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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Syela Akhul Khalimi - 5024231015

2025

1 Langkah-Langkah Percobaan

1.1 Konfigurasi Pemblokiran ICMP dan Content Blocking

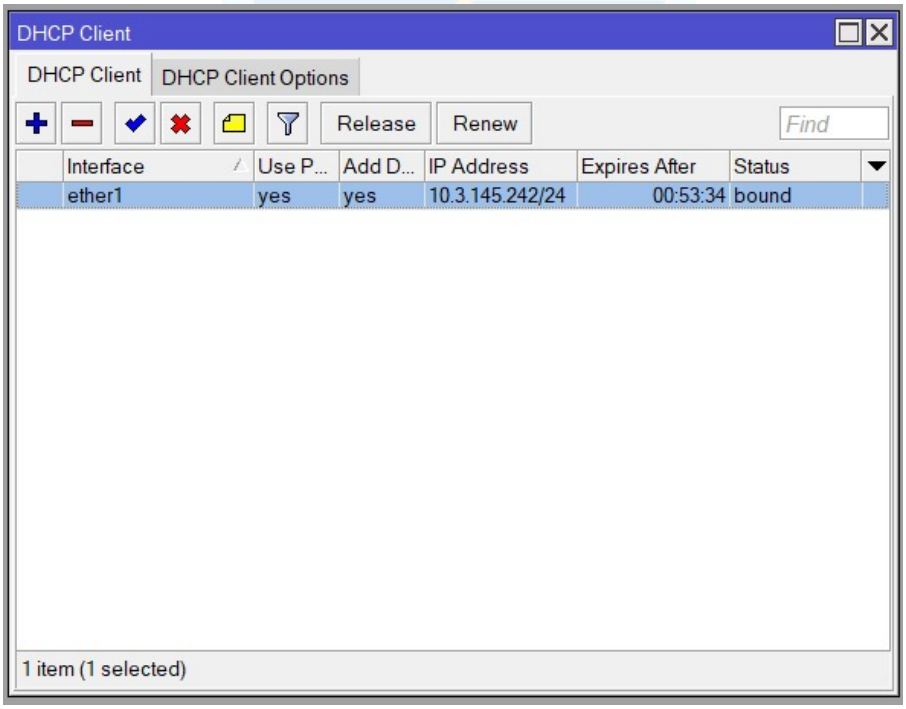
Alat dan Bahan yang Digunakan:

Terdapat beberapa perangkat dan perlengkapan yang harus disiapkan terlebih dahulu sebelum memulai proses konfigurasi. Berikut adalah daftar alat dan bahan yang dibutuhkan:

1. **Tiga buah kabel UTP**
2. **Dua unit router**
3. **Dua unit laptop**
4. **Dua unit LAN to USB adapter**

Tahapan Pelaksanaan Konfigurasi:

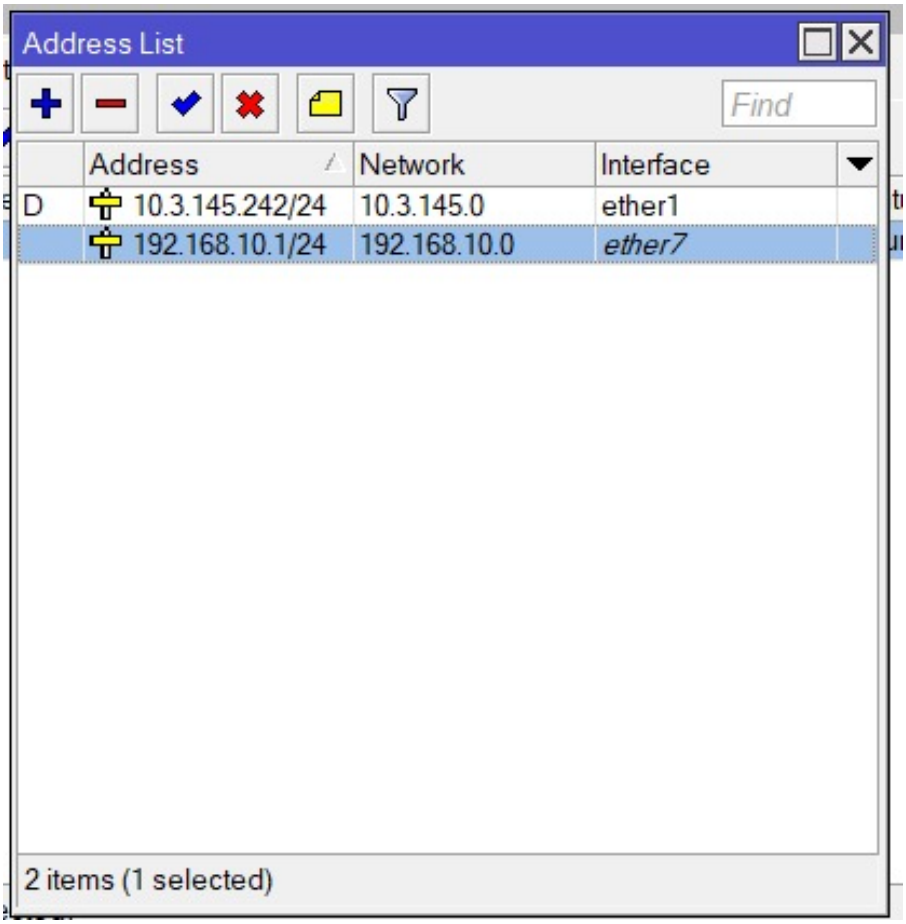
1. **Persiapan Peralatan** Seluruh perangkat dan bahan yang diperlukan
2. **Pemasangan dan Koneksi Perangkat** Kabel UTP dipasangkan ke masing-masing router Mikrotik dan laptop. Pastikan setiap ujung kabel terhubung dengan port yang sesuai
3. **Akses Router Melalui Winbox** Setelah semua perangkat terhubung, buka aplikasi Winbox pada masing-masing laptop untuk melakukan reset default
4. **Aktivasi DHCP Client** Langkah berikutnya adalah menambahkan DHCP client di ether 1



Gambar 1: DHCP Client

5. **Pengaturan Alamat IP Statis pada Ether7** Langkah berikutnya adalah mengatur alamat IP statis untuk interface Ether7. Buka menu IP → Addresses, lalu klik tombol + untuk menambahkan

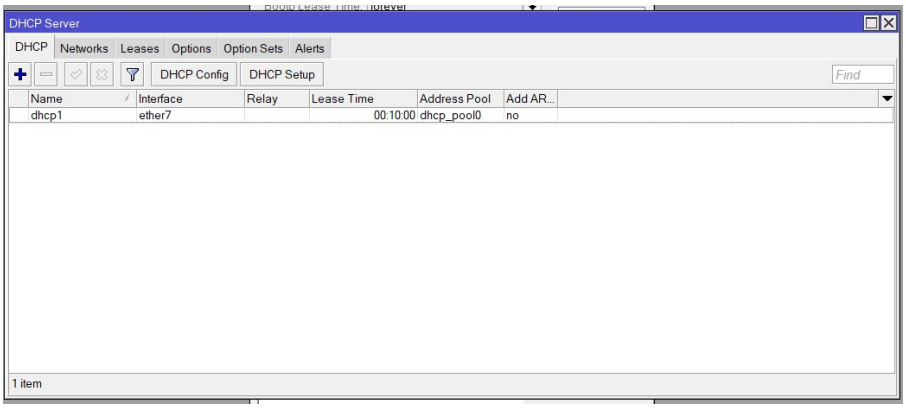
alamat baru. Masukkan IP 192.168.10.1/24 dan pastikan memilih Ether7 sebagai interface agar konfigurasi berjalan dengan benar dan tidak terjadi konflik IP.



Gambar 2: Alamat IP

6. Langkah selanjutnya adalah mengaktifkan DHCP Server pada interface Ether7. Masuk ke menu IP → DHCP Server, lalu klik tombol + untuk menambahkan konfigurasi baru. Pilih Ether7 sebagai interface agar perangkat yang terhubung ke jaringan LAN dapat memperoleh alamat IP secara otomatis.

7. **Pembuatan Aturan NAT (Network Address Translation)**

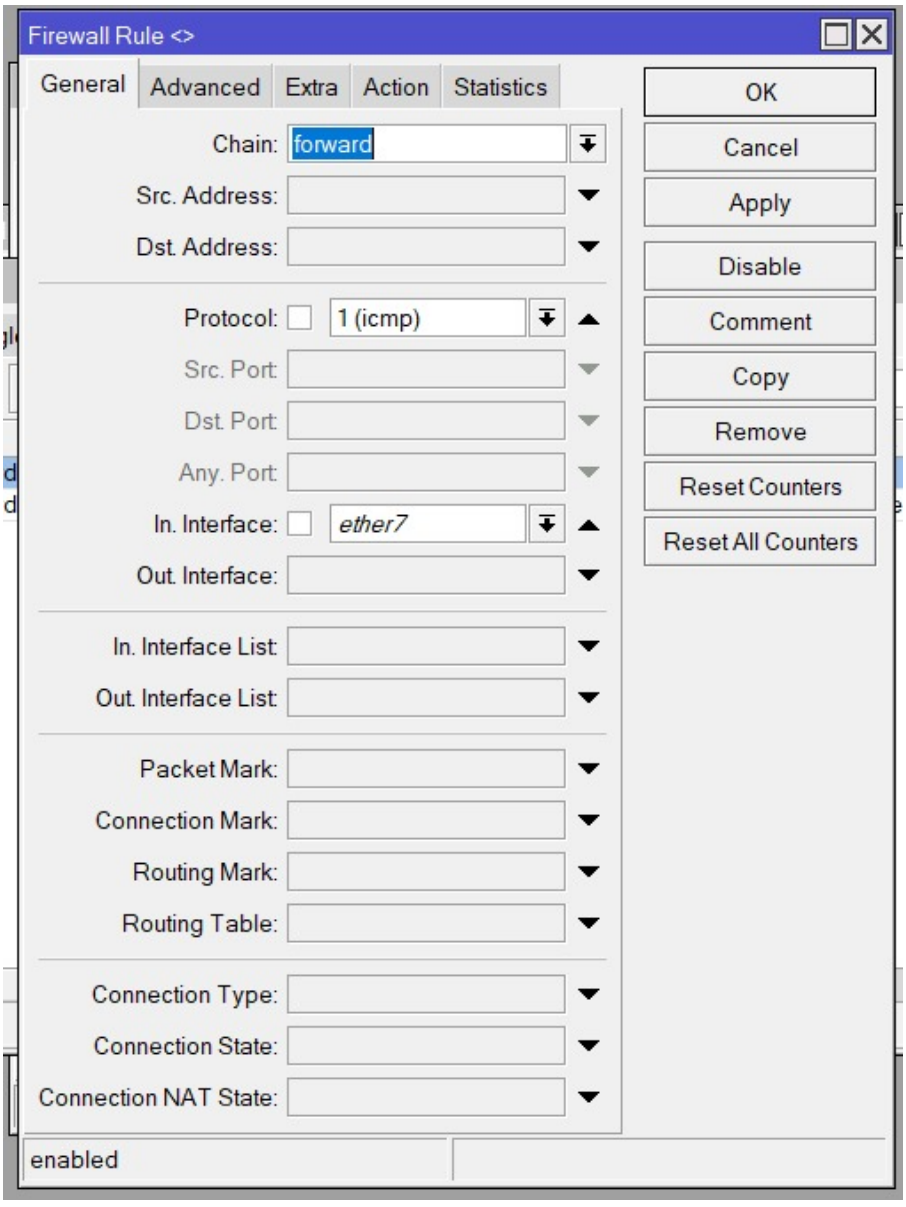


Gambar 3: NAT

Setelah mengatur alamat IP statis pada interface Ether7, tambahkan konfigurasi NAT agar client

dapat mengakses internet. Buka menu IP → Firewall, lalu masuk ke tab NAT dan klik tombol +. Pilih Chain: srcnat, kemudian pada bagian Out. Interface, pilih interface yang terhubung ke internet (misalnya Ether1). Pada tab Action, pilih masquerade. Konfigurasi ini akan menyembunyikan alamat IP lokal di balik IP publik router, memungkinkan client LAN untuk terhubung ke internet.

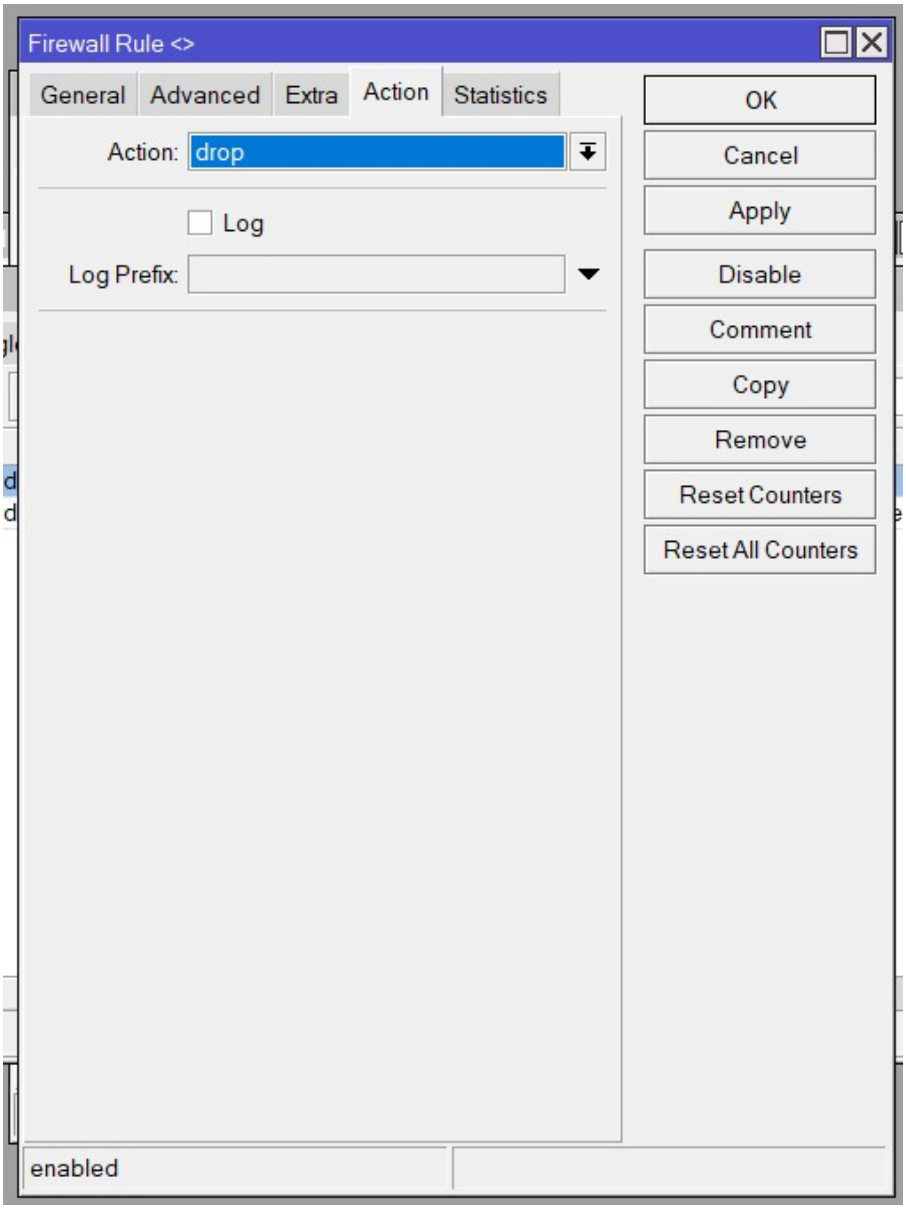
8. **Menambahkan Rule Forward untuk Trafik ICMP dari LAN**



Gambar 4: Rule Forward

Tambahkan rule baru pada IP → Firewall → Filter Rules dengan Chain: forward dan In. Interface: ether7, serta protokol ICMP (untuk ping). Ini digunakan untuk mengontrol trafik dari LAN ke jaringan lain.

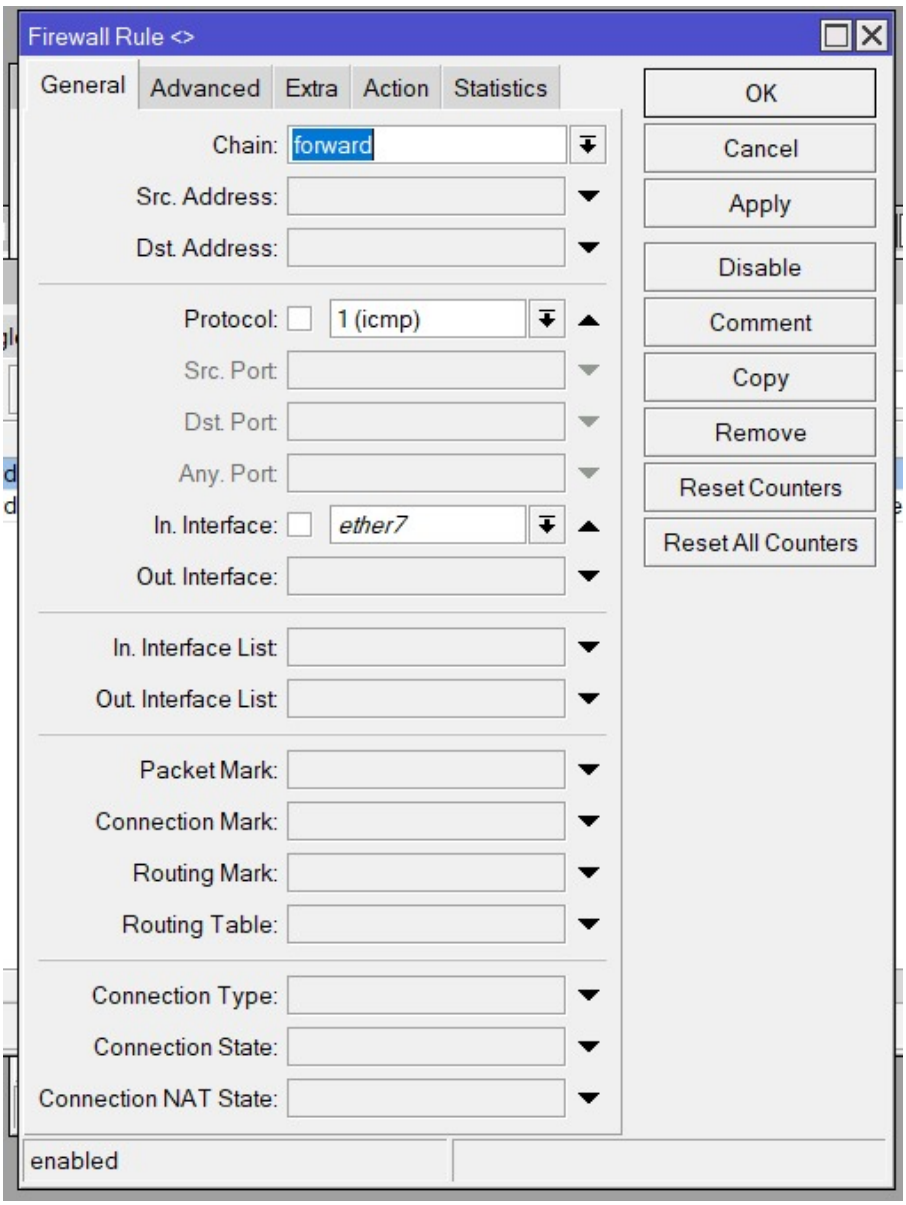
9. **Menetapkan Aksi Drop dan Logging**



Gambar 5: Drop dan Logging

Pada tab Action, pilih drop dan aktifkan log jika diperlukan. Rule ini akan memblokir trafik sesuai kriteria yang ditentukan, sekaligus mencatatnya ke log.

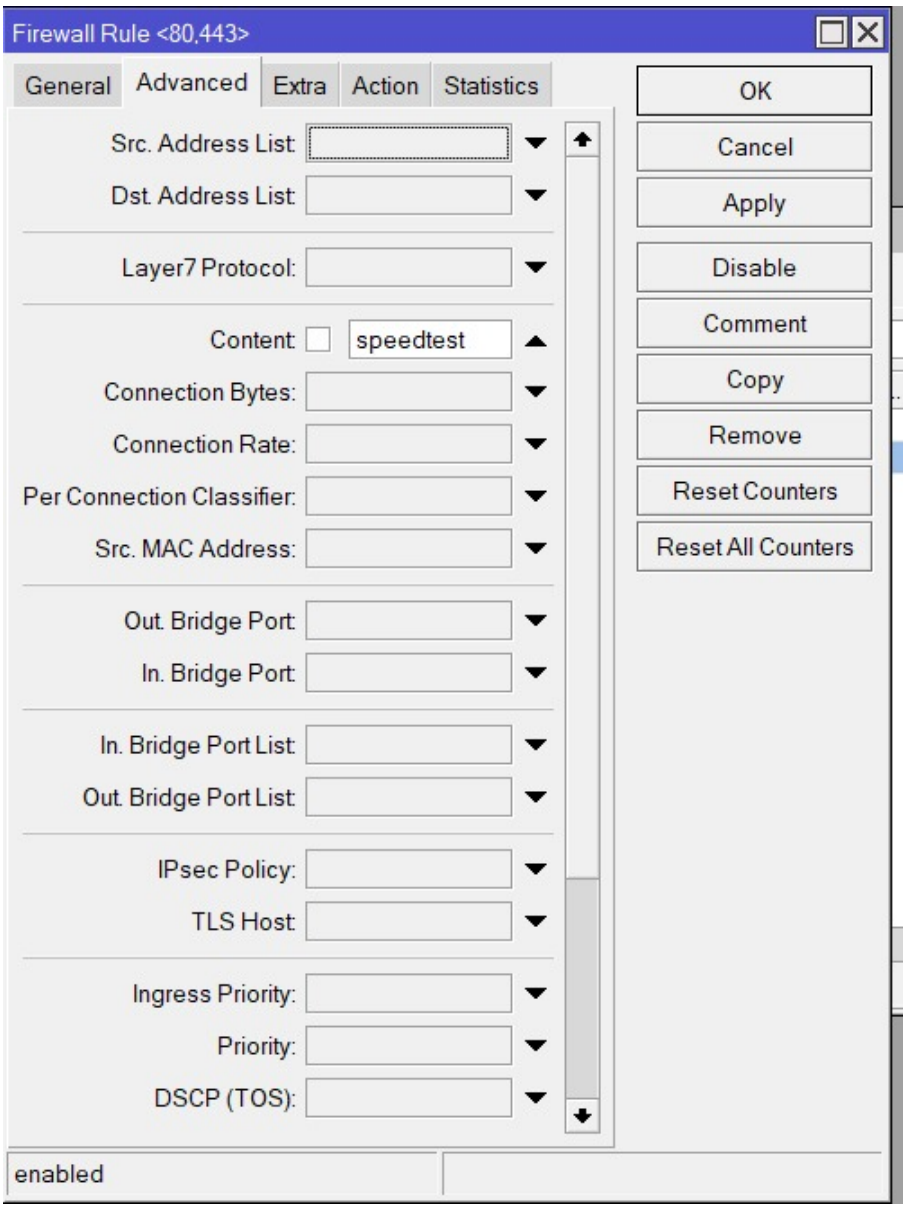
10. **Memblokir Akses ke Port**



Gambar 6: Blokir akses ke port

Contoh konfigurasi firewall untuk memblokir akses ke port 443 (HTTPS) dari jaringan LAN (ether7) ke internet (ether1). Bisa digunakan untuk membatasi akses tertentu.

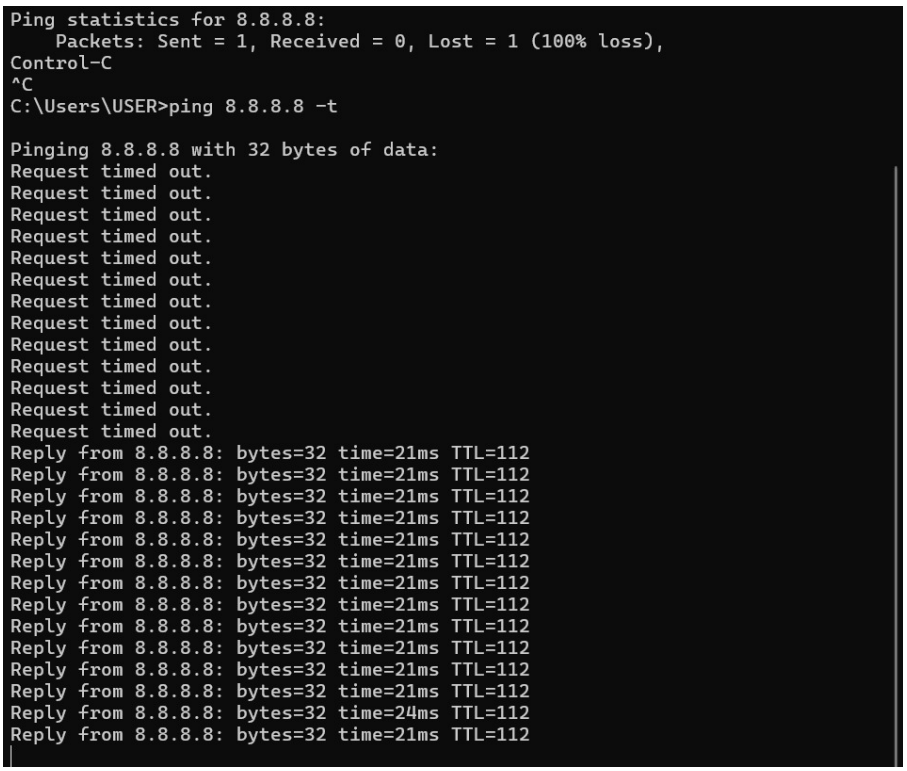
11. **Memblokir Akses Speedtest Menggunakan Layer7 Protocol**



Gambar 7: Blokir spreedtest

Menggunakan fitur Layer7 Protocol dengan pola speedtest, rule ini digunakan untuk memblokir akses ke layanan Speedtest.net agar tidak mengganggu bandwidth utama.

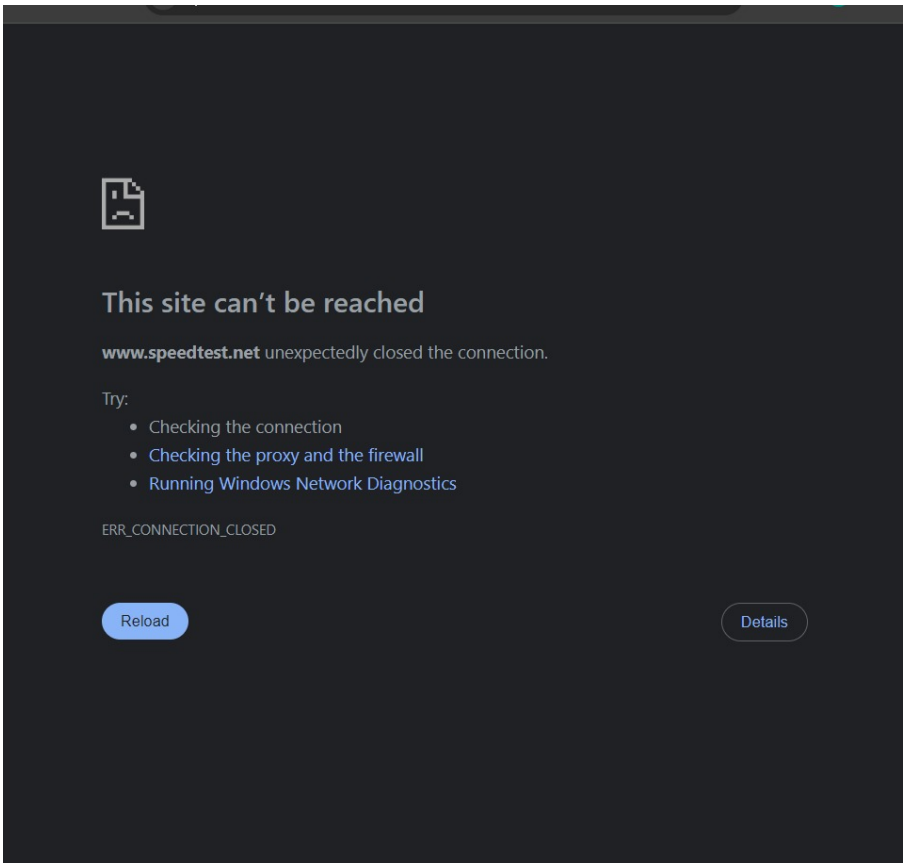
12. **Hasil ping ke 8.8.8.8**



```
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 8: Hasil ping

13. **Hasil pemblokiran pada akses web speedtest.net**



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

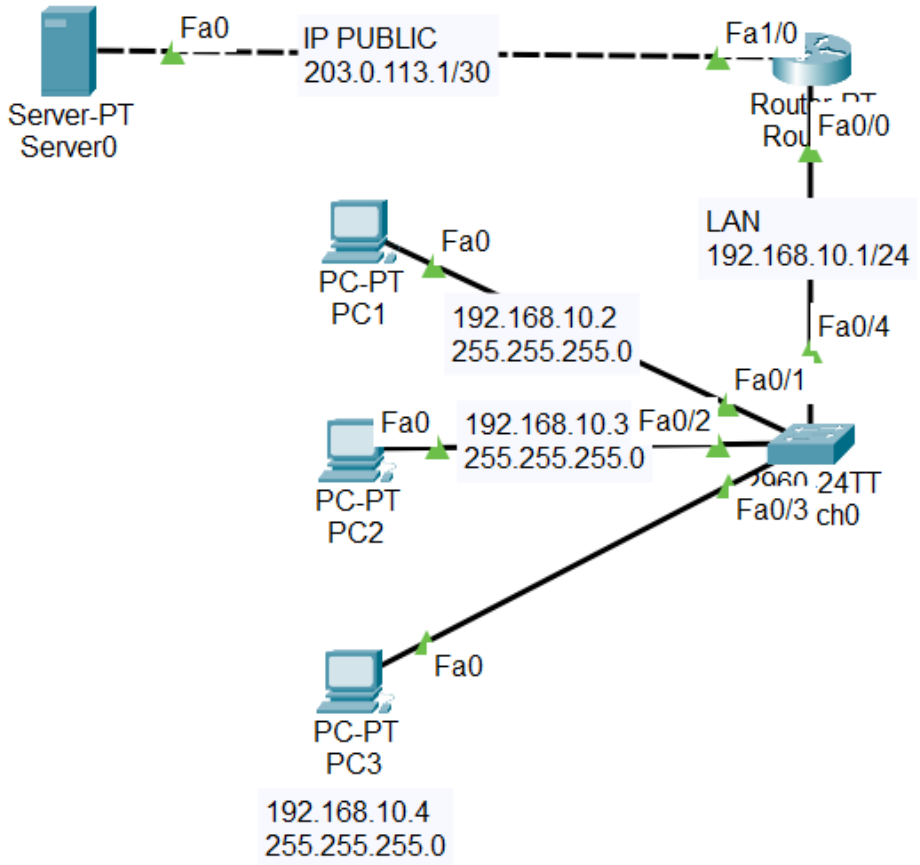
Gambar 9: hasil pemblokiran web

2 Analisis Hasil Percobaan

Dalam percobaan ini, dilakukan pengaturan jaringan untuk mengelola koneksi dan membatasi akses dari jaringan lokal ke internet. NAT diaktifkan untuk memungkinkan perangkat di LAN terhubung ke internet dengan menerjemahkan IP privat ke IP publik. Kemudian, rule firewall ditambahkan untuk memblokir akses ke DNS Google (8.8.8.8) dan layanan Speedtest sebagai langkah pembatasan akses tertentu, baik demi keamanan maupun efisiensi penggunaan bandwidth. Selain itu, interface ether1 yang terhubung ke ISP dikonfigurasi sebagai DHCP Client agar dapat menerima IP secara otomatis. Di sisi lain, router juga berfungsi sebagai DHCP Server bagi perangkat LAN, sehingga tiap klien mendapatkan alamat IP tanpa perlu pengaturan manual.

3 Hasil Tugas Modul

1. **Perancangan Topologi di cisco Packet Tracer**



Gambar 10: Hasil Tugas Modul

Jaringan ini menghubungkan semua perangkat dengan alamat IP masing-masing. Server memiliki IP publik (203.0.113.1), sedangkan router dan PC berada pada jaringan lokal 192.168.10.0-/24. Koneksi dibuat agar semua perangkat dapat saling berkomunikasi sesuai fungsi yang diinginkan.

2. **Pengaturan NAT (Network Addres translation)** NAT dikonfigurasi agar semua PC pada jaringan lokal dapat mengakses server menggunakan alamat IP publik milik router. Hal ini memungkinkan komunikasi antara jaringan privat dan internet melalui translasi alamat jaringan.

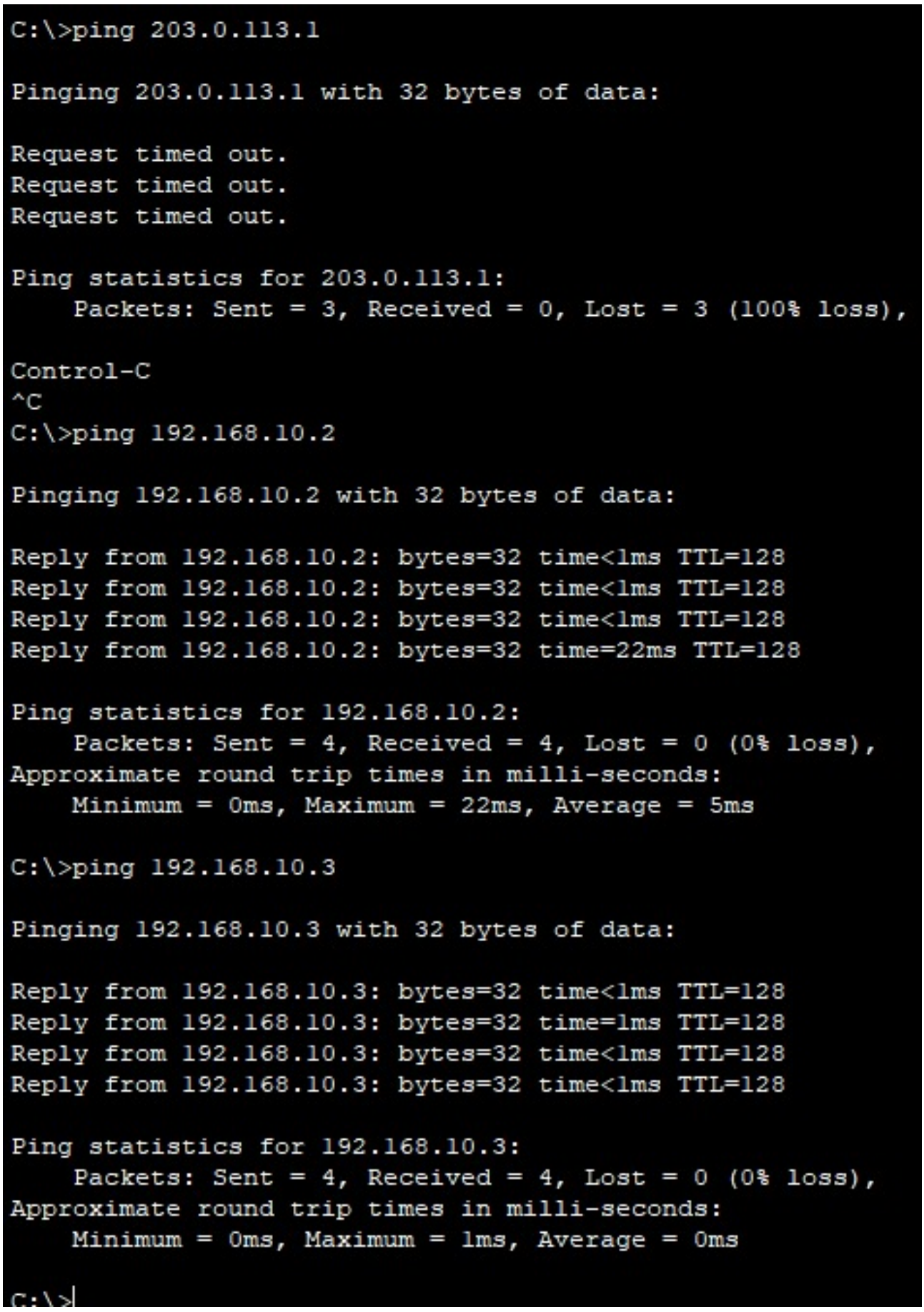
3. **Pengaturan Firewall dengan ACL**

```
C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

Reply from 203.0.113.1: bytes=32 time<1ms TTL=127
Reply from 203.0.113.1: bytes=32 time<1ms TTL=127
Reply from 203.0.113.1: bytes=32 time<1ms TTL=127
Reply from 203.0.113.1: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 11: menunjukkan bahwa PC1 berhasil melakukan ping ke server (203.0.113.1) dan juga ke perangkat lain di jaringan lokal.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Control-C
^C
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Gambar 12: memperlihatkan bahwa PC2 tidak dapat menjangkau server karena permintaan ping mengalami request timed out, tetapi tetap dapat terhubung dengan perangkat lain di LAN.



Gambar 13: menggambarkan kondisi serupa untuk PC3, yang gagal menjangkau server tetapi tetap bisa berkomunikasi dengan PC1 dan PC2.

Dengan konfigurasi ini, hanya PC1 yang memiliki izin untuk berkomunikasi dengan server publik, sedangkan seluruh PC masih bisa saling berhubungan dalam jaringan lokal.

4 Kesimpulan

Berdasarkan hasil percobaan, dapat disimpulkan bahwa penggunaan NAT berperan penting dalam menghubungkan perangkat LAN ke internet melalui IP publik router. Konfigurasi firewall yang membatasi akses ke DNS Google dan layanan Speedtest menunjukkan penerapan kontrol akses demi keamanan dan pengelolaan trafik. Selain itu, dengan mengaktifkan DHCP Client pada interface menuju ISP, router dapat menerima IP publik secara otomatis. Sementara itu, fungsi DHCP Server di sisi LAN memudahkan pembagian IP ke perangkat secara otomatis tanpa pengaturan manual.