



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

# **Laporan Akhir Praktikum Jaringan Komputer**

## **Modul Firewall dan NAT**

Alfito Ichsan Galaksi - 5024231071

2025

# 1 Langkah-Langkah Percobaan

## 1.1 1. Reset Router

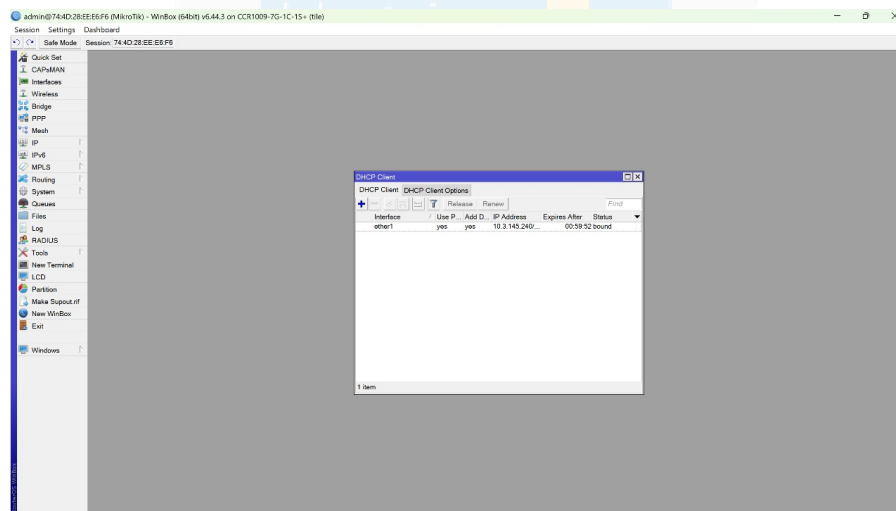
1. Akses router menggunakan aplikasi Winbox.
2. Masuk ke menu **System > Reset Configuration**.
3. Centang opsi *No Default Configuration*.
4. Klik *Reset Configuration*.

## 1.2 2. Login ke Router

- Gunakan Winbox, login menggunakan MAC address atau IP default.
- Username: admin, password dikosongkan jika belum diatur.

## 1.3 3. Konfigurasi DHCP Client pada Router A (ether1)

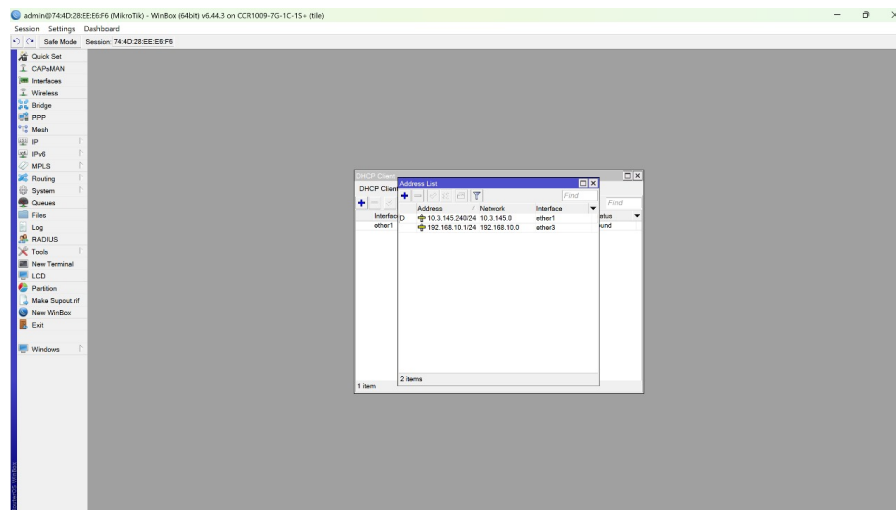
- Masuk ke **IP > DHCP Client**, klik +.
- Pilih interface: ether1, lalu klik *Apply* hingga status menjadi bound.



Gambar 1: Konfigurasi DHCP Client

## 1.4 4. Penambahan IP pada Ether3

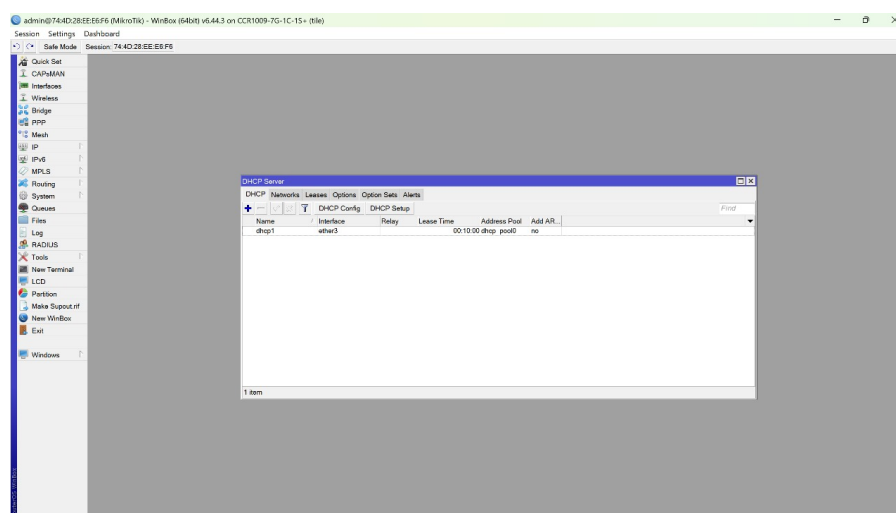
- Masuk ke **IP > Addresses**, klik +.
- Address: 192.168.10.1/24, Interface: ether3.



**Gambar 2:** Penambahan IP pada Ether3

## 1.5 5. Konfigurasi DHCP Server

- Masuk ke **IP > DHCP Server**, klik DHCP Setup.
- Pilih interface: ether3.
- DHCP Address Space: 192.168.10.0/24.
- Gateway: 192.168.10.1.
- IP Range: 192.168.10.2-192.168.10.254.
- DNS: 8.8.8.8, 8.8.4.4.
- Lease Time: 00:10:00.

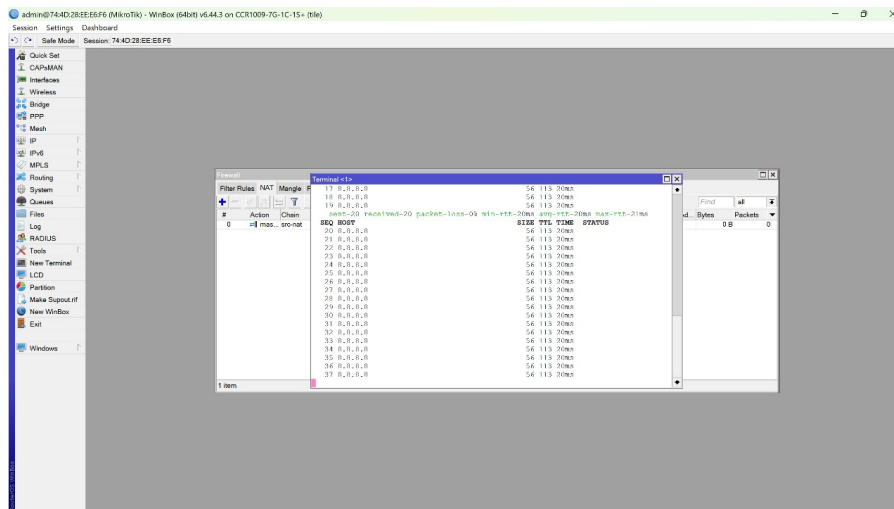


**Gambar 3:** Konfigurasi DHCP Server

## 1.6 6. Konfigurasi NAT

- Masuk ke **IP > Firewall > NAT**, klik +.
- **General:** Chain = src-nat.

- **Action:** masquerade.
- Lakukan uji coba konektivitas menggunakan ping 8.8.8.8.

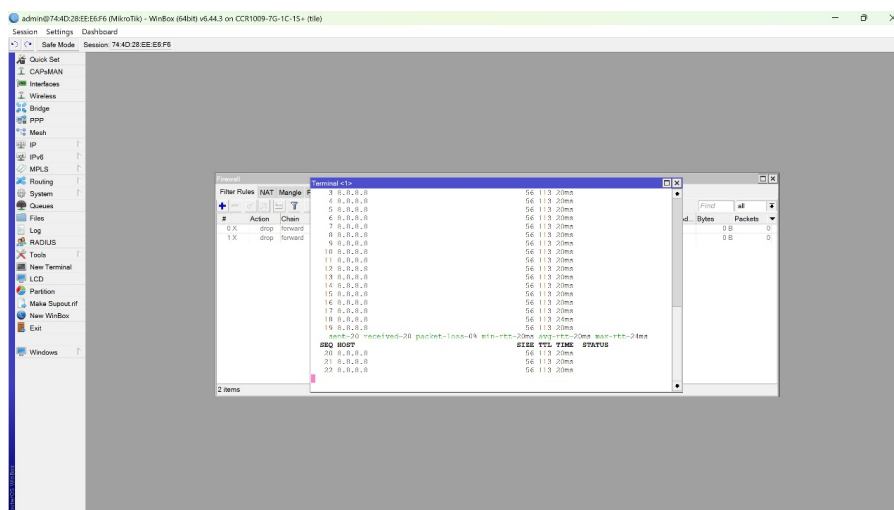


**Gambar 4:** Konfigurasi NAT dengan Masquerade

## 1.7 7. Konfigurasi Firewall

### 1.7.1 Blokir ICMP

- Chain: forward, Protocol: icmp, In.Interface: ether3.
- Action: drop.



**Gambar 5:** Firewall Rule untuk Blokir ICMP

### 1.7.2 Blokir Konten Web Tertentu

- Chain: forward, Protocol: tcp, Dst.Port: 80,443.
- In.Interface: ether7, Out.Interface: ether1.
- Advanced > Content: speedtest, Action: drop.



```

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e2cd:fab6:3efd:f768%14
    IPv4 Address. . . . . : 192.168.10.254
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 2001:db8:a::1
                                192.168.10.1

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 8:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : its.ac.id
    Link-local IPv6 Address . . . . . : fe80::f23e:3720:629a:1508%5
    IPv4 Address. . . . . : 10.125.149.248
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 10.125.128.1

C:\Users\Atria>

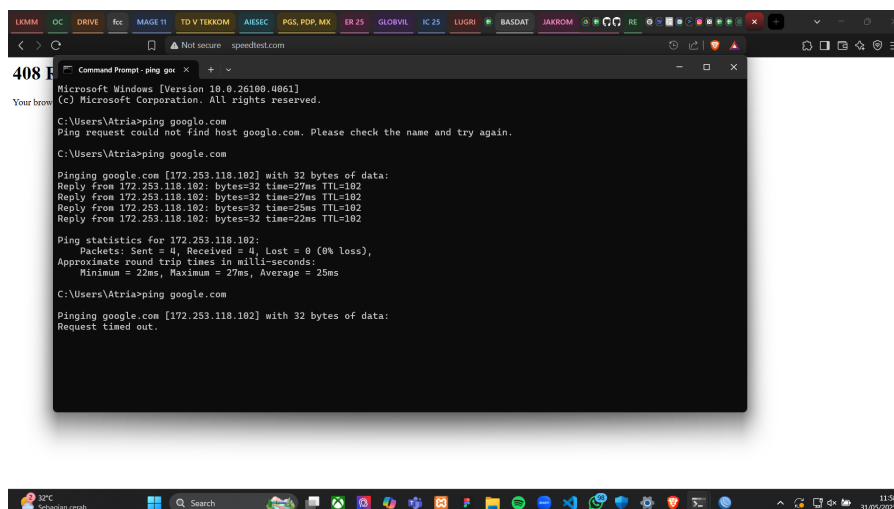
```

Gambar 8: Pengujian IP Laptop

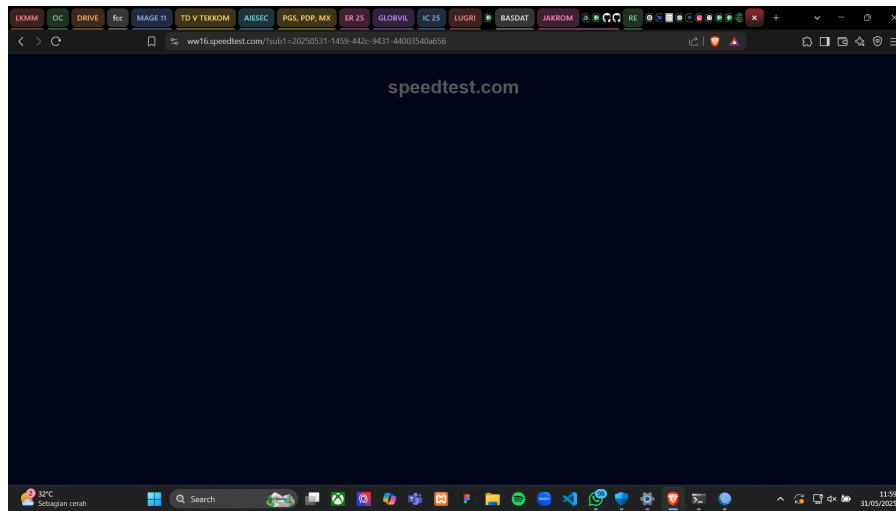
## 1.10 10. Uji Coba Konfigurasi

### 1.10.1 Pengujian Konektivitas ICMP

- Lakukan ping 8.8.8.8 dari laptop.
- Jika firewall aktif, hasil: Request Timed Out.
- Nonaktifkan aturan firewall untuk menguji perubahan.



Gambar 9: Uji Ping firewall aktif ke Internet dari Laptop



**Gambar 10:** Test Internet dari Laptop

## 2 Analisis Hasil Percobaan

Selama percobaan konfigurasi firewall, NAT, dan connection tracking menggunakan dua router Mikrotik dan dua laptop, seluruh langkah dilakukan secara bertahap berdasarkan prosedur yang telah ditentukan. Laptop 1 digunakan untuk melakukan konfigurasi awal dari langkah 1 hingga langkah 7, yang mencakup pengaturan IP Address, pembuatan aturan NAT, serta konfigurasi mangle dan firewall. Selanjutnya, Laptop 2 digunakan untuk menyelesaikan langkah 8 dan 9, yaitu pengujian konektivitas dan koneksi internet dari sisi client.

Secara umum, semua konfigurasi dapat diterapkan dengan baik dan sesuai dengan skenario yang diharapkan. Router A dan Router B berhasil terhubung, dan pengujian menunjukkan bahwa fitur-fitur seperti NAT dan connection tracking dapat berfungsi sebagaimana mestinya. Namun, selama proses percobaan terdapat kendala pada Laptop 2, di mana koneksi ethernet dari jaringan WiFi ITS ke Laptop 2 tidak selalu stabil. Koneksi tersebut kadang tersambung dan kadang tidak, sehingga menyebabkan proses pengujian sedikit tertunda. Setelah dilakukan beberapa upaya seperti pengecekan kabel, pengaturan ulang IP, dan restart koneksi, akhirnya koneksi berhasil stabil dan pengujian dapat dilanjutkan. Kendala tersebut menunjukkan pentingnya kesiapan perangkat keras dan konektivitas saat melakukan konfigurasi jaringan. Secara keseluruhan, percobaan berhasil diselesaikan dengan baik dan semua fitur berjalan sesuai tujuan.

## 3 Kesimpulan

Berdasarkan percobaan yang telah dilakukan, seluruh konfigurasi jaringan yang melibatkan dua router Mikrotik dan dua laptop berhasil dilakukan dengan baik. Seluruh langkah konfigurasi dari tahap penetapan IP, pengaturan NAT, hingga penerapan firewall mangle dan pengujian koneksi berjalan lancar.

Namun, selama pelaksanaan terdapat kendala teknis, khususnya pada saat menyambungkan koneksi ethernet ke Laptop 2 yang terhubung melalui jaringan WiFi kampus (ITS). Koneksi tersebut sempat tidak stabil dan sulit tersambung, yang menyebabkan keterlambatan dalam pengujian. Setelah beberapa kali percobaan dan penyesuaian, koneksi berhasil stabil dan semua pengujian dapat diselesaikan dengan baik.

Percobaan ini memberikan pemahaman praktis mengenai implementasi firewall, NAT, dan connection tracking pada perangkat Mikrotik serta pentingnya kesiapan perangkat keras (hardware) dan jaringan dalam mendukung proses konfigurasi jaringan.