



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

Laporan Akhir Praktikum Jaringan Komputer

Firewall & NAT

Atria Caesariano Tinto - 5024231068

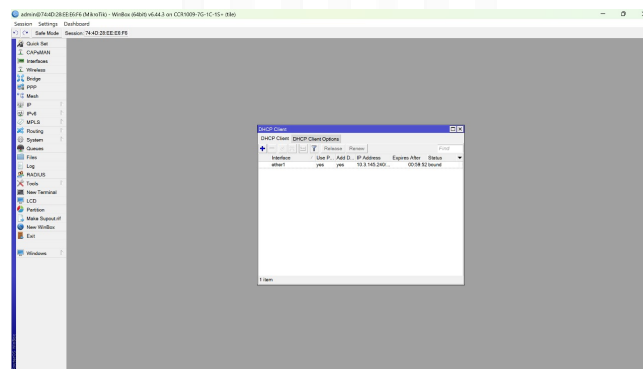
2025

1 Langkah-Langkah Percobaan

Konfigurasi Jaringan Router A dan Router B

Konfigurasi Router A (Sebagai Gateway dan DHCP Server)

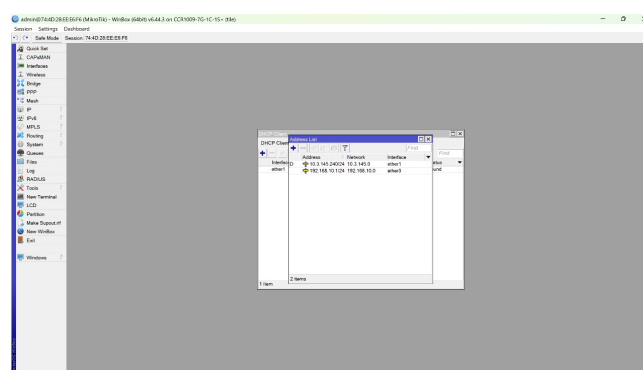
1. **Reset Router:** Gunakan Winbox, masuk ke *System* → *Reset Configuration*, centang *No Default Configuration*, lalu klik *Reset Configuration*.
2. **Login ke Router:** Gunakan Winbox via MAC Address atau IP default dengan username *admin* (tanpa password jika belum disetel).
3. **Konfigurasi DHCP Client (ether1):**
 - Menu IP → DHCP Client.
 - Tambahkan DHCP Client pada interface *ether1*.
 - Klik *Apply* dan pastikan status berubah menjadi *bound*.



Gambar 1: Konfigurasi DHCP Client

4. Penambahan Alamat IP (ether7):

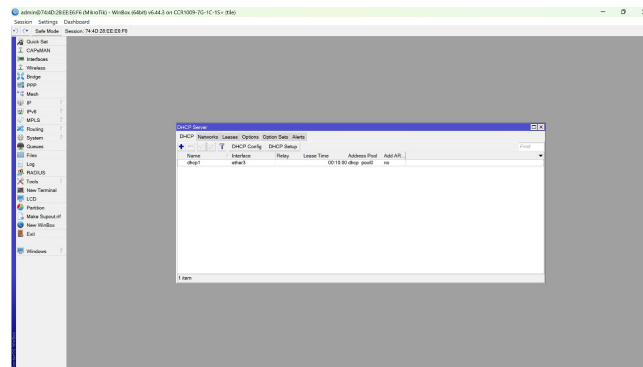
- Menu IP → Addresses.
- Tambahkan IP 192.168.10.1/24 pada interface *ether7*.



Gambar 2: Penambahan IP Address

5. Konfigurasi DHCP Server (ether7):

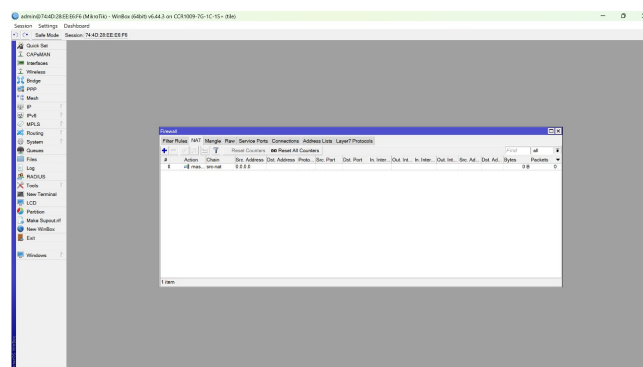
- Menu IP → DHCP Server, klik DHCP Setup.
- Interface: ether7, Address Space: 192.168.10.0/24, Gateway: 192.168.10.1, Address Pool: 192.168.10.2-192.168.10.254, DNS: otomatis, Lease Time: 00:10:00.



Gambar 3: Konfigurasi DHCP Server

6. Konfigurasi NAT:

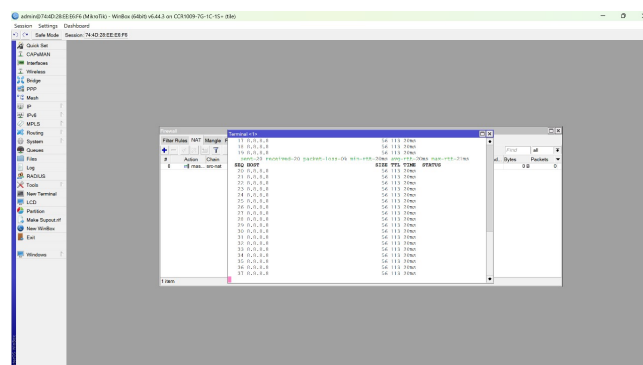
- Menu IP → Firewall → NAT, klik +.
- Tab *General*: Chain = src-nat, Tab *Action*: Action = masquerade.



Gambar 4: Konfigurasi NAT

7. Pengujian Internet:

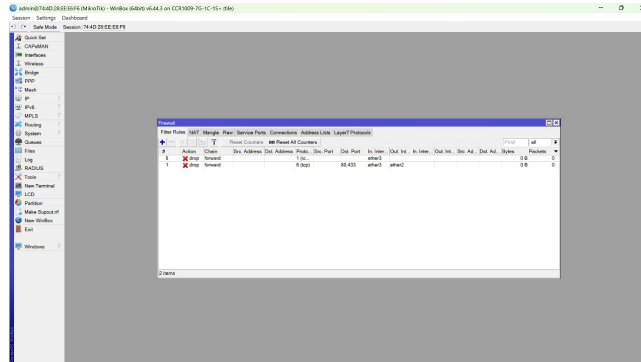
- Buka Terminal Winbox, jalankan perintah ping 8.8.8.8.



Gambar 5: Test Ping

8. Konfigurasi Firewall:

- *Blokir ICMP*: IP → Firewall → Filter Rules, tambahkan rule: Chain = forward, Protocol = icmp, In. Interface = ether7, Action = drop.
- *Blokir Akses Situs (Content Filtering)*: Chain = forward, Protocol = tcp, Dst. Port = 80, 443, In. Interface = ether7, Out. Interface = ether1, Content = speedtest, Action = drop.

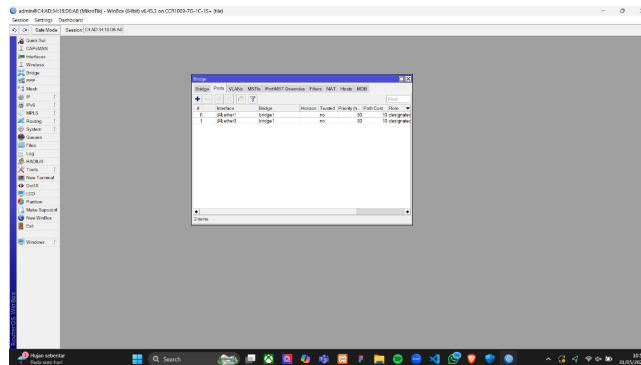


Gambar 6: Konfigurasi Firewall

Konfigurasi Router B (Sebagai Bridge)

1. Konfigurasi Bridge:

- Menu Bridge → klik + untuk membuat bridge baru, klik Apply dan OK.
- Tambahkan port ke dalam bridge melalui tab Port, masukkan interface yang terhubung ke laptop dan ke Router A.



Gambar 7: Konfigurasi Bridge

Konfigurasi Laptop

1. Pastikan pengaturan IP di laptop menggunakan **DHCP (Automatic)**.
2. Buka Command Prompt dan ketik ipconfig untuk mengecek apakah IP yang diterima berada di rentang DHCP (misal: 192.168.10.x).

```

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>

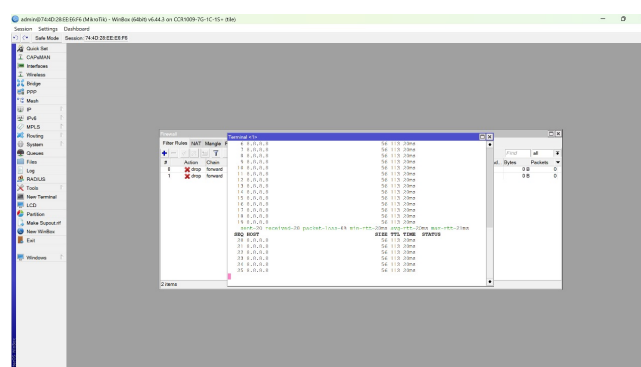
```

Gambar 8: Konfigurasi IP Laptop

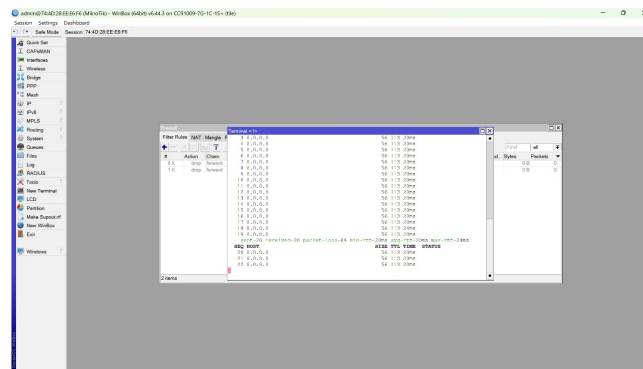
Uji Coba Konfigurasi

1. Pengujian ICMP:

- Lakukan ping 8.8.8.8 dari laptop.
- Ketika firewall ICMP aktif, hasilnya seharusnya Request Timed Out.
- Disable rule firewall ICMP (klik X pada rule) dan lakukan ping kembali, hasilnya seharusnya Reply from 8.8.8.8.



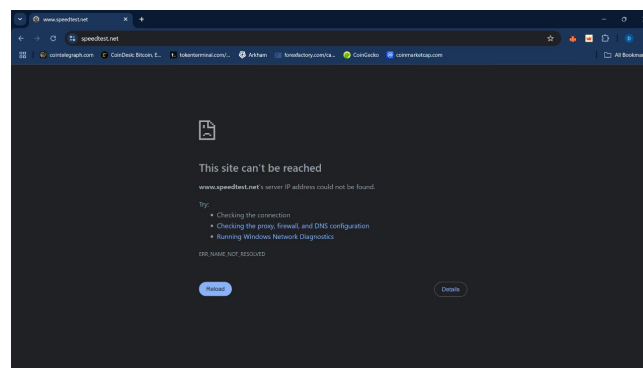
Gambar 9: Firewall Hidup



Gambar 10: Firewall Mati

2. Pengujian Pemblokiran Situs:

- Akses situs seperti `www.speedtest.net`.
- Saat firewall aktif, halaman tidak akan tampil sempurna atau gagal dimuat.
- Nonaktifkan rule firewall konten, lalu akses ulang halaman untuk memastikan firewall tidak lagi menghalangi.



Gambar 11: Test Akses Situs

2 Analisis Hasil Percobaan

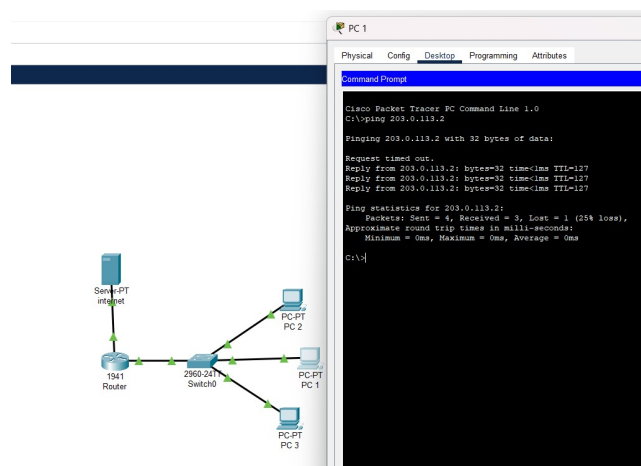
Berdasarkan hasil percobaan yang dilakukan, seluruh konfigurasi pada Router MikroTik seperti DHCP Client, DHCP Server, NAT, dan Firewall berhasil dilakukan dengan baik. Dengan laptop yang mampu mendapat alamat IP secara otomatis melalui DHCP Server yang dikonfigurasi pada ether7 Router A. Selain itu, ketika NAT diaktifkan, perangkat dapat mengakses internet, serta aturan firewall yang dibuat juga berjalan dengan baik. Ketika aturan pemblokiran ICMP aktif, perangkat tidak dapat melakukan ping ke internet dan menghasilkan Request Timed Out, sedangkan ketika aturan tersebut dinonaktifkan, koneksi kembali normal. Begitu pula dengan firewall untuk pemblokiran konten berbasis kata kunci, yang berhasil mencegah akses ke situs saat diaktifkan, dan akses kembali normal ketika dinonaktifkan.

Namun, selama percobaan berlangsung, terdapat kendala berupa koneksi Ethernet dari jaringan WiFi ITS yang digunakan untuk menghubungkan router ke internet tidak selalu stabil. Koneksi terkadang berhasil terhubung, namun di lain waktu terputus tanpa sebab yang jelas. Kondisi ini diduga disebabkan oleh ketidakstabilan jaringan WiFi ITS, konflik pengaturan jaringan, atau gangguan pada

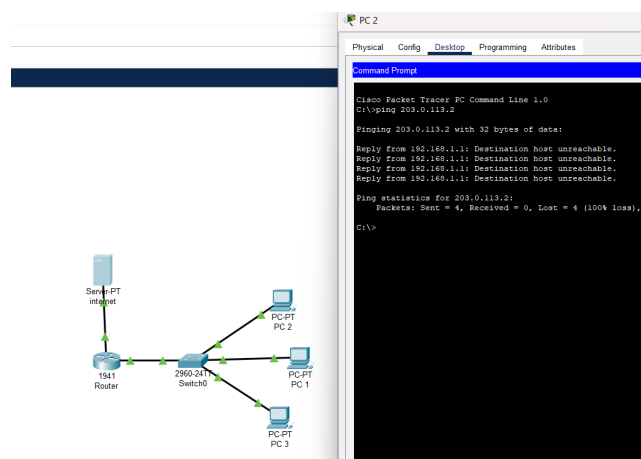
kabel. Akibatnya, router tidak selalu dapat memperoleh alamat IP secara dinamis, sehingga koneksi ke internet menjadi tidak konsisten.

3 Hasil Tugas Modul

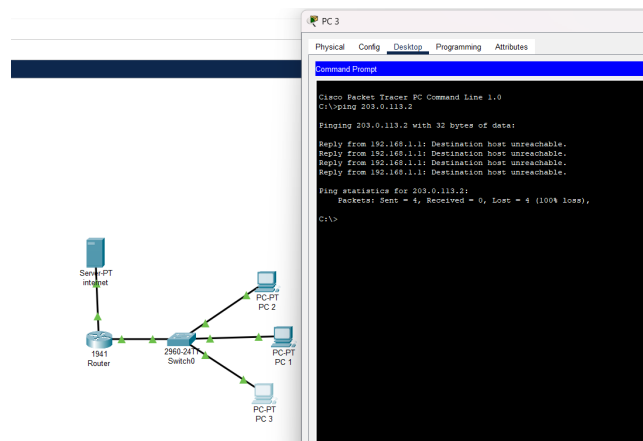
Semua PC di jaringan LAN dapat mengakses server di jaringan publik menggunakan IP publik router. Namun, melalui penerapan ACL (Access Control List) sebagai firewall, akses ke server dibatasi, hanya PC 1 yang dapat mengakses server, sementara PC2 dan PC3 diblokir. Hasil dengan 'ping' menunjukkan bahwa PC1 berhasil mencapai server (reachable), sedangkan PC 2 dan PC 3 gagal (unreachable), namun ketiga PC tetap dapat saling terhubung dalam LAN tanpa gangguan, membuktikan bahwa firewall hanya berlaku untuk akses eksternal ke server tanpa memengaruhi konektivitas internal.



Gambar 12: Ping dari PC 1



Gambar 13: Ping dari PC 2



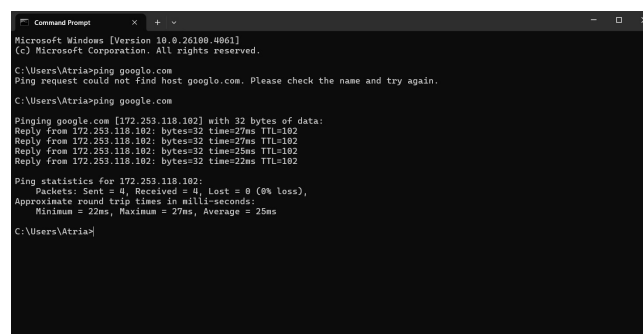
Gambar 14: Ping dari PC 3

4 Kesimpulan

Konfigurasi jaringan dasar pada Router MikroTik, meliputi DHCP Client, DHCP Server, NAT, dan Firewall, berhasil dilakukan dengan baik dan sesuai fungsinya. Perangkat klien mampu mendapatkan IP secara otomatis, mengakses internet setelah konfigurasi NAT, serta merespons aturan firewall dengan benar, baik untuk pemblokiran ICMP maupun konten tertentu. Percobaan ini menunjukkan pentingnya konfigurasi jaringan yang tepat dalam mengatur lalu lintas data dan pengamanan akses. Namun, terdapat kendala berupa koneksi Ethernet dari jaringan WiFi ITS yang tidak stabil, sehingga menyebabkan router terkadang gagal mendapatkan IP dan mengganggu akses internet.

5 Lampiran

5.1 Dokumentasi saat praktikum



Gambar 15: Test Ping Google 1


```
Command Prompt
Microsoft Windows [Version 10.0.26100.4861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Atria>ping google.com
Ping request could not find host google.com. Please check the name and try again.

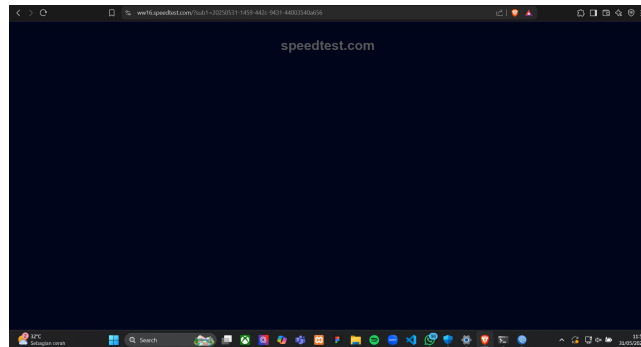
C:\Users\Atria>ping google.com

Pinging google.com [172.253.118.102] with 32 bytes of data:
Reply from 172.253.118.102: bytes=32 time=27ms TTL=102
Reply from 172.253.118.102: bytes=32 time=27ms TTL=102
Reply from 172.253.118.102: bytes=32 time=25ms TTL=102
Reply from 172.253.118.102: bytes=32 time=22ms TTL=102

Ping statistics for 172.253.118.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 27ms, Average = 25ms

C:\Users\Atria>
```

Gambar 16: Test Ping Google 2



Gambar 17: Test Speedtest