



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

Laporan Akhir Praktikum Jaringan Komputer

Firewall & NAT

I Gusti Ngurah Eka Febrian Suantara Putra - 5024231078

2025

1 Langkah-Langkah Percobaan

1. Melakukan Reset pada Router

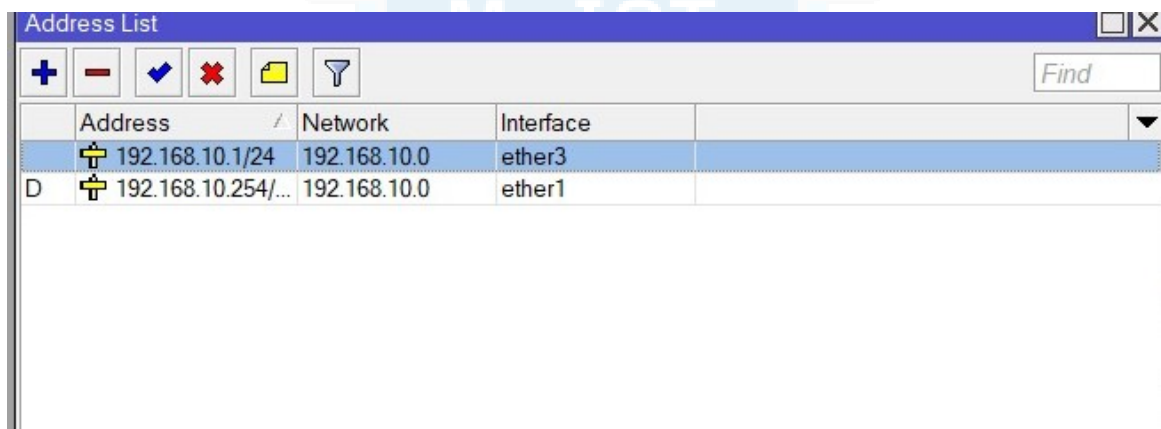
Tahapan awal dalam konfigurasi router adalah mereset perangkat agar kembali ke kondisi default pabrik. Tindakan ini bertujuan untuk menghapus konfigurasi sebelumnya yang mungkin masih tersimpan dan berpotensi menyebabkan konflik. Proses reset dilakukan melalui aplikasi Winbox, dengan membuka menu System > Reset Configuration. Kemudian centang opsi "No Default Configuration" dan klik tombol "Reset Configuration" untuk memulai proses reset ke pengaturan awal.

2. Masuk ke Antarmuka Router

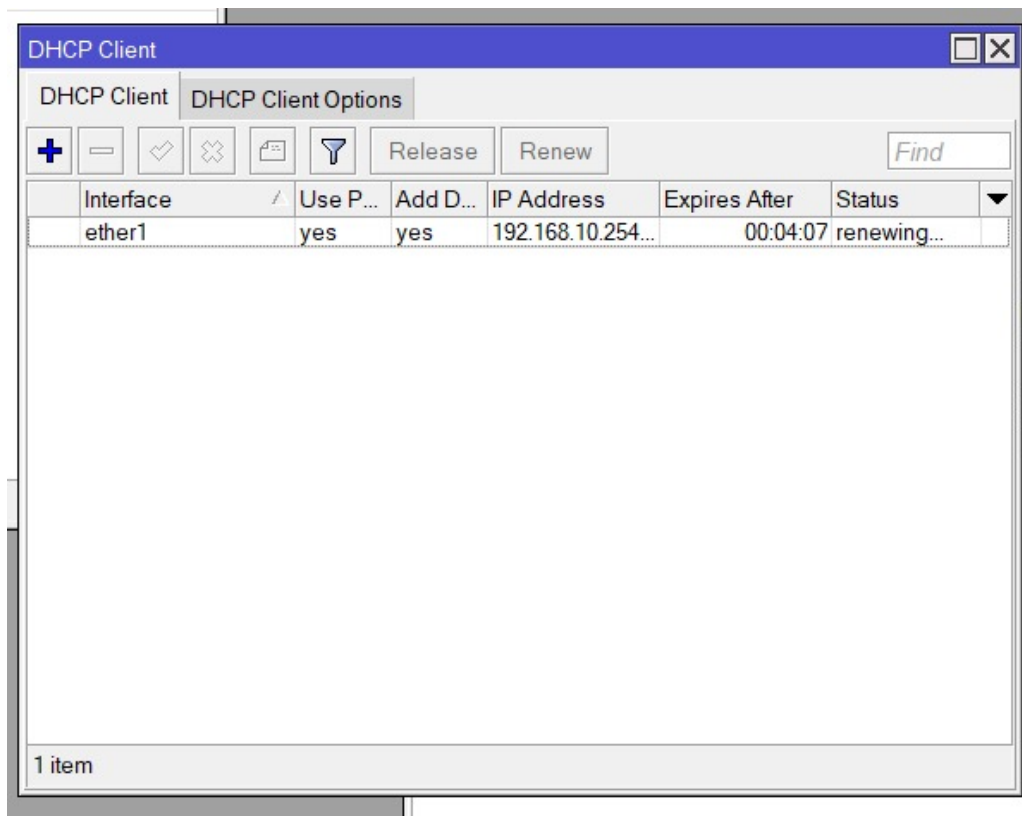
Setelah proses reset selesai, selanjutnya adalah mengakses router menggunakan aplikasi Winbox. Koneksi dapat dilakukan baik melalui MAC Address maupun IP default dari perangkat. Biasanya, login dilakukan dengan username "admin" tanpa password, kecuali jika sebelumnya sudah ditentukan kata sandi khusus.

3. Mengatur DHCP Client di Router A pada Port Ether1

Langkah selanjutnya adalah mengaktifkan DHCP Client pada ether1, yaitu port yang akan menerima koneksi dari internet. Sambungkan kabel internet ke ether1, kemudian buka menu IP > DHCP Client dan tekan ikon "+" untuk membuat entri baru. Pilih ether1 sebagai interface, klik Apply. Jika koneksi berhasil, status akan berubah menjadi "bound", menandakan router berhasil mendapatkan IP secara otomatis dari server DHCP.



	Address	Network	Interface
	192.168.10.1/24	192.168.10.0	ether3
D	192.168.10.254/...	192.168.10.0	ether1

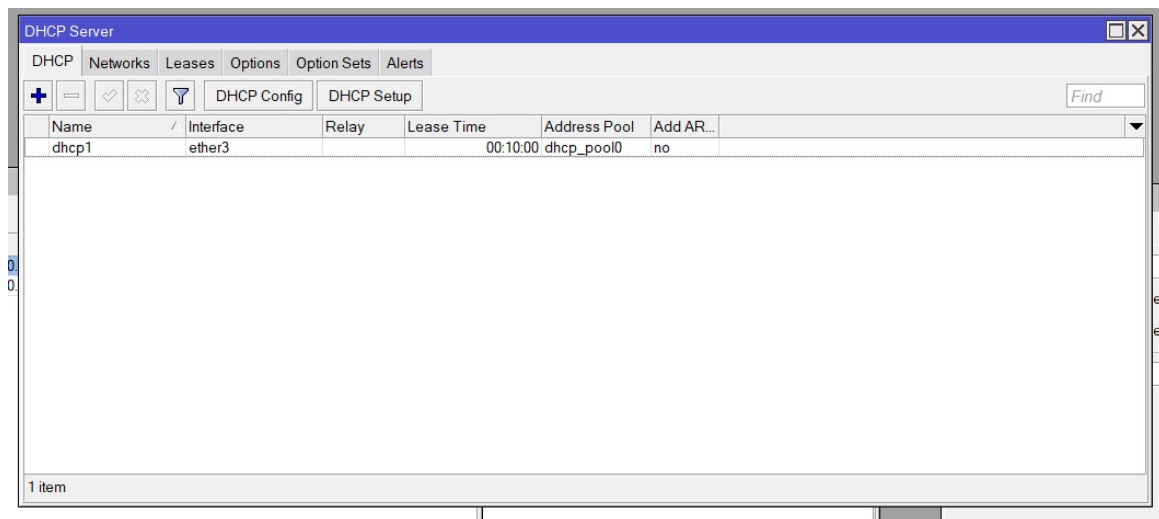


4. Menambahkan IP Address pada Ether7

Untuk menghubungkan Router A dengan perangkat lain melalui Switch, alamat IP harus ditetapkan pada port ether7. Buka menu IP > Addresses, tekan ikon "+" dan masukkan alamat IP 192.168.10.1/24. Pilih interface ether7, kemudian klik Apply dan OK untuk menyimpan perubahan.

5. Menyiapkan DHCP Server di Router MikroTik

Agar router dapat memberikan alamat IP secara otomatis ke klien, konfigurasi DHCP Server diperlukan. Buka menu IP > DHCP Server, klik tombol "DHCP Setup", lalu pilih ether7 sebagai interface DHCP. Setelah itu, tentukan parameter jaringan seperti network (192.168.10.0/24), gateway (192.168.10.1), rentang IP (192.168.10.2 hingga 192.168.10.254), dan DNS Server (misal: 8.8.8.8 dan 8.8.4.4). Atur waktu lease (misal: 10 menit) dan selesaikan proses setup.

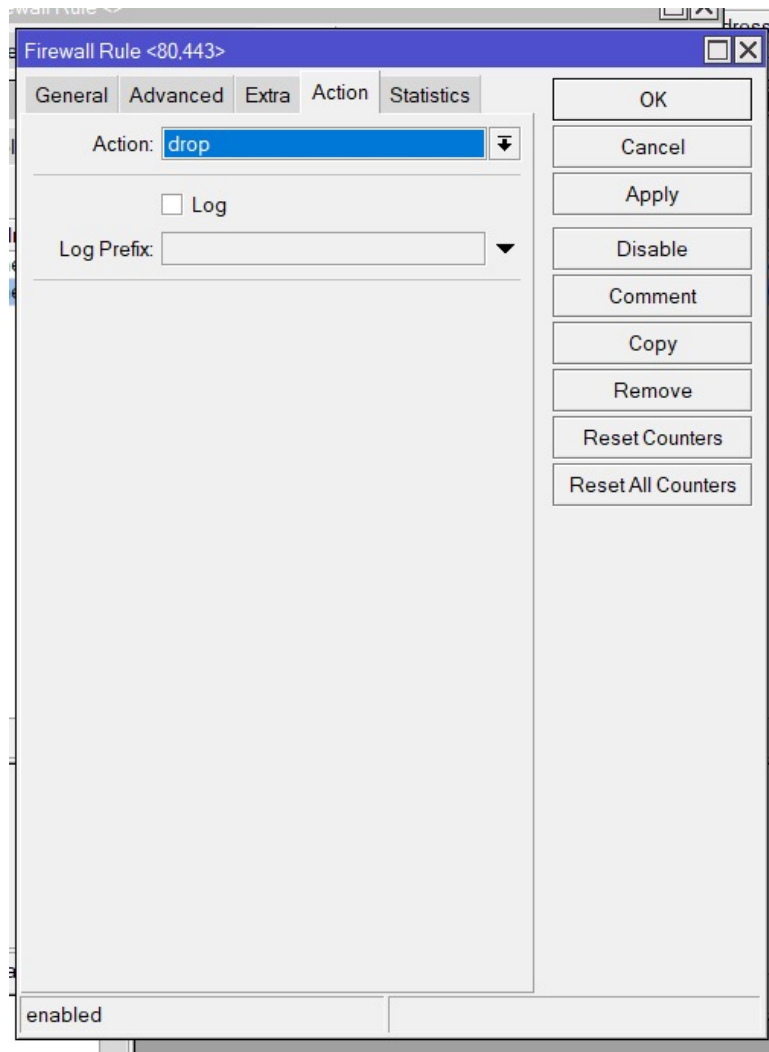


6. Mengaktifkan NAT (Network Address Translation)

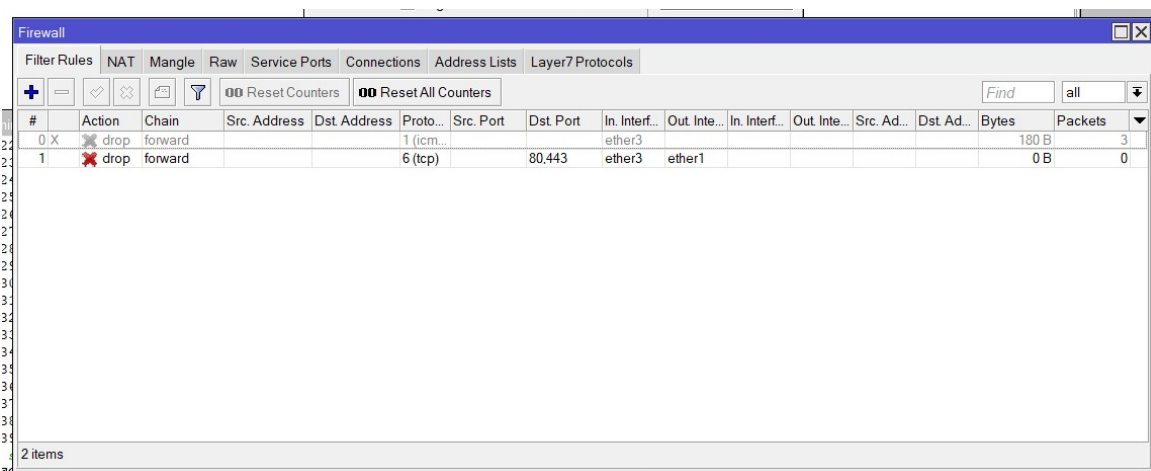
Agar perangkat yang terhubung ke router bisa mengakses internet, konfigurasi NAT diperlukan. Masuk ke menu IP > Firewall > NAT dan klik ikon "+". Pada tab "General", pilih opsi Chain: src-nat, dan pada tab "Action" pilih masquerade. Klik Apply dan OK. Untuk menguji koneksi, buka Terminal di Winbox dan jalankan 'ping 8.8.8.8', lalu perhatikan apakah ada balasan.

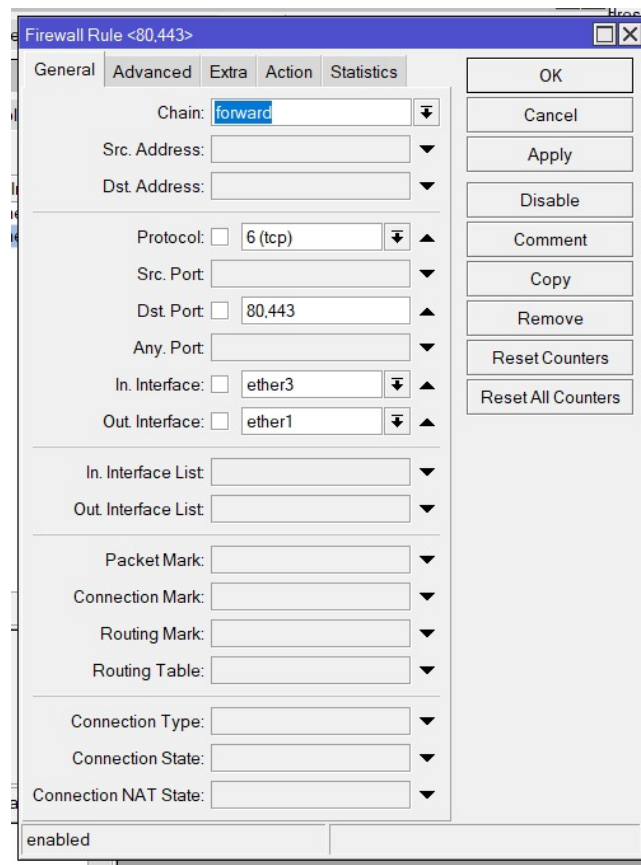
7. Pengaturan Firewall

Firewall digunakan untuk membatasi lalu lintas data tertentu. Untuk memblokir ping (ICMP), buka IP > Firewall > Filter Rules, klik ikon "+", lalu isi Chain: forward, Protocol: icmp, In. Interface: ether7, dan pada tab Action pilih drop.



Untuk menyaring akses ke situs tertentu, buat aturan baru dengan Chain: forward, Protocol: tcp, Dst. Port: 80,443, In. Interface: ether7, dan Out. Interface: ether1. Pada tab Advanced, isikan kolom Content dengan kata kunci seperti "speedtest". Lanjutkan ke tab Action dan pilih drop.





8. Membuat Bridge pada Router B

Agar Router B dapat berfungsi sebagai penghubung (hub), kita perlu membuat bridge. Buka menu Bridge dan klik ikon "+" untuk menambahkan bridge baru, lalu Apply dan OK. Setelah itu, tambahkan port yang akan dimasukkan ke dalam bridge lewat menu Bridge > Ports. Klik ikon "+" dan pilih dua interface: satu terhubung ke laptop dan satu lagi ke Router A.

9. Mengatur IP Address Otomatis di Laptop

Pastikan laptop dikonfigurasi untuk menerima IP secara otomatis dari DHCP. Buka pengaturan jaringan pada sistem operasi dan aktifkan mode DHCP. Untuk memverifikasi, jalankan 'ipconfig' pada Command Prompt dan cek apakah IP telah diterima.

10. Melakukan Pengujian Konfigurasi

Tahapan terakhir adalah pengujian keseluruhan konfigurasi. Untuk mengetes koneksi, gunakan perintah ping ke 8.8.8.8. Jika aturan firewall ICMP aktif, hasilnya akan "Request Timed Out". Setelah aturan tersebut dinonaktifkan, ulangi perintah ping dan pastikan ada balasan.

```
Terminal <2>
22 8.8.8.8          56 113 20ms
23 8.8.8.8          56 113 20ms
24 8.8.8.8          56 113 20ms
25 8.8.8.8          56 113 20ms
26 8.8.8.8          56 113 20ms
27 8.8.8.8          56 113 20ms
28 8.8.8.8          56 113 20ms
29 8.8.8.8          56 113 20ms
30 8.8.8.8          56 113 20ms
31 8.8.8.8          56 113 20ms
32 8.8.8.8          56 113 20ms
33 8.8.8.8          56 113 20ms
34 8.8.8.8          56 113 20ms
35 8.8.8.8          56 113 20ms
36 8.8.8.8          56 113 20ms
37 8.8.8.8          56 113 20ms
38 8.8.8.8          56 113 20ms
39 8.8.8.8          56 113 20ms
  sent=40 received=40 packet-loss=0% min-rtt=20ms avg-rtt=20ms max-rtt=20ms
SEQ HOST          SIZE TTL TIME  STATUS
40 8.8.8.8          56 113 20ms
  sent=41 received=41 packet-loss=0% min-rtt=20ms avg-rtt=20ms max-rtt=20ms
[admin@MikroTik] >
```

Untuk menguji pemblokiran situs, coba akses alamat seperti www.speedtest.net. Jika firewall aktif, situs tidak akan terbuka. Namun, setelah aturan firewall dinonaktifkan, akses ke situs kembali normal.

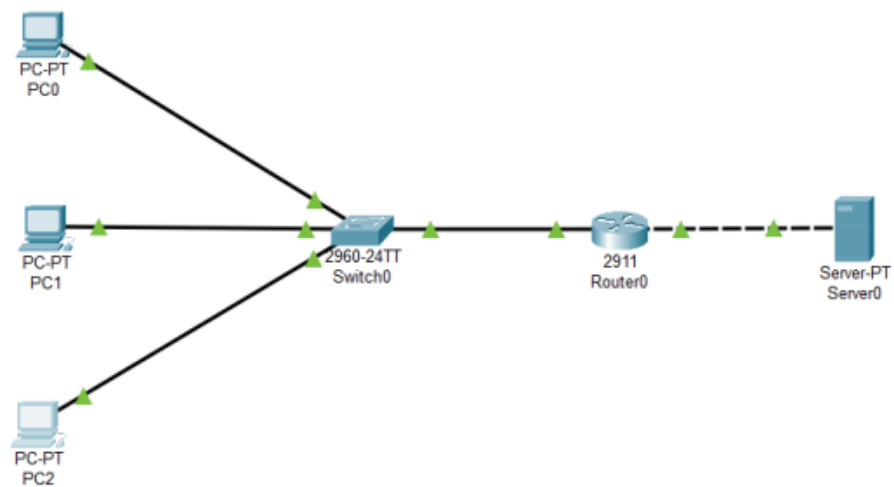
2 Analisis Hasil Percobaan

Berdasarkan hasil praktikum, dapat disimpulkan bahwa implementasi NAT dan Firewall pada router dalam percobaan ini telah berhasil dilakukan dengan sesuai. Konfigurasi NAT menggunakan metode masquerade memungkinkan perangkat-perangkat yang terhubung di jaringan lokal untuk mengakses internet melalui satu alamat IP publik yang dibagikan oleh DHCP client, sehingga meningkatkan efisiensi dan menghemat IP pada jumlah perangkat yang besar. Selain itu, DHCP Server juga berhasil dikonfigurasi oleh praktikan untuk membagikan alamat IP secara otomatis kepada perangkat-perangkat klien dalam suatu jaringan, yang dimana pada percobaan ini berada pada rentang alamat 192.168.10.2 hingga 192.168.10.254 dengan konfigurasi DNS yang mengarah ke 8.8.8.8 dan 8.8.4.4. Konfigurasi Firewall menunjukkan bahwa filter rule yang diterapkan bekerja sesuai dengan yang diharapkan dalam memblokir dan memfilter konten. Ketika Firewall diaktifkan, laptop tidak dapat melakukan ping ke luar jaringan karena filter yang memblokir protokol ICMP aktif, sehingga menghasilkan respon Request Timed Out. Selain itu, rule tambahan untuk memblokir akses ke situs speedtest melalui pemfilteran konten HTTP dan HTTPS juga berfungsi dengan baik, terbukti dari kegagalan akses ke situs yang melanggar rule tersebut saat Firewall aktif dan keberhasilan dalam akses saat firewall dinonaktifkan. Penggunaan bridge pada router B pada praktikum ini juga berhasil menghubungkan dua interface sehingga router dapat berfungsi sebagai perantara antar perangkat secara transparan. Secara keseluruhan, praktikum ini berhasil menunjukkan bagaimana Firewall dapat digunakan untuk mengontrol lalu lintas jaringan dan konten yang diakses oleh user serta NAT yang memungkinkan perangkat lokal mengakses internet dengan aman dan efisien.

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 1: topologi


```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Reply from 203.0.113.10: bytes=32 time=1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.
Reply from 192.168.10.254: Destination host unreachable.

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Reply from 203.0.113.10: bytes=32 time=1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

C:\>ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:

Reply from 203.0.113.10: bytes=32 time=1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127
Reply from 203.0.113.10: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Gambar 2: Simulasi Tugas Modul



Gambar 3: Simulasi Tugas Modul

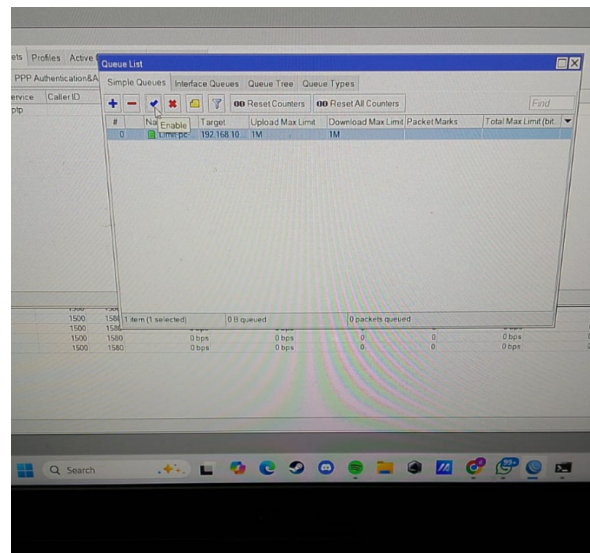
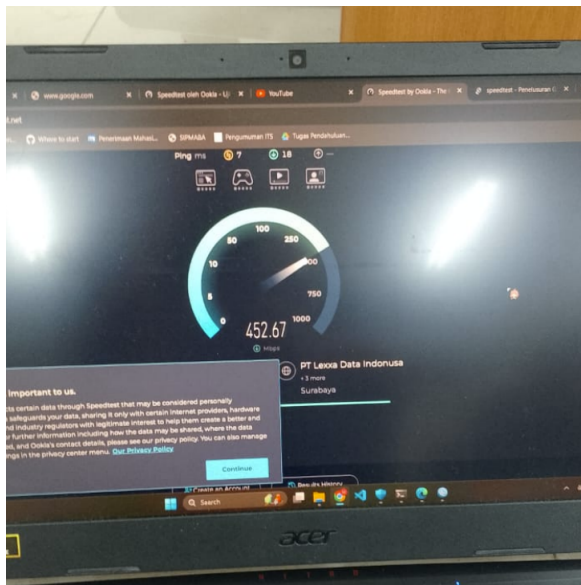
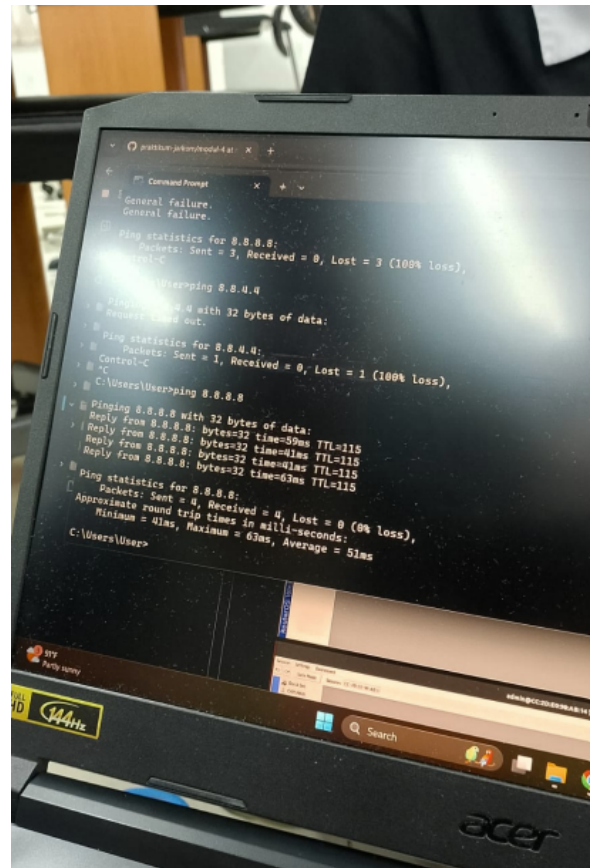
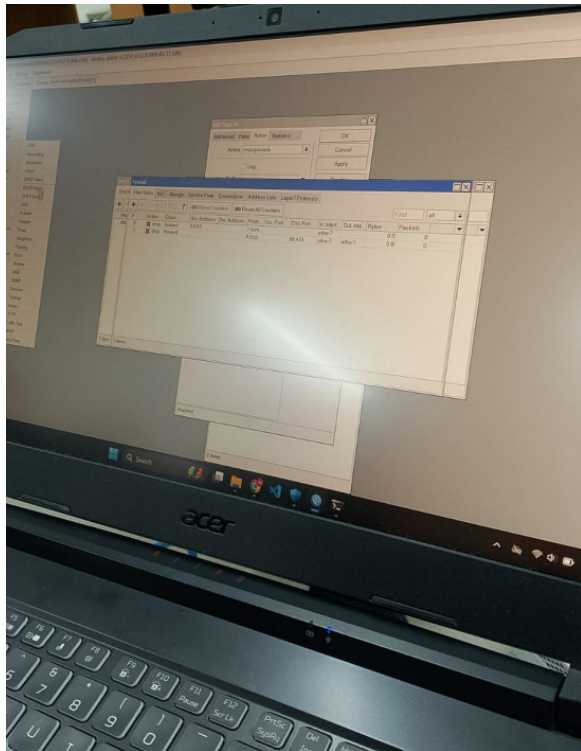
4 Kesimpulan

Praktikum ini memberikan pemahaman mendalam mengenai konfigurasi dasar jaringan menggunakan perangkat router MikroTik. Dimulai dari proses reset dan pengaturan DHCP client pada interface ether1, router berhasil dikonfigurasi untuk memperoleh alamat IP secara otomatis dari jaringan utama. Selanjutnya, pemberian IP statis pada interface ether7 dan pengaktifan DHCP server menunjukkan bahwa router mampu mendistribusikan alamat IP kepada perangkat klien secara otomatis dan sesuai dengan skema yang telah dirancang. Implementasi Network Address Translation (NAT) dengan metode masquerade terbukti efektif dalam membagikan koneksi internet dari jaring-

an publik ke jaringan lokal, di mana perangkat klien dapat mengakses internet dengan baik. Selain itu, konfigurasi firewall memberikan kontrol selektif terhadap lalu lintas jaringan, seperti pembatasan akses melalui protokol ICMP dan pemblokiran situs tertentu, yang memperkuat aspek keamanan jaringan. Pada bagian akhir, penggunaan mode bridge pada Router B berhasil menyatukan dua segmen jaringan secara transparan tanpa perlu mengubah pengalamatan IP atau pengaturan routing. Seluruh konfigurasi diuji melalui pengiriman paket dan akses internet, dengan hasil yang menunjukkan keberhasilan dan konsistensi dari setiap tahap konfigurasi. Dengan demikian, praktikum ini memperkuat pemahaman tentang prinsip-prinsip dasar jaringan seperti manajemen IP, konektivitas internet, pengamanan trafik, dan integrasi segmen jaringan melalui bridge.

5 Lampiran

5.1 Dokumentasi saat praktikum



Gambar 4: Lampiran Praktikum