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

Laporan Akhir
Praktikum Jaringan Komputer

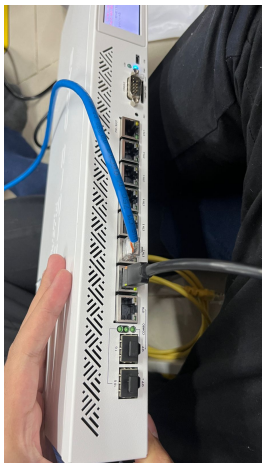
Firewall dan NAT

Aminah Nur'aini Muchayati - 5024231034

2025

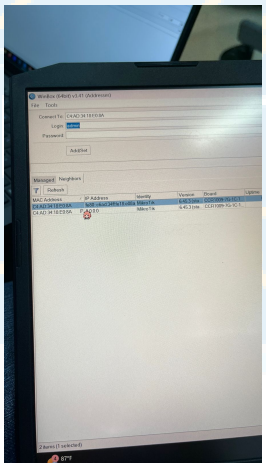
1 Langkah-Langkah Percobaan

1. Menyiapkan 2 mikrotik, 2 laptop, dan 3 kabel LAN. Kemudian menghubungkan router MikroTik ke laptop menggunakan kabel UTP.



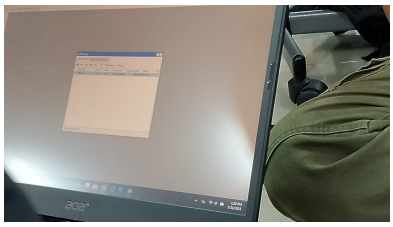
Gambar 1: Langkah Pertama

2. Buka aplikasi Winbox di laptop, lalu akses router dengan memasukkan MAC Address-nya.



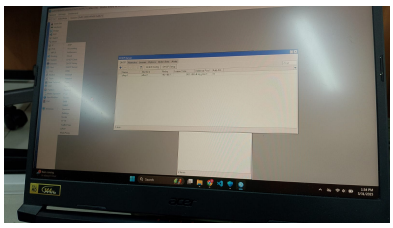
Gambar 2: Langkah Kedua

3. Konfigurasi DHCP Client pada Router A dengan menyambungkan ke Ether 1



Gambar 3: Langkah Ketiga

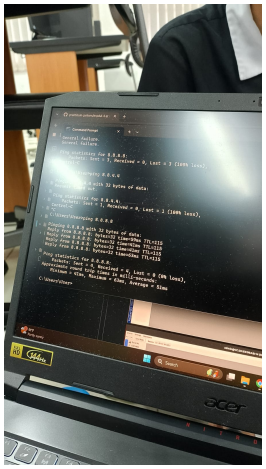
4. Menambahkan alamat IP 192.168.10.1/24 pada ether7 untuk konektivitas dengan Switch kemudian Konfigurasi DHCP Server untuk secara otomatis mendistribusikan alamat IP kepada perangkat klien yang terhubung.



Gambar 4: Langkah Keempat

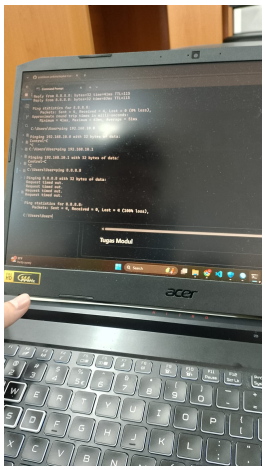
5. Konfigurasi NAT (Network Address Translation) untuk menyediakan konektivitas internet melalui Akses menu IP > Firewall > NAT.

6. test ping ke "ping 8.8.8.8".



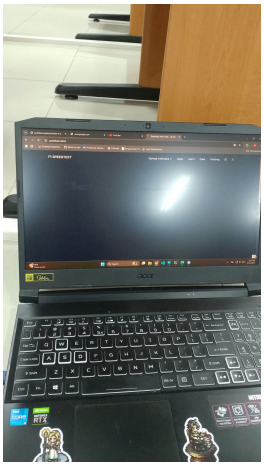
Gambar 5: Langkah Keenam

7. Konfigurasi Firewall dengan melakukan pemblokiran ICMP (Internet Control Message Protocol) dan Akses Situs Web Berdasarkan Konten (Content Blocking) kemudian uji ping

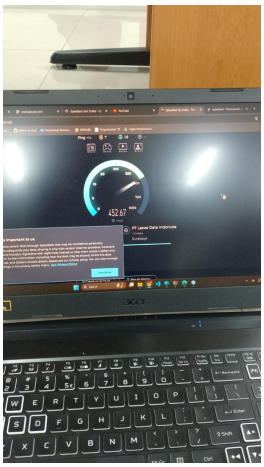


Gambar 6: Langkah Ketujuh

8. Pada laptop 2 :
    - konfigurasi bridge untuk mengubah fungsi Router B menjadi hub melalui Akses menu Bridge.
    - Menambahkan port ke dalam bridge yang telah dibuat
    - Konfigurasi Alamat IP pada Laptop secara otomatis melalui DHCP
    - Uji test PING dari Laptop 2 ke alamat Laptop 1
9. Uji coba pemblokiran konten



Gambar 7: Saat Firewall dinyalakan



Gambar 8: Saat Firewall dimatikan

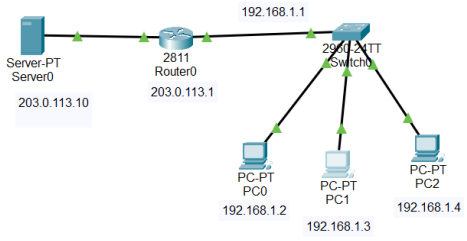
2 Analisis Hasil Percobaan

Berdasarkan hasil praktikum, konfigurasi NAT (Network Address Translation) dan Firewall pada router berhasil dilakukan dengan baik. Penerapan NAT menggunakan metode masquerade memungkinkan seluruh perangkat dalam jaringan lokal untuk mengakses internet melalui satu alamat IP publik, yang secara otomatis dialokasikan oleh DHCP client. Hal ini memberikan efisiensi penggunaan IP publik dan mendukung skalabilitas jaringan. Selain itu, DHCP Server juga berhasil diatur untuk membagikan alamat IP secara dinamis dalam rentang 192.168.10.2 hingga 192.168.10.254, dengan DNS

diarahkan ke 8.8.8.8, sehingga perangkat klien dapat langsung terhubung ke jaringan tanpa konfigurasi manual.
Pengujian firewall menunjukkan bahwa filter rule yang diterapkan bekerja sesuai fungsi. Ketika aturan untuk memblokir protokol ICMP diaktifkan, perangkat dalam jaringan tidak dapat melakukan ping ke luar dan menghasilkan respon RTO (Request Timed Out), membuktikan bahwa firewall mampu menyaring jenis lalu lintas tertentu. Selain itu, aturan pemblokiran akses ke situs berbasis HTTP dan HTTPS juga berhasil dijalankan, yang terlihat dari kegagalan mengakses situs seperti Speedtest saat firewall aktif, namun kembali normal ketika firewall dinonaktifkan.
Praktikum ini juga mencakup penggunaan bridge pada router untuk menghubungkan dua interface, memungkinkan lalu lintas data mengalir secara langsung tanpa penghalang. Secara keseluruhan, konfigurasi NAT dan Firewall berhasil menunjukkan fungsinya dalam mengelola akses jaringan dan meningkatkan keamanan. NAT berperan penting dalam koneksi keluar dari jaringan lokal, sementara firewall dapat digunakan untuk mengontrol jenis akses dan melindungi jaringan dari lalu lintas yang tidak diinginkan.

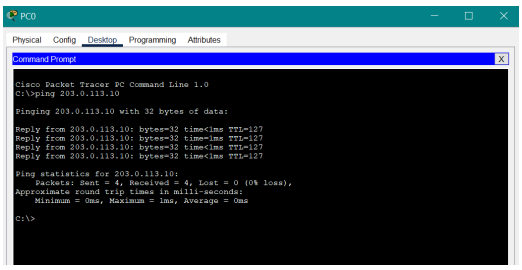
3 Hasil Tugas Modul

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

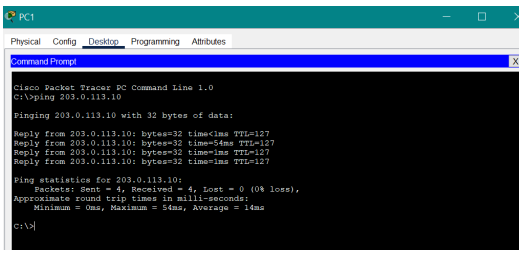


Gambar 9: Topologi

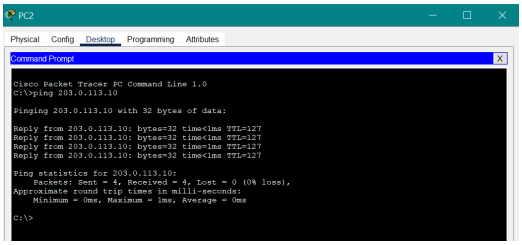
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.



Gambar 10: Uji ping PC0



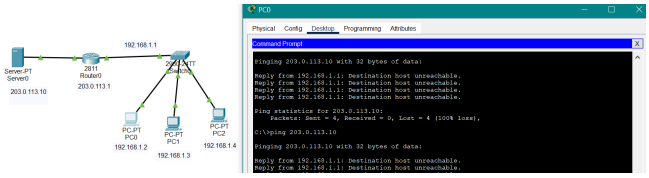
Gambar 11: Uji ping PC1



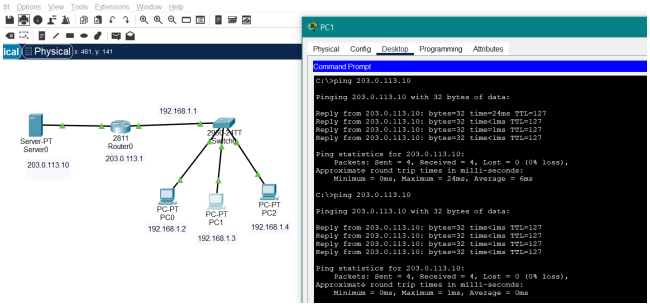
Gambar 12: uji ping PC2

3. Konfigurasi Firewall (ACL):

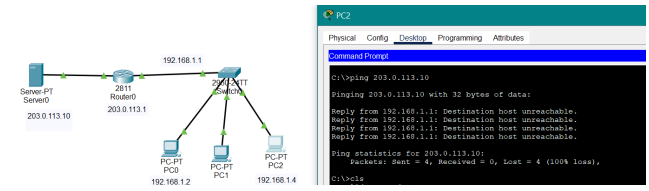
- Izinkan hanya PC1 yang dapat mengakses Server.
- Blokir PC1 dan PC3 dari mengakses Server.
- Semua PC harus tetap bisa saling terhubung di LAN.



Gambar 13: Uji ping PC0



Gambar 14: Uji ping PC1



Gambar 15: Uji ping PC2

4 Kesimpulan

Dari praktikum yang telah dilakukan, dapat disimpulkan bahwa konfigurasi NAT dan Firewall pada router berperan penting dalam pengelolaan dan pengamanan jaringan. NAT memungkinkan perangkat di jaringan lokal untuk terhubung ke internet menggunakan satu alamat IP publik secara efisien, sementara Firewall dapat mengatur dan membatasi lalu lintas data berdasarkan aturan tertentu, seperti pemblokiran protokol ICMP atau akses ke situs tertentu. Kedua konfigurasi ini berjalan dengan baik dan sesuai dengan tujuan, serta memberikan gambaran nyata tentang bagaimana administrator jaringan dapat mengontrol akses dan menjaga keamanan jaringan secara efektif.

5 Lampiran

5.1 Dokumentasi saat praktikum