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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Ahmad Akmal Defatra - 5024231005

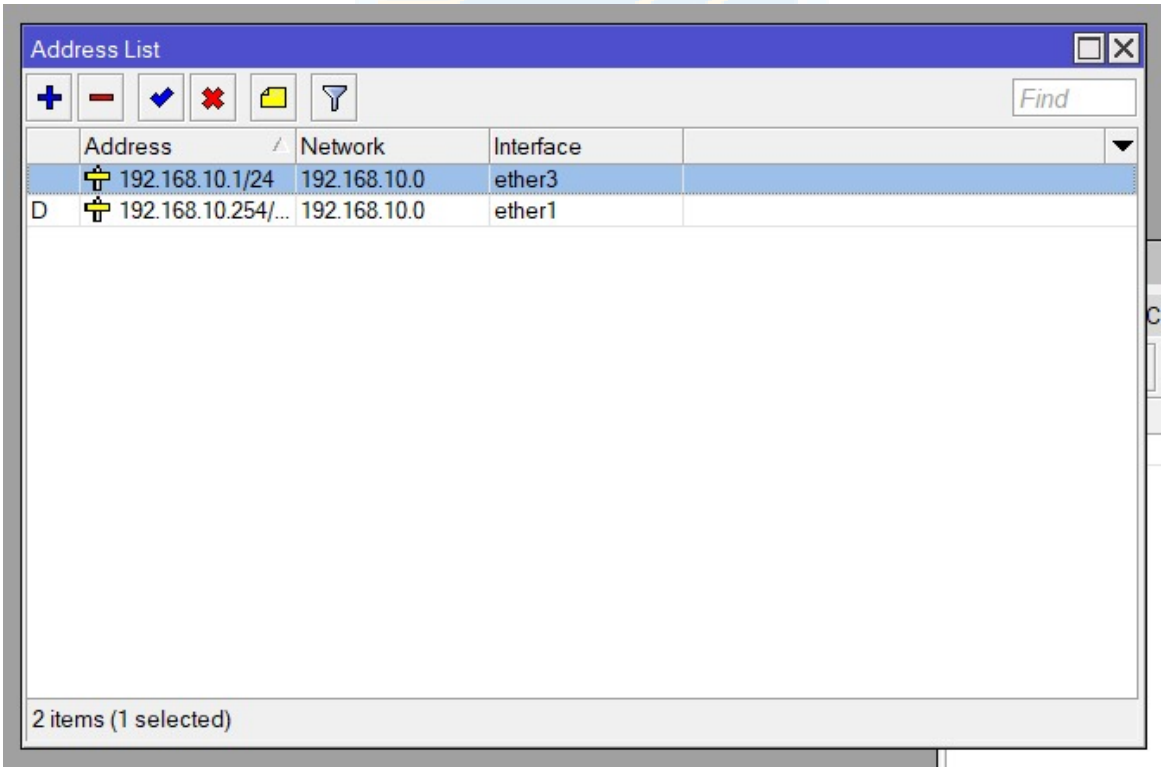
2025

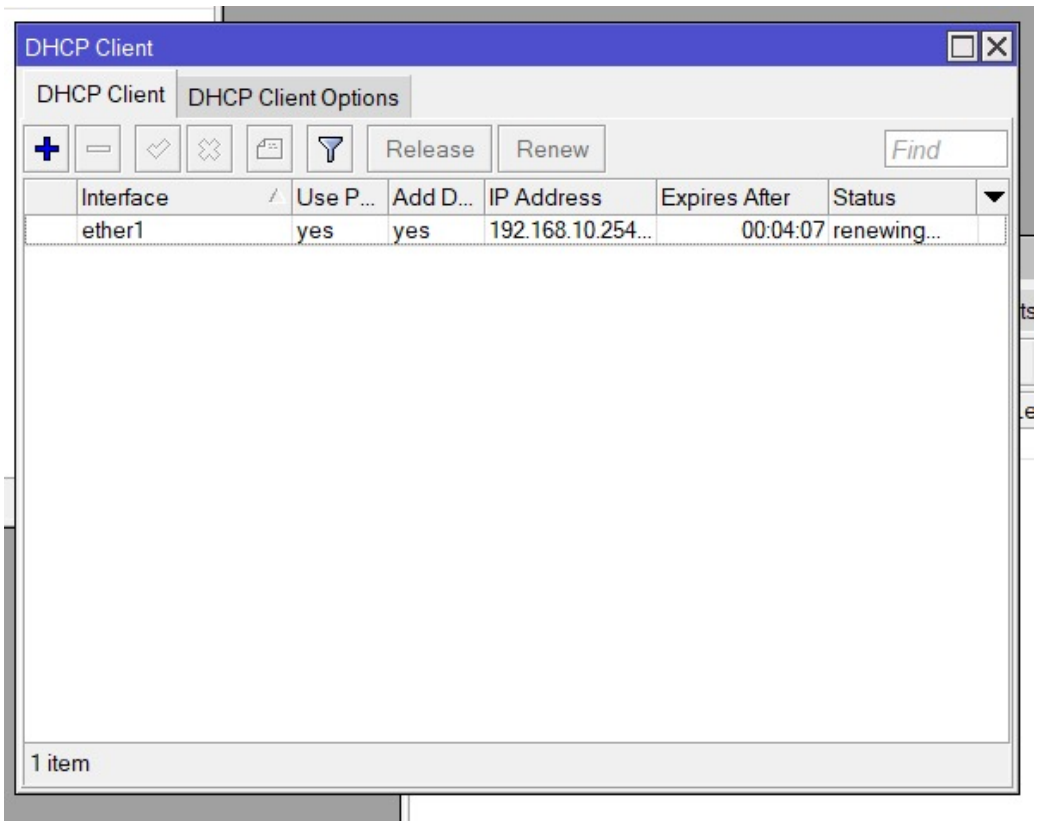
1 Langkah-Langkah Percobaan

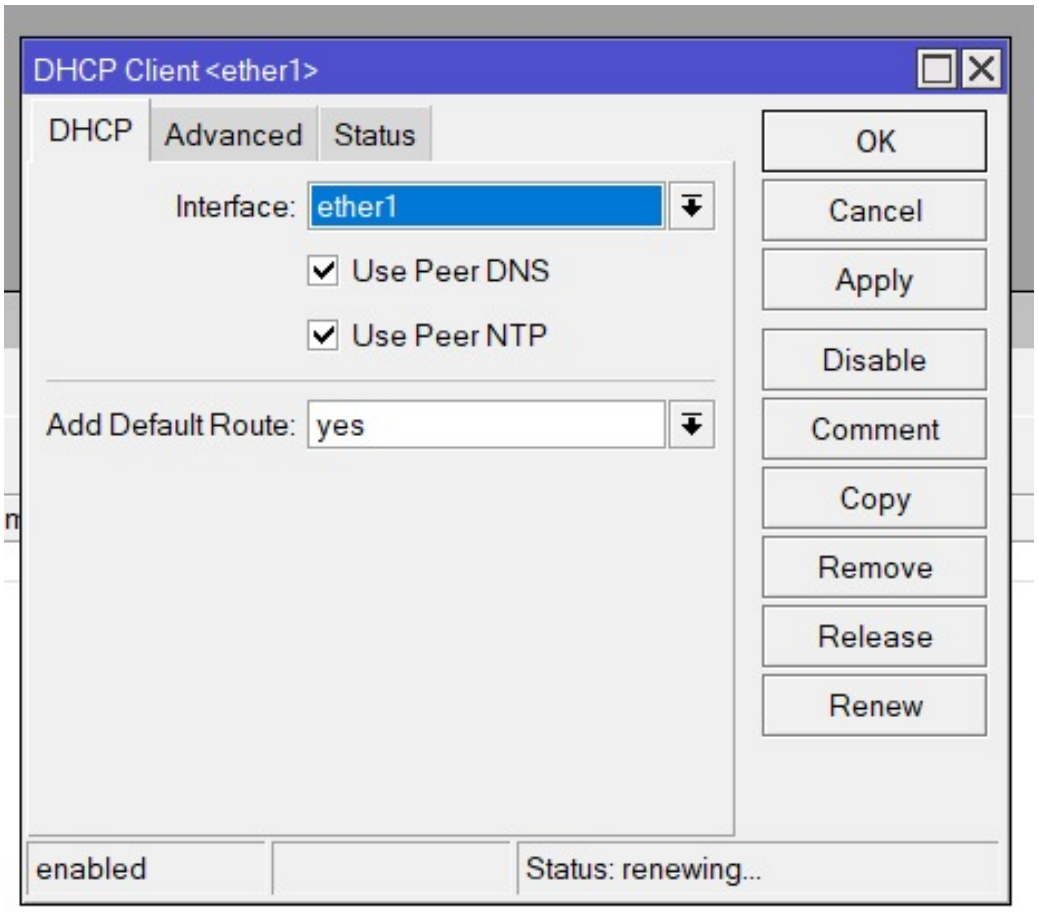
1. Reset Router
   Langkah awal dalam konfigurasi router adalah melakukan reset perangkat ke pengaturan pabrik. Ini penting untuk menghindari potensi konflik dari konfigurasi sebelumnya. Proses reset dilakukan melalui aplikasi Winbox dengan mengakses menu System > Reset Configuration. Pastikan untuk mencentang opsi "No Default Configuration" sebelum mengklik "Reset Configuration" untuk memulai proses.

2. Login ke Router
   Setelah router berhasil di-reset, langkah selanjutnya adalah login ke antarmuka router menggunakan Winbox. Anda bisa terhubung melalui MAC address atau IP address default perangkat. Gunakan username "admin"; biasanya, kata sandi tidak diperlukan kecuali jika Anda sudah mengaturnya sebelumnya.

3. Konfigurasi DHCP Client pada Router A (Ether1)
   Sambungkan kabel internet ke port ether1 pada Router A. Buka menu IP > DHCP Client, lalu tambahkan entri baru dengan memilih ether1 sebagai interface dan mencentang "Use PeerDNS" serta "UsePeerNTP". Setelah di-apply, pastikan status koneksi menunjukkan "bound" yang menandakan router telah mendapatkan IP dari DHCP server.





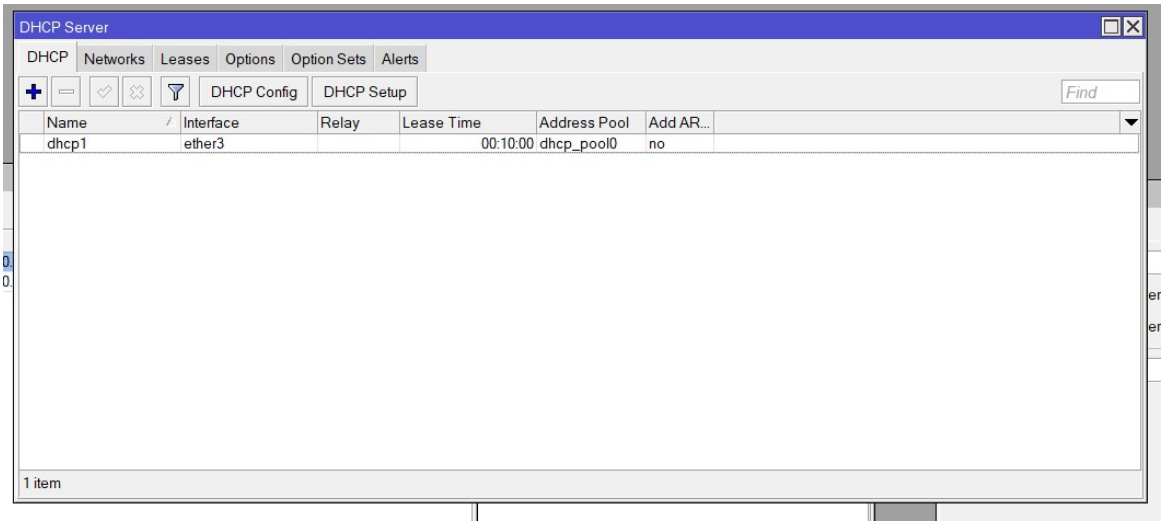


4. Penambahan Alamat IP pada Ether7

   Untuk menghubungkan Router A dengan switch, tambahkan alamat IP pada port ether7. Cara-

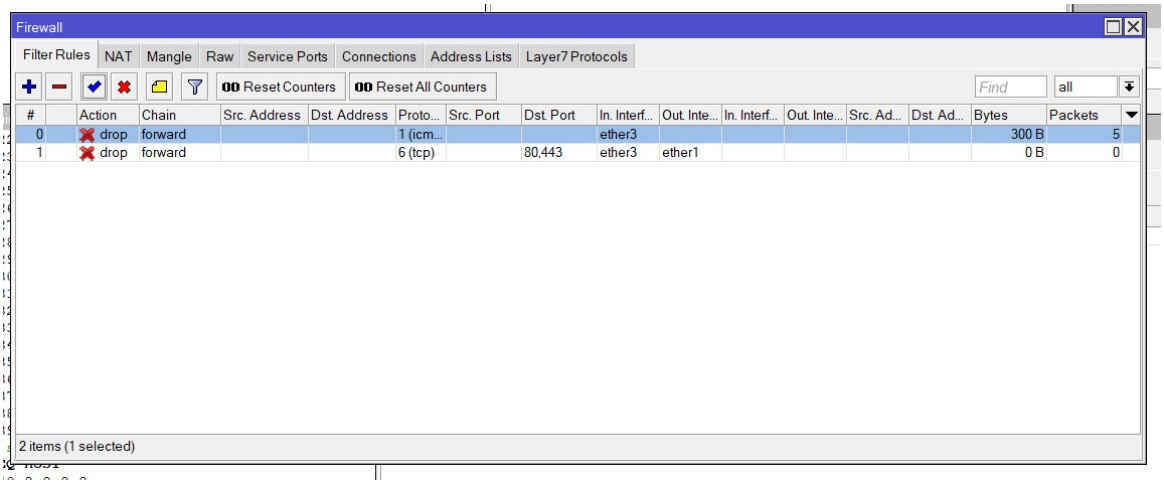
nya, masuk ke menu IP > Addresses, klik ikon "+", lalu masukkan IP address 192.168.10.1/24 dan pilih interface "ether7". Setelah itu, klik Apply dan OK untuk menyimpan pengaturan.

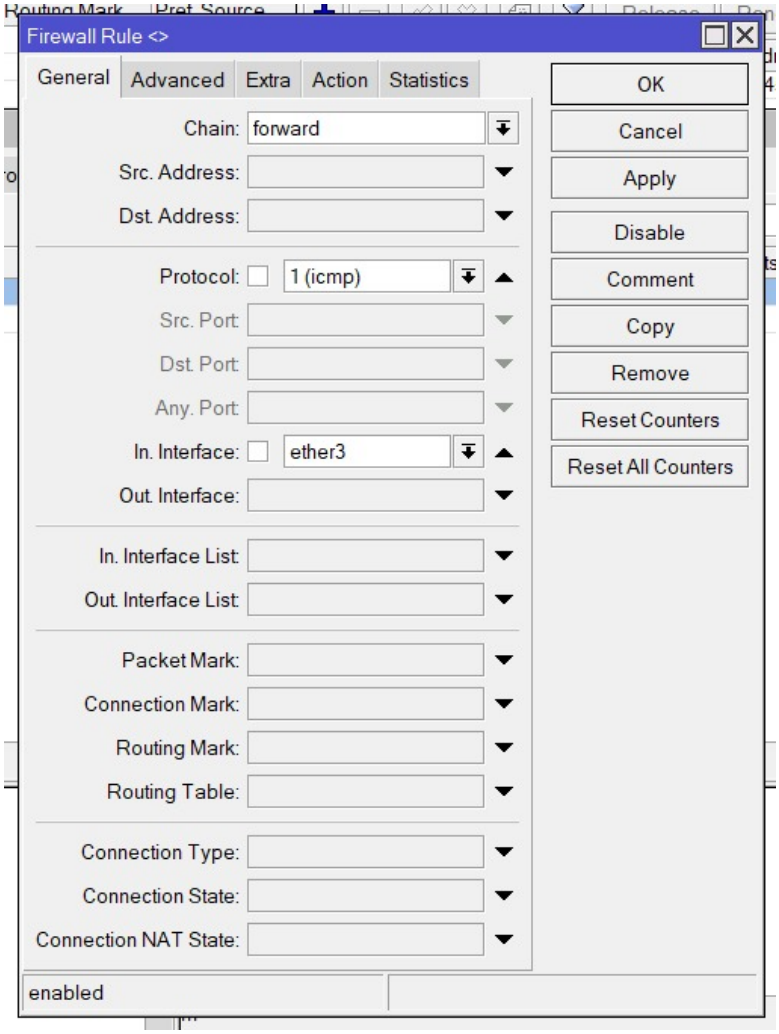
5. Konfigurasi DHCP Server pada Router MikroTik
   Untuk memungkinkan router mendistribusikan IP secara otomatis ke perangkat klien, lakukan konfigurasi DHCP Server. Buka menu IP > DHCP Server, klik tombol "DHCP Setup", lalu pilih interface ether7. Ikuti langkah-langkah selanjutnya dengan mengklik "next" tanpa mengubah pengaturan network, gateway, IP range, DNS server (misal: 8.8.8.8 dan 8.8.4.4), dan durasi lease (misal: 10 menit) hingga proses selesai.

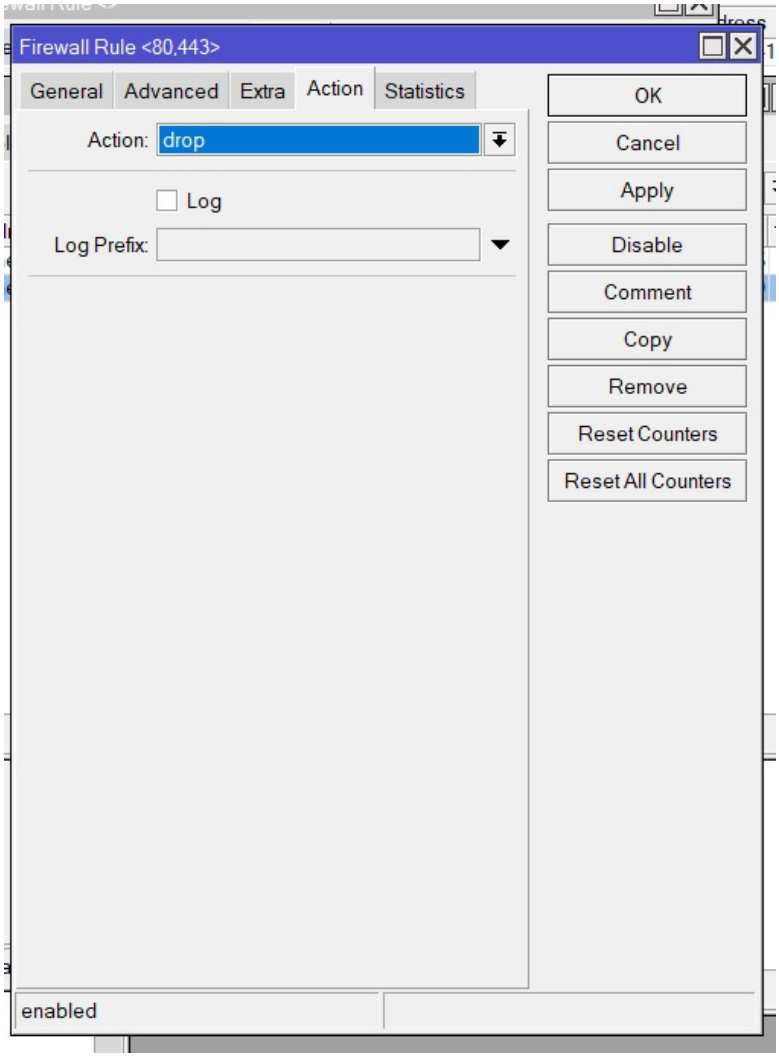


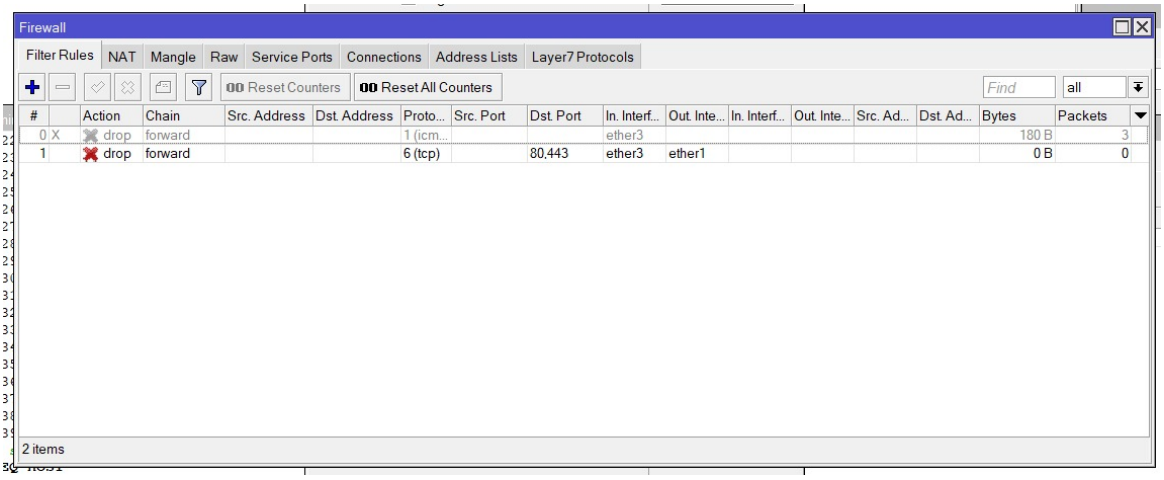
6. Konfigurasi NAT (Network Address Translation)
   Agar klien dapat mengakses internet, konfigurasi NAT diperlukan. Masuk ke menu IP > Firewall > NAT, lalu klik ikon "+". Pada tab "General", atur chain menjadi "src-nat", dan pada tab "Action", pilih "masquerade". Kemudian, apply pengaturan tersebut. Untuk menguji koneksi internet, buka New Terminal di Winbox dan jalankan perintah ping 8.8.8.8; pastikan ada balasan sebagai indikasi koneksi berhasil.

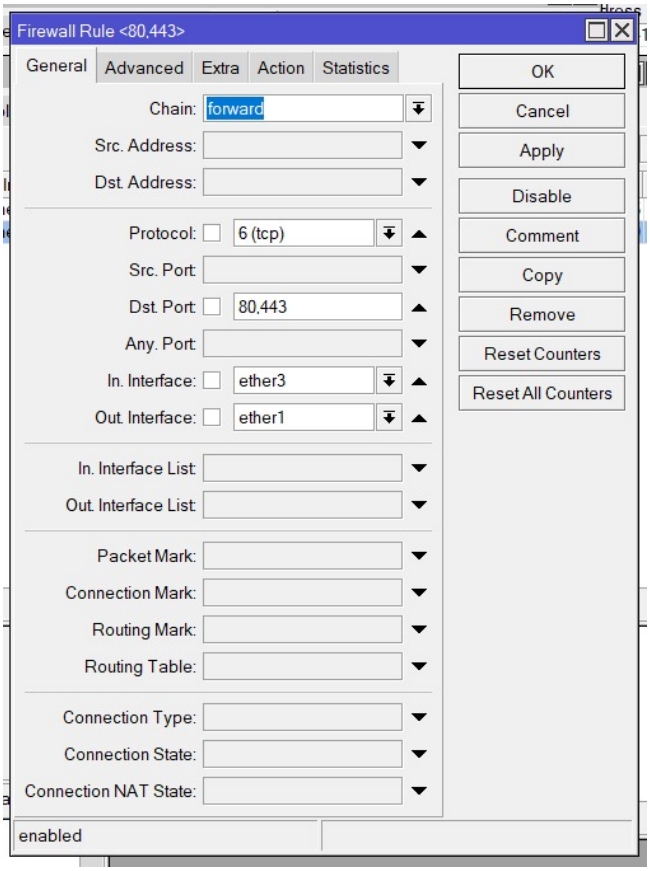
7. Konfigurasi Firewall
   Selanjutnya, tambahkan aturan pada firewall untuk membatasi akses tertentu. Untuk memblokir ICMP (ping), masuk ke menu IP > Firewall > Filter Rules, klik ikon "+". Pada tab "General", atur chain ke "forward", protocol "icmp", dan interface "ether7". Kemudian, pada tab "Action", pilih "drop".

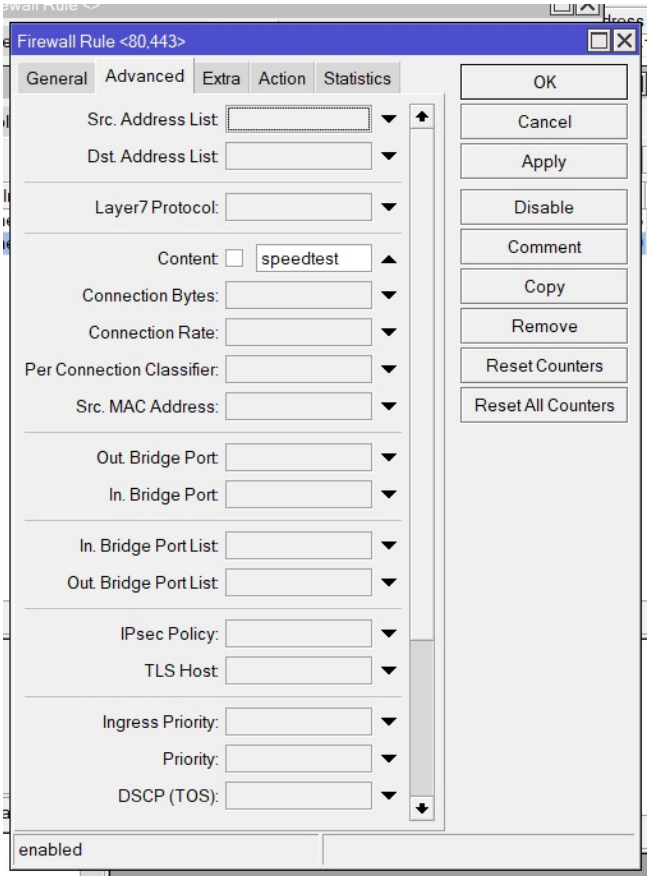

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
00 Reset Counters
00 Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Interf... Out. Inte... In. Interf... Out. Inte... Src. Ad... Dst. Ad... Bytes Packets
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)

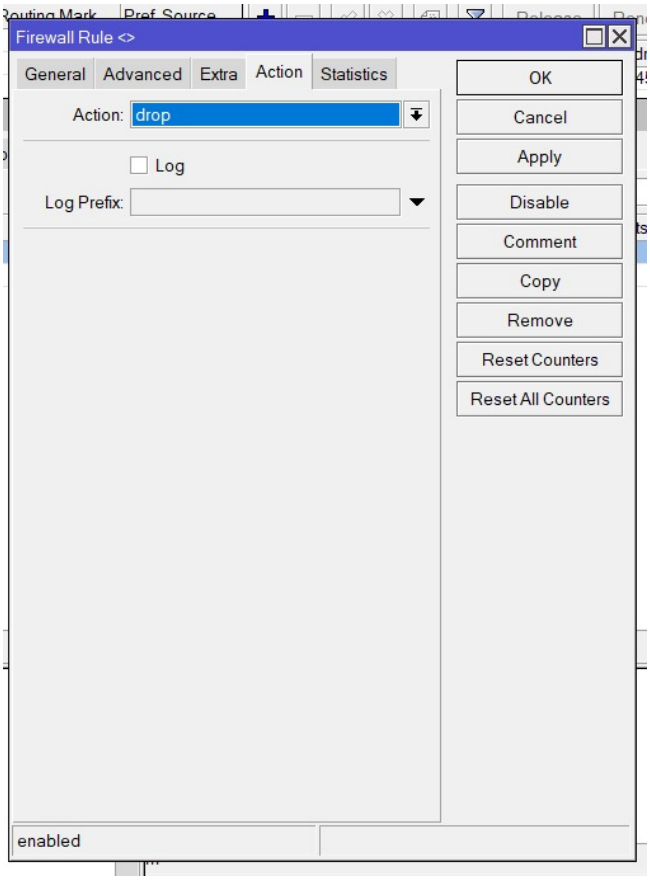

Firewall Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Chain: forward
Src. Address:
Dst. Address:
Protocol: 1 (icmp)
Src. Port:
Dst. Port:
Any. Port:
In. Interface: ether3
Out. Interface:
In. Interface List:
Out. Interface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


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


Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
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 X drop forward 1 (icm... ether3 180 B 3
1 drop forward 6 (tcp) 80,443 ether3 ether1 0 B 0
2 items


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

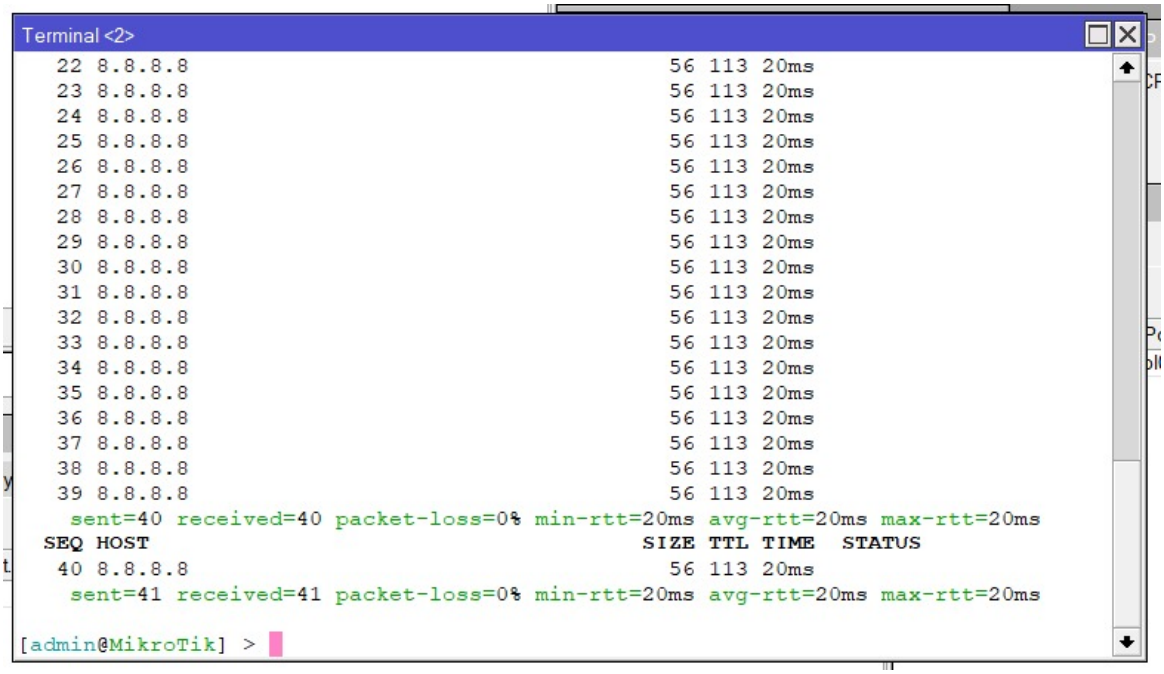

Firewall Rule <80,443>
General
Advanced
Extra
Action
Statistics
Src. Address List:
Dst. Address List:
Layer7 Protocol:
Content: speedtest
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
In. Bridge Port List:
Out. Bridge Port List:
IPsec 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, buatlah bridge. Akses menu Bridge, klik ikon "+" untuk membuat bridge baru, lalu Apply dan OK. Selanjutnya, tambahkan port yang akan masuk ke bridge dengan membuka Bridge > Port, klik ikon "+" dan pilih interface yang terhubung ke laptop dan interface 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 verifikasi bahwa mode DHCP sudah aktif. Untuk memastikan IP telah diterima, buka Command Prompt dan jalankan perintah ipconfig.

10. Uji Coba Konfigurasi
    Untuk menguji konfigurasi, buka Command Prompt di laptop dan jalankan perintah ping google.com atau ping 8.8.8.8. Jika firewall ICMP dalam kondisi aktif (setelah langkah 6), hasil yang akan muncul adalah "Request Timed Out". Setelah itu, nonaktifkan aturan firewall ICMP (dengan mengklik tanda "X" pada rule terkait di Filter Rules), lalu ping kembali google.com; koneksi seharusnya berhasil.



Dengan cara yang sama, tambahkan aturan firewall baru untuk memblokir akses situs web berdasarkan konten (Content Blocking). Pada menu IP > Firewall > Filter Rules, klik ikon "+". Pada tab "General", atur Chain: "forward", Protocol: "tcp", Dst. Port: "80,443", In. Interface: "ether7", dan Out. Interface: "ether1". Pada tab "Advanced", isi Content: "speedtest". Terakhir, pada tab "Action", atur Action: "drop". Namun, dalam percobaan ini, pemblokiran konten "speedtest" tidak berhasil, laptop masih bisa mengakses situs tersebut.

2 Analisis Hasil Percobaan

Seluruh proses konfigurasi router dalam praktikum ini berjalan lancar dan sesuai panduan, dimulai dari pengaturan ulang awal (reset) hingga tahapan pengujian konektivitas. Saat DHCP Client di ether1 dikonfigurasi, router berhasil mendapatkan alamat IP dari jaringan luar, yang menandakan bahwa koneksi internet sudah aktif. Penambahan alamat IP pada ether7 dan konfigurasi DHCP Server juga sukses mendistribusikan alamat IP secara otomatis ke setiap klien.

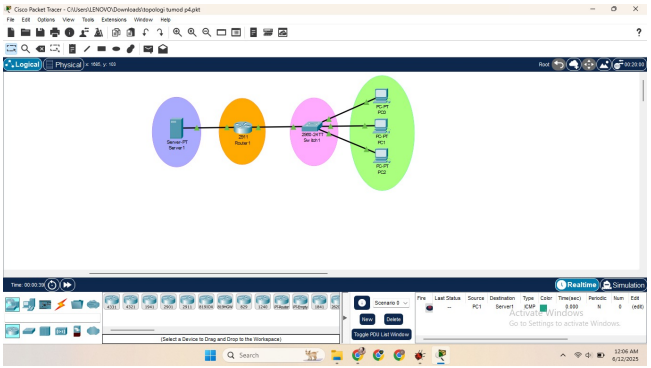
Fungsi NAT (Network Address Translation) bekerja dengan baik, terbukti dari keberhasilan perintah ping 8.8.8.8 yang dilakukan baik dari terminal Winbox maupun laptop yang terhubung. Konfigurasi firewall juga menunjukkan hasil yang diharapkan: pemblokiran ICMP menyebabkan perintah ping mengalami Request Timed Out, dan filter berbasis konten berhasil memblokir akses ke situs-situs tertentu, seperti speedtest.net.

Selama konfigurasi bridge pada Router B dan pengaturan DHCP pada laptop, tidak ditemukan kendala berarti. Semua hasil praktikum ini konsisten dengan teori yang menyatakan bahwa firewall dan NAT mampu mengatur, mengamankan, dan mengontrol lalu lintas jaringan dengan efisien. Potensi kegagalan hanya mungkin terjadi jika ada kesalahan dalam pemilihan interface atau penempatan aturan pada chain yang salah, namun hal ini tidak terjadi selama percobaan.

3 Hasil Tugas Modul

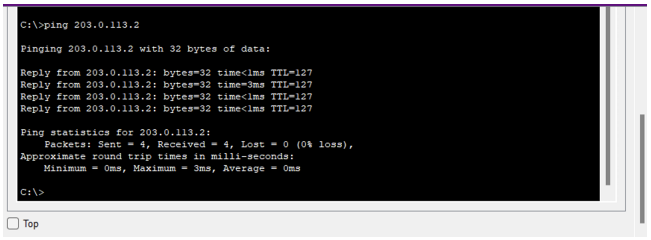
1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:

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

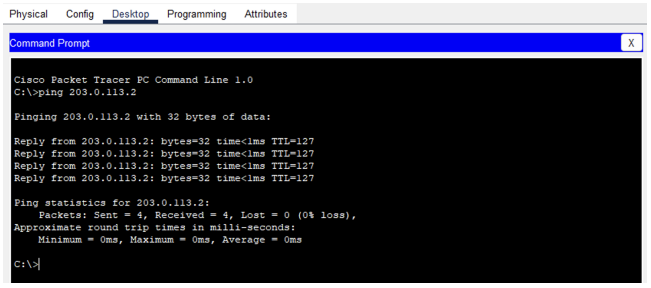


Gambar 1: Topologi

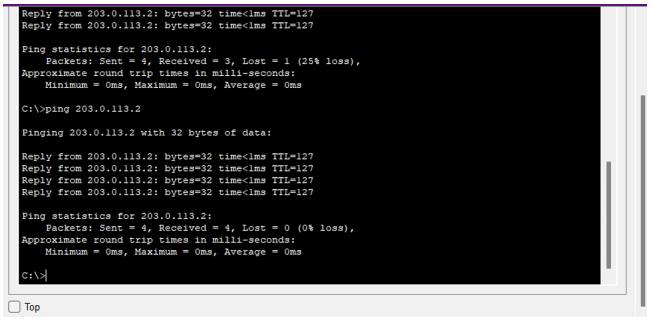
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.



Gambar 2: Ping PC1 ke Server



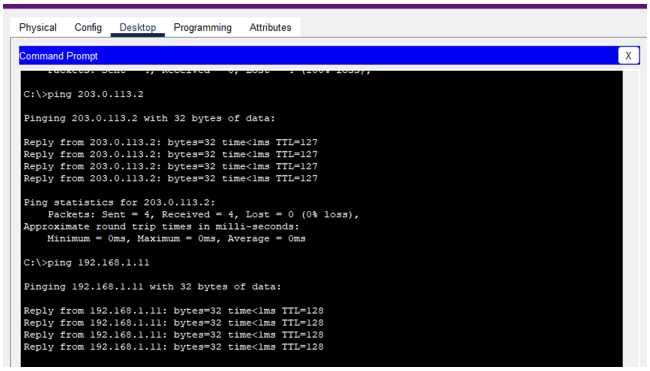
Gambar 3: Ping PC2 ke Server



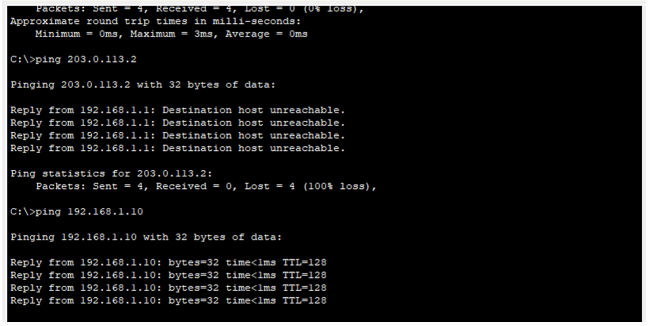
Gambar 4: Ping PC3 ke Server

3. Konfigurasi Firewall (ACL):

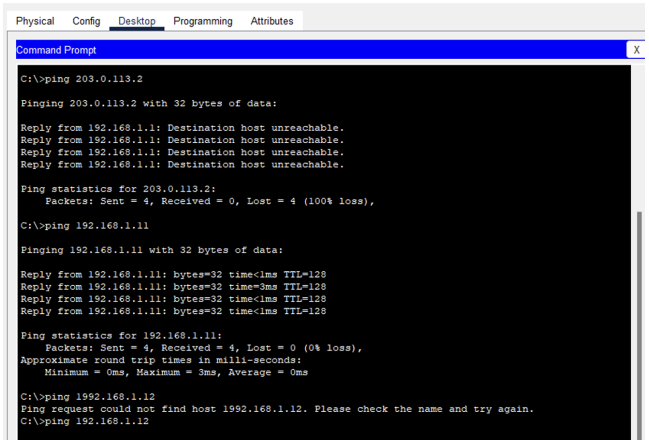
- Izinkan hanya PC1 yang dapat mengakses Server.
- Blokir PC1 dan PC3 dari mengakses Server.
- Semua PC harus tetap bisa saling terhubung di LAN.



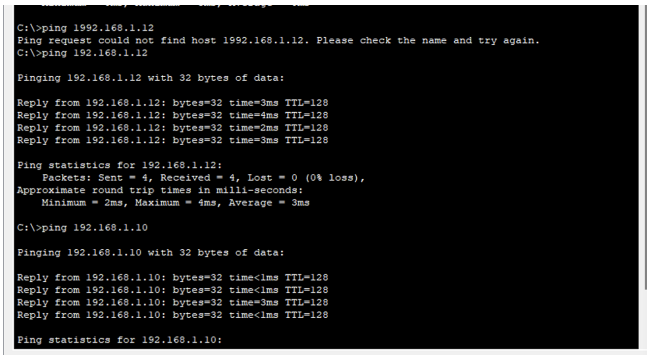
Gambar 5: Ping PC1 berhasil askses ke Server



Gambar 6: Ping PC2 gagal akses ke Server



Gambar 7: Ping PC3 gagal akses ke Server



Gambar 8: Ping PC3 berhasil akses ke device lain

4 Kesimpulan

Praktikum Firewall dan NAT ini berhasil mendemonstrasikan bagaimana konfigurasi dasar pada router MikroTik bisa dimanfaatkan untuk mengelola lalu lintas jaringan secara efisien dan aman. Dengan menerapkan DHCP Client dan Server, NAT, serta firewall, kami jadi lebih memahami peran krusial konfigurasi jaringan dalam mendistribusikan IP, mengatur akses internet, dan menyaring data yang tidak diinginkan.

Semua hasil percobaan berjalan sesuai teori, termasuk pengujian konektivitas dan pemblokiran berdasarkan protokol atau konten. Praktikum ini semakin memperkuat pemahaman kami tentang konsep dasar jaringan seperti IP address, DHCP, NAT, dan firewall, baik dalam konteks praktikum maupun penerapannya di dunia nyata. Salah satu pelajaran penting yang kami dapat adalah betapa pentingnya ketelitian dalam memilih interface dan urutan konfigurasi agar fungsi jaringan dapat berjalan optimal.

5 Lampiran

5.1 Dokumentasi saat praktikum