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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

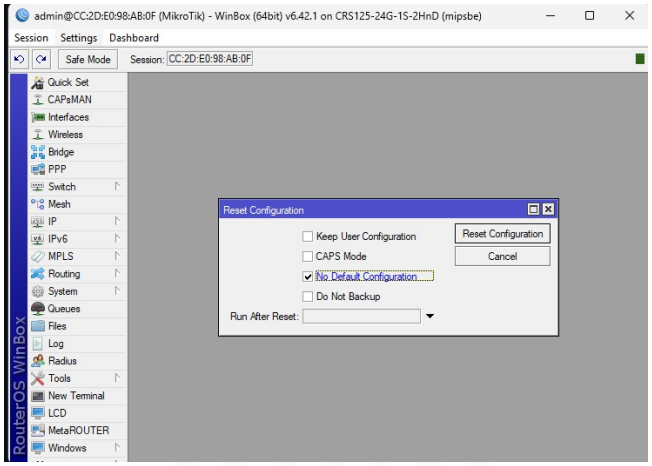
Muhammad Tamim Nugraha - 502423060

31 Mei 2025

1 Langkah-Langkah Percobaan

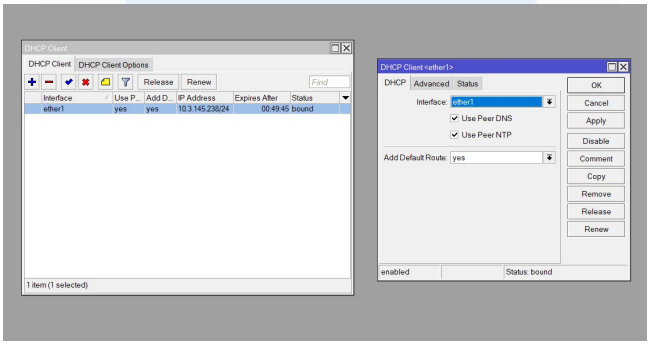
1.1 Percobaan 1 : Firewall dan NAT

1. Siapkan seluruh alat dan bahan yang diperlukan, lalu lakukan pengembalian konfigurasi Mikrotik ke pengaturan awal melalui Winbox dengan fungsi *Reset Configuration*.



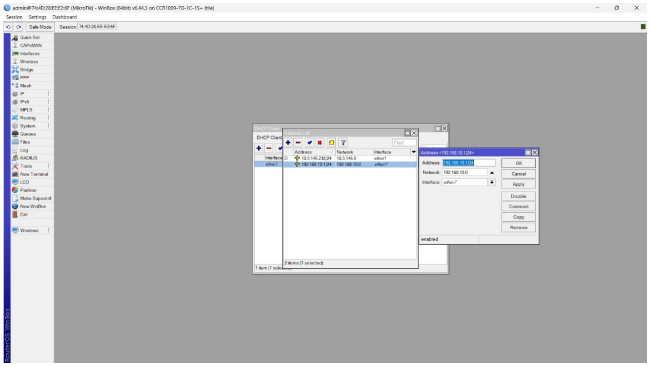
Gambar 1: Pengembalian konfigurasi Mikrotik ke setelan pabrik

2. Di Router A, buka menu IP > DHCP Client. Buat sebuah entri baru yang diterapkan pada antarmuka `ether1`. Pastikan untuk mencentang opsi *Use PeerDNS* dan *Use PeerNTP*, kemudian setelah diterapkan, verifikasi bahwa statusnya adalah "Bound".



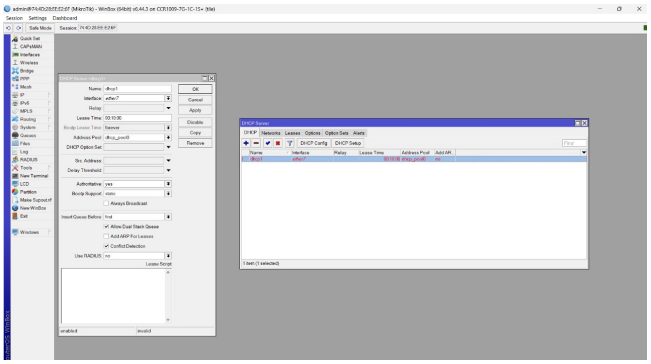
Gambar 2: Melakukan pengaturan pada DHCP Client

3. Selanjutnya, tambahkan sebuah alamat IP untuk `ether7` yang terhubung ke switch. Proses ini dilakukan melalui menu IP > Addresses dengan menambahkan konfigurasi: Address: `192.168.10.1/24`, dan Interface: `ether7`, lalu Apply.



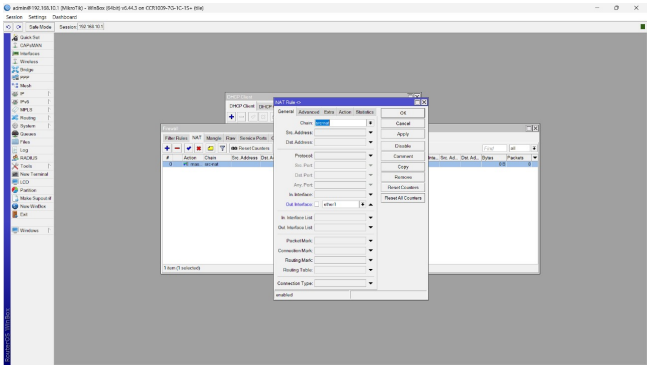
Gambar 3: Menetapkan alamat IP untuk koneksi ke Switch

4. Lakukan konfigurasi DHCP Server pada router dengan mengakses menu IP > DHCP Server dan memilih DHCP Setup. Tentukan `ether7` sebagai antarmuka DHCP dan lanjutkan proses dengan menekan *Next* hingga selesai tanpa ada perubahan konfigurasi.

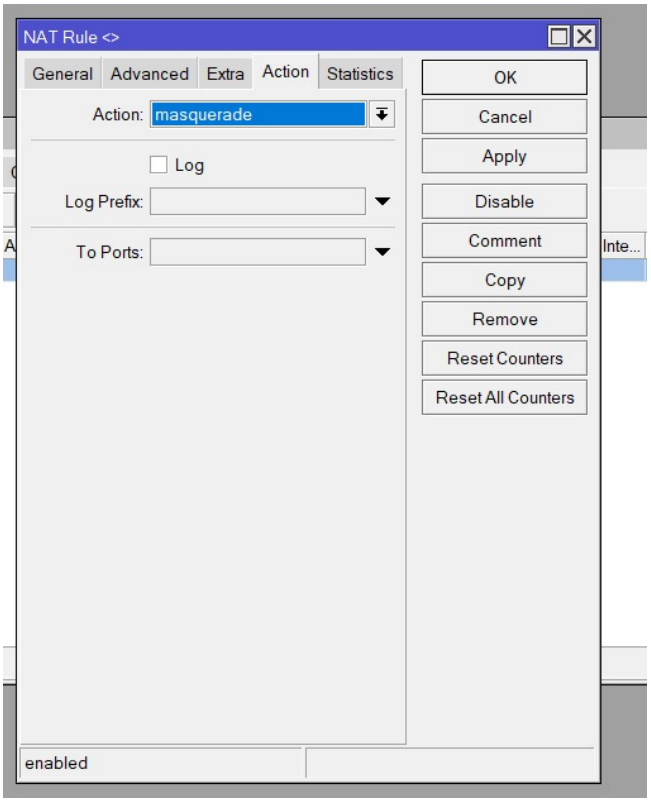


Gambar 4: Melakukan pengaturan pada DHCP Server

5. Langkah berikutnya adalah mengatur NAT. Buka IP > Firewall > NAT. Tambahkan sebuah aturan baru di mana pada tab General, *chain* diatur menjadi `src-nat`, dan pada tab Action, *action* diatur menjadi `masquerade`. Terapkan perubahan tersebut.

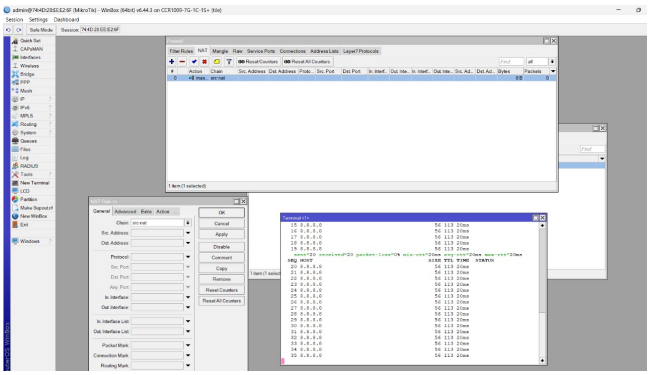


Gambar 5: Proses konfigurasi NAT



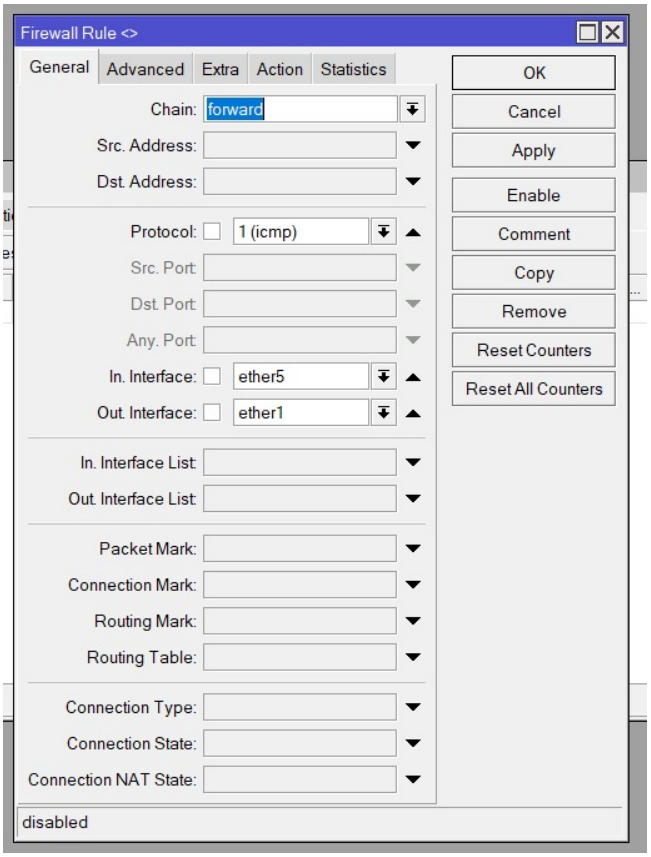
Gambar 6: Pengaturan action pada aturan NAT

6. Uji konektivitas internet dari router dengan menjalankan perintah `ping 8.8.8.8` pada New Terminal.



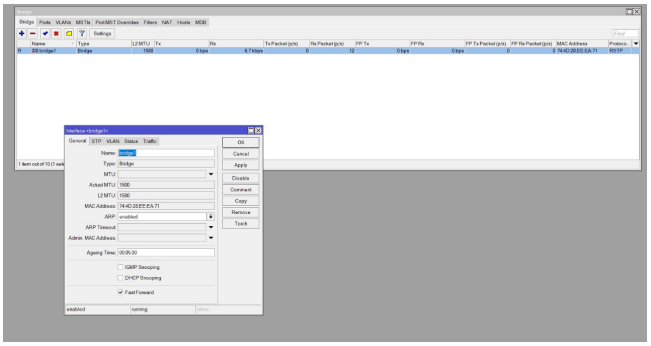
Gambar 7: Uji koneksi ping ke 8.8.8.8

7. Setelah itu, konfigurasikan sebuah *Filter Rule* di Firewall untuk memblokir trafik ICMP. Di menu IP > Firewall, tambahkan aturan dengan parameter: pada tab General, Chain: `forward`, Protocol: `icmp`, In. Interface: `ether7`. Pada tab Action, atur Action: `drop`.



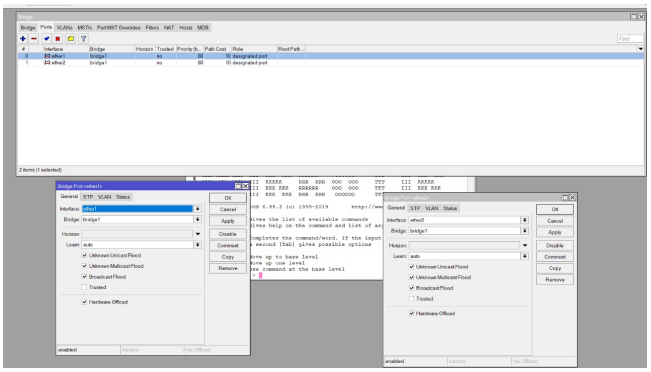
Gambar 8: Pengaturan firewall untuk memblokir protokol ICMP

8. Pada perangkat Router B, buat sebuah bridge baru dengan mengakses menu Bridge, lalu klik tambah dan Apply.



Gambar 9: Membuat bridge baru pada Router B

9. Masih di menu Bridge, buka tab Ports. Tambahkan antarmuka yang tersambung ke laptop dan antarmuka yang terhubung ke Router A ke dalam bridge.



Gambar 10: Menambahkan antarmuka ke dalam port bridge

10. Di sisi laptop, pastikan konfigurasi IP diatur ke DHCP (otomatis). Kemudian, buka Command Prompt dan lakukan ping ke alamat `google.com`.

```
C:\Users\Lolwkwk123>ping google.com

Pinging google.com [172.253.118.101] with 32 bytes of data:
Request timed out.

Ping statistics for 172.253.118.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
```

Gambar 11: Uji ping ke google.com dengan aturan ICMP aktif

11. Untuk sementara, nonaktifkan aturan firewall ICMP dengan mengklik tanda "X" (*disable*) pada daftar *Filter Rules*. Lakukan kembali ping ke `google.com`.

```
C:\Users\Lolwkwk123>ping google.com

Pinging google.com [172.253.118.101] with 32 bytes of data:
Reply from 172.253.118.101: bytes=32 time=21ms TTL=105
Reply from 172.253.118.101: bytes=32 time=21ms TTL=105
Reply from 172.253.118.101: bytes=32 time=21ms TTL=105
Reply from 172.253.118.101: bytes=32 time=21ms TTL=105

Ping statistics for 172.253.118.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 21ms, Average = 21ms

C:\Users\Lolwkwk123>
```

Gambar 12: Uji ping ke google.com setelah aturan ICMP dinonaktifkan

12. Dengan metode yang sama, tambahkan aturan firewall baru untuk memblokir konten situs. Parameter pada tab General adalah: Chain: `forward`, Protocol: `tcp`, Dst. Port: `80,443`, In. Interface: `ether7`, Out. Interface: `ether1`. Pada tab Advanced, isi Content dengan "speedtest". Pada tab Action, pilih Action: `drop`. Namun, hasil percobaan menunjukkan kegagalan, karena laptop masih dapat mencari dan mengakses konten "speedtest".

2 Analisis Hasil Percobaan

Pada tahap awal percobaan, router Mikrotik dikembalikan ke pengaturan awal menggunakan fitur *Reset Configuration*, kemudian dilakukan konfigurasi DHCP Client pada antarmuka `ether1` agar

router memperoleh IP otomatis dari jaringan eksternal. Selanjutnya, `ether7` dikonfigurasi dengan IP statis dan difungsikan sebagai jalur distribusi DHCP Server untuk perangkat di jaringan lokal. Keberhasilan distribusi IP ditunjukkan dengan status “Bound” pada DHCP Client dan laptop yang berhasil menerima alamat IP.

Konfigurasi NAT menggunakan metode *masquerade* juga berjalan dengan baik. Hal ini dibuktikan dengan kemampuan perangkat dalam jaringan lokal untuk mengakses internet dan merespons perintah `ping` ke alamat publik seperti `8.8.8.8`, yang menunjukkan bahwa proses penyamaran IP lokal ke IP publik berjalan dengan benar.

Pengujian firewall dilakukan dengan membuat aturan untuk memblokir lalu lintas ICMP melalui *filter rule* dengan `chain "forward"` dan `protocol "icmp"`. Hasilnya, permintaan `ping` dari laptop ke `google.com` gagal, dan ketika aturan tersebut dinonaktifkan, koneksi kembali normal. Ini membuktikan bahwa fungsi firewall beroperasi sesuai konfigurasi yang diterapkan.

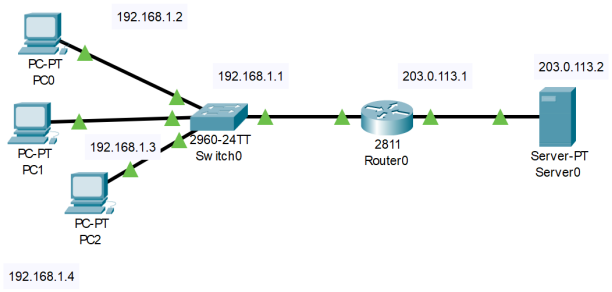
Selanjutnya, konfigurasi *bridge* pada Router B serta penambahan port yang terhubung ke laptop dan Router A berhasil dilakukan, dibuktikan dengan jaringan tetap tersambung dan dapat diakses melalui laptop.

Namun, pada percobaan akhir yang bertujuan melakukan *content filtering* terhadap kata “speedtest” pada port TCP `80` dan `443`, konfigurasi firewall tidak berhasil. Walaupun aturan telah dibuat secara teoritis benar, konten yang mengandung kata tersebut masih bisa diakses lewat *browser*. Kegagalan ini diduga disebabkan oleh dua hal: kemungkinan adanya malfungsi pada sistem Mikrotik yang digunakan, atau karena protokol HTTPS (port `443`) yang mengenkripsi lalu lintas sehingga Mikrotik tidak dapat membaca isi konten dan menerapkan penyaringan berbasis kata kunci secara efektif.

3 Hasil Tugas Modul

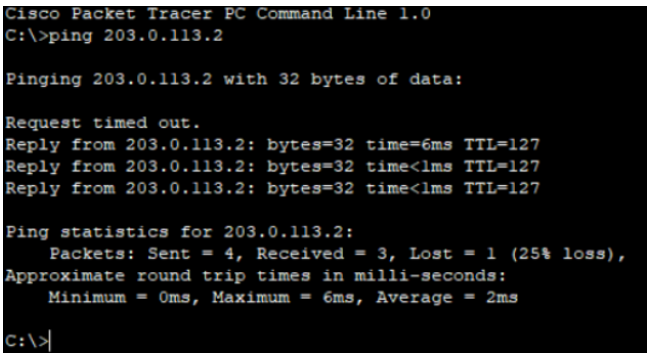
1. Membuat sebuah topologi sederhana dalam perangkat lunak Cisco Packet Tracer dengan komponen-komponen berikut:

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

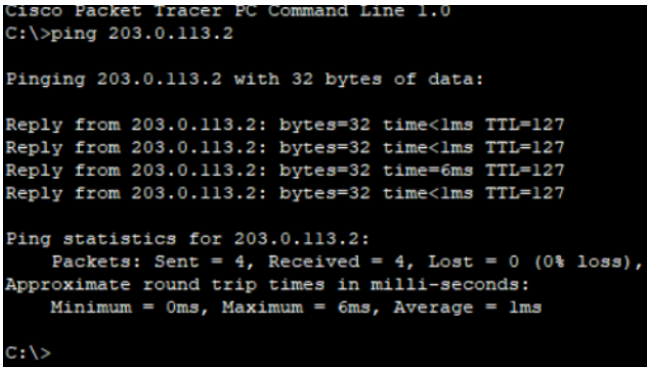


Gambar 13: Rancangan topologi jaringan

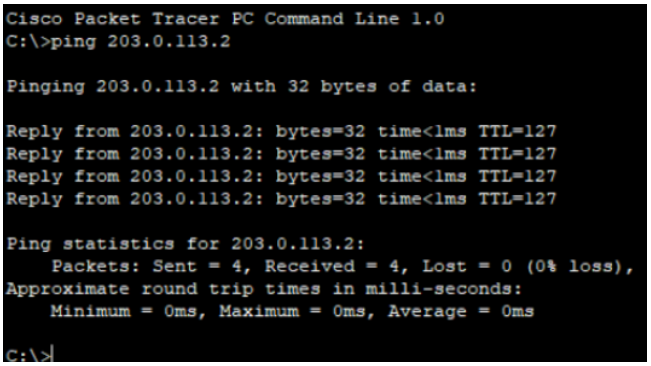
2. Mengonfigurasi NAT dengan tujuan agar setiap PC dapat mengakses Server dengan memanfaatkan IP publik yang ada pada Router.



Gambar 14: Uji konektivitas dari PC1 menuju Server

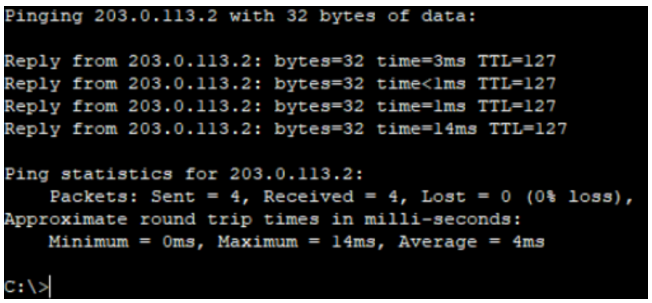


Gambar 15: Uji konektivitas dari PC2 menuju Server

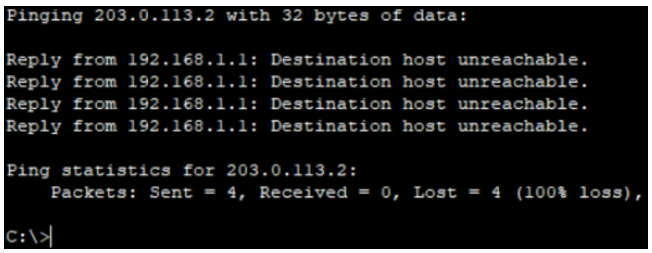


Gambar 16: Uji konektivitas dari PC3 menuju Server

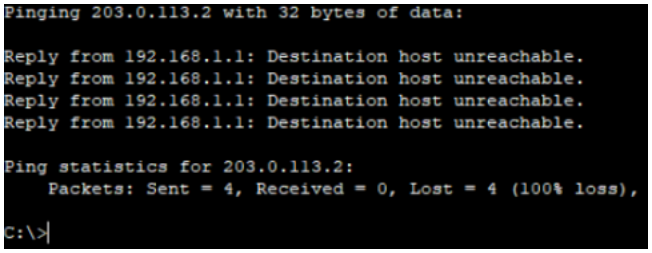
3. Mengonfigurasi Firewall (ACL) dengan kebijakan sebagai berikut:
    - Memberikan izin akses ke Server hanya untuk PC1.
    - Memblokir akses dari PC2 dan PC3 ke Server.
    - Memastikan semua PC masih bisa terhubung satu sama lain di dalam jaringan LAN.



Gambar 17: Hasil ping dari PC1 ke Server setelah ACL diterapkan



Gambar 18: Hasil ping dari PC2 ke Server setelah ACL diterapkan



Gambar 19: Hasil ping dari PC3 ke Server setelah ACL diterapkan

4 Kesimpulan

Berdasarkan hasil eksperimen konfigurasi Firewall dan NAT pada perangkat Mikrotik, dapat disimpulkan bahwa beberapa konfigurasi dasar seperti pengaturan DHCP Client, pemberian IP statis, penerapan NAT dengan teknik masquerade, serta penyusunan DHCP Server berhasil diterapkan dan berfungsi sebagaimana mestinya. Pengujian firewall terhadap protokol ICMP juga menunjukkan keberhasilan Mikrotik dalam memblokir lalu lintas tertentu sesuai dengan aturan yang telah ditetapkan. Selain itu, konfigurasi bridge pada Router B berjalan lancar tanpa mengganggu koneksi jaringan ke perangkat pengguna. Meskipun begitu, uji coba content filtering tidak berhasil. Hal ini mengindikasikan bahwa fitur penyaringan konten berbasis kata kunci kurang efektif, terutama dalam menangani lalu lintas HTTPS yang telah dienkripsi. Selain faktor enkripsi, kemungkinan adanya gangguan pada sistem Mikrotik turut menjadi penyebab kegagalan fungsi filter konten secara optimal.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 20: Foto dokumentasi selama kegiatan praktikum berlangsung