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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

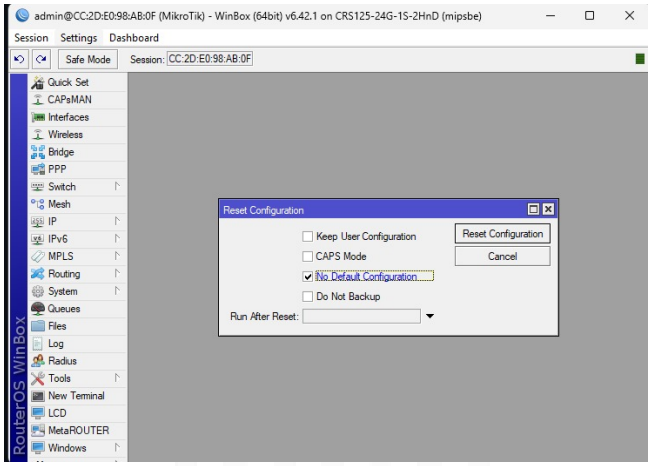
Aaron Smeraldo Olivier Manik - 502423070

31 Mei 2025

1 Langkah-Langkah Percobaan

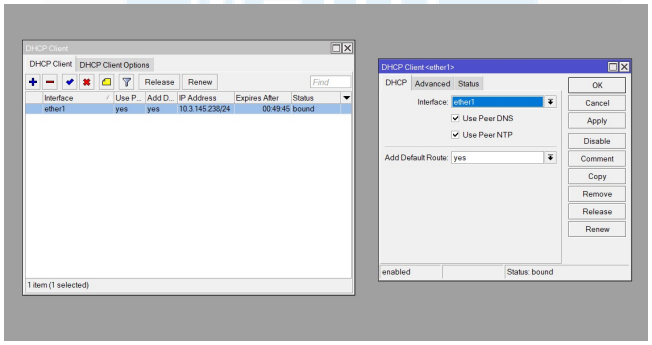
1.1 Percobaan 1 : Firewall dan NAT

1. Siapkan alat dan bahan lalu reset mikrotik dengan masuk ke aplikasi winbox lalu klik reset configuration



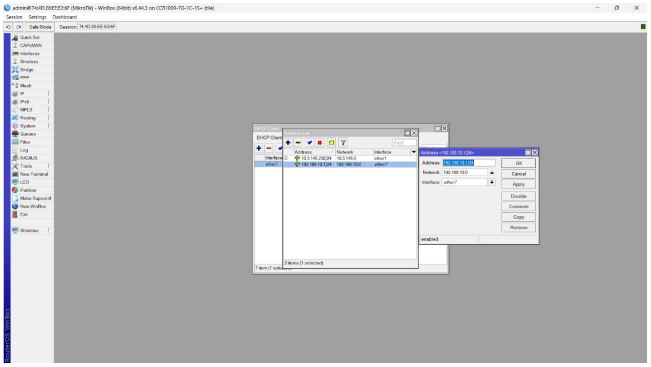
Gambar 1: Mereset mikrotik

2. Pada router A, masuk menu IP lalu DHCP Client lalu tambahkan pada interface ether1, centang Use PeerDNS dan UsePeerNTP, setelah diapply pastikan Statusnya "Bound"



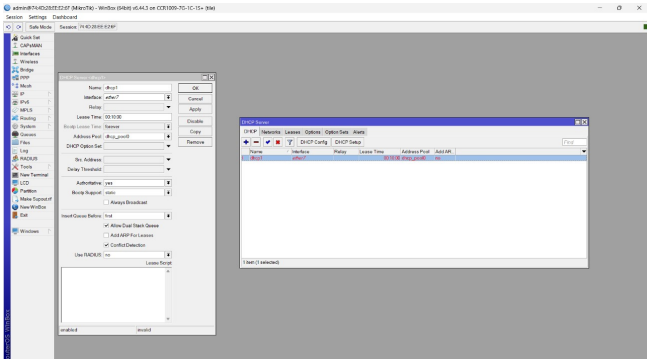
Gambar 2: Setting DHCP Client

3. Lalu tambahkan IP Address untuk Ether7 yang terhubung dengan switch dengan masuk ke menu IP lalu Addresses lalu tambahkan IP, Address : 192.168.10.1/24, Interface: "ether7", lalu Apply



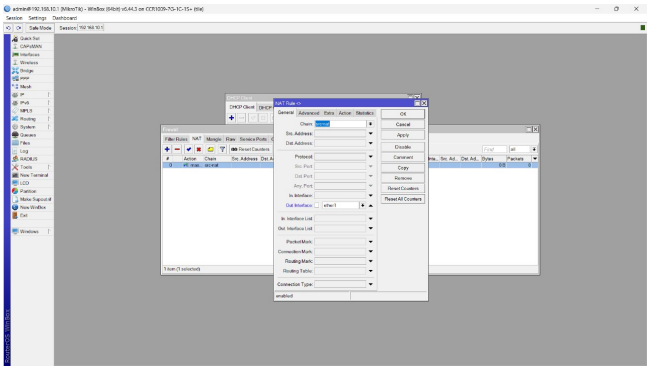
Gambar 3: Setting IP Address untuk Switch

4. Lalu konfigurasi DHCP Server pada router mikrotik dengan menekan menu IP lalu DHCP Server lalu DHCP Setup lalu klick interface ether7, lalu klik next hingga selesai tanpa mengubah apapun

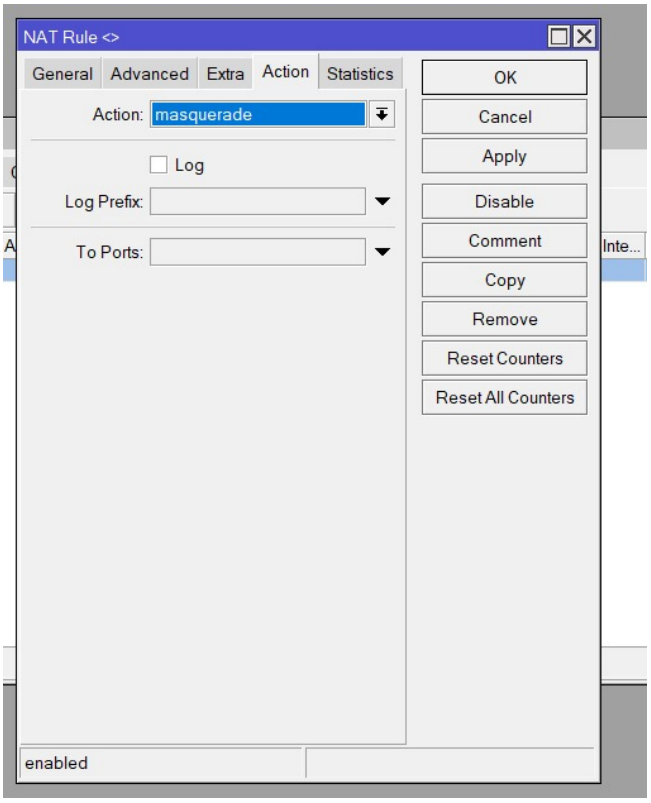


Gambar 4: Setting DHCP Server

5. Lalu mensetting NAT, dengan menekan menu IP lalu Firewall lalu NAT lalu klik tambah, pada tab general, atur chain menjadi "src-nat", dan pada tab action atur menjadi "masquerade" lalu apply

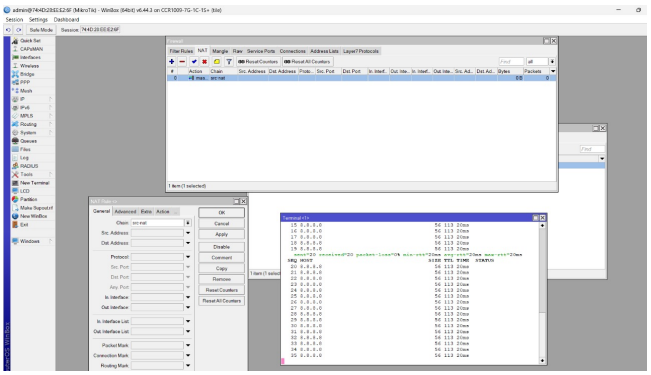


Gambar 5: Konfigurasi NAT



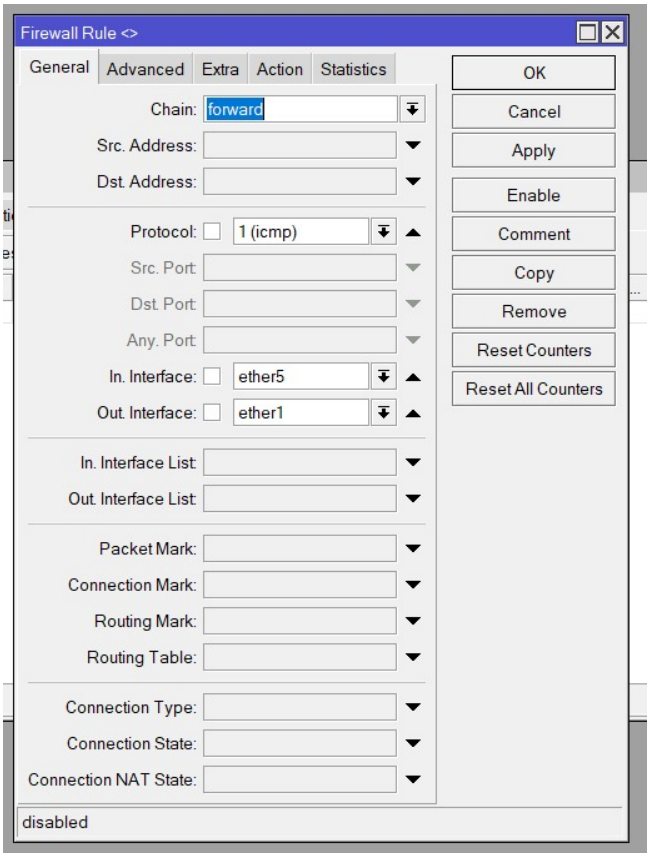
Gambar 6: Konfigurasi NAT

6. Lalu melakukan perintah ping pada menu New Terminal, dengan menekan "ping 8.8.8.8"



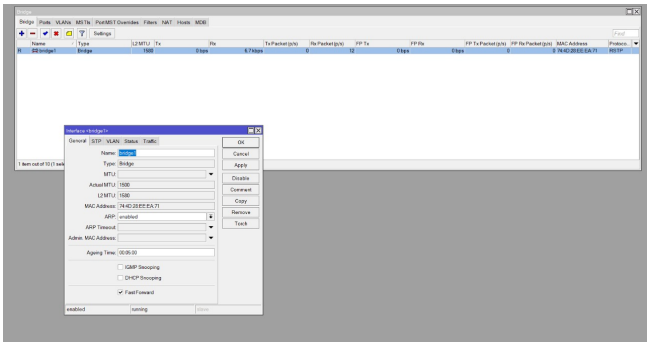
Gambar 7: Ping 8.8.8.8

7. Setelah itu, melakukan konfigurasi Firewall dengan menekan IP lalu Firewall lalu Filter Rule. Lalu tambahkan pemblokiran ICMP atau Internet Control Message Protocol, pada tab general, atur chain ke "forward" lalu protocol "icmp" lalu interface "ether7" lalu ke tab action dengan atur action : "drop"



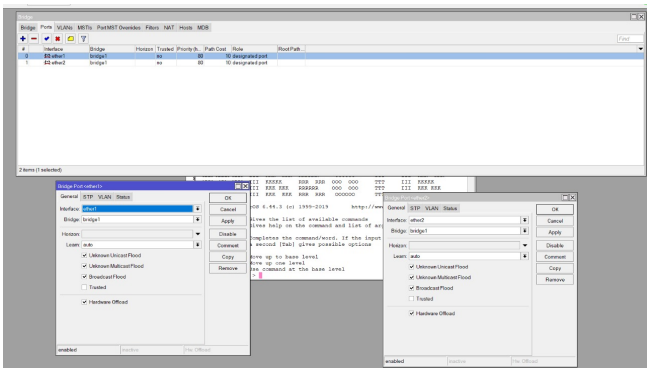
Gambar 8: Setting firewall dengan metode ICMP

8. Pada router B, melakukan konfigurasi Bridge dengan menekan menu bridge lalu tambahkan bridge lalu Apply



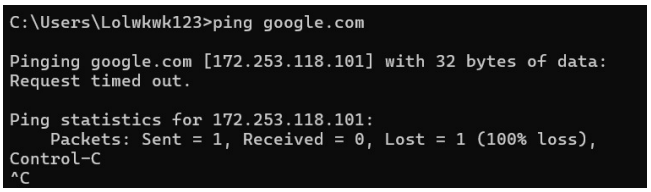
Gambar 9: Menambahkan bridge pada Router B

9. Lalu masuk ke menu Bridge lalu Port lalu tambahkan dengan interface yang terhubung pada laptop dan interface yang terhubung pada Router A



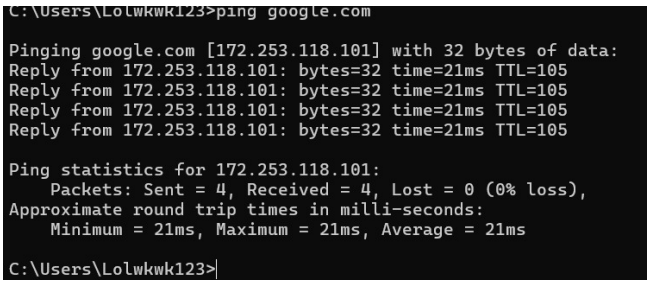
Gambar 10: Menambahkan port bridge sesuai interface

10. lalu pada setting laptop, pastikan konfigurasi jaringan pada laptop menggunakan DHCP (automatic) lalu ping google.com pada command prompt laptop



Gambar 11: Ping google.com dengan ICMP nyala

11. Lalu nonaktifkan firewall ICMP dengan menekan tanda "X" (disable) pada peraturan terkait di Filter Rules lalu ping kembali google.com



Gambar 12: Ping google.com dengan ICMP mati

12. Dengan cara yang sama seperti di atas, tambah firewall dengan menekan menu IP lalu firewall lalu Filter RUle lalu klik tambahkan untuk Pemblokiran Akses Situs Web Berdasarkan Konten (Content Blocking), pada tab General, atur Chain: "forward", atur Protocol: "tcp", atur Dst. Port: "80,443", atur In. Interface: "ether7", atur Out. Interface: "ether1", pada tab advanced atur Content: "speedtest", Pada tab Action, atur Action: "drop". Namun pada percobaannya gagal, laptop masih bisa melakukan searching pada konten speedtest.

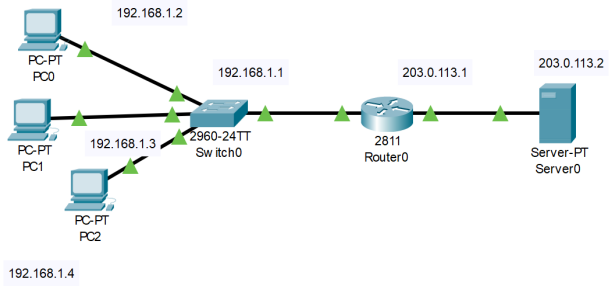
2 Analisis Hasil Percobaan

Pada awal percobaan, router Mikrotik dikonfigurasi ulang menggunakan fitur Reset Configuration, lalu dilakukan pengaturan DHCP Client pada antarmuka ether1 yang memungkinkan router menda-

patkan IP secara otomatis dari jaringan luar. Selanjutnya, ether7 diberikan IP statik dan dijadikan jalur distribusi DHCP Server untuk perangkat dalam jaringan lokal, yang ditandai dengan status "Bound" pada DHCP Client dan distribusi IP yang berhasil dilakukan ke perangkat seperti laptop. Pengaturan NAT dilakukan dengan menggunakan metode masquerade, yang terbukti berhasil karena perangkat dalam jaringan lokal dapat mengakses internet dan merespons perintah ping ke alamat publik seperti 8.8.8.8. Hal ini menandakan bahwa proses NAT berjalan dengan baik dalam menyamarkan alamat IP lokal ke IP publik router. Kemudian, firewall diuji dengan memblokir lalu lintas ICMP menggunakan filter rule dengan chain "forward" dan protokol "icmp". Pemblokiran ini berhasil ditunjukkan dengan gagalnya ping dari laptop ke google.com, dan saat aturan dinonaktifkan (disabled), koneksi ICMP kembali normal, yang membuktikan bahwa fungsi firewall bekerja sesuai pengaturan. Langkah selanjutnya yaitu konfigurasi bridge pada Router B dan penambahan port sesuai dengan antarmuka yang terhubung ke laptop dan Router A juga berhasil, ditunjukkan dengan tetap terdistribusinya jaringan melalui laptop. Namun, pada konfigurasi terakhir yang bertujuan melakukan content filtering terhadap kata "speedtest" melalui port TCP 80 dan 443, fungsi firewall mengalami kegagalan. Meskipun rule telah dibuat dengan benar secara teori, namun konten yang mengandung kata “speedtest” tetap bisa diakses melalui browser. Gagalnya pemblokiran ini diduga karena adanya malfungsi pada sistem Mikrotik yang digunakan, yang kemungkinan besar tidak menjalankan fitur content blocking secara penuh. Selain itu, kemungkinan juga disebabkan oleh penggunaan protokol HTTPS (port 443) yang telah terenkripsi, sehingga Mikrotik tidak mampu membaca isi konten dan menerapkan filter berbasis kata kunci secara efektif pada traffic terenkripsi.

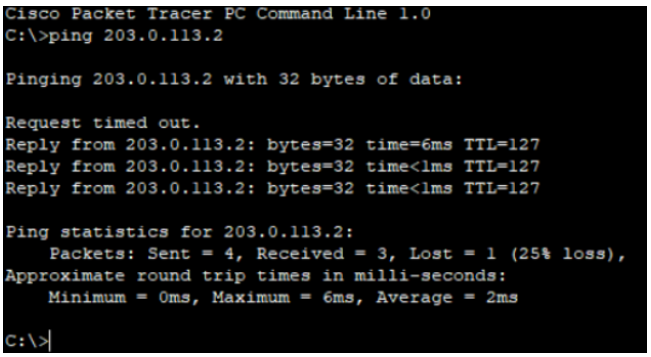
3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:
    - 1 Router
    - 1 Switch
    - 3 PC (LAN)
    - 1 Server (Internet/Public)

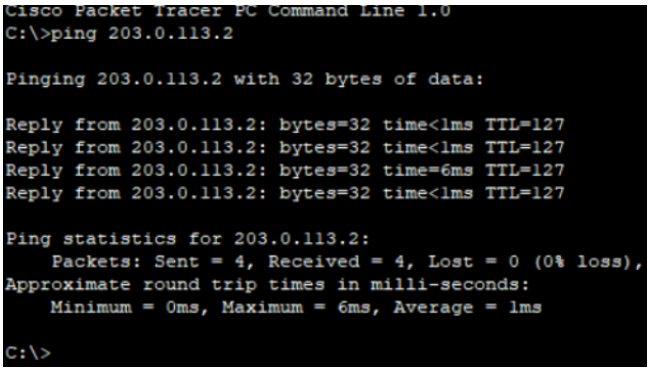


Gambar 13: Topologi

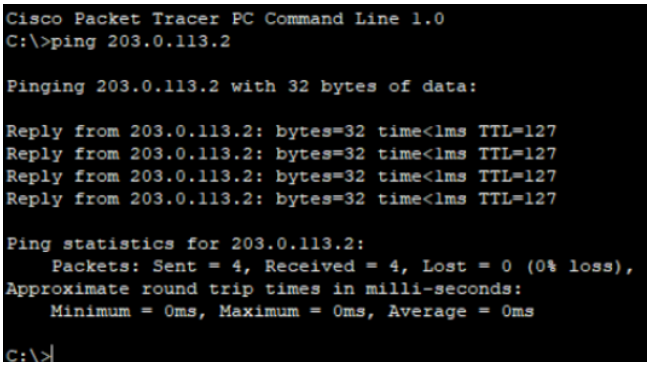
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.



Gambar 14: Ping PC1 ke Server

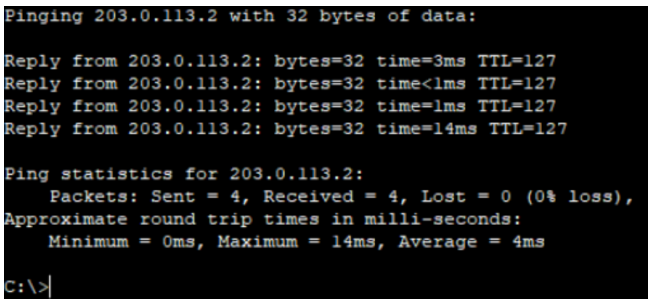


Gambar 15: Ping PC2 ke Server

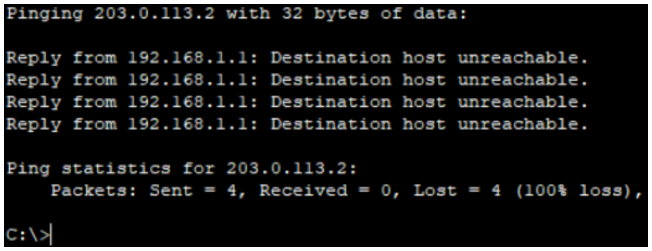


Gambar 16: Ping PC3 ke Server

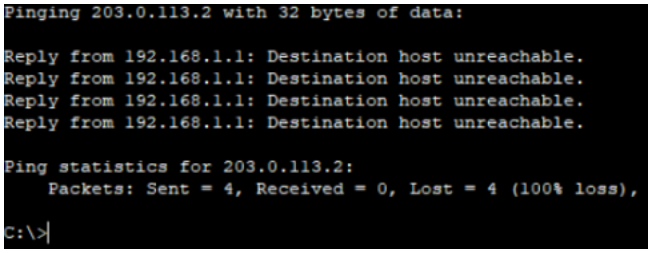
3. Konfigurasi Firewall (ACL):
    - Izinkan hanya PC1 yang dapat mengakses Server.
    - Blokir PC1 dan PC3 dari mengakses Server.
    - Semua PC harus tetap bisa saling terhubung di LAN.



Gambar 17: Ping PC1 ke Server dengan konfigurasi firewall ACL



Gambar 18: Ping PC2 ke Server dengan konfigurasi firewall ACL



Gambar 19: Ping PC3 ke Server dengan konfigurasi firewall ACL

4 Kesimpulan

Berdasarkan hasil percobaan konfigurasi Firewall dan NAT pada Mikrotik, dapat disimpulkan bahwa proses konfigurasi dasar seperti pengaturan DHCP Client, pemberian IP statik, konfigurasi NAT dengan metode masquerade, serta implementasi DHCP Server berhasil dilakukan dan berfungsi sesuai harapan. Pengujian firewall terhadap protokol ICMP juga berhasil menunjukkan bahwa Mikrotik mampu memblokir lalu lintas tertentu berdasarkan aturan yang telah dibuat. Konfigurasi bridge pada Router B pun berjalan dengan baik dan tidak mengganggu distribusi jaringan ke perangkat akhir. Namun, percobaan content filtering mengalami kegagalan. Hal ini menunjukkan bahwa fitur pemblokiran konten berbasis kata kunci tidak efektif, terutama saat menghadapi lalu lintas HTTPS yang terenkripsi. Selain faktor enkripsi, kemungkinan malfungsi pada sistem Mikrotik juga menjadi penyebab tidak berfungsinya filter konten secara optimal.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 20: Dokumentasi setelah praktikum