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

# Laporan Akhir
# Praktikum Jaringan Komputer

## Firewall & NAT

Mohammad Rizky Ibrahim Diswarin - 5024231055

2025

# 1 Langkah-Langkah Praktikum

1. **Reset Router**

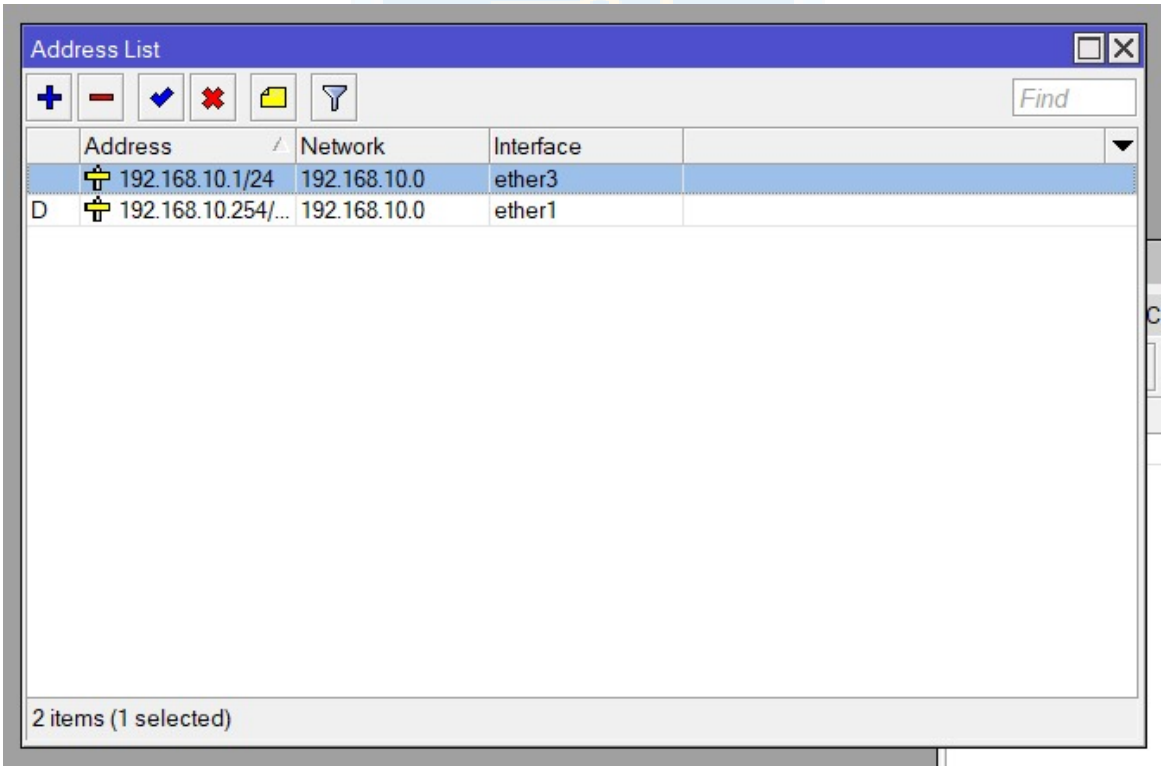
   Langkah awal sebelum melakukan konfigurasi adalah mereset router untuk menghapus seluruh pengaturan sebelumnya dan mengembalikan perangkat ke kondisi default. Proses reset dilakukan melalui aplikasi Winbox dengan mengakses menu *System* > *Reset Configuration*. Aktifkan opsi *"No Default Configuration"* dan klik tombol *"Reset Configuration"* untuk memulai proses.

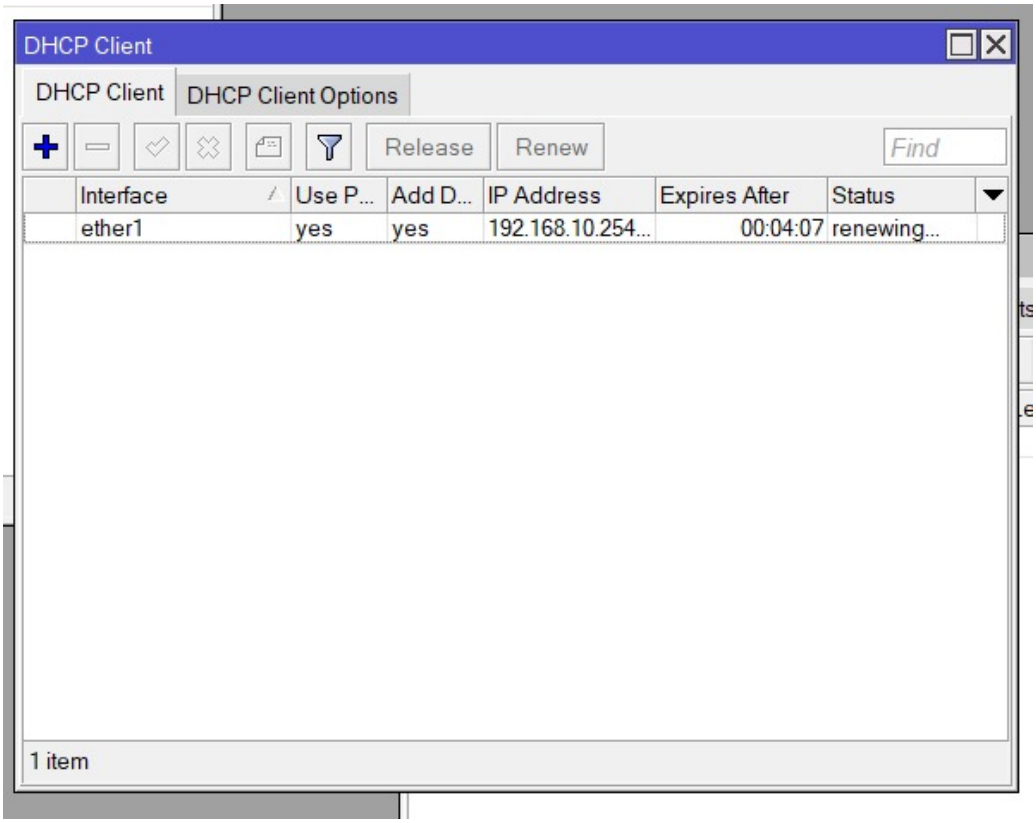
2. **Login ke Antarmuka Router**

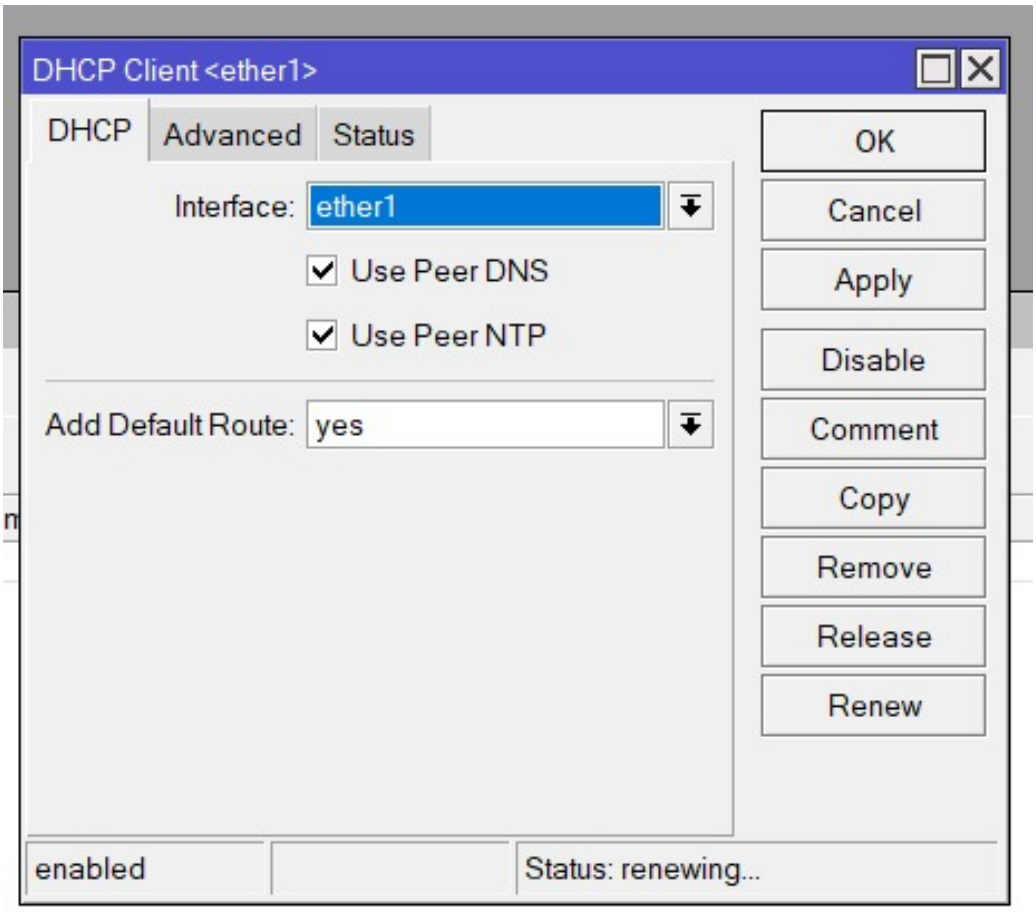
   Setelah proses reset selesai, hubungkan ke router menggunakan aplikasi Winbox, baik melalui MAC Address atau IP default. Masukkan username “admin” dan biarkan bagian password kosong jika belum pernah diatur sebelumnya.

3. **Mengaktifkan DHCP Client pada Router A (Ether1)**

   Hubungkan kabel internet ke ether1 pada Router A, lalu buka *IP* > *DHCP Client*. Tambahkan entri baru dengan memilih ether1 sebagai interface, klik *Apply*, dan pastikan status menunjukkan “bound”, yang berarti IP telah berhasil didapatkan dari DHCP server.





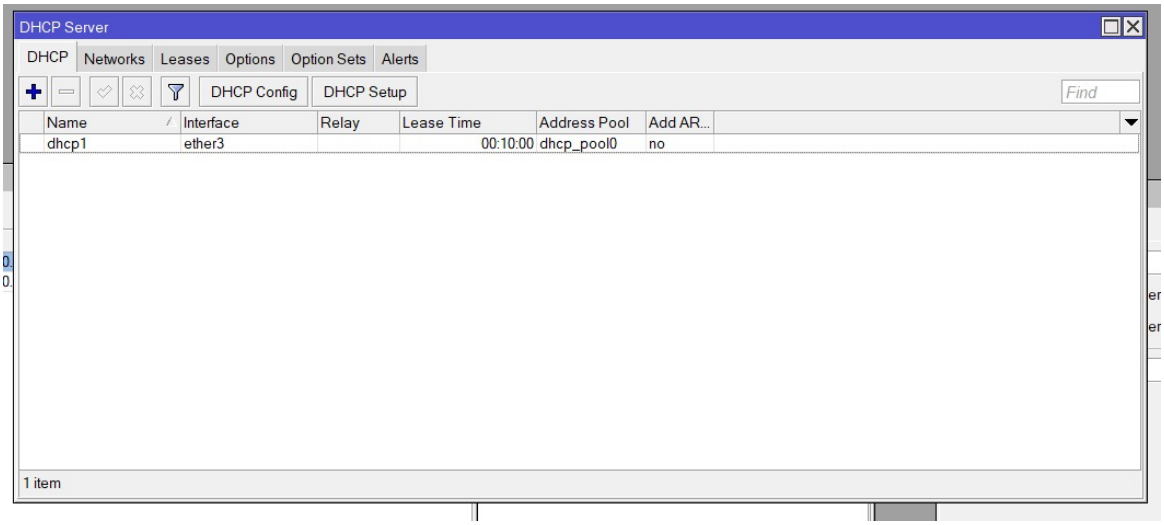

4. **Menambahkan IP Address pada Ether7**

   Untuk koneksi ke Switch, tambahkan alamat IP ke interface ether7 melalui menu *IP* > *Addresses*.

Klik ikon “+”, masukkan IP 192.168.10.1/24, pilih ether7, lalu klik *Apply* dan *OK*.

5. **Membuat DHCP Server pada Router**

   Router dikonfigurasi untuk mendistribusikan IP otomatis dengan fitur DHCP Server. Buka *IP* > *DHCP Server*, lalu klik *DHCP Setup*. Pilih ether7 sebagai interface, verifikasi network (192.168.10.0/24), gateway (192.168.10.1), rentang IP (192.168.10.2–192.168.10.254), DNS (misal: 8.8.8.8 dan 8.8.4.4), dan lease time (misal: 10 menit). Klik *Next* hingga selesai.

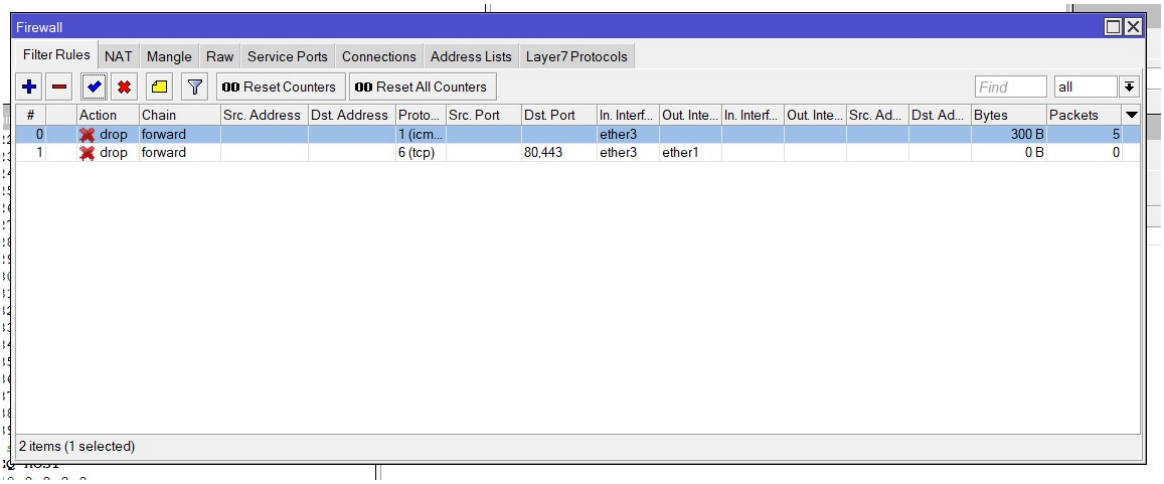


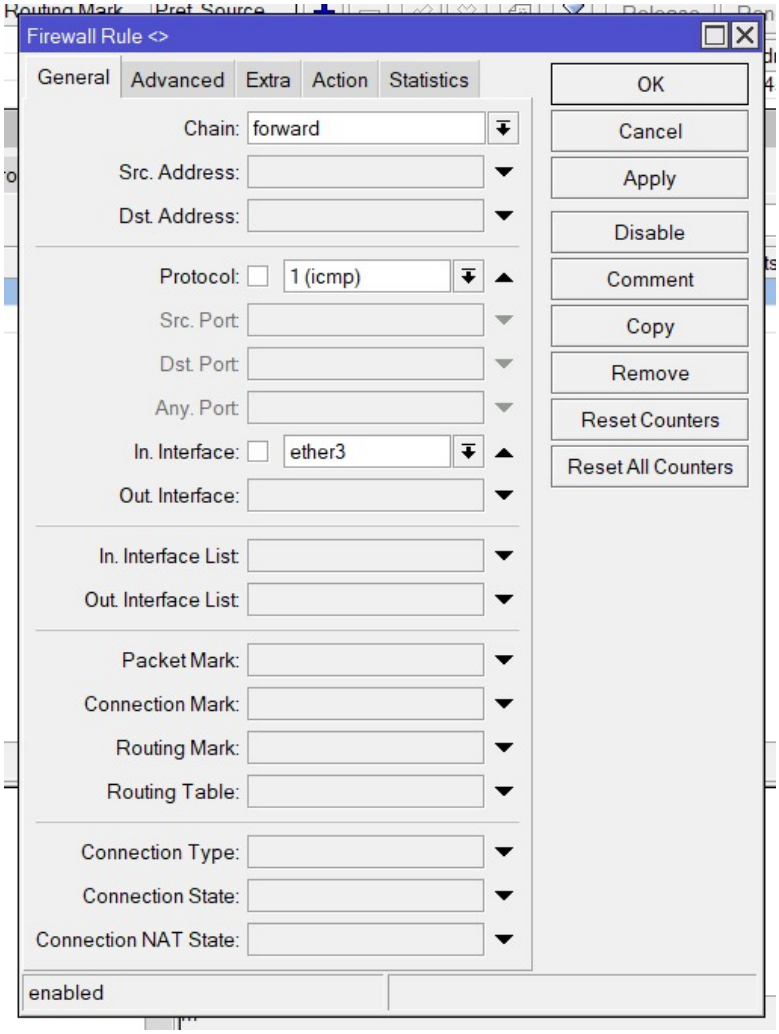

6. **Mengaktifkan NAT (Network Address Translation)**

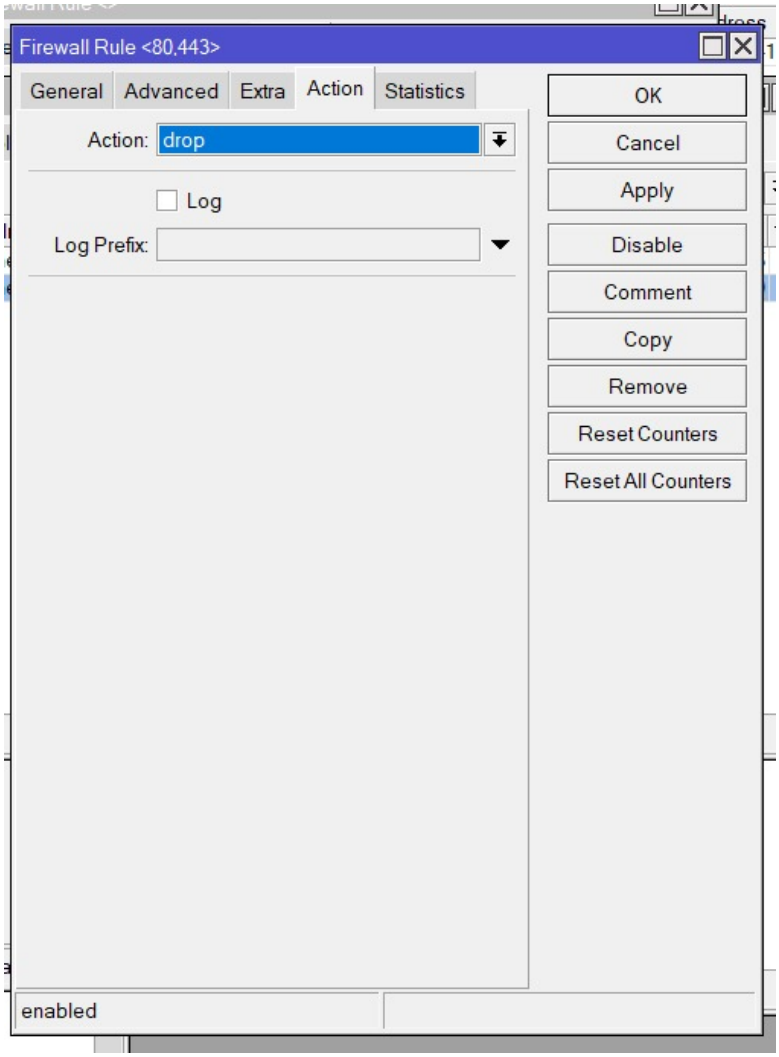
   Agar klien dapat mengakses internet, tambahkan aturan NAT pada menu *IP* > *Firewall* > *NAT*. Klik ikon “+”, di tab *General* pilih *Chain: src-nat*, lalu di tab *Action*, pilih *masquerade*. Klik *Apply* dan *OK*. Uji koneksi dengan menjalankan `ping 8.8.8.8` di terminal.

7. **Konfigurasi Firewall**

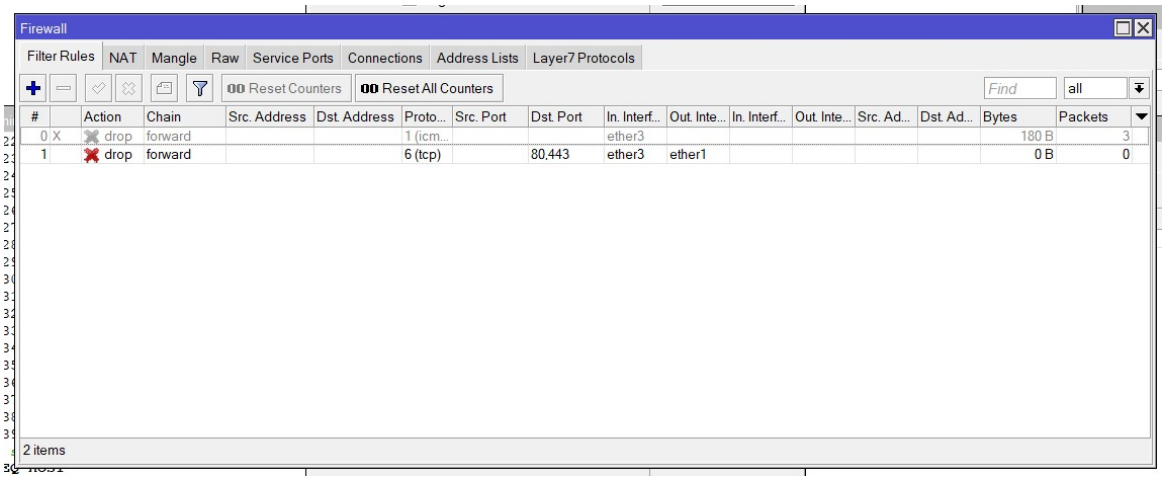
   Untuk membatasi akses, tambahkan aturan firewall. Untuk memblokir ping (ICMP), buka *IP* > *Firewall* > *Filter Rules*, klik “+”, atur *Chain: forward*, *Protocol: icmp*, *In. Interface: ether7*, lalu pada tab *Action*, pilih *drop*.

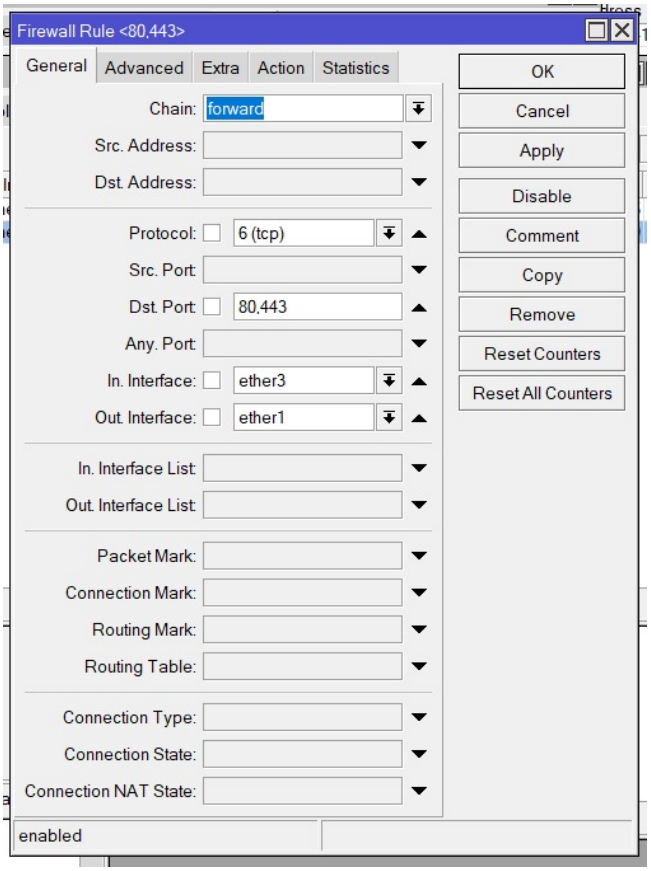


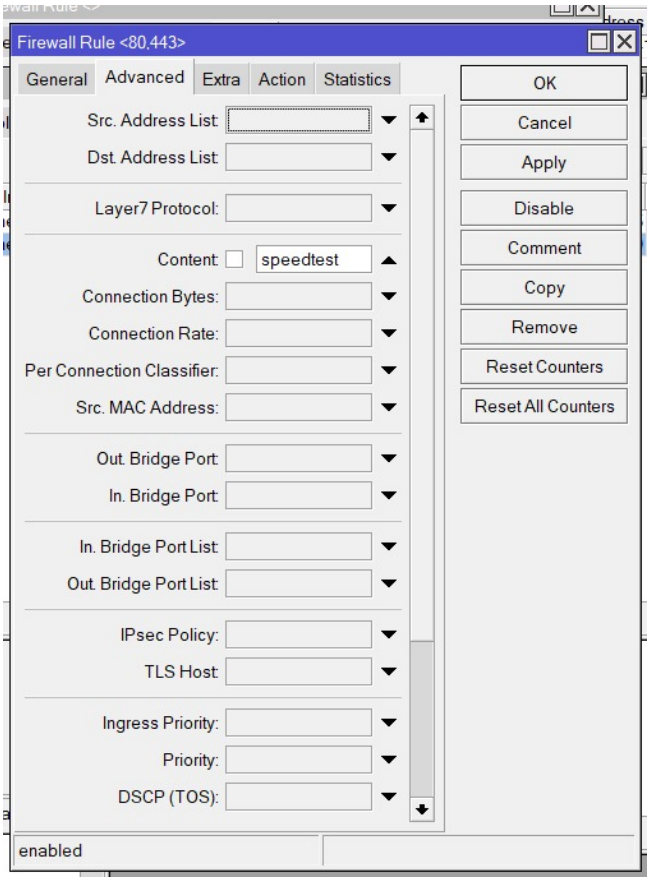

Firewall Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain: forward
Src. Address:
Dst. Address:
Protocol: 1 (icmp)
Src. Port:
Dst. Port:
Any. Port:
In. Interface: ether3
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:
enabled

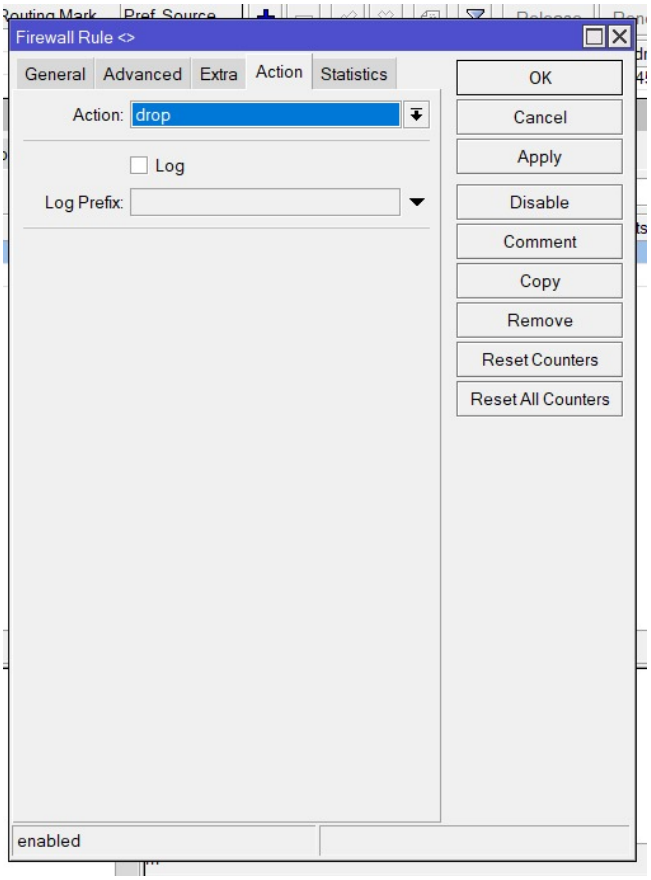



Untuk memblokir akses ke situs tertentu, buat aturan dengan *Chain: forward*, *Protocol: tcp*, *Dst. Port: 80,443*, *In. Interface: ether7*, *Out. Interface: ether1*. Pada tab *Advanced*, isi kata kunci seperti “speedtest” pada kolom *Content*, lalu pada tab *Action*, pilih *drop*.




Firewall Rule <80,443>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain: forward
Src. Address:
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port: 80,443
Any. Port:
In. Interface: ether3
Out. Interface: ether1
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:
enabled


Firewall Rule <80,443>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content: speedtest
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
In. Bridge Port List:
Out. Bridge Port List:
IPsec Policy:
TLS Host:
Ingress Priority:
Priority:
DSCP (TOS):
enabled




8. **Membuat Bridge pada Router B**

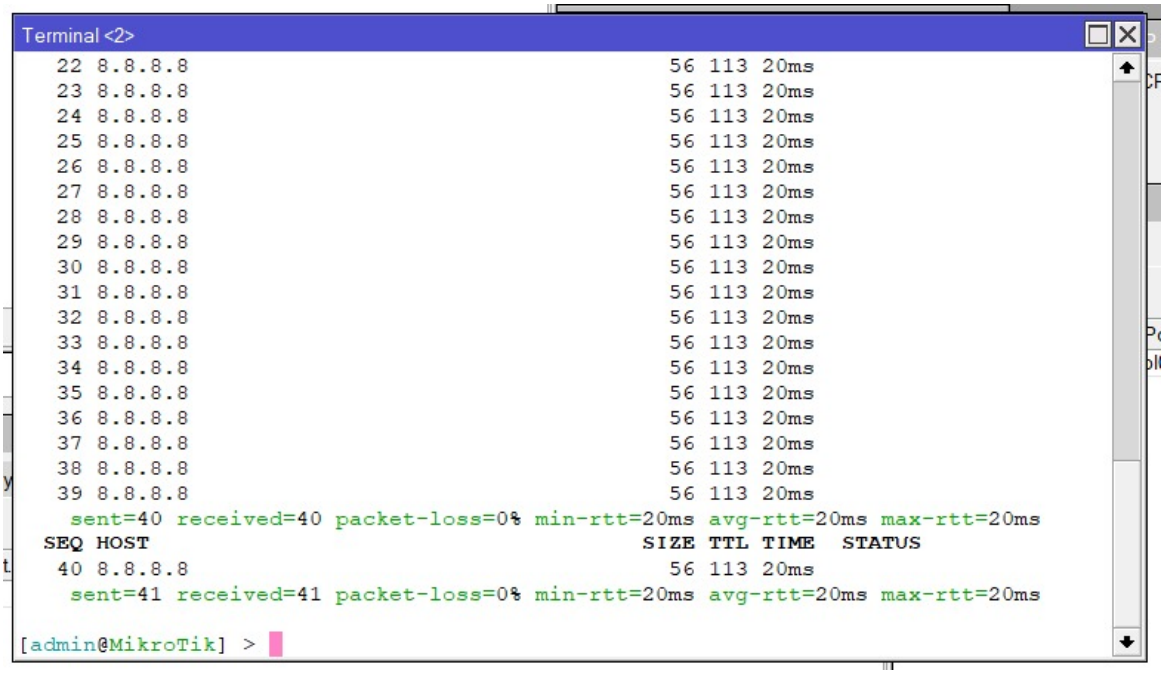
   Untuk menjadikan Router B sebagai penghubung antar perangkat, buka menu *Bridge*, klik ikon "+" untuk membuat bridge baru, lalu klik *Apply* dan *OK*. Tambahkan dua interface ke dalam bridge melalui *Bridge* > *Ports*.

9. **Pengaturan IP Otomatis pada Laptop**

   Pastikan pengaturan jaringan laptop berada dalam mode DHCP. Cek konfigurasi IP melalui `ipconfig` di Command Prompt untuk memastikan IP diperoleh secara otomatis.

10. **Pengujian Jaringan**

    Lakukan uji koneksi dengan perintah `ping 8.8.8.8`. Jika aturan firewall ICMP aktif, akan muncul pesan *Request Timed Out*. Setelah aturan firewall dinonaktifkan, ping akan berhasil.




Untuk menguji filter konten, akses situs seperti `www.speedtest.net`. Jika aturan masih aktif, situs akan gagal dimuat. Setelah dinonaktifkan, akses akan kembali normal.

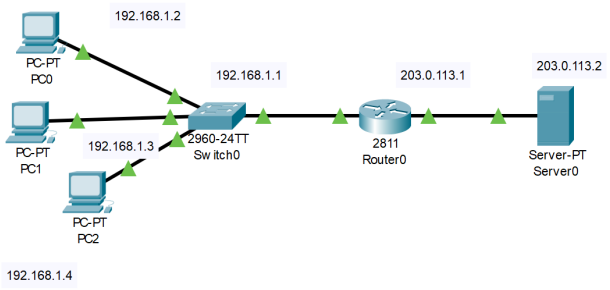
## 2 Analisis Percobaan

Seluruh proses konfigurasi berhasil dijalankan dengan baik, mulai dari reset hingga pengujian. Router memperoleh IP melalui DHCP Client ether1, dan distribusi IP kepada klien melalui DHCP Server berjalan tanpa kendala. Fungsi NAT terbukti sukses melalui uji ping ke internet, dan firewall mampu memblokir akses sesuai aturan yang dibuat.

Pembuatan bridge pada Router B serta pengaturan IP otomatis pada laptop juga berjalan mulus. Tidak ditemukan kendala teknis berarti, dan konfigurasi telah sesuai teori yang menyatakan bahwa NAT dan firewall mampu mengatur serta mengamankan jaringan secara efektif. Potensi kesalahan hanya bisa terjadi jika salah memilih interface atau menempatkan rule pada chain yang tidak tepat.

## 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 1:** Topologi

2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.

```
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.
Reply from 203.0.113.2: bytes=32 time=6ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>
```

**Gambar 2:** Ping PC1 ke Server

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

Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time=6ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

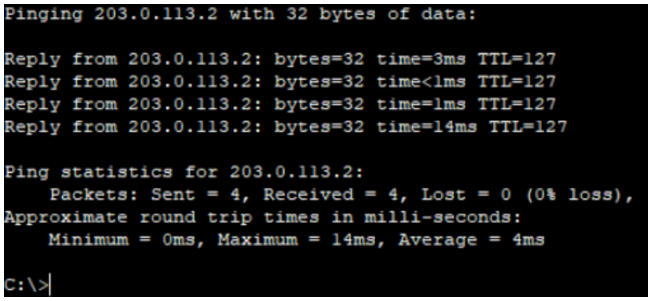
**Gambar 3:** Ping PC2 ke Server

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

Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

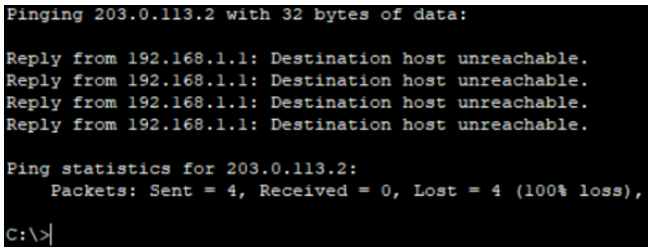
**Gambar 4:** Ping PC3 ke Server

3. Konfigurasi Firewall (ACL):

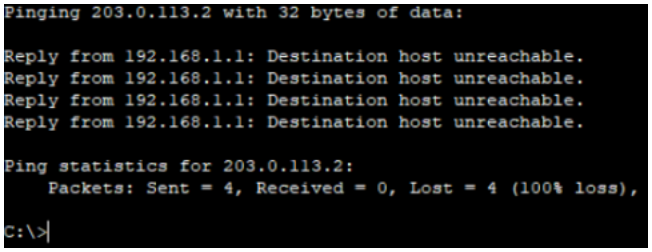
   - Izinkan hanya PC1 yang dapat mengakses Server.
   - Blokir PC1 dan PC3 dari mengakses Server.
   - Semua PC harus tetap bisa saling terhubung di LAN.




**Gambar 5:** Ping PC1 ke Server dengan konfigurasi firewall ACL




**Gambar 6:** Ping PC2 ke Server dengan konfigurasi firewall ACL




**Gambar 7:** Ping PC3 ke Server dengan konfigurasi firewall ACL

# 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 Kesimpulan

Praktikum mengenai Firewall dan NAT berhasil memperlihatkan penerapan konfigurasi dasar pada router MikroTik yang efektif dalam mengatur lalu lintas data. Melalui pengaturan DHCP, NAT, serta firewall, peserta mampu memahami cara kerja distribusi IP, konektivitas internet, dan kontrol akses jaringan.

Pengujian yang dilakukan menunjukkan hasil sesuai dengan teori dan konfigurasi yang diterapkan. Praktikum ini memperdalam pemahaman konsep jaringan seperti IP, DHCP, NAT, dan firewall, serta penerapannya dalam situasi nyata. Ketelitian saat memilih interface dan urutan konfigurasi menjadi kunci utama dalam keberhasilan penerapan konfigurasi jaringan.

# 6 Lampiran

## 6.1 Dokumentasi Praktikum