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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Joycelyn Emmanuella Passandaran - 5024231001

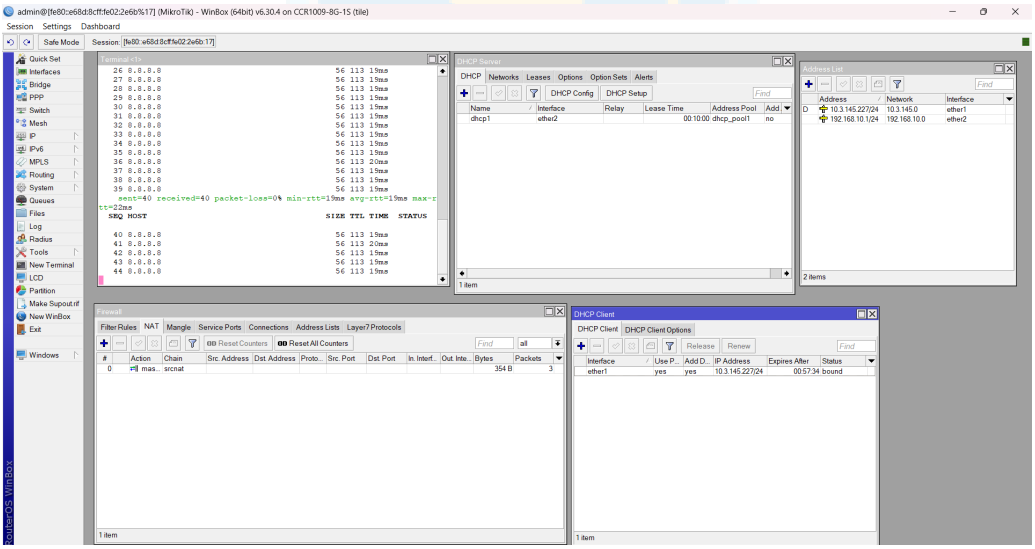
2025

1 Langkah-Langkah Percobaan

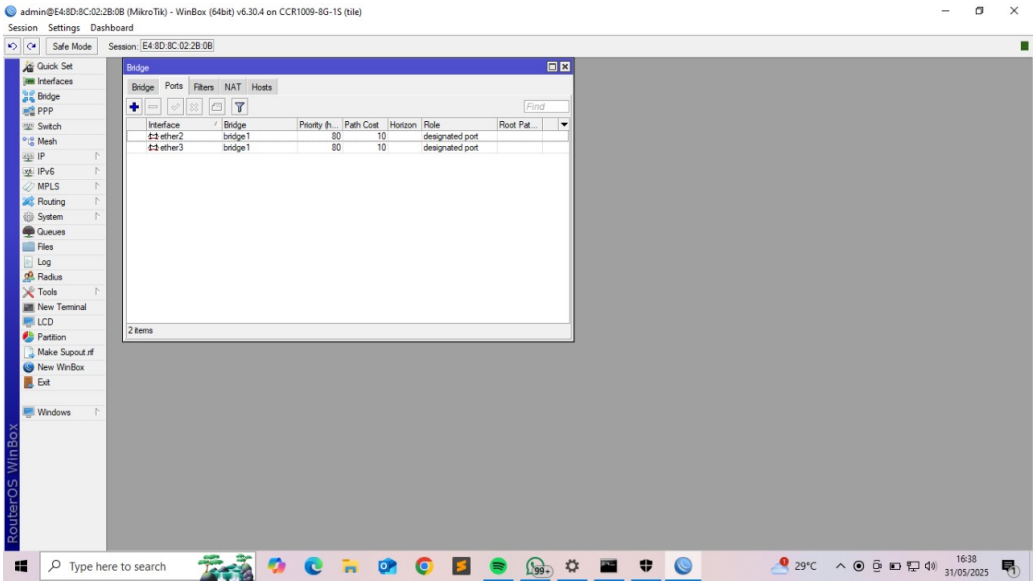
Pada modul P4, praktikum diawali dengan proses reset pada perangkat Router A dan Router B guna memastikan konfigurasi sebelumnya telah dihapus. Tahapan berikutnya adalah penambahan alamat IP pada ether7 Router A untuk koneksi ke switch. Melalui IP -> Addresses, ditambahkan IP address 192.168.10.1/24 pada interface ether7. Setelah itu, konfigurasi DHCP Server dilakukan untuk mendistribusikan IP kepada perangkat klien. Dengan menggunakan menu IP -> DHCP Server lalu memilih DHCP Setup, dipilih interface ether7 dan ditentukan parameter seperti address space (192.168.10.0/24), gateway (192.168.10.1), rentang IP (192.168.10.2–192.168.10.254), serta DNS (otomatis menggunakan 8.8.8.8 dan 8.8.4.4). Setelah DHCP berhasil disiapkan, konfigurasi NAT (Network Address Translation) dilakukan melalui IP > Firewall > NAT. Tambahan rule dilakukan dengan mengatur chain ke src-nat dan action ke masquerade. Untuk memastikan koneksi internet aktif, dilakukan pengujian ping ke 8.8.8.8 melalui terminal Winbox.

Konfigurasi Firewall dilanjutkan dengan dua jenis aturan. Pertama, untuk memblokir ICMP (ping) dari perangkat yang terhubung ke ether7, rule dibuat dengan chain: forward, protocol: icmp, dan in-interface: ether7, dengan action drop. Kedua, untuk pemblokiran akses konten tertentu, dibuat rule dengan protocol: tcp, dst-port: 80,443, serta content: speedtest, dan action diatur ke drop. Pada Router B, dilakukan konfigurasi bridge untuk mengubah fungsinya menjadi hub. Melalui menu Bridge, dibuat bridge baru dan ditambahkan interface yang terhubung ke laptop dan Router A ke dalam bridge melalui tab Port.

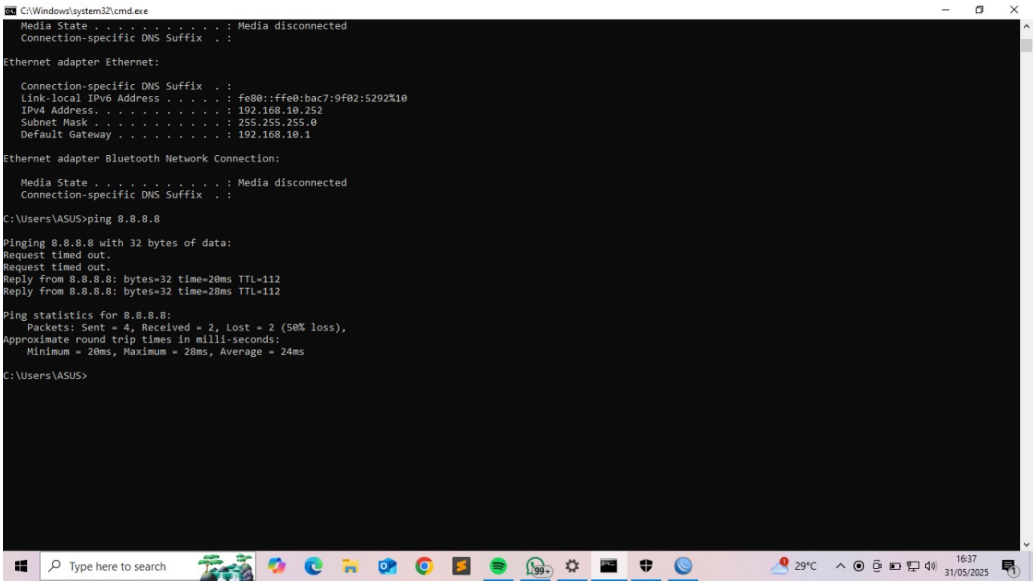
Laptop yang terhubung ke ether7 Router A dikonfigurasi agar memperoleh IP secara otomatis (DHCP). Setelah mendapatkan alamat IP, dilakukan pengujian konektivitas melalui ping ke 8.8.8.8. Saat firewall ICMP aktif, hasil ping menunjukkan Request Timed Out (RTO). Setelah rule dinonaktifkan, ping berhasil dilakukan. Pengujian pemblokiran konten dilakukan dengan mencoba mengakses situs speedtest.net. Saat rule aktif, situs tidak dapat diakses. Setelah firewall dinonaktifkan, situs berhasil dibuka.



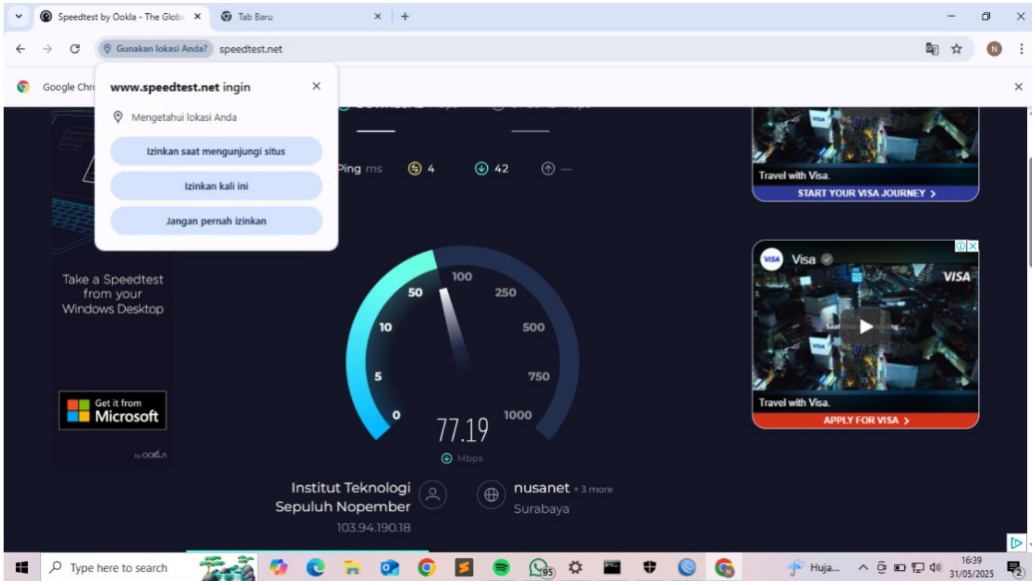
Gambar 1: Konfigurasi Laptop A



Gambar 2: Konfigurasi Laptop B



Gambar 3: Hasil Ping 8.8.8



Gambar 4: Hasil Uji Speedtest

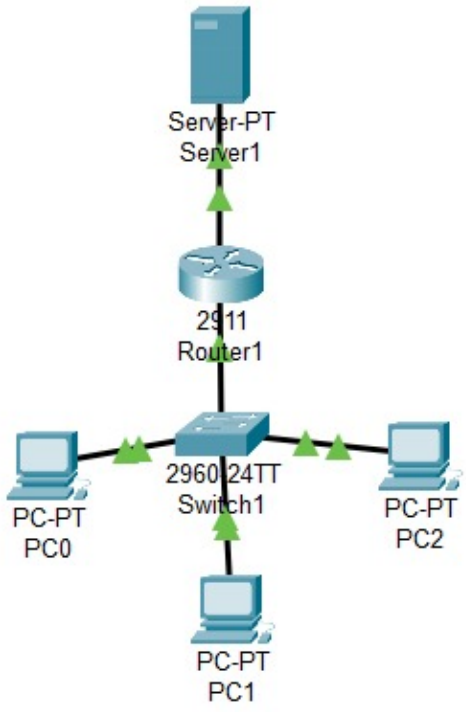
2 Analisis Percobaan

Dari hasil praktikum, konfigurasi firewall dan NAT pada Router MikroTik berjalan dengan baik sesuai dengan tujuan yang diinginkan. DHCP Client pada ether1 berhasil mendapatkan alamat IP dari internet, sedangkan DHCP Server pada ether7 dapat memberikan IP address secara otomatis kepada perangkat klien yang terhubung ke switch. Hal ini membuktikan konfigurasi DHCP berjalan dengan lancar dan efektif. Konfigurasi NAT dengan aturan masquerade berhasil mendapatkan konektivitas internet kepada perangkat di jaringan lokal. Pengujian ping ke alamat 8.8.8.8 pada terminal Winbox menunjukkan respon yang baik, menandakan koneksi internet aktif dan NAT bekerja. Pada konfigurasi firewall, aturan untuk memblokir ICMP berhasil dilakukan, di mana saat firewall aktif, perangkat tidak dapat melakukan ping ke luar jaringan sehingga memperlihatkan fungsi filter yang berjalan efektif. Ketika aturan firewall ICMP dinonaktifkan, konektivitas kembali normal dan ping dapat dilakukan. Pengujian pemblokiran konten dilakukan dengan mencoba mengakses situs speedtest.net. Saat rule aktif, situs tidak dapat diakses. Setelah firewall dinonaktifkan, situs berhasil dibuka.

Namun, terdapat beberapa kendala dalam pendokumentasian praktikum, khususnya pada bagian pengujian akses situs speedtest.net yang kurang terdokumentasi secara rinci. Walaupun demikian, secara keseluruhan seluruh tahapan konfigurasi firewall dan NAT berjalan dengan baik dan sesuai prosedur, dan hasil pengujian sesuai dengan keberhasilan praktikum.

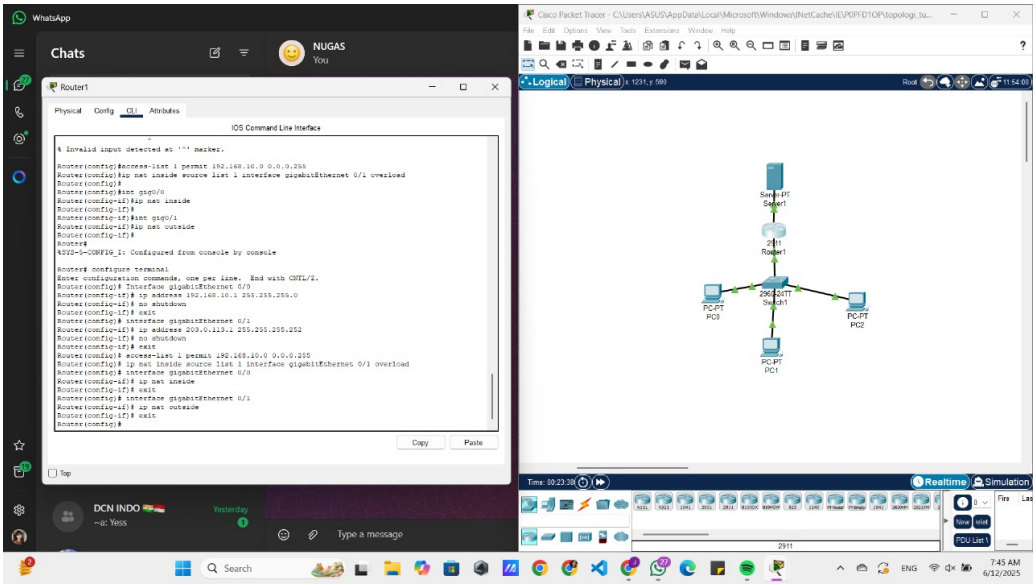
3 Hasil Tugas Modul

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



Gambar 5: Topologi sederhana dengan router, switch, pc (LAN), dan server

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



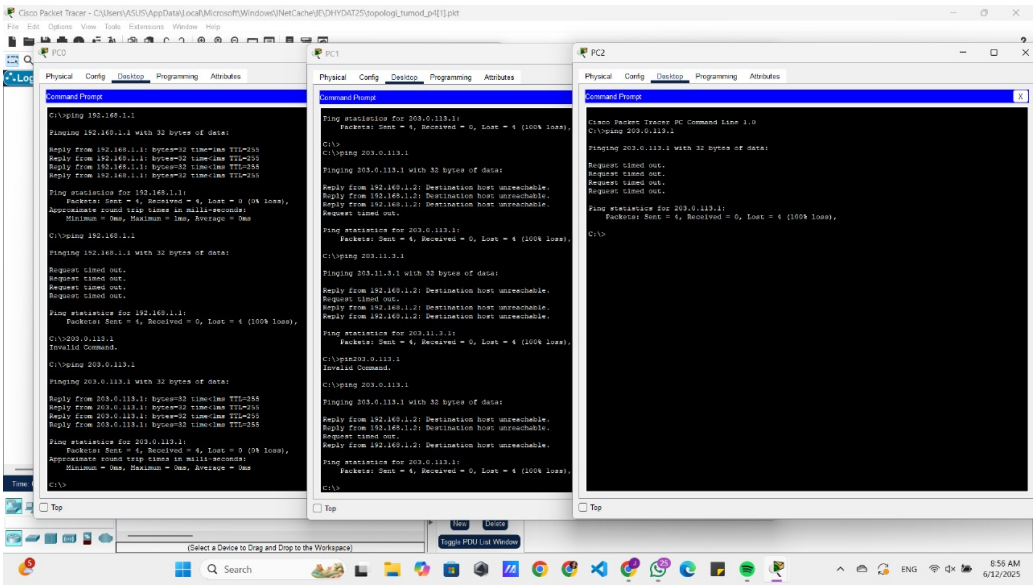
Gambar 6: Konfigurasi NAT

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.

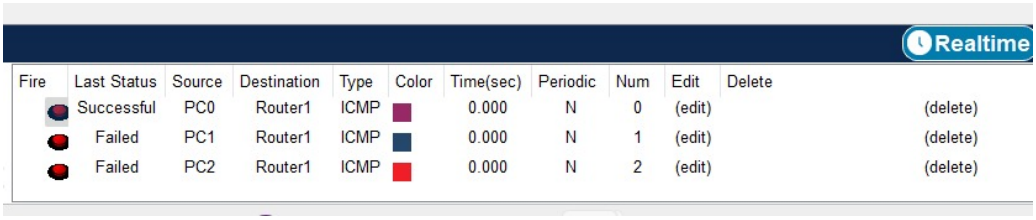
```
% Invalid input detected at     marker.

Router(config)# access-list 100 permit ip host 192.168.10.3 host 203.0.113.2
Router(config)# access-list 100 deny ip 192.168.10.0 0.0.0.255 host 203.0.113.2
Router(config)# access-list 100 permit ip any any
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip access-group 100 out
Router(config-if)# exit
Router(config)#
```

Copy

Gambar 7: Konfigurasi Firewall



Gambar 8: Hasil Ping setiap PC ke router

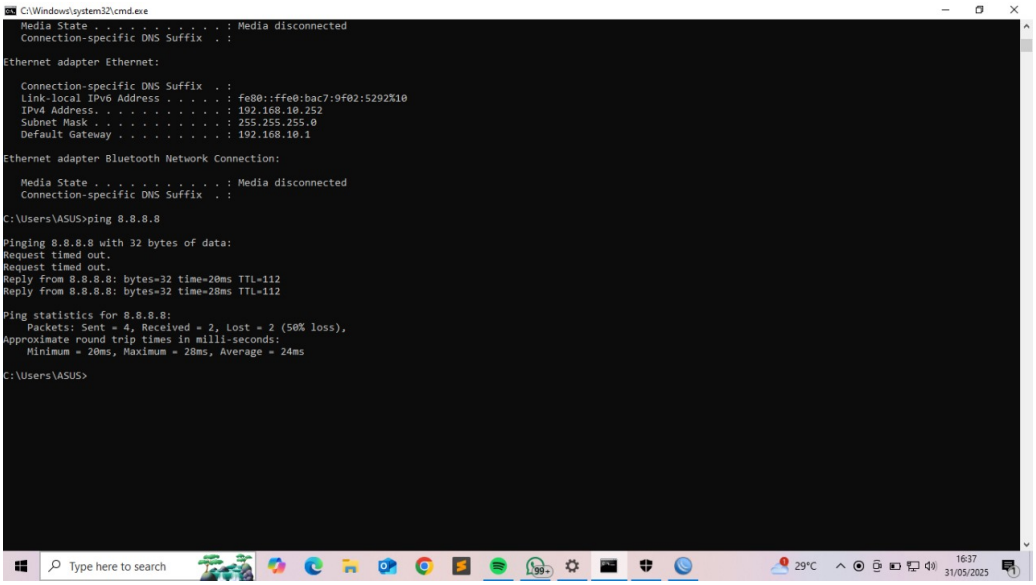


Gambar 9: Ping PC 0,1, dan 2

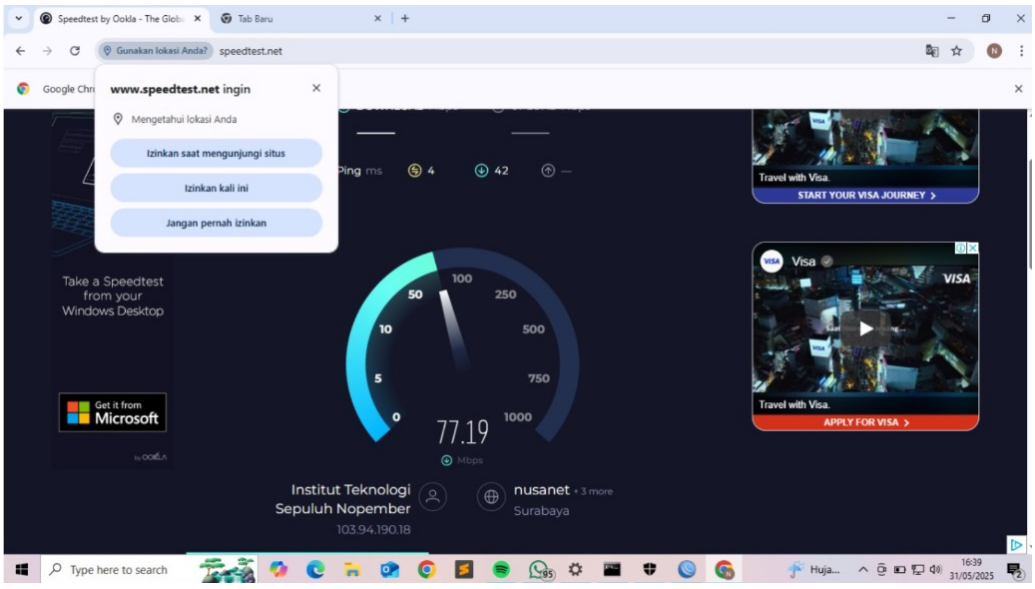
4 Kesimpulan

Berdasarkan praktikum yang telah dilakukan pada modul P4 mengenai Firewall dan NAT, dapat disimpulkan bahwa seluruh proses konfigurasi berjalan dengan baik dan sesuai tujuan. DHCP Server pada interface ether7 berhasil mendistribusikan IP address secara otomatis kepada perangkat klien, sedangkan NAT dengan metode masquerade memungkinkan perangkat lokal untuk mengakses internet melalui IP publik. Konfigurasi firewall juga berhasil diterapkan untuk membatasi akses jaringan. Aturan untuk memblokir ICMP (ping) bekerja sebagaimana mestinya, di mana perangkat tidak dapat melakukan ping saat rule diaktifkan, dan kembali normal saat rule dinonaktifkan. Secara keseluruhan, praktikum ini dapat memberikan pemahaman tentang peran penting NAT dalam konektivitas internet dan firewall dalam pengamanan jaringan. Meskipun terdapat beberapa kendala, hasil konfigurasi menunjukkan bahwa sistem berjalan sesuai prosedur.

5 Lampiran



Gambar 10: Hasil Ping 8.8.8.8 Saat Praktikum



Gambar 11: Hasil Uji Speedtest Saat Praktikum