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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

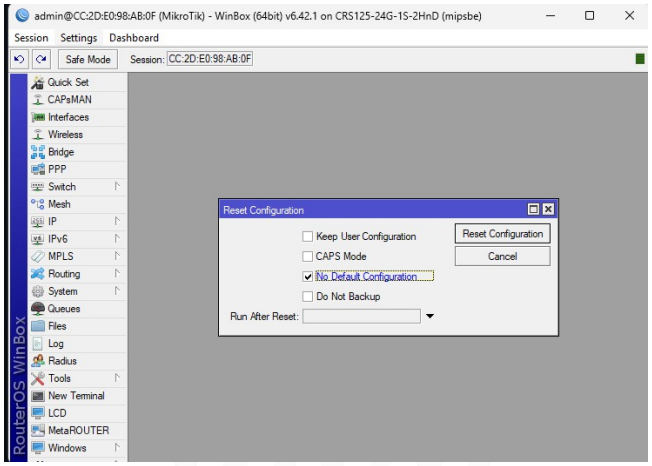
Andriy Shevtiyan - 5024231080

31 Mei 2025

1 Langkah-Langkah Percobaan

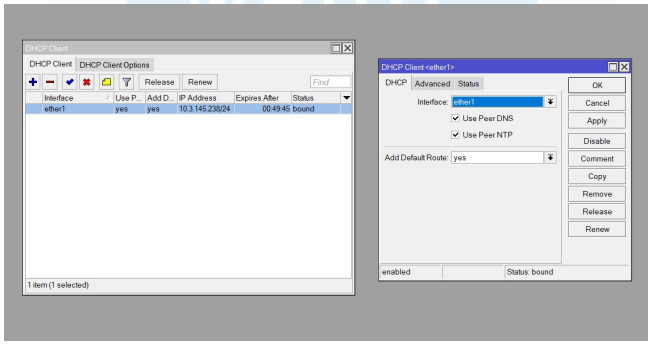
1.1 Percobaan 1 : Firewall dan NAT

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



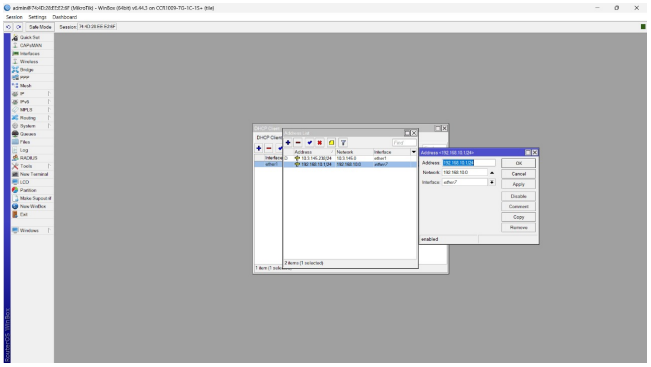
Gambar 1: Mereset mikrotik

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"



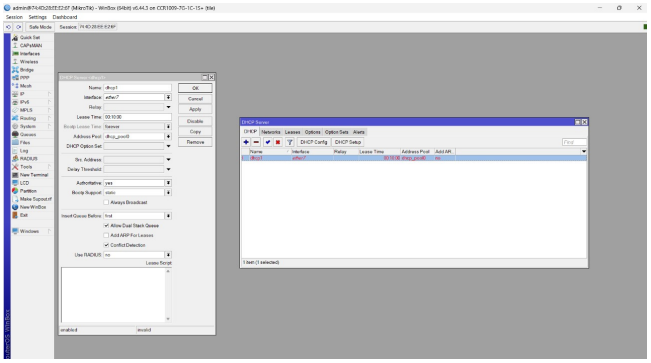
Gambar 2: Setting DHCP Client

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



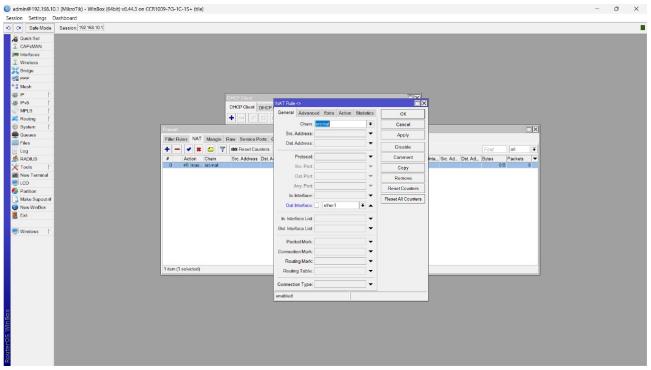
Gambar 3: Setting IP Address untuk Switch

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

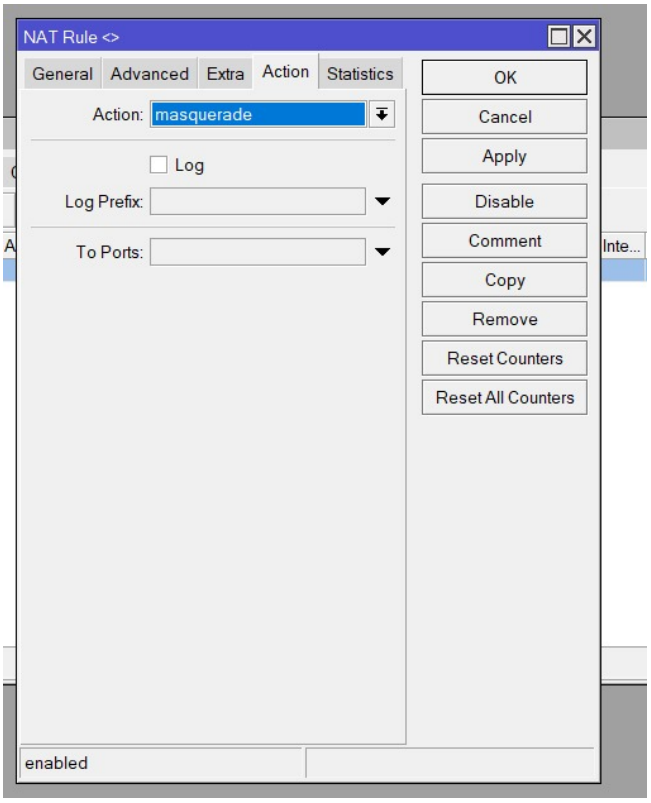


Gambar 4: Setting DHCP Server

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

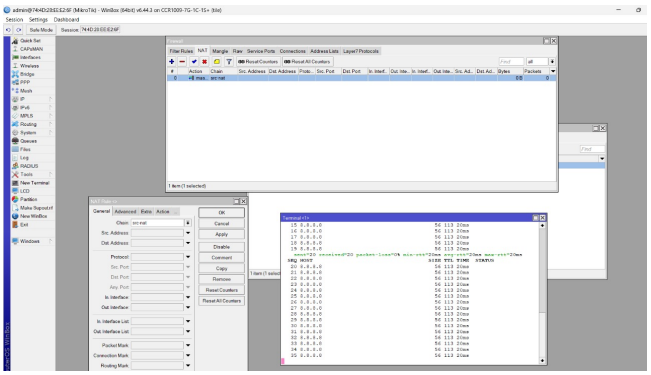


Gambar 5: Konfigurasi NAT



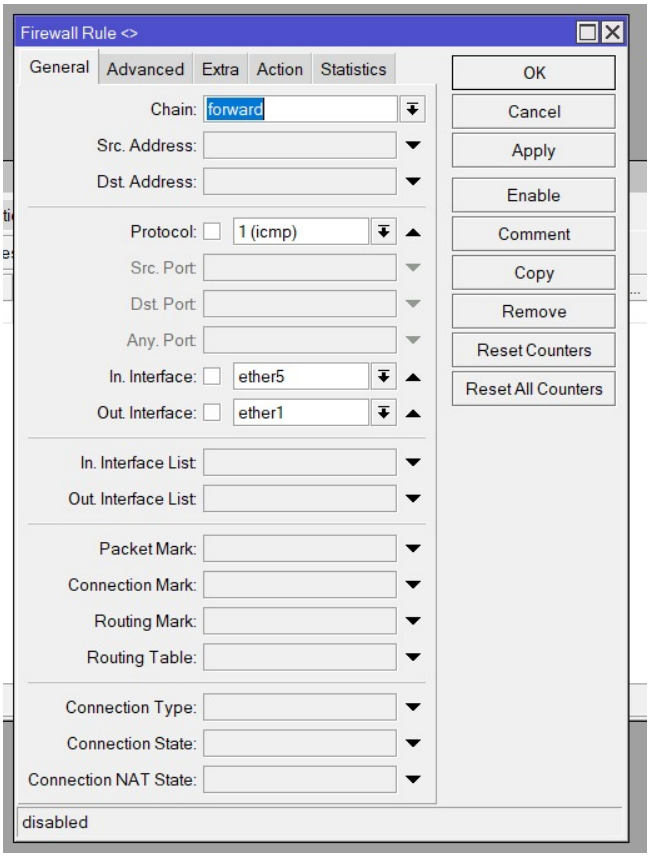
Gambar 6: Konfigurasi NAT

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



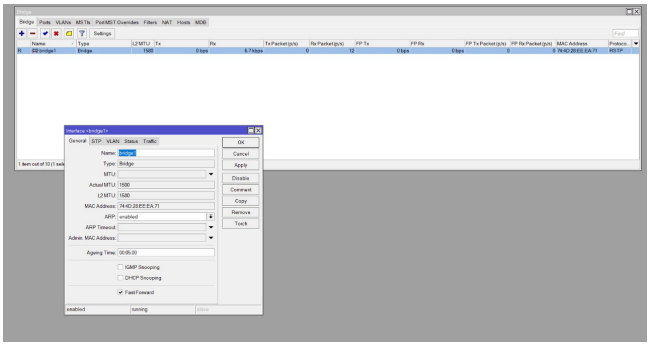
Gambar 7: Ping 8.8.8.8

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"



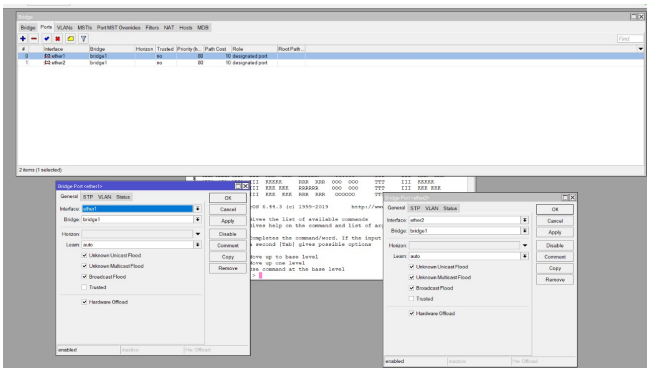
Gambar 8: Setting firewall dengan metode ICMP

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



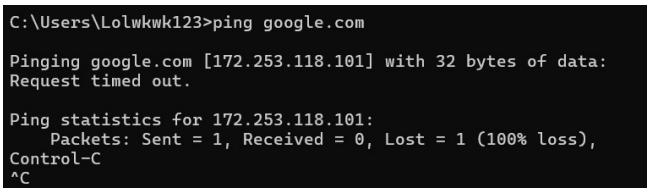
Gambar 9: Menambahkan bridge pada Router B

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



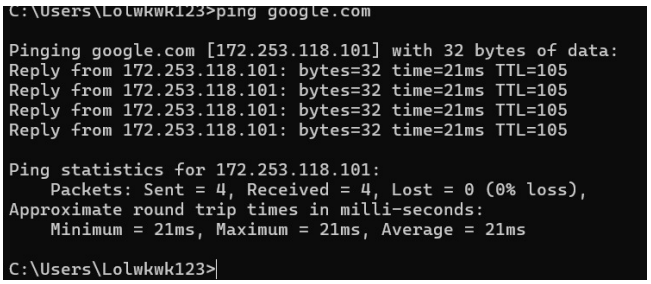
Gambar 10: Menambahkan port bridge sesuai interface

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 tahap awal eksperimen, router Mikrotik dikembalikan ke konfigurasi default dengan memanfaatkan fitur Reset Configuration. Setelah itu, antarmuka ether1 diatur sebagai DHCP Client agar

router dapat secara otomatis memperoleh alamat IP dari jaringan luar. Sementara itu, ether7 dikonfigurasi dengan alamat IP statis dan dijadikan sebagai jalur distribusi dari DHCP Server ke perangkat lokal. Indikator keberhasilan ditunjukkan oleh status "Bound" pada DHCP Client dan fakta bahwa laptop dalam jaringan berhasil menerima IP dari server.

Konfigurasi NAT menggunakan metode masquerade juga berjalan lancar. Bukti keberhasilannya tampak dari kemampuan perangkat lokal mengakses internet serta merespons perintah ping ke alamat publik seperti 8.8.8.8, yang menunjukkan bahwa translasi alamat dari IP privat ke IP publik telah berfungsi dengan baik.

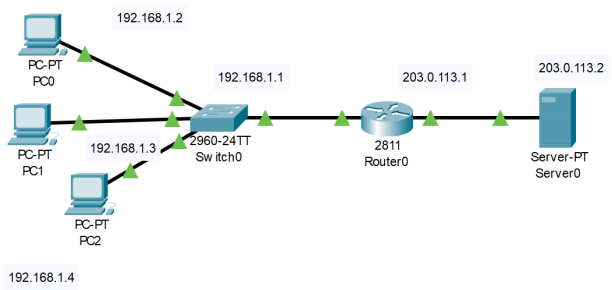
Pengujian terhadap fitur firewall dilakukan dengan menambahkan aturan pada chain forward untuk memblokir protokol ICMP. Ketika aturan aktif, permintaan ping dari laptop ke google.com gagal terkirim. Namun, setelah aturan tersebut dinonaktifkan, koneksi kembali normal, membuktikan bahwa mekanisme firewall bekerja sesuai konfigurasi yang diterapkan.

Selanjutnya, dilakukan konfigurasi bridge pada Router B, termasuk menambahkan port yang menghubungkan laptop dan Router A ke dalam bridge interface. Hasilnya menunjukkan bahwa koneksi tetap stabil dan perangkat pengguna tetap dapat mengakses jaringan tanpa hambatan.

Pada bagian akhir percobaan, dilakukan uji content filtering terhadap kata kunci speedtest melalui port TCP 80 dan 443. Namun, upaya ini tidak membuahkan hasil; konten yang dimaksud masih dapat diakses melalui browser meskipun aturan firewall telah diterapkan. Kegagalan ini kemungkinan besar disebabkan oleh dua faktor utama: pertama, karena lalu lintas HTTPS pada port 443 bersifat terenkripsi sehingga Mikrotik tidak mampu membaca isi data untuk disaring, dan kedua, adanya kemungkinan kendala teknis atau keterbatasan pada sistem Mikrotik itu sendiri yang menghambat fungsi penyaringan berbasis kata kunci.

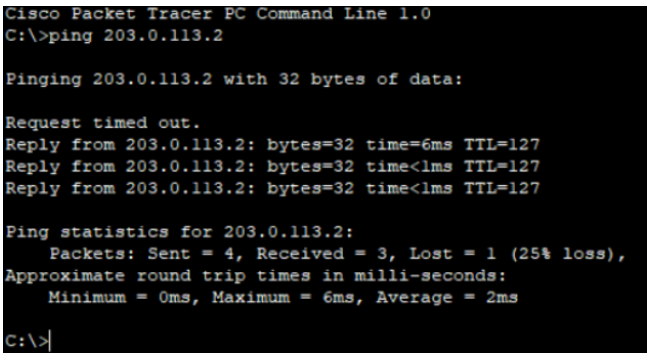
3 Hasil Tugas Modul

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

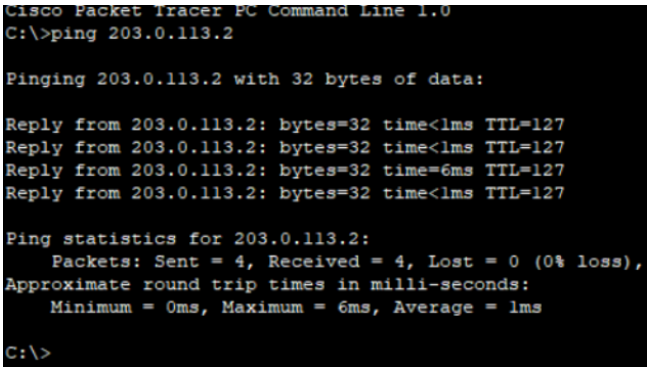


Gambar 13: Topologi

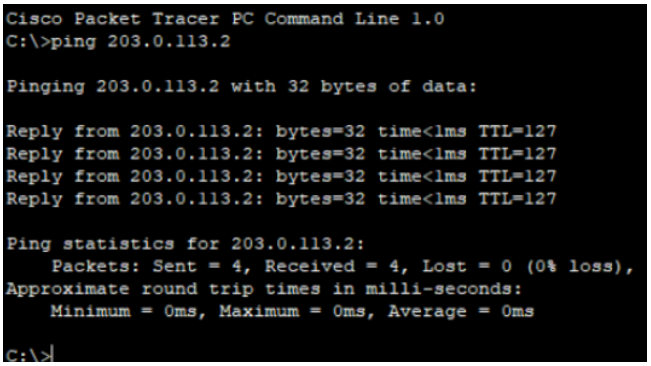
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.



Gambar 14: Ping PC1 ke Server

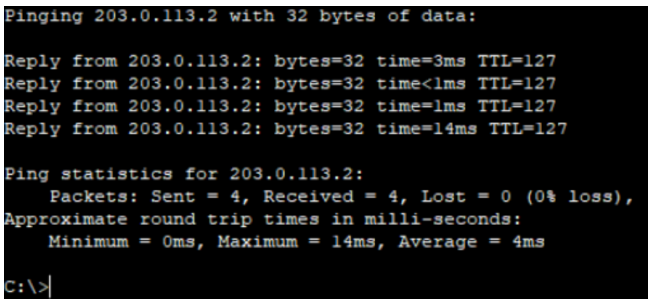


Gambar 15: Ping PC2 ke Server

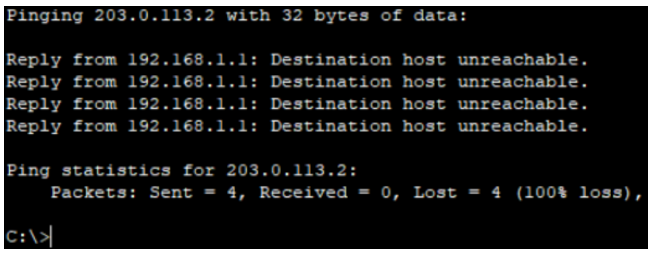


Gambar 16: Ping PC3 ke Server

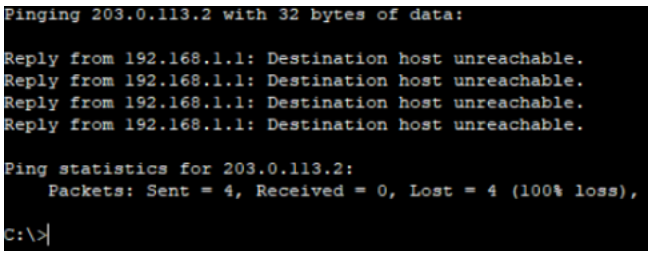
3. Konfigurasi Firewall (ACL):
    - Izinkan hanya PC1 yang dapat mengakses Server.
    - Blokir PC1 dan PC3 dari mengakses Server.
    - Semua PC harus tetap bisa saling terhubung di LAN.



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

Dari percobaan yang dilakukan, terlihat bahwa konfigurasi dasar—meliputi aktivasi DHCPClient, penetapan IP statik, pembuatan aturan NAT dengan metode masquerade, serta pengaturan DHCPServer—berhasil diterapkan dan bekerja sebagaimana mestinya. Uji firewall menggunakan protokolICMP pun membuktikan bahwa router Mikrotik mampu memblokir lalu lintas tertentu sesuai kebijakan yang dibuat.

Pada sisi lain, proses bridging di RouterB berjalan mulus tanpa menimbulkan gangguan bagi perangkat pengguna yang tersambung. Namun, fitur content filtering berbasis kata kunci tidak memberikan hasil yang diharapkan. Ketidakefektifan ini terutama disebabkan oleh lalu lintas HTTPS yang terenkripsi, dan mungkin juga dipengaruhi oleh keterbatasan atau bug pada sistemMikrotik, sehingga mekanisme penyaringan tidak dapat berfungsi optimal.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 20: Dokumentasi setelah praktikum