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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Devanka Raditanti Citasevi - 5024231053

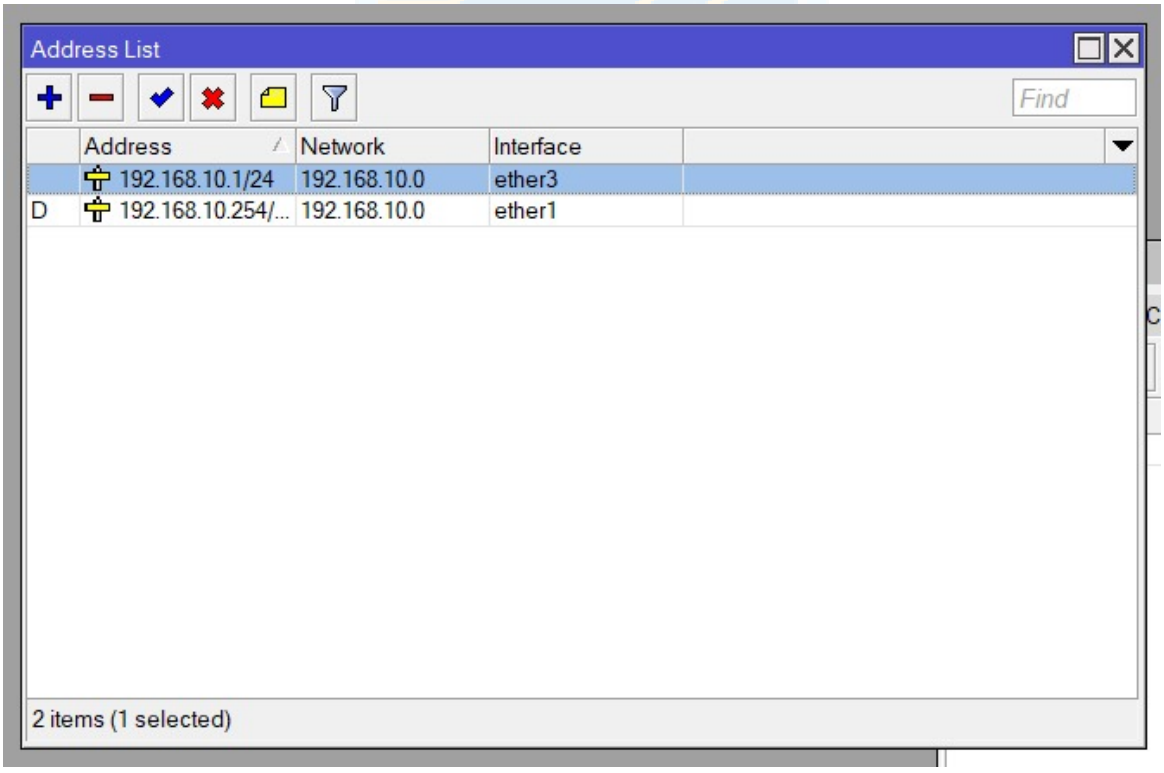
2025

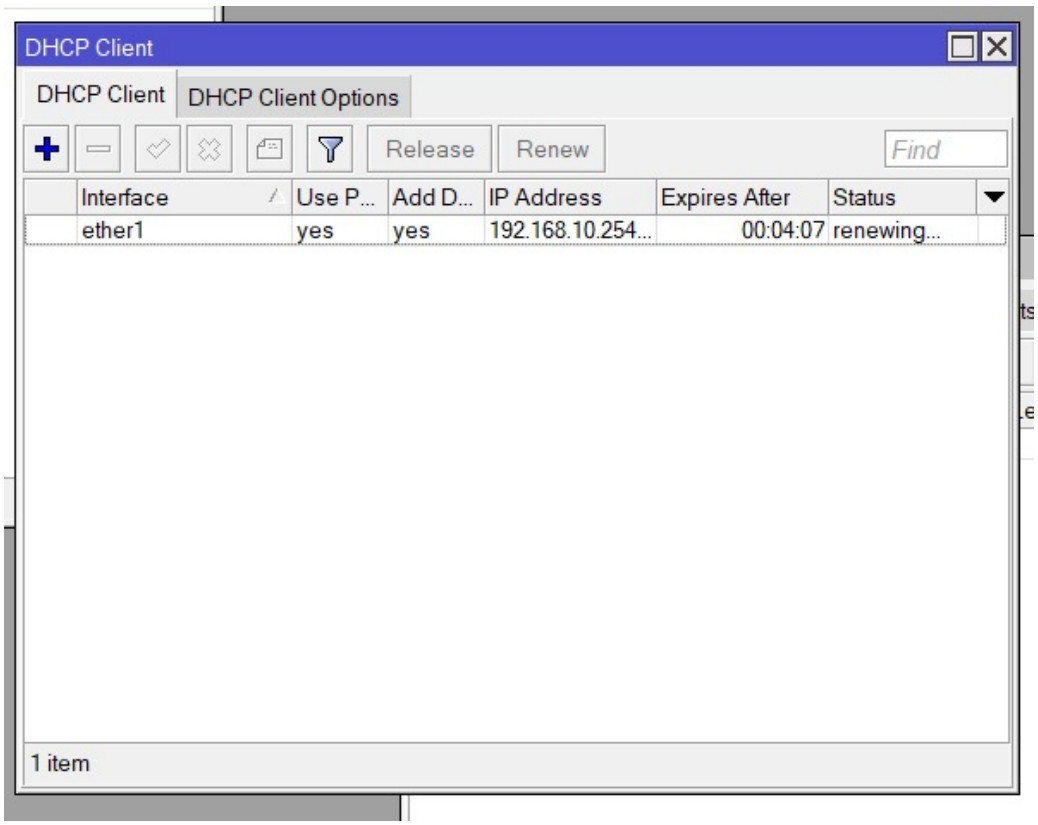
1 Langkah-Langkah Percobaan

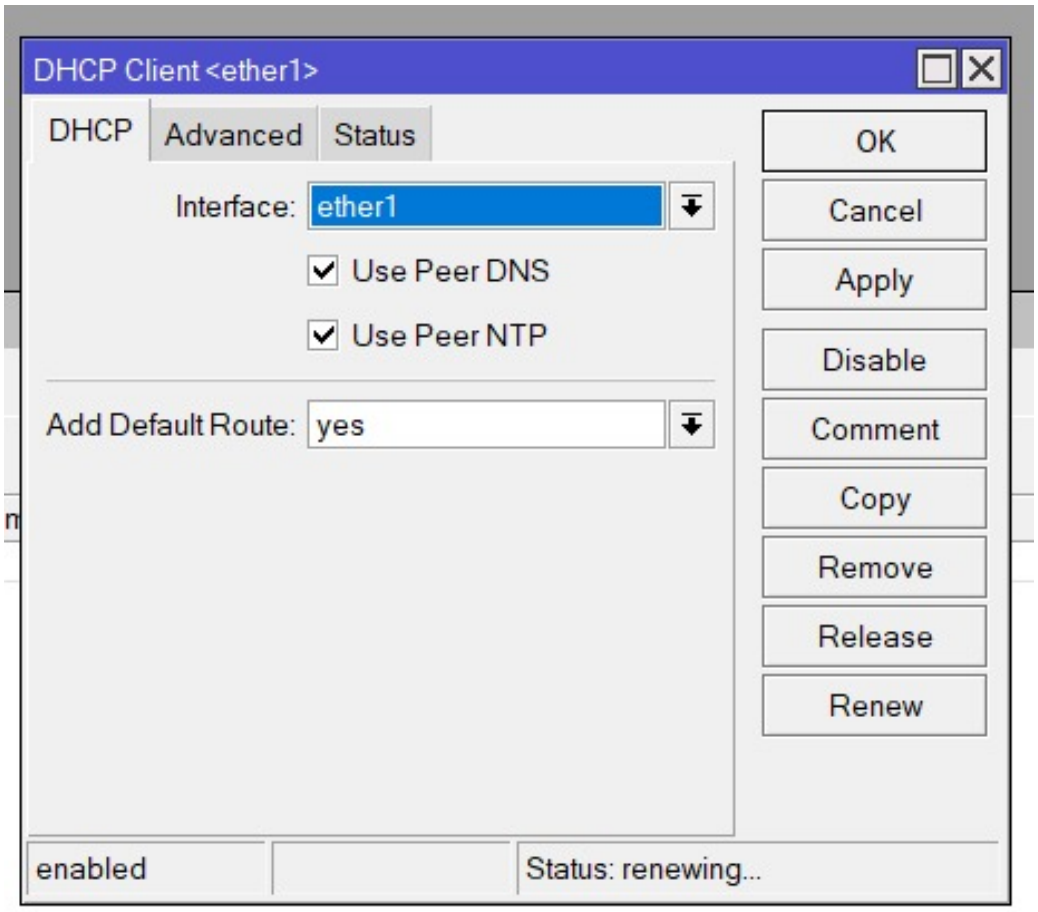
1. Reset Router
   Langkah pertama dalam proses konfigurasi router adalah melakukan reset untuk mengembalikan perangkat ke pengaturan awal. Hal ini penting guna menghindari potensi konflik dari konfigurasi sebelumnya. Reset dilakukan dengan mengakses router melalui aplikasi Winbox, lalu masuk ke menu System > Reset Configuration. Selanjutnya, centang opsi "No Default Configuration" dan klik "Reset Configuration" untuk memulai proses pengaturan ulang.

2. Login ke Router
   Setelah router di-reset, langkah berikutnya adalah melakukan login ke antarmuka router menggunakan Winbox. Koneksi dapat dilakukan melalui MAC address atau alamat IP default perangkat. Gunakan username "admin" tanpa perlu mengisi kata sandi, kecuali jika sudah pernah ditetapkan sebelumnya.

3. Konfigurasi DHCP Client pada Router A (Ether1)
   Sambungkan kabel internet ke port ether1 pada Router A untuk memulai konfigurasi DHCP Client. Buka menu IP > DHCP Client dan klik ikon "+" untuk menambahkan entri baru. Pilih ether1 sebagai interface yang digunakan, lalu klik Apply. Pastikan status koneksi menunjukkan "bound" sebagai tanda bahwa router telah memperoleh IP dari DHCP server.





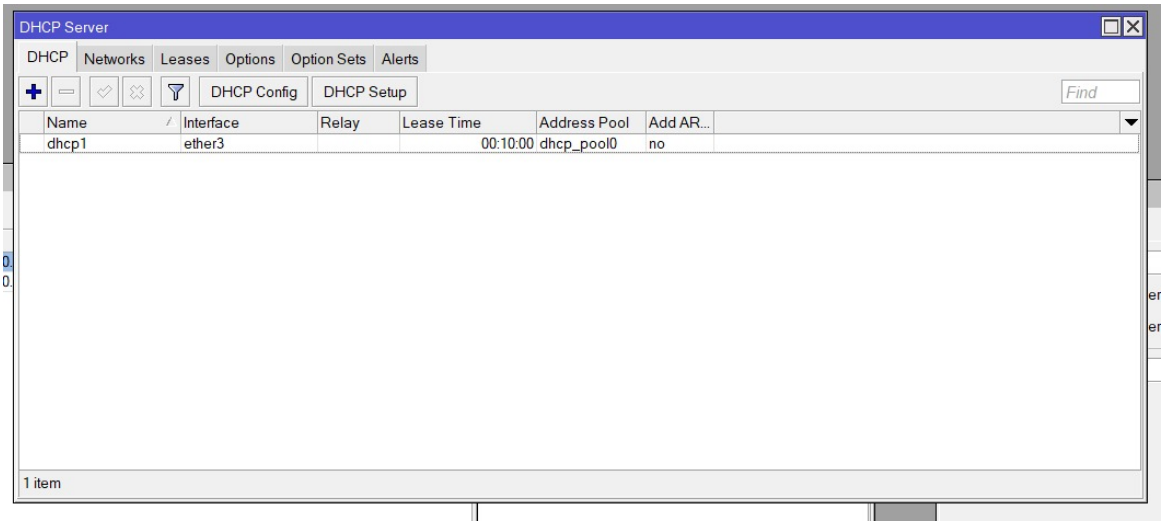


4. Penambahan Alamat IP pada Ether7

   Untuk menghubungkan Router A dengan Switch, tambahkan alamat IP pada port ether7. Ma-

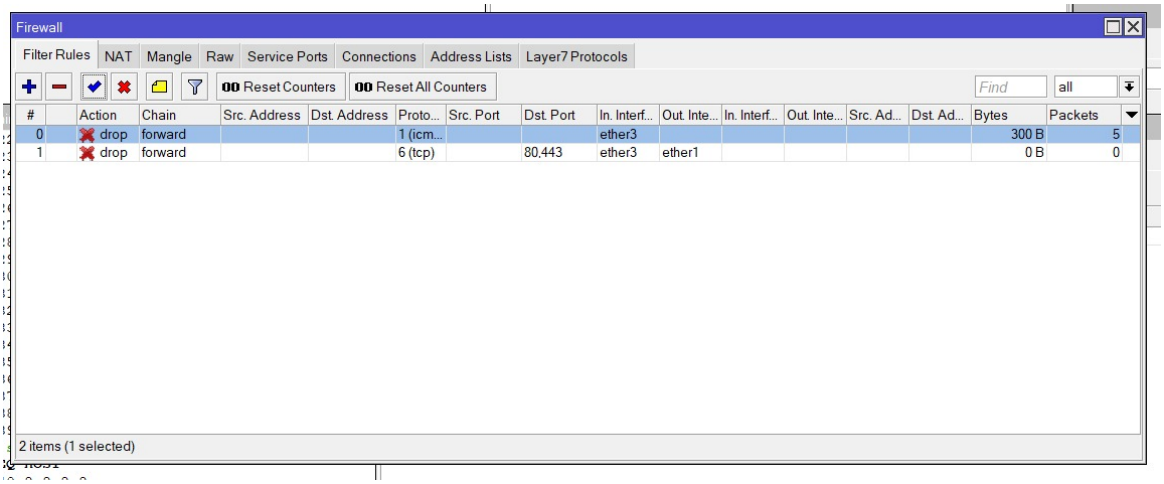
suk ke menu IP > Addresses, klik ikon "+" untuk menambahkan alamat baru, lalu masukkan IP address 192.168.10.1/24 dan pilih interface ether7. Klik Apply lalu OK untuk menyimpan pengaturan.

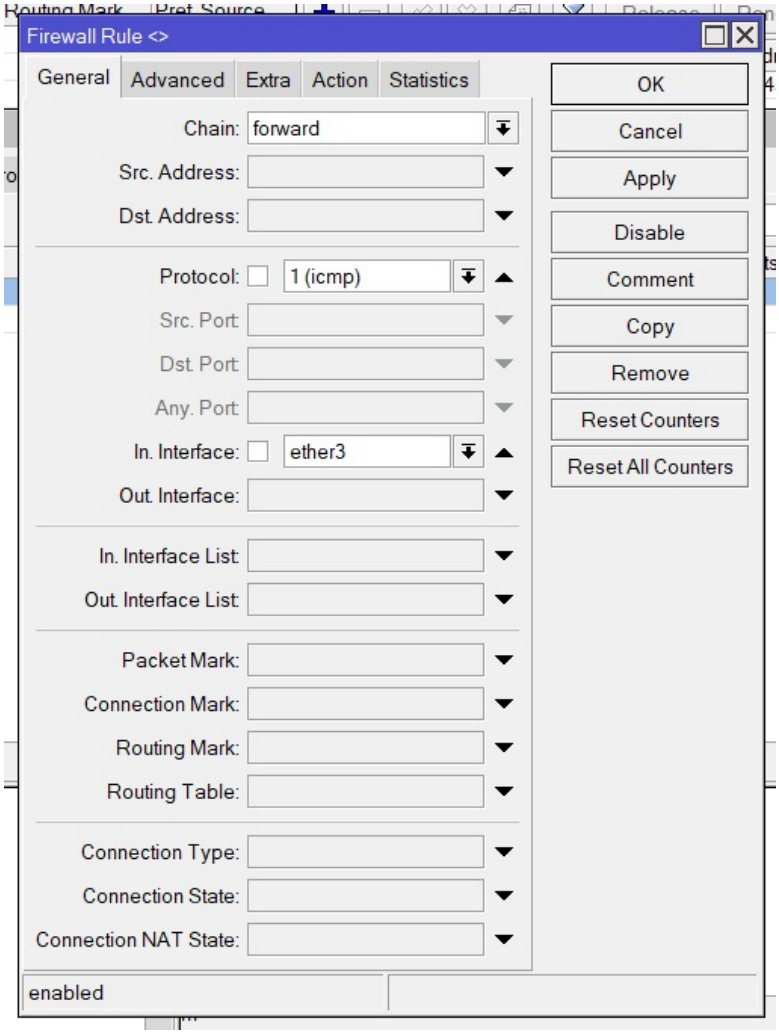
5. Konfigurasi DHCP Server pada Router MikroTik
   Router dikonfigurasi agar dapat secara otomatis mendistribusikan IP kepada perangkat klien dengan menggunakan fitur DHCP Server. Buka menu IP > DHCP Server dan klik tombol "DHCP Setup". Pada tahap pertama, pilih interface yang akan digunakan sebagai server DHCP, misalnya ether7. Selanjutnya, verifikasi alamat network (misal: 192.168.10.0/24), gateway (192.168.10.1), dan rentang alamat IP yang akan diberikan (192.168.10.2-192.168.10.254). Masukkan juga alamat DNS Server seperti 8.8.8.8 dan 8.8.4.4, kemudian atur durasi lease, misalnya 10 menit. Jika semua konfigurasi benar, sistem akan menampilkan pesan bahwa pengaturan telah selesai.

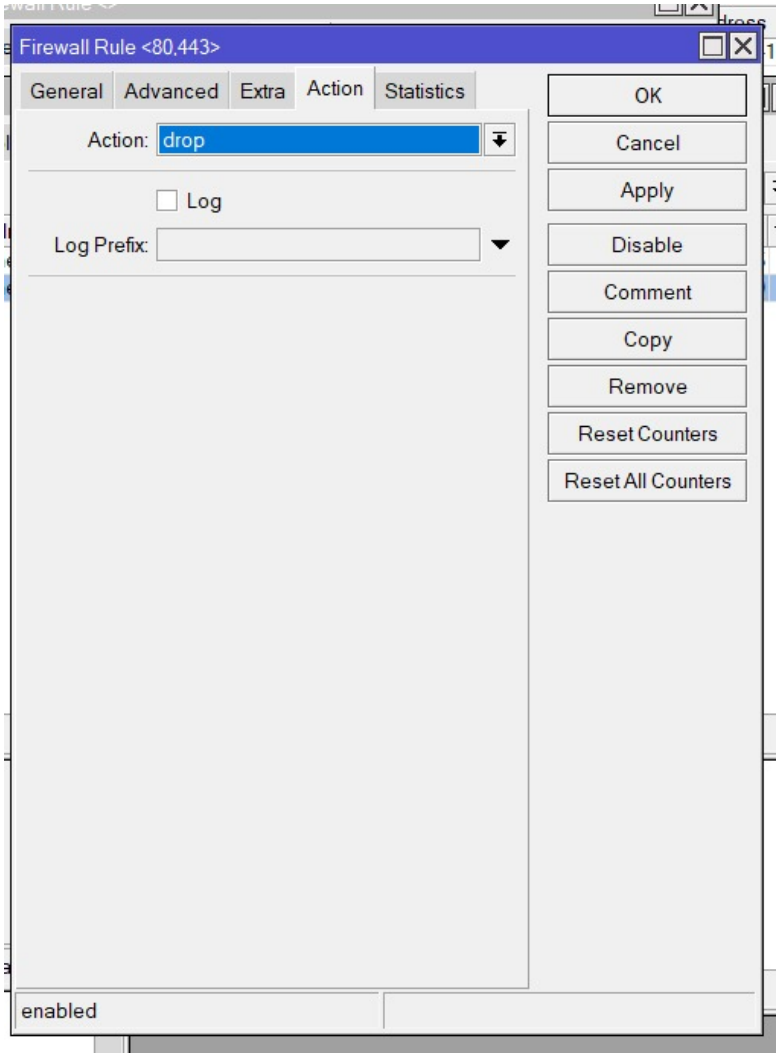


6. Konfigurasi NAT (Network Address Translation)
   Agar klien dapat mengakses internet, perlu dilakukan konfigurasi NAT. Masuk ke menu IP > Firewall > NAT dan klik ikon "+" untuk menambah aturan baru. Pada tab "General", pilih src-nat pada kolom Chain, kemudian pada tab "Action", pilih masquerade. Klik Apply dan OK untuk menyimpan pengaturan. Untuk menguji koneksi internet, buka Terminal di Winbox dan jalankan perintah ping 8.8.8.8, pastikan terdapat balasan sebagai tanda koneksi berhasil.

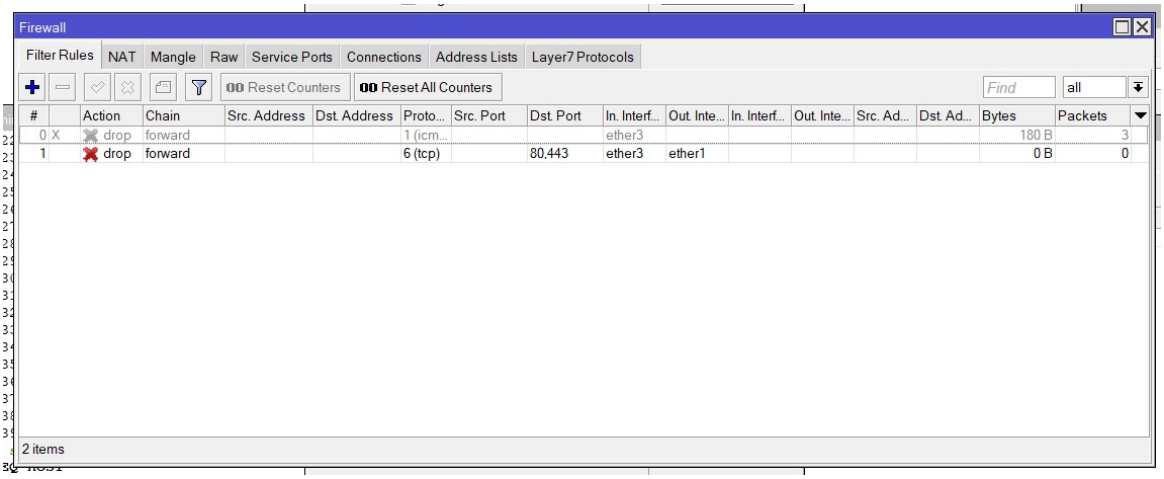
7. Konfigurasi Firewall
   Langkah selanjutnya adalah menambahkan aturan pada firewall untuk membatasi akses tertentu. Untuk memblokir ICMP (ping), masuk ke menu IP > Firewall > Filter Rules, klik ikon "+" dan atur Chain: forward, Protocol: icmp, In. Interface: ether7, lalu pada tab "Action", pilih drop.

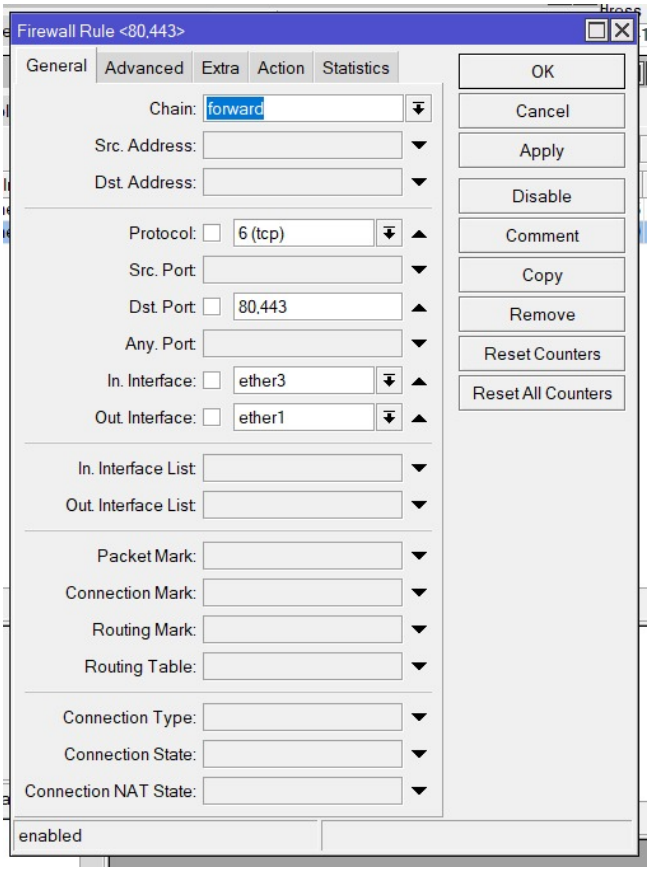

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
00 Reset Counters
00 Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Interf... Out. Inte... In. Interf... Out. Inte... Src. Ad... Dst. Ad... Bytes Packets
0 drop forward 1 (icm... ether3 300 B 5
1 drop forward 6 (tcp) 80,443 ether3 ether1 0 B 0
2 items (1 selected)

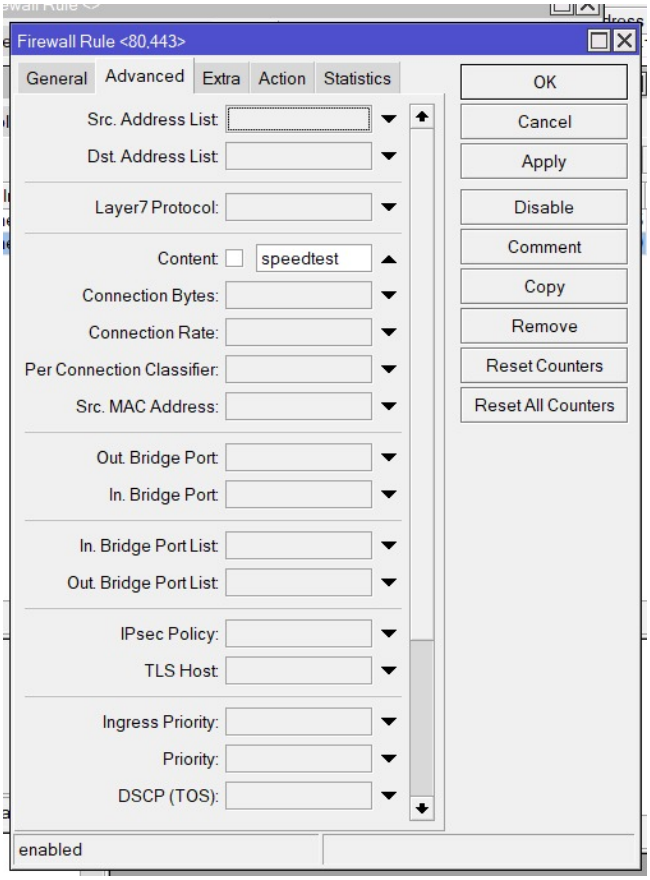

Firewall Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain: forward
Src. Address:
Dst. Address:
Protocol: 1 (icmp)
Src. Port:
Dst. Port:
Any. Port:
In. Interface: ether3
Out. Interface:
In. Interface List:
Out. Interface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

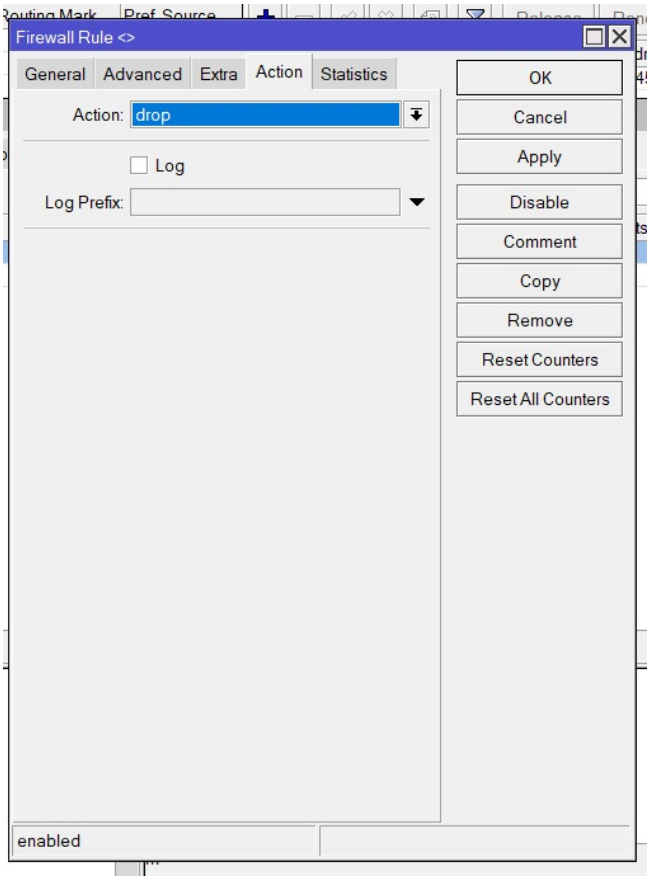


Untuk memblokir situs dengan konten tertentu, tambahkan aturan baru dengan Chain: forward, Protocol: tcp, Dst. Port: 80,443, In. Interface: ether7, dan Out. Interface: ether1. Pada tab "Advanced", isi bagian Content dengan kata kunci yang ingin diblokir seperti "speedtest", lalu pada tab "Action", pilih drop.




Firewall Rule <80,443>
General
Advanced
Extra
Action
Statistics
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:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled

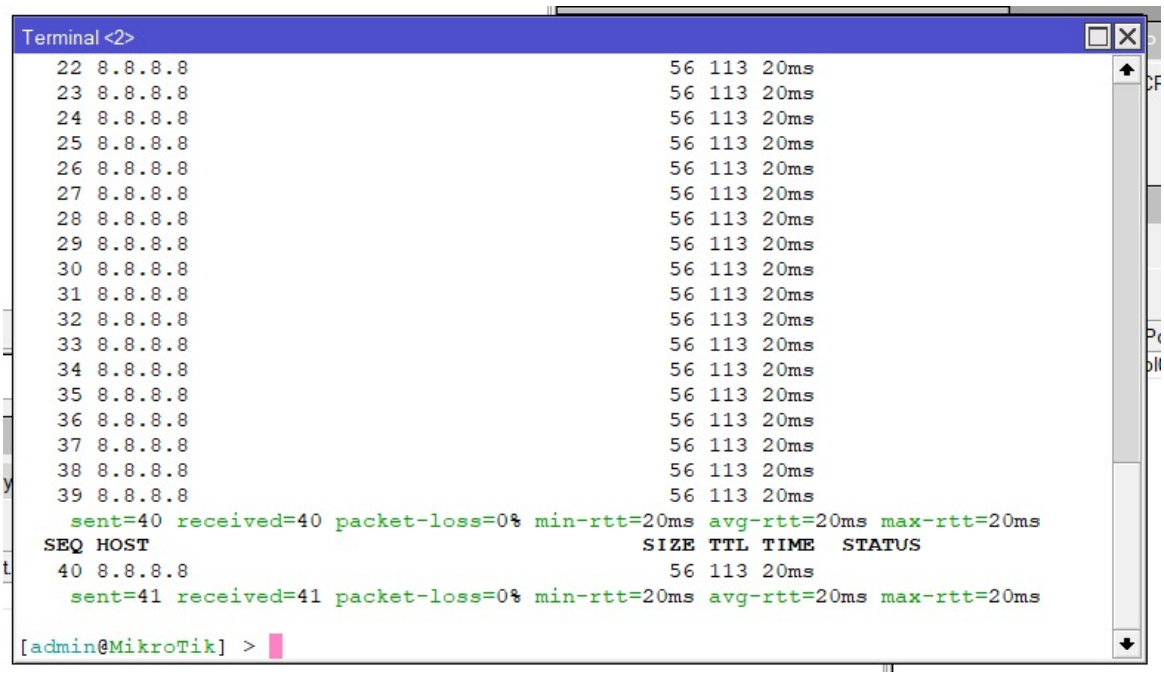

Firewall Rule <80,443>
General
Advanced
Extra
Action
Statistics
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content: speedtest
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
In. Bridge Port List:
Out. Bridge Port List:
IPsec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



8. Konfigurasi Bridge pada Router B
   Untuk menjadikan Router B berfungsi sebagai hub, perlu dibuat bridge. Akses menu Bridge, klik ikon "+" untuk membuat bridge baru, lalu klik Apply dan OK. Selanjutnya, tambahkan port yang ingin dimasukkan ke dalam bridge dengan membuka Bridge > Port, klik ikon "+" dan pilih dua interface: satu yang terhubung ke laptop dan satu lagi yang terhubung ke Router A.

9. Konfigurasi Alamat IP pada Laptop
   Pada perangkat laptop, pastikan pengaturan jaringan dikonfigurasi secara otomatis melalui DHCP. Buka pengaturan jaringan di sistem operasi dan pastikan mode DHCP aktif. Untuk memverifikasi apakah laptop telah menerima IP, buka Command Prompt dan jalankan perintah ipconfig, lalu periksa informasi alamat IP yang diperoleh.

10. Uji Coba Konfigurasi
    Langkah akhir adalah melakukan pengujian untuk memastikan seluruh konfigurasi berjalan dengan benar. Untuk menguji konektivitas, buka Terminal di laptop dan jalankan perintah ping 8.8.8.8. Jika firewall ICMP aktif, hasil yang ditampilkan adalah Request Timed Out. Nonaktifkan aturan firewall tersebut, lalu jalankan kembali perintah ping, dan seharusnya koneksi berhasil.



Untuk menguji pemblokiran konten, coba akses situs seperti www.speedtest.net menggunakan browser. Jika firewall aktif, situs akan gagal dimuat. Setelah aturan firewall dinonaktifkan, akses ke situs tersebut akan kembali normal.

2 Analisis Hasil Percobaan

Selama praktikum, seluruh tahapan konfigurasi router berhasil dilakukan sesuai dengan panduan, mulai dari reset awal hingga pengujian konektivitas. Ketika DHCP Client pada ether1 dikonfigurasi dengan benar, router berhasil memperoleh IP dari jaringan eksternal yang menandakan bahwa koneksi internet tersedia. Penambahan alamat IP pada ether7 dan konfigurasi DHCP Server terbukti efektif dalam mendistribusikan alamat IP secara otomatis kepada klien.

Fungsi NAT berjalan sebagaimana mestinya, ditunjukkan dengan suksesnya perintah ping 8.8.8.8 dari terminal Winbox dan laptop yang terhubung. Konfigurasi firewall juga memberikan hasil sesuai harapan: pemblokiran ICMP menyebabkan perintah ping mengalami Request Timed Out, dan filter berdasarkan konten berhasil menghalangi akses ke situs tertentu seperti speedtest.net.

Tidak ditemukan kendala signifikan selama konfigurasi bridge pada Router B dan pengaturan DHCP pada laptop. Seluruh hasil praktikum sesuai dengan teori yang menyatakan bahwa firewall dan NAT dapat mengatur, mengamankan, serta mengontrol lalu lintas jaringan secara efisien. Faktor yang berpotensi memengaruhi keberhasilan hanya berkisar pada kesalahan pemilihan interface atau penempatan aturan pada chain yang salah, namun tidak terjadi dalam percobaan ini.

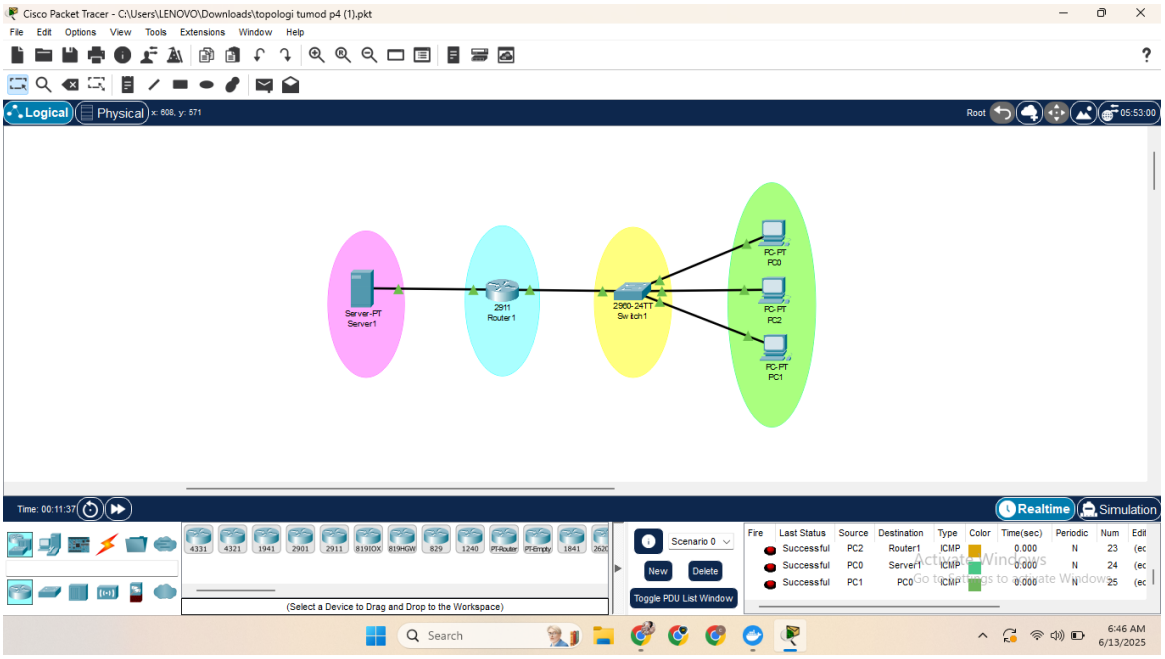
3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:
    - 1 Router
    - 1 Switch

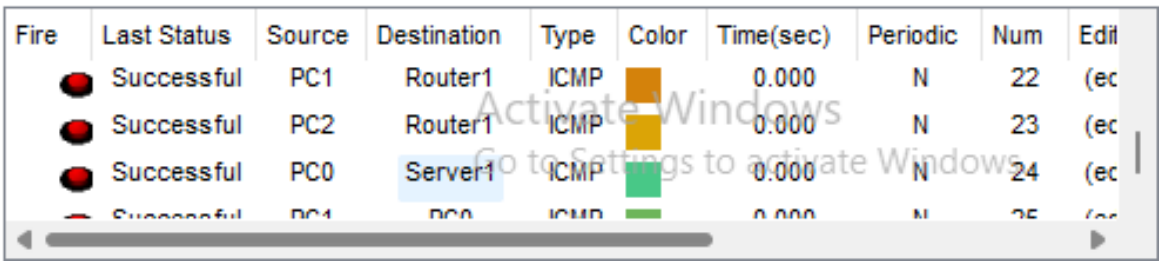
- 3 PC (LAN)
- 1 Server (Internet/Public)

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

   Uji koneksi menggunakan ping dan dokumentasikan hasilnya.



Gambar 1: Topologi



Gambar 2: Test Ping

4 Kesimpulan

Praktikum Firewall & NAT berhasil menunjukkan bagaimana konfigurasi dasar router MikroTik dapat digunakan untuk mengatur lalu lintas jaringan secara efisien dan aman. Melalui penerapan DHCP Client dan Server, NAT, serta firewall, praktikan dapat memahami peran penting konfigurasi jaringan dalam mendistribusikan IP, mengatur akses internet, serta menyaring lalu lintas data yang tidak diinginkan.

Semua hasil percobaan berjalan sesuai dengan teori, termasuk pengujian konektivitas dan pemblokiran berdasarkan protokol atau konten. Praktikum ini memperkuat pemahaman mengenai penerapan konsep dasar jaringan seperti IP address, DHCP, NAT, dan firewall serta penerapannya baik di lingkungan praktikum maupun dunia nyata. Pembelajaran penting yang diperoleh adalah pentingnya ketelitian dalam pemilihan interface dan urutan konfigurasi agar fungsi jaringan dapat berjalan dengan optimal.

5 Lampiran

5.1 Dokumentasi saat praktikum