara otomatis. Di sisi lain, router juga dikonfigurasi sebagai DHCP Server untuk jaringan lokal, sehingga setiap perangkat klien di LAN dapat menerima alamat IP secara otomatis tanpa perlu konfigurasi manual.

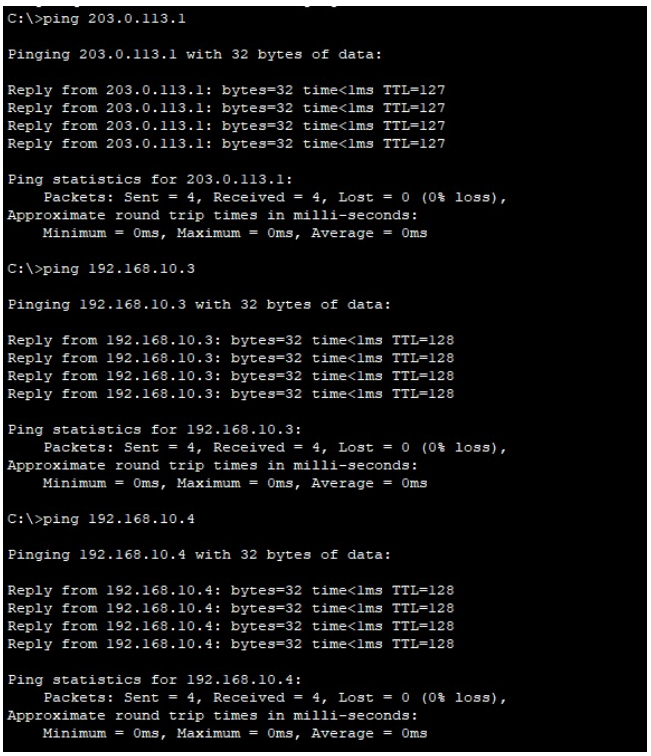
3 Hasil Tugas Modul

1. Buatlah topologi sederhana di **Cisco Packet Tracer** dengan:
    - 1 Router
    - 1 Switch
    - 3 PC (LAN)
    - 1 Server (Internet/Public)



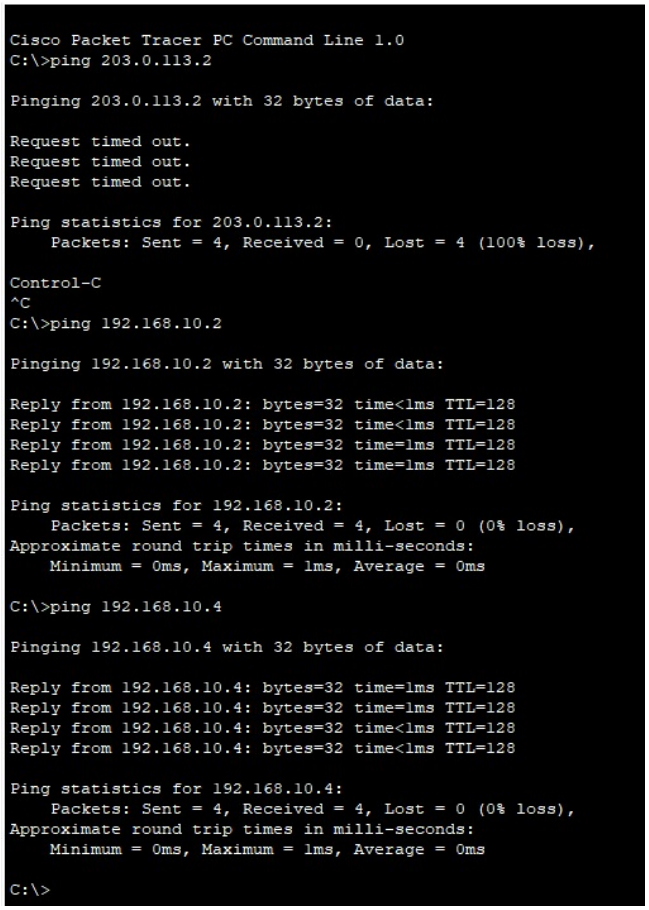
Gambar 13: Topologi

2. **Konfigurasi NAT:** Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
3. **Konfigurasi Firewall (ACL):**
    - Izinkan hanya **PC1** yang dapat mengakses Server.



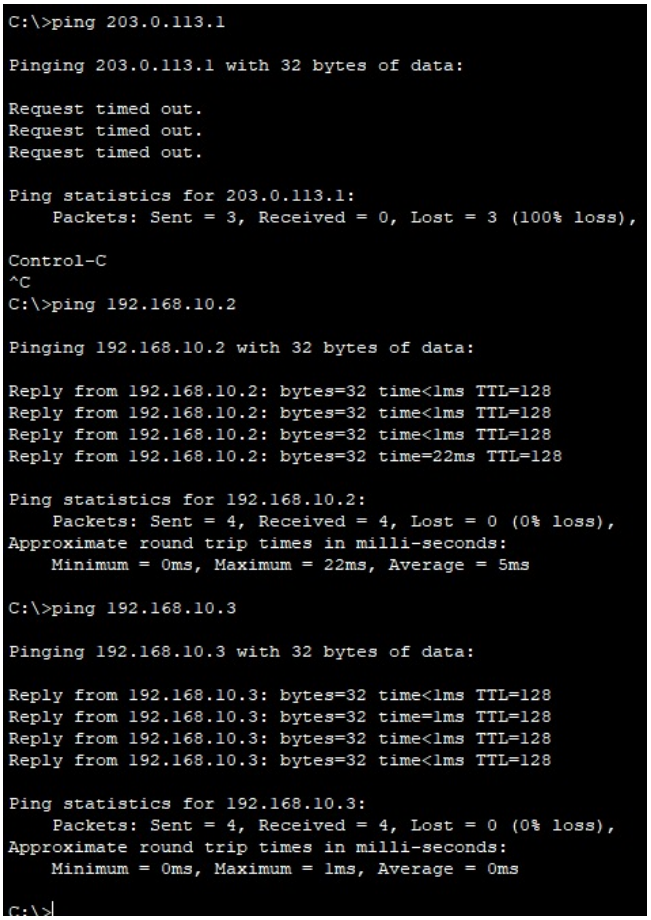
Gambar 14: ping pc 1 ke server dan LAN

- Blokir **PC2 dan PC3** dari mengakses Server.



Gambar 15: ping pc 2 ke server dan LAN

- Semua PC harus tetap bisa saling terhubung di LAN.



Gambar 16: ping pc 3 ke server dan LAN

4 Kesimpulan

Dari percobaan yang dilakukan, dapat disimpulkan bahwa konfigurasi NAT sangat penting agar perangkat di jaringan lokal dapat mengakses internet melalui IP publik router. Penerapan firewall untuk memblokir akses ke layanan tertentu seperti DNS Google dan situs Speedtest menunjukkan bagaimana kontrol akses dapat diterapkan untuk tujuan keamanan dan manajemen lalu lintas jaringan. Selain itu, aktivasi DHCP Client pada interface yang terhubung ke ISP memungkinkan router memperoleh IP publik secara otomatis, sehingga koneksi internet dapat berlangsung tanpa konfigurasi manual. Untuk memudahkan manajemen IP di sisi jaringan lokal, router juga dikonfigurasi sebagai DHCP Server yang memberikan alamat IP secara otomatis kepada perangkat-perangkat LAN.