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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Mochamad Rafila Putra Firmansyah - 5024231066

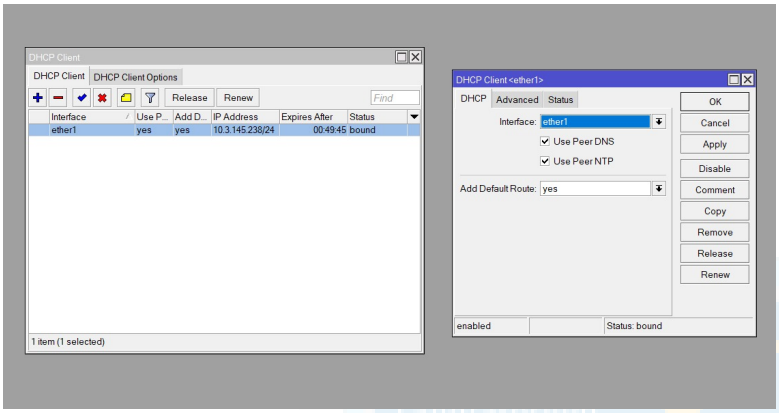
2025

1 Langkah-Langkah Percobaan

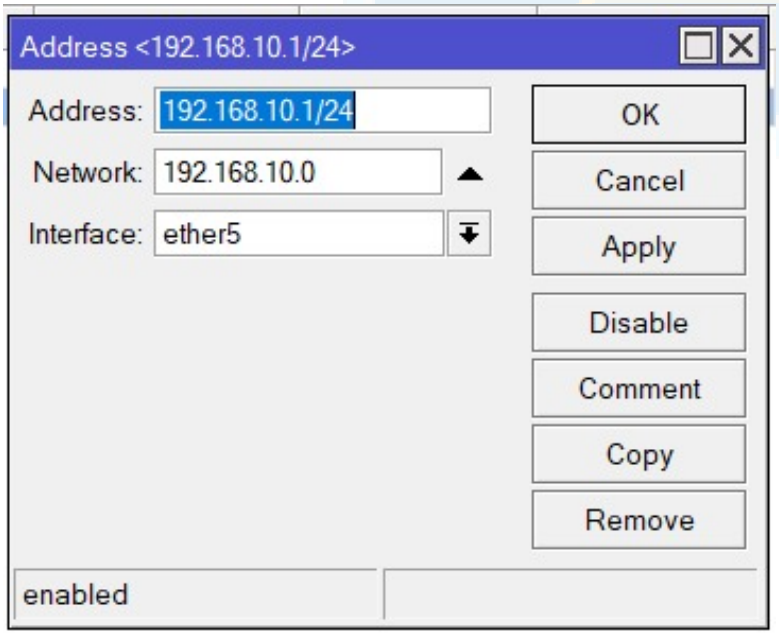
1. **Reset Router**
   Akses *Winbox* > System > Reset Configuration. Centang *No Default Configuration*, lalu klik *Reset Configuration*.

2. **Login ke Router**
   Hubungkan router via *Winbox* menggunakan MAC address atau IP default. Username: `admin`, tanpa password jika belum diatur.

3. **Konfigurasi DHCP Client pada ether1 (Router A)**
   Akses *IP* > *DHCP Client*, klik `+`, pilih `ether1`, klik *Apply*. Status koneksi harus `bound`.



4. **Penambahan IP pada ether5**
   Akses *IP* > *Addresses*, klik `+`, isi address `192.168.10.1/24`, pilih interface `ether5`, klik *Apply* dan *OK*.

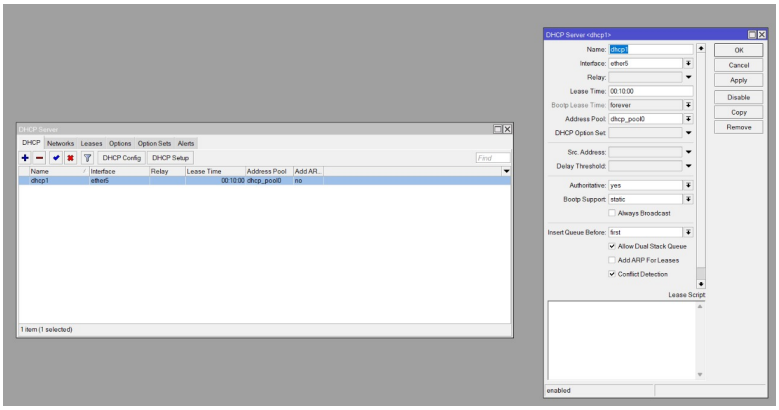


5. **Konfigurasi DHCP Server**
   Akses *IP* > *DHCP Server*, klik *DHCP Setup*, lalu:

   - Interface: `ether5`
   - Address Space: `192.168.10.0/24`

- Gateway: `192.168.10.1`
- Address Range: `192.168.10.2-192.168.10.254`
- DNS: `8.8.8.8`, `8.8.4.4`
- Lease Time: `00:10:00`

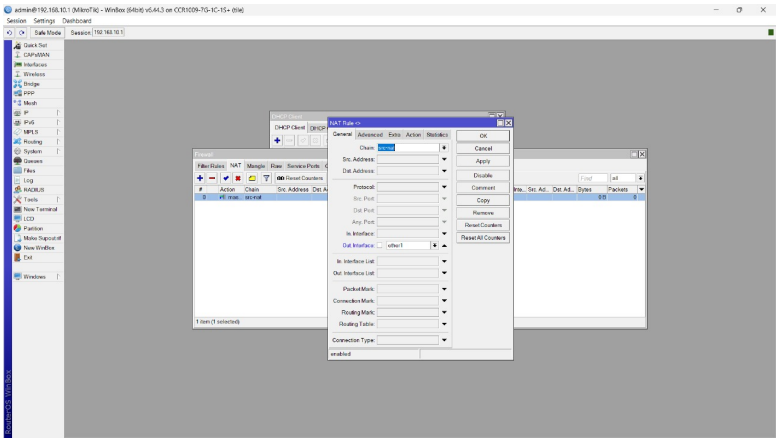
Selesaikan wizard hingga muncul pesan *Setup has completed successfully*.



6. **Konfigurasi NAT**
   Akses *IP* > *Firewall* > *NAT*, klik `+`. Atur:

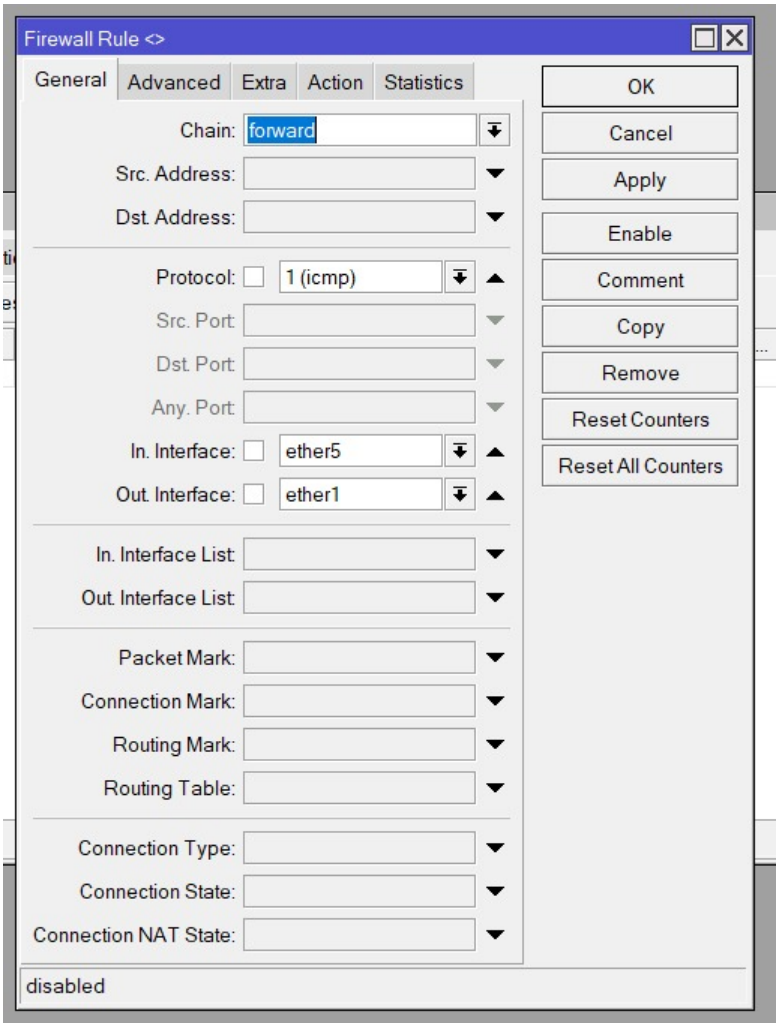
   - Tab General: `Chain = src-nat`
   - Tab Action: `Action = masquerade`

   Klik *Apply* dan *OK*, lalu lakukan `ping 8.8.8.8` di Terminal untuk uji koneksi.



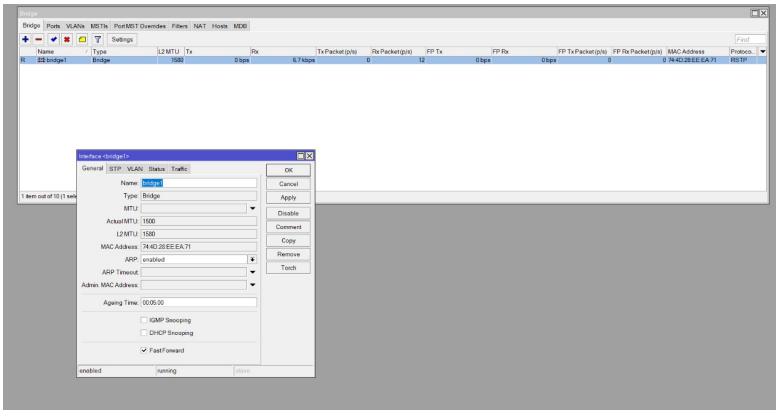
7. **Konfigurasi Firewall**
   Akses *IP* > *Firewall* > *Filter Rules*, klik `+`.

   - **Blok ICMP:**
     Chain: `forward`, Protocol: `icmp`, In Interface: `ether5`, Action: `drop`
   - **Blok Konten:**
     Chain: `forward`, Protocol: `tcp`, Dst Port: `80,443`, In: `ether5`, Out: `ether1`, Content: `speedtest`, Action: `drop`



8. **Konfigurasi Bridge pada Router B**
   Akses *Bridge*, klik +, klik *Apply* dan *OK*.
   Tambahkan port:

   - Akses *Bridge* > *Port*, klik +, masukkan dua interface (ke laptop dan ke Router A).



9. **Konfigurasi IP Laptop**
   Atur agar laptop mendapat IP via DHCP. Cek dengan `ipconfig` di CMD.

10. **Uji Coba Konfigurasi**

    - **Uji Koneksi (ICMP)**:

Ping `8.8.8.8`. Saat firewall aktif, seharusnya `Request Timed Out`. Nonaktifkan firewall ICMP dan ulangi ping.

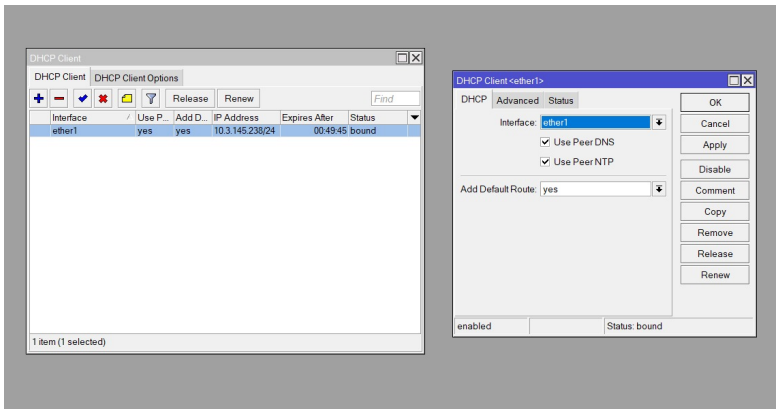
```
C:\Users\Lolwkwk123>ping google.com

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
```

- **Uji Pemblokiran Konten**:
  Akses situs dengan kata `speedtest`. Seharusnya gagal. Nonaktifkan aturan, lalu akses ulang.

2 Analisis Hasil Percobaan

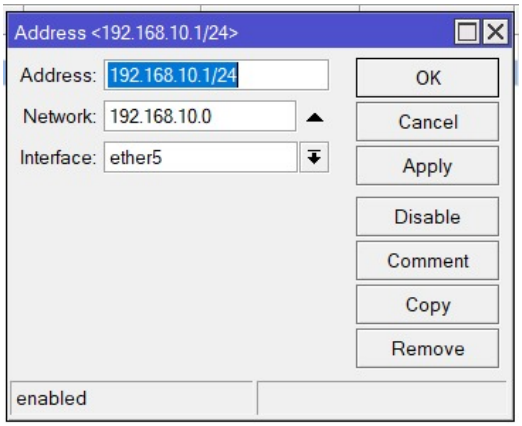
Berdasarkan konfigurasi dan hasil pengujian, seluruh tahapan praktikum Firewall dan NAT telah berhasil dijalankan dengan baik.

Pada konfigurasi **DHCP Client** yang ditampilkan pada Gambar 1, interface `ether1` berhasil mendapatkan alamat IP secara dinamis dari penyedia layanan internet (contoh: `10.3.145.238/24`) dengan status *bound*. Hal ini menandakan Router A terhubung ke jaringan luar.



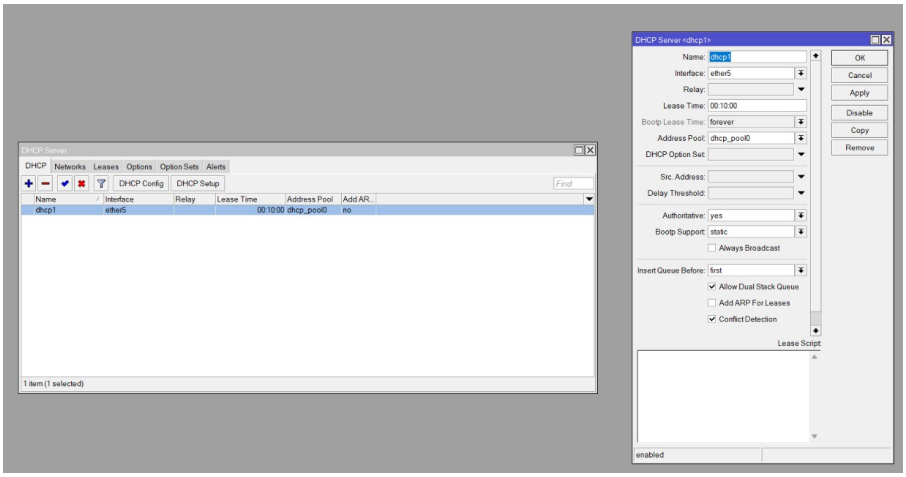
Gambar 1: Konfigurasi DHCP Client pada ether1

Selanjutnya, Gambar 2 menunjukkan pemberian IP statis `192.168.10.1/24` pada interface lokal (dalam gambar: `ether5`), yang menjadi gateway untuk jaringan internal.



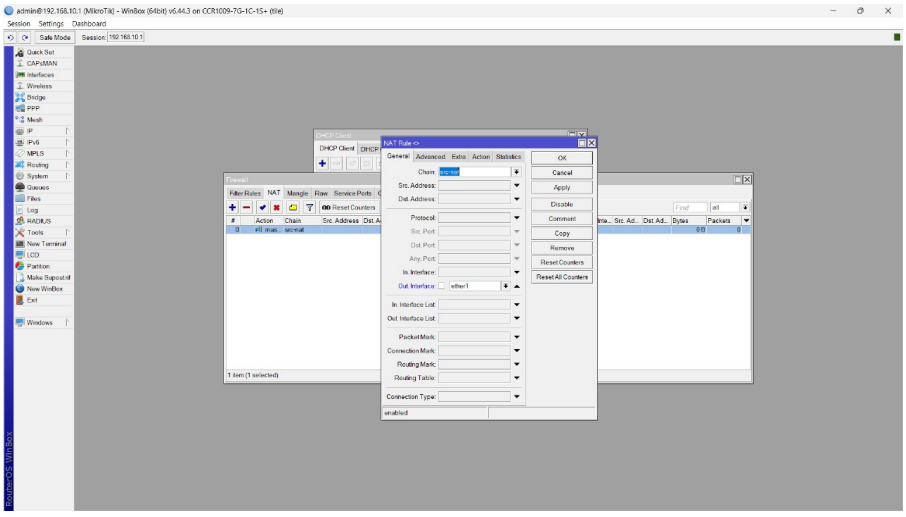
Gambar 2: Penambahan alamat IP lokal pada ether7

Gambar 3 memperlihatkan konfigurasi DHCP Server pada interface lokal, lengkap dengan waktu sewa (lease time) dan pool alamat IP. Ini memungkinkan distribusi IP ke klien secara otomatis.



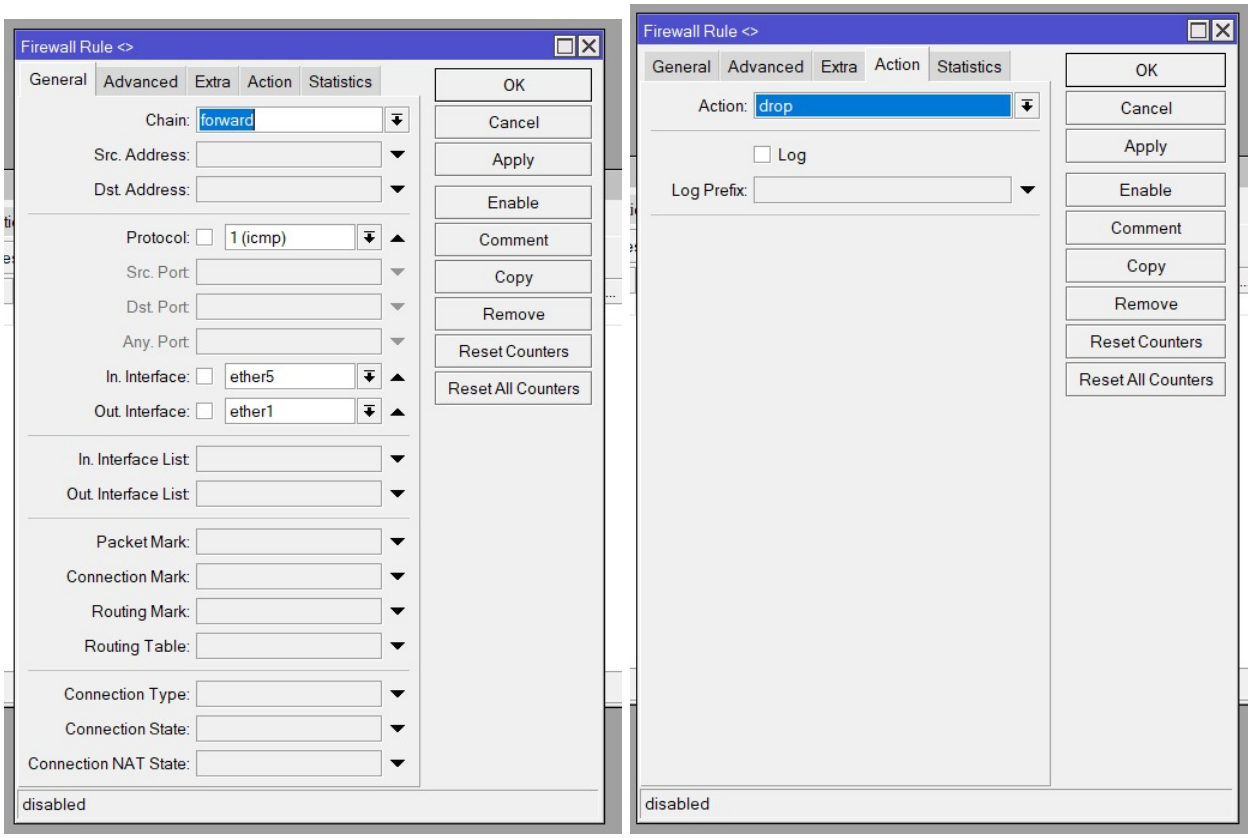
Gambar 3: Konfigurasi DHCP Server pada ether5

Konfigurasi NAT juga telah dilakukan seperti terlihat pada Gambar 4, menggunakan teknik `masquerade` agar perangkat dengan IP privat bisa mengakses internet menggunakan IP publik router.



Gambar 4: Konfigurasi NAT dengan teknik masquerade

Firewall diuji dengan memblokir paket ICMP. Gambar 5 menunjukkan aturan firewall yang dibuat, dan Gambar 6 menunjukkan hasil ping yang gagal karena rule tersebut aktif.

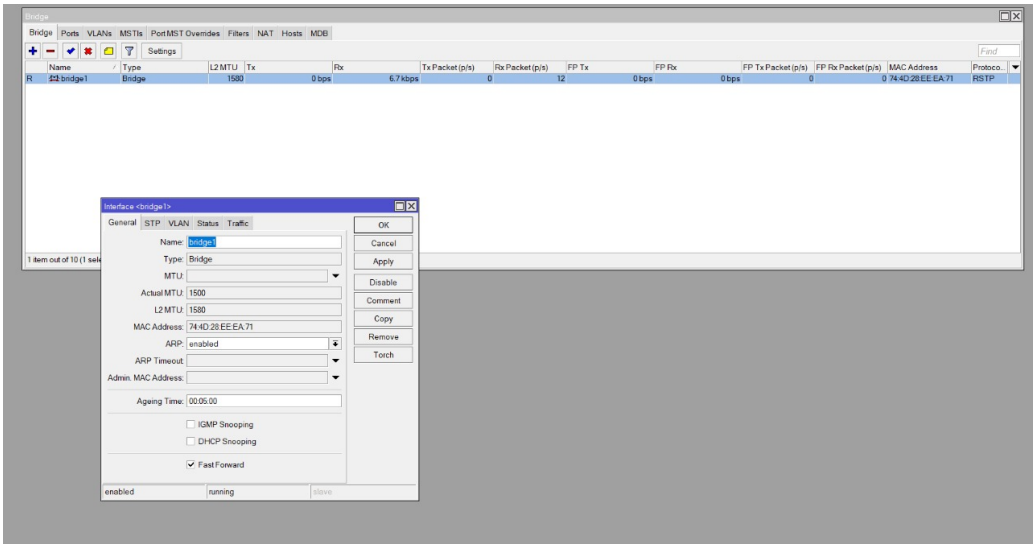


Gambar 5: Firewall Rule untuk memblokir paket ICMP

```
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 6: Hasil ping menunjukkan koneksi diblokir (RTO)

Terakhir, konfigurasi bridge pada Router B ditampilkan pada Gambar 9. Bridge ini memungkinkan router bertindak sebagai switch, meneruskan lalu lintas antar port tanpa proses routing.



Gambar 7: Konfigurasi bridge pada Router B

Seluruh konfigurasi yang diterapkan sesuai dengan rancangan dan memberikan hasil yang diharapkan: koneksi internet tersedia melalui NAT, distribusi IP berjalan otomatis melalui DHCP, dan rule firewall berhasil memfilter trafik yang tidak diizinkan.

3 Hasil Tugas Modul

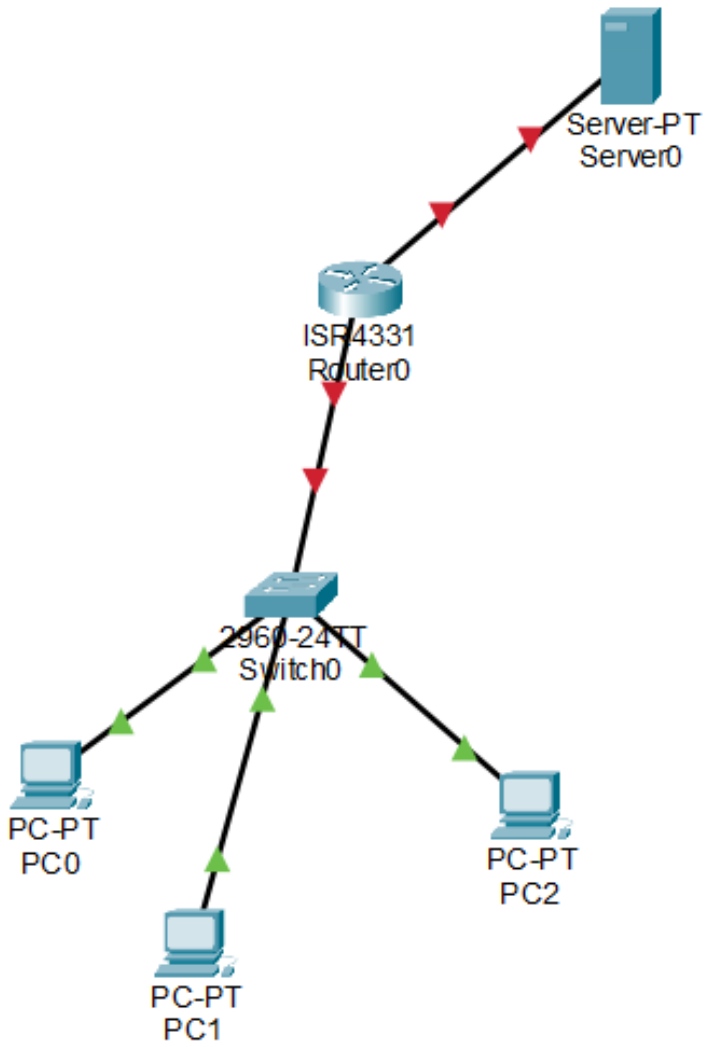
1. Desain Topologi

Topologi jaringan yang digunakan dalam simulasi ini terdiri dari:

- 1 Router (Cisco 2911)
- 1 Switch (Cisco 2960)
- 3 PC (PC1, PC2, PC3)
- 1 Server (sebagai server Internet/Public)

Topologi jaringan yang dibuat dapat dilihat pada Gambar 8 berikut.
Alamat IP yang digunakan adalah sebagai berikut:

- **Router Gig0/0 (LAN)**: 192.168.1.1/24
- **Router Gig0/1 (WAN)**: 203.0.113.1/30
- **PC1**: 192.168.1.10
- **PC2**: 192.168.1.11
- **PC3**: 192.168.1.12
- **Server (Public)**: 203.0.113.2/30



Gambar 8: Topologi Jaringan NAT dan ACL

2. Konfigurasi NAT

Konfigurasi NAT dilakukan agar semua PC dapat mengakses server melalui IP publik dari router. Berikut adalah konfigurasi NAT pada router:

```
conf t
interface Gig0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
exit

interface Gig0/1
```

```
 ip address 203.0.113.1 255.255.255.252
 ip nat outside
exit

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface Gig0/1 overload
```

3. Konfigurasi Firewall (ACL)

Agar hanya PC2 yang dapat mengakses server, konfigurasi Access Control List (ACL) diterapkan sebagai berikut:

```
access-list 100 permit ip host 192.168.1.11 host 203.0.113.2
access-list 100 deny ip host 192.168.1.10 host 203.0.113.2
access-list 100 deny ip host 192.168.1.12 host 203.0.113.2
access-list 100 permit ip any any

interface Gig0/1
 ip access-group 100 out
```

Konfigurasi di atas memastikan bahwa hanya PC2 yang dapat mengakses server (IP 203.0.113.2), sementara PC1 dan PC3 diblokir. Namun, seluruh PC masih dapat saling terhubung melalui LAN.

4. Pengujian dan Dokumentasi

Pengujian koneksi dilakukan dengan menggunakan perintah `ping` dari masing-masing PC:

- PC1, PC2, dan PC3 dapat saling ping satu sama lain melalui jaringan LAN.
- PC2 berhasil melakukan `ping` ke Server.
- PC1 dan PC3 gagal `ping` ke Server.

4 Kesimpulan

Praktikum Firewall dan NAT pada MikroTik berhasil menunjukkan pentingnya peran manajemen lalu lintas jaringan dalam menjaga keamanan serta efisiensi akses internet. Konfigurasi DHCP memungkinkan distribusi IP secara otomatis ke perangkat klien, sedangkan pengaturan NAT dengan metode `masquerade` memungkinkan seluruh jaringan lokal mengakses internet menggunakan satu IP publik. Pengujian firewall berhasil membuktikan bahwa rule tertentu seperti pemblokiran ICMP dapat efektif mencegah aktivitas jaringan yang tidak diinginkan. Selain itu, konfigurasi bridge pada Router B berfungsi dengan baik sebagai penghubung antar perangkat tanpa fungsi routing. Dengan demikian, seluruh tujuan praktikum dapat tercapai dan sistem jaringan berjalan sesuai dengan skenario yang dirancang.

Selain memberikan pemahaman teknis tentang konfigurasi jaringan menggunakan MikroTik, praktikum ini juga menekankan pentingnya ketelitian dalam menerapkan setiap aturan firewall dan NAT agar tidak mengganggu konektivitas yang sah. Kesalahan kecil dalam pemilihan interface, chain, atau

action dapat berdampak langsung terhadap akses internet maupun distribusi IP dalam jaringan. Oleh karena itu, praktikum ini tidak hanya meningkatkan keterampilan konfigurasi, tetapi juga membentuk pemahaman konseptual mengenai bagaimana perangkat jaringan bekerja secara terintegrasi untuk memenuhi kebutuhan komunikasi data yang aman, efisien, dan terkendali.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 9: Dokumentasi praktikum Firewall dan NAT