



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

# Laporan Akhir Praktikum Jaringan Komputer

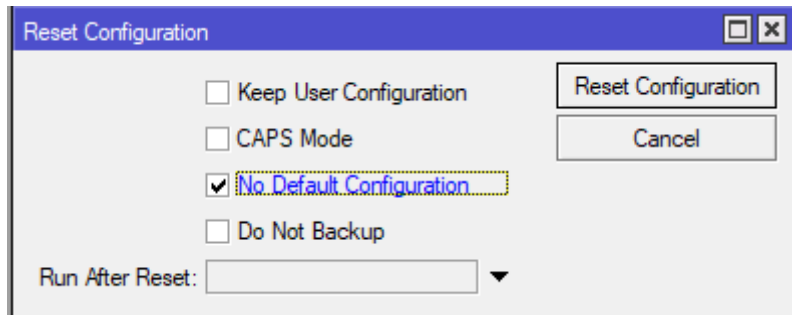
## Firewall dan NAT

Kadek Candra Dwi Yanti - 5024231067

2025

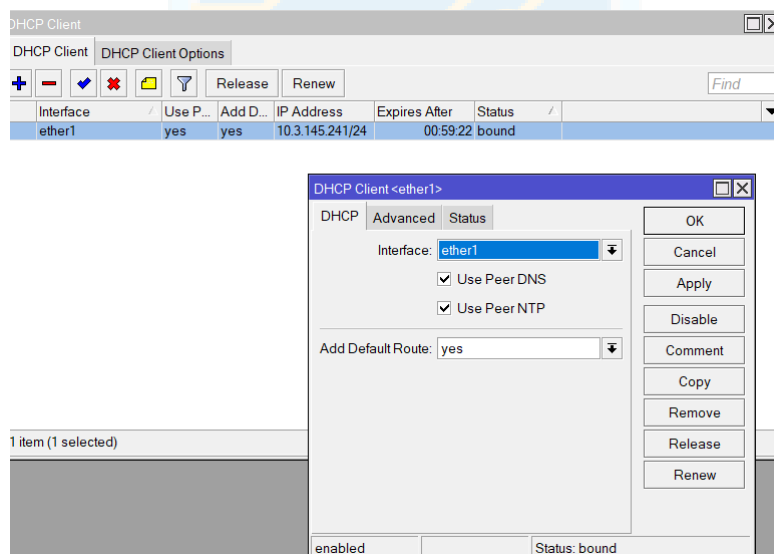
# 1 Langkah-Langkah Percobaan

1. Reset perangkat router untuk menghindari konflik pengaturan dengan konfigurasi sebelumnya. Gunakan aplikasi Winbox dan pilih menu System, kemudian pilih Reset Configuration. Pastikan opsi "No Default Configuration" dicentang, lalu klik "Reset Configuration."



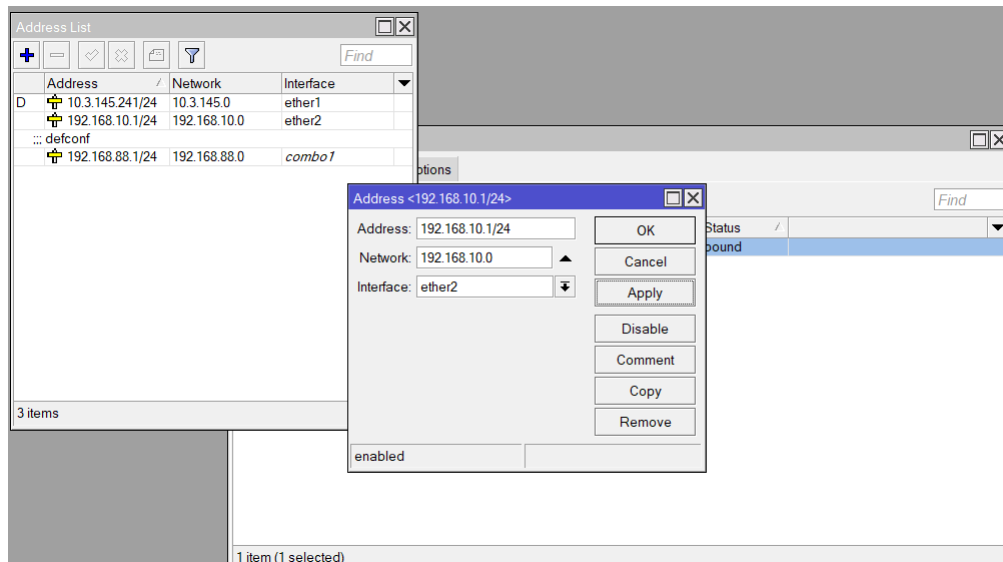
**Gambar 1:** Reset Router

2. Sambungkan kabel internet ke ether1 pada Router A dan konfigurasi DHCP Client dengan mengakses menu IP dan memilih DHCP Client. Klik "+" untuk menambah entri baru dan pilih "ether1" sebagai Interface. Klik "Apply" dan pastikan status koneksi menunjukkan "bound."



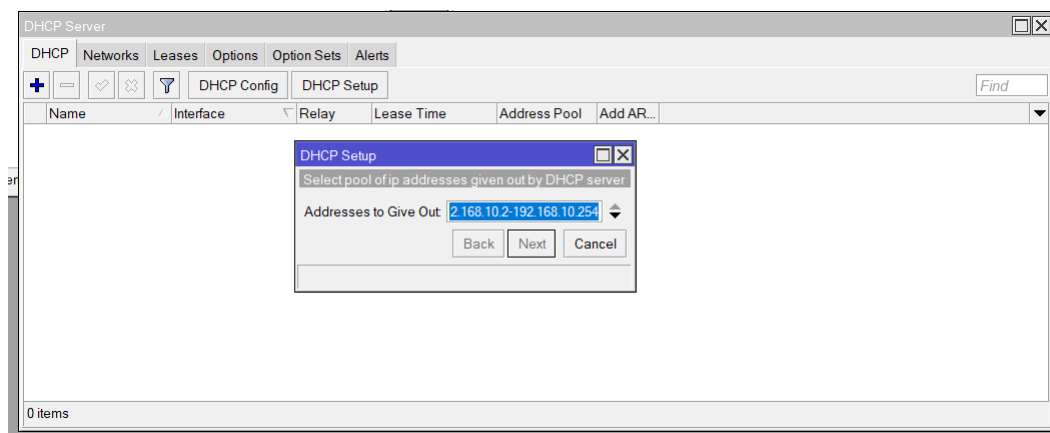
**Gambar 2:** Konfigurasi DHCP Client pada Router A (Ether 1)

3. Tambahkan alamat IP pada ether2 untuk konektivitas dengan Switch. Masuk ke menu IP dan pilih Addresses, kemudian klik "+" dan masukkan alamat IP (misalnya 192.168.10.1/24). Pilih Interface "ether2" dan klik "Apply."



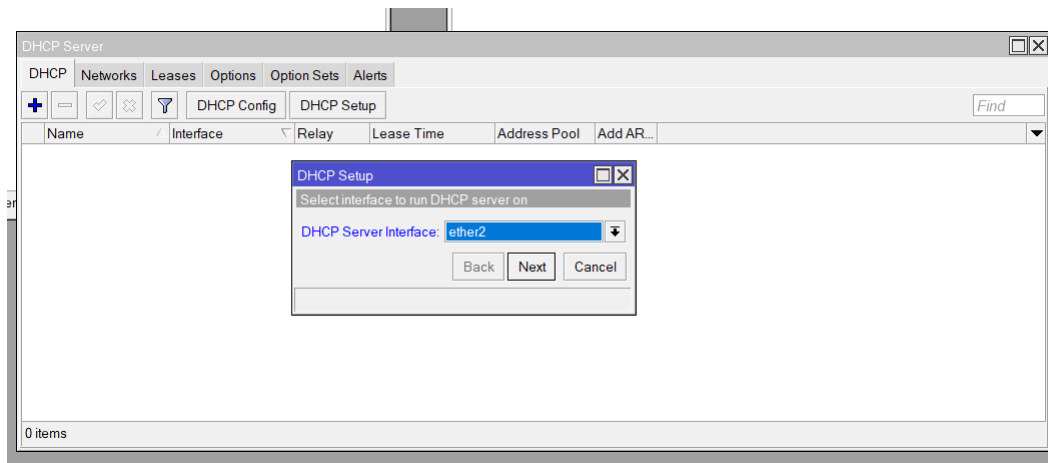
**Gambar 3:** Penambahan Alamat IP pada Ether 7

4. Akses menu IP dan pilih DHCP Server, lalu klik tombol "DHCP Setup." Kemudian melakukan beberapa setup yaitu,



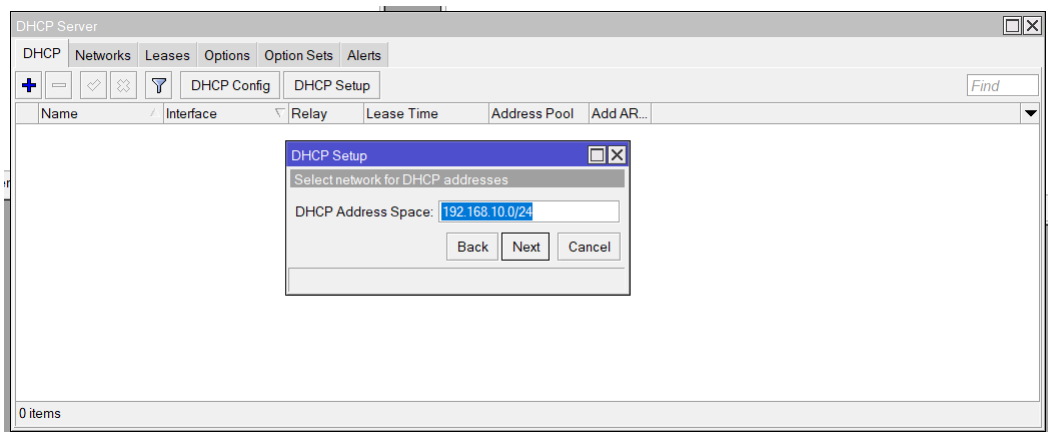
**Gambar 4:** DHCP Setup

- Pada jendela DHCP Server Setup, pilih interface yang akan digunakan untuk distribusi IP kepada klien. Pilih ether2 sebagai interface yang akan mendistribusikan alamat IP lalu klik "Next"



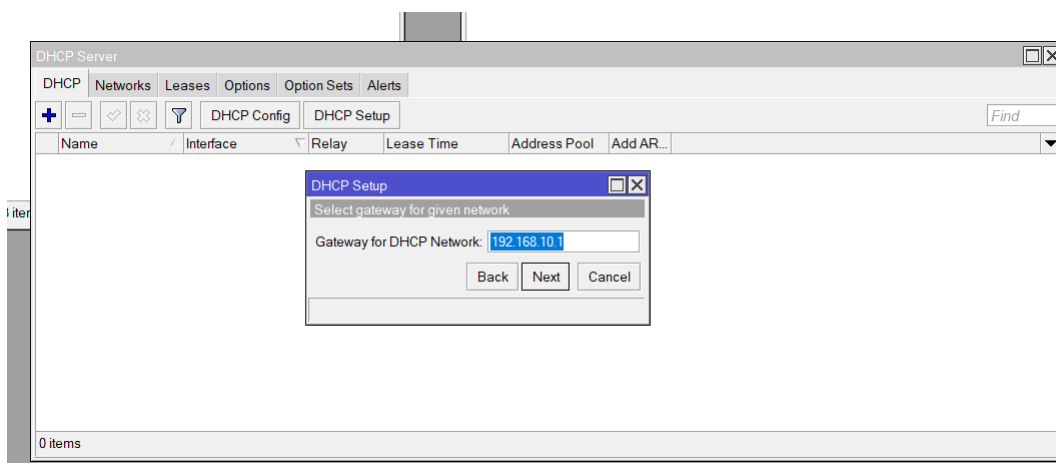
**Gambar 5:** DHCP Server Interface

- Pada jendela DHCP Server Interface, pastikan jaringan yang digunakan sudah benar, 192.168.10.0/24 lalu klik "Next"
- Verifikasi gateway yang akan diberikan kepada klien, 192.168.10.1 lalu klik "Next"



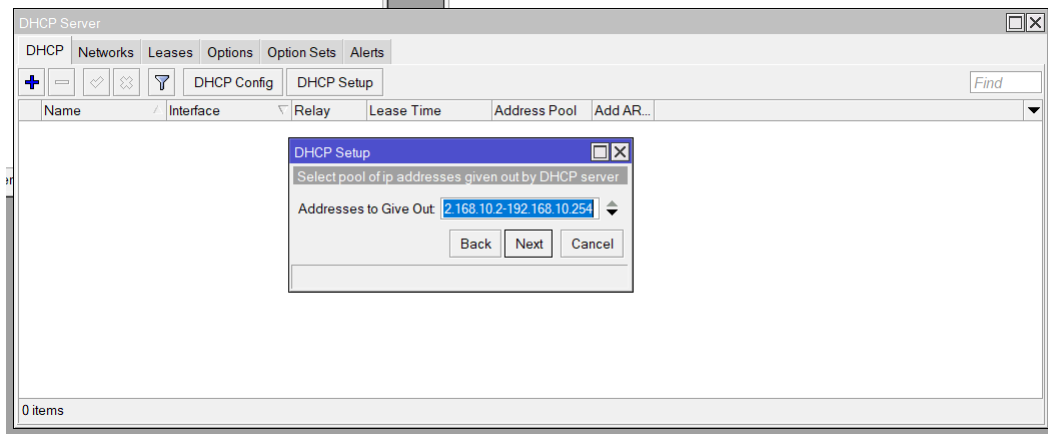
**Gambar 6:** DHCP Address Space

- Pada jendela Gateway for DHCP Network, tentukan alamat IP yang akan diberikan kepada klien sebagai gateway, yaitu 192.168.10.1 lalu klik "Next"



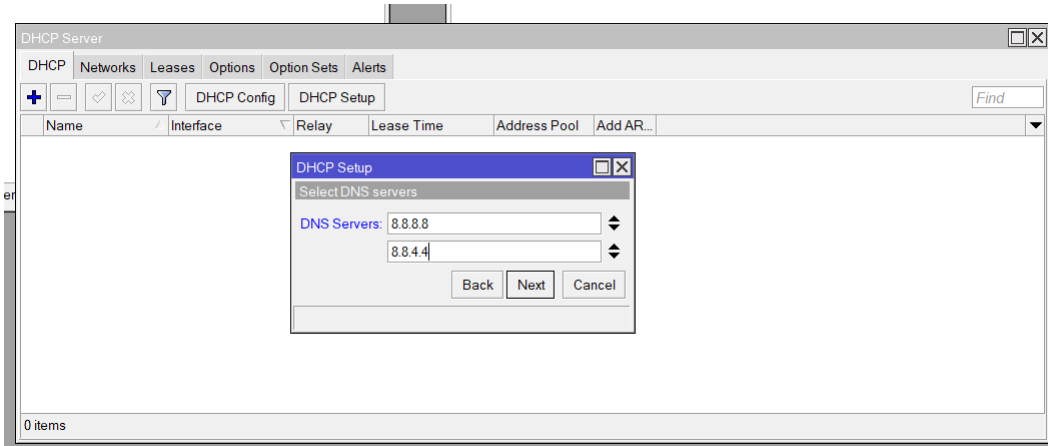
**Gambar 7:** Gateway for DHCP Network

- Pada jendela Addresses to Give Out, tentukan rentang alamat IP yang akan didistribusikan kepada perangkat klien. Sebagai contoh, rentang alamat IP yang diberikan bisa mulai dari 192.168.10.2 hingga 192.168.10.254 lalu klik "Next"



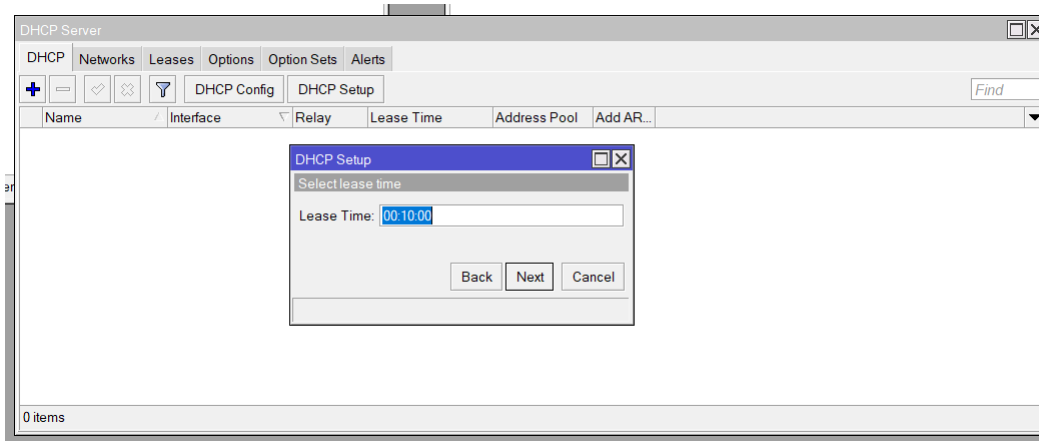
**Gambar 8:** Addresses to Give Out

- Pada jendela DNS Servers, masukkan alamat DNS server yang akan digunakan oleh klien, seperti 8.8.8.8 dan 8.8.4.4 lalu klik "Next"



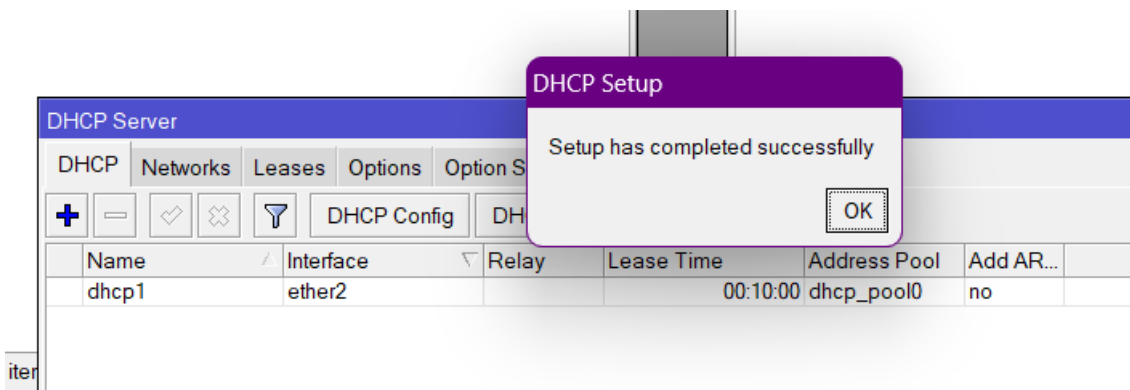
**Gambar 9:** DNS Servers

- Pada jendela Lease Time, tentukan durasi waktu lease alamat IP yang diberikan kepada klien, yaitu 00:10:00 (10 menit) lalu klik "Next"

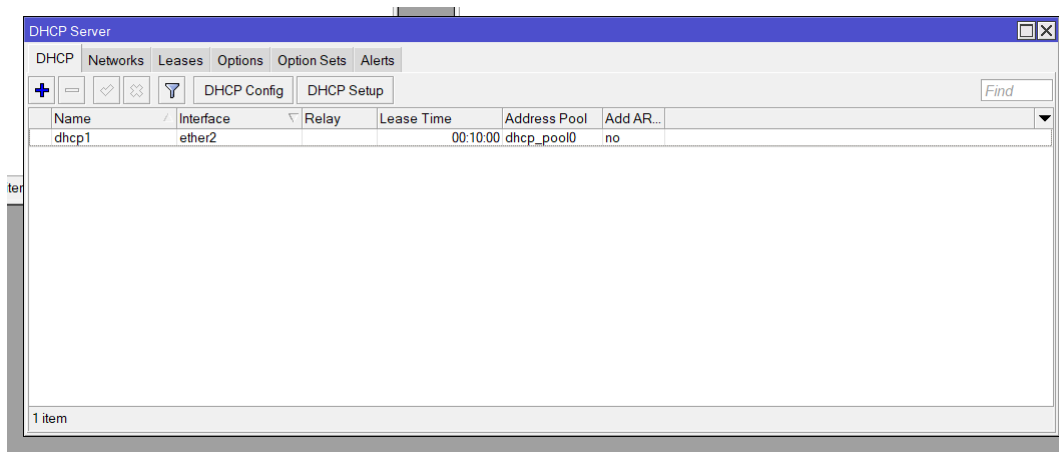


**Gambar 10:** Lease Time

- Setelah semua langkah selesai, akan muncul pesan "Setup has completed successfully". Klik "OK"



**Gambar 11:** Setup Selesai



**Gambar 12:** Hasil Setup DHCP Server

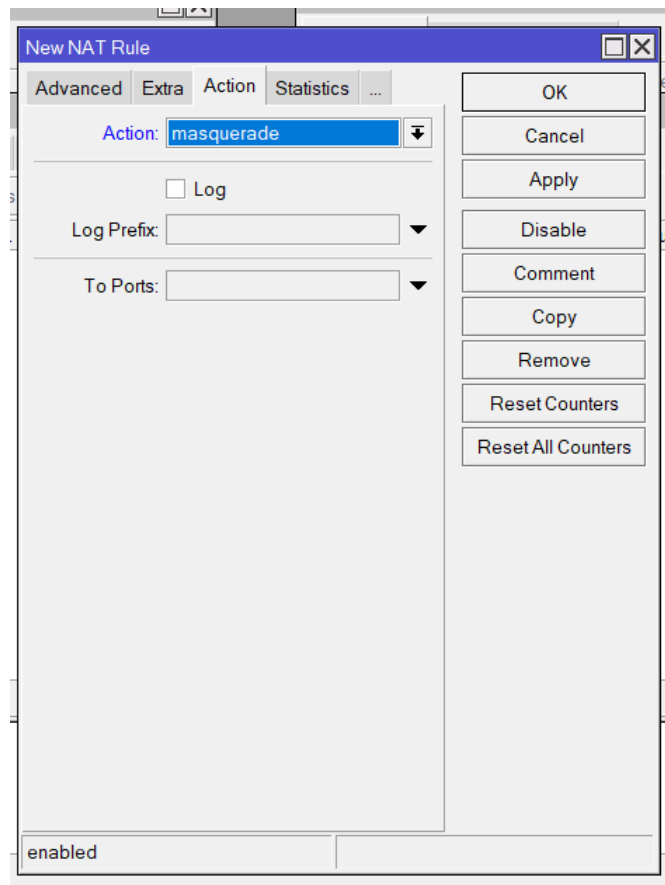
5. Lakukan konfigurasi NAT dengan mengakses menu IP, kemudian pilih Firewall dan NAT. Klik "+" untuk membuat aturan baru, pilih Chain "src-nat" dan Action "masquerade." Klik "Apply" dan "OK." Cek koneksi dengan ping ke 8.8.8.8 menggunakan Terminal di Winbox.

The image shows a 'New NAT Rule' dialog box with the following configuration in the General tab:

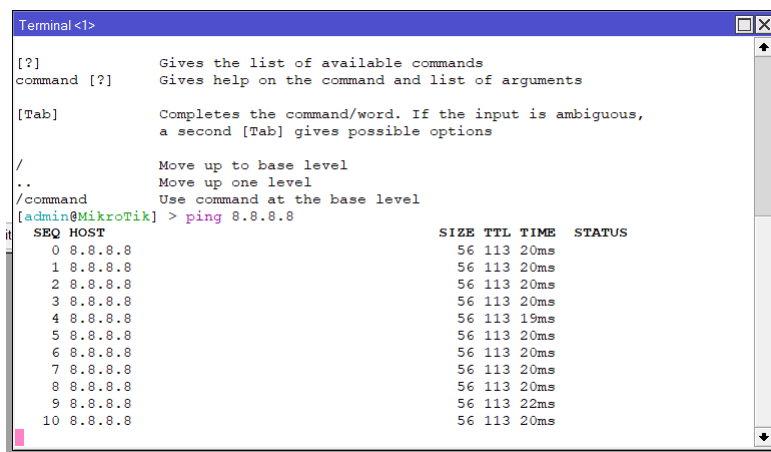
- Chain:** srcnat
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Protocol:** (empty)
- Src. Port:** (empty)
- Dst. Port:** (empty)
- Any. Port:** (empty)
- In. Interface:** ☐ ether1
- Out. Interface:** (empty)
- In. Interface List:** (empty)
- Out. Interface List:** (empty)
- Packet Mark:** (empty)
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Routing Table:** (empty)

At the bottom left, the rule is set to **enabled**. On the right side, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

**Gambar 13:** Konfigurasi NAT Pada Bagian General



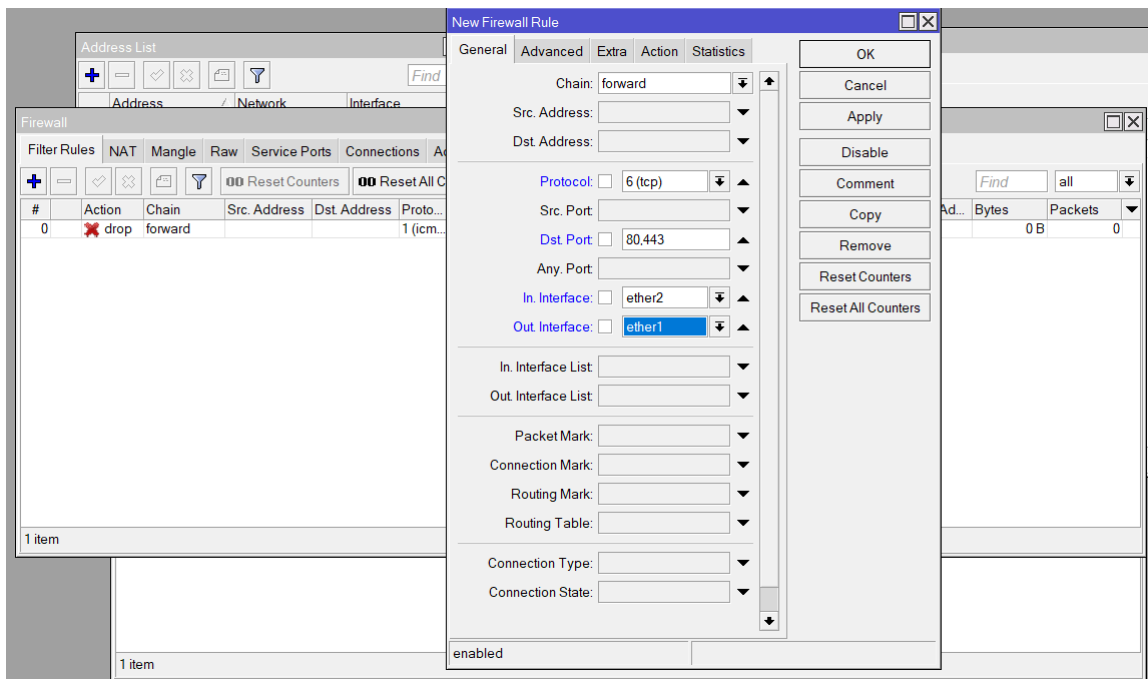
**Gambar 14:** Konfigurasi NAT Pada Bagian Action



**Gambar 15:** Uji Ping Pada Winbox

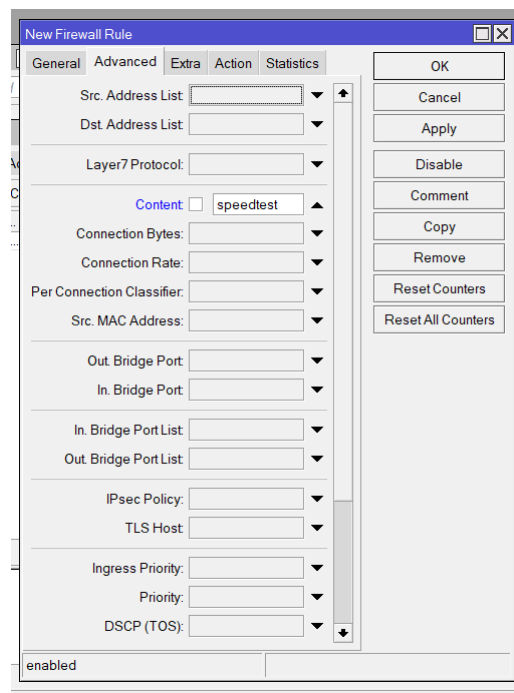
6. Tambahkan aturan filter untuk memblokir ICMP dan akses situs berdasarkan konten. Pada menu IP, pilih Firewall dan Filter Rule, lalu klik "+" dan tentukan Chain "forward", Protocol "icmp"



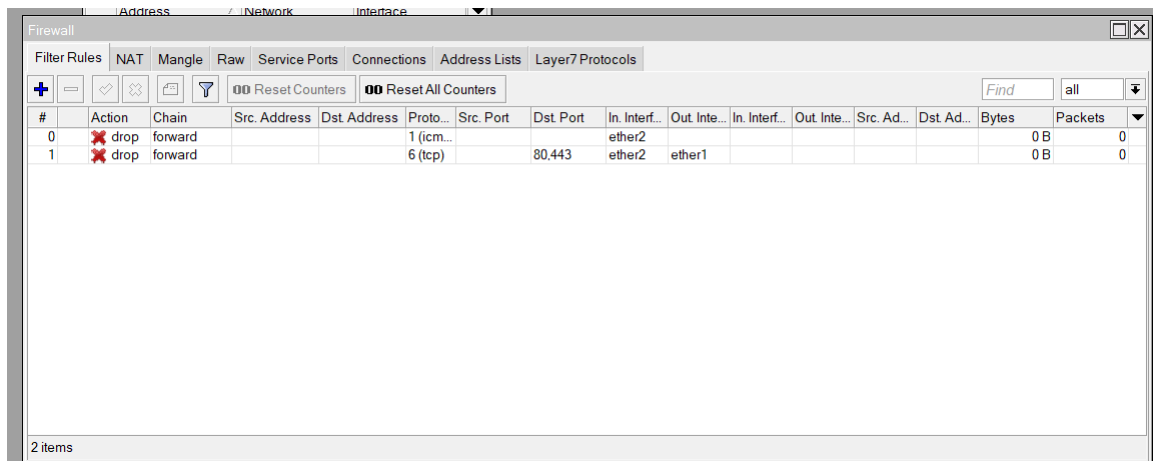


**Gambar 16:** Pemblokiran Akses Situs Web Berdasarkan Konten Pada Bagian General

- Set bagian Action ke "drop" untuk pemblokiran ICMP. Untuk pemblokiran situs web berdasarkan konten, set Action ke "drop" dengan menggunakan kata kunci tertentu (misalnya "speedtest")

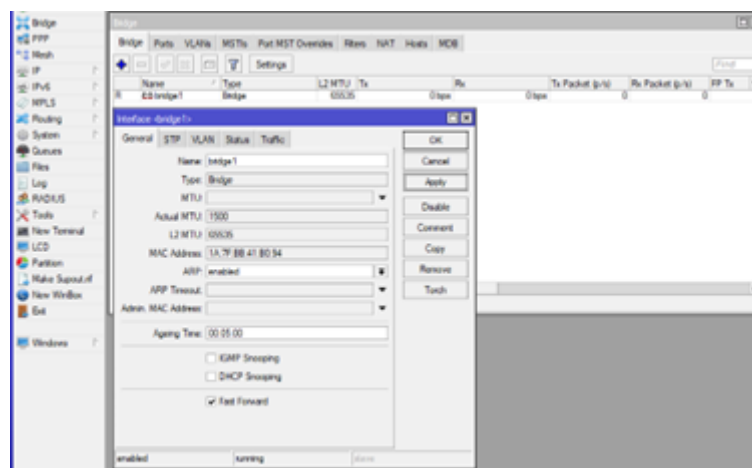


**Gambar 17:** Pemblokiran Akses Situs Web Berdasarkan Konten Pada Bagian Advanced

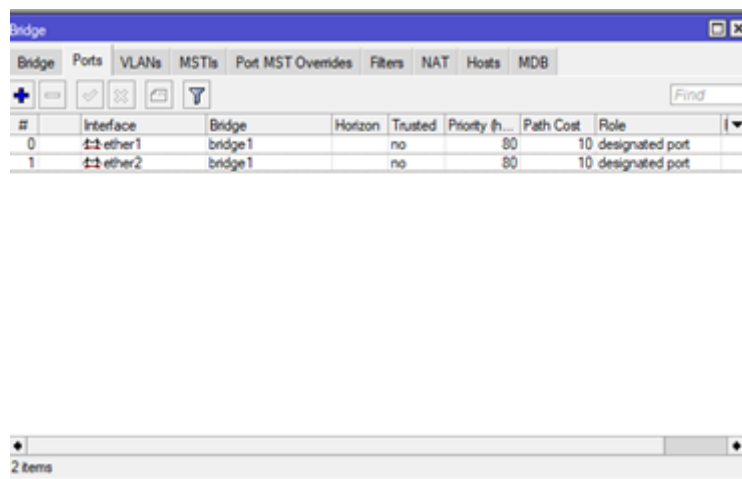


**Gambar 18:** Hasil Konfigurasi Firewall

8. Untuk mengubah Router B menjadi hub, akses menu Bridge dan klik "+", kemudian pilih port yang akan ditambahkan ke bridge. Tambahkan interface yang terhubung ke perangkat laptop dan Router A.

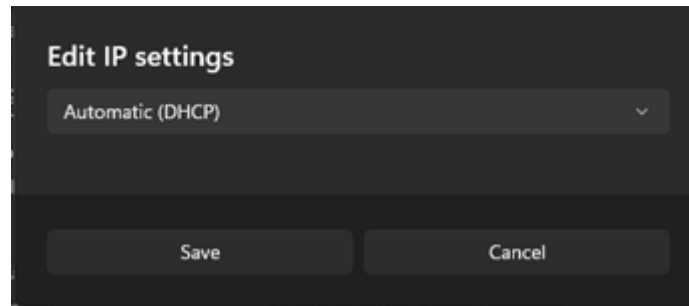


**Gambar 19:** Konfigurasi Bridge Pada Router B



**Gambar 20:** Hasil Konfigurasi Bridge Pada Router B

9. Pastikan laptop dikonfigurasi untuk menerima alamat IP secara otomatis melalui DHCP. Periksa alamat IP yang diterima dengan membuka Command Prompt dan menggunakan perintah "ipconfig."



**Gambar 21:** Konfigurasi menjadi IP Secara Otomatis Melalui DHCP

10. Lakukan pengujian konektivitas dan pemblokiran. Untuk pengujian konektivitas, lakukan ping ke 8.8.8.8, dan pastikan responsnya sesuai dengan aturan firewall yang diterapkan

```
C:\Users\hilmy>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\hilmy>ping 8.8.8.8
```

**Gambar 22:** Uji Coba Konfigurasi ping 8.8.8.8 (Saat Firewall Aktif)

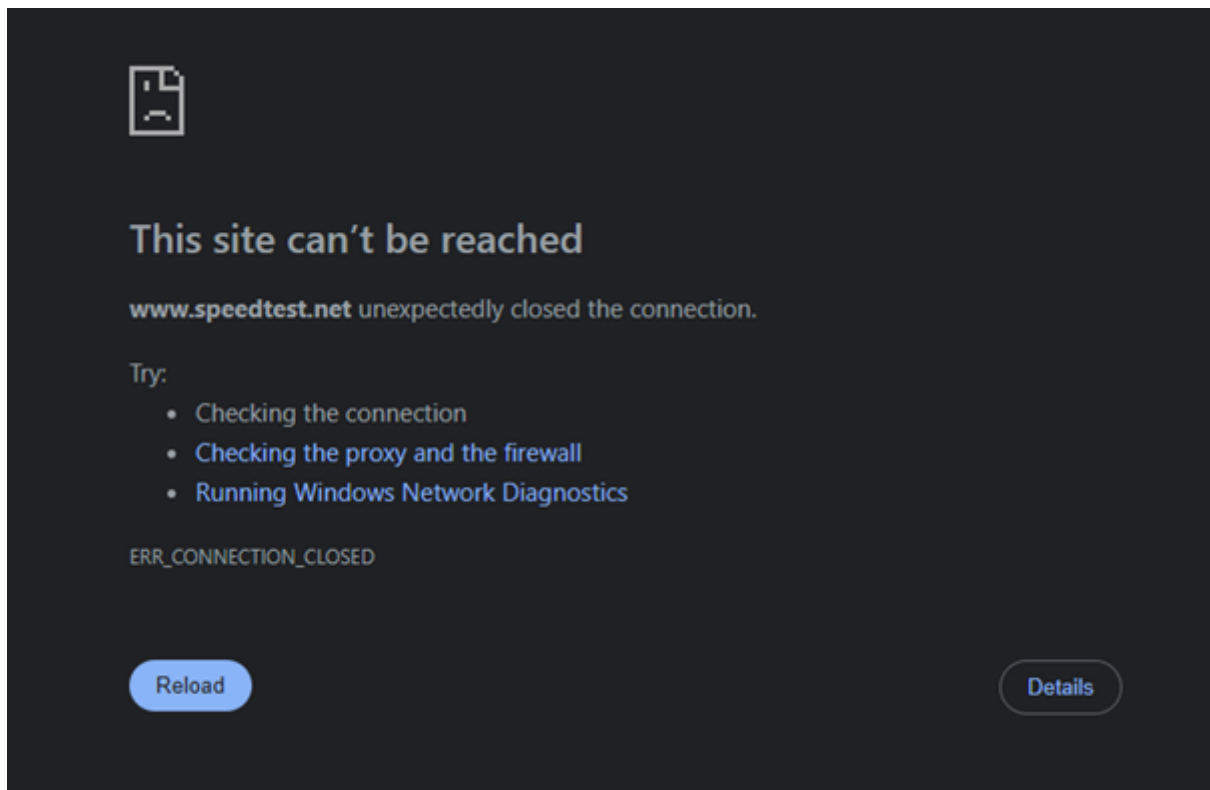
```
C:\Users\hilmy>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112

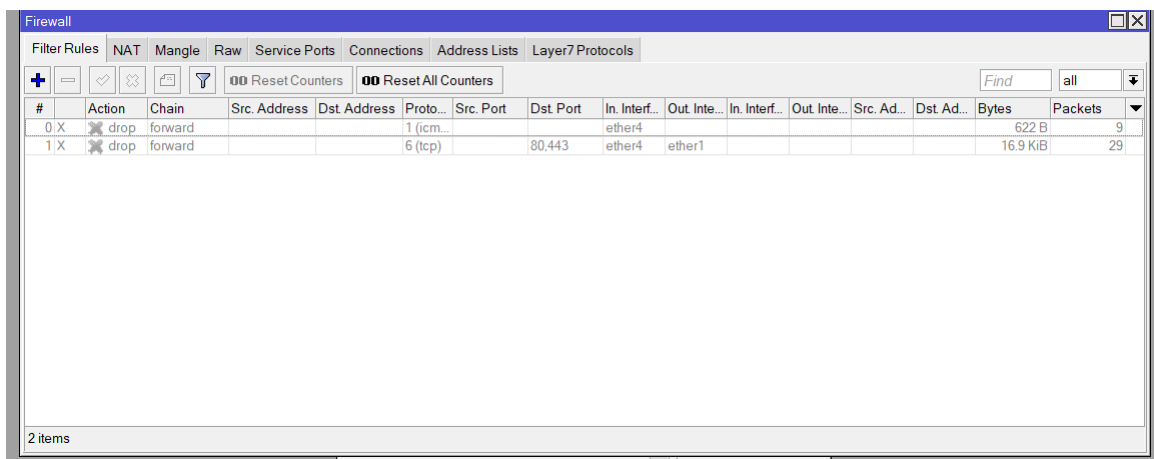
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

**Gambar 23:** Uji Coba Konfigurasi ping 8.8.8.8 (Saat Firewall Mati)

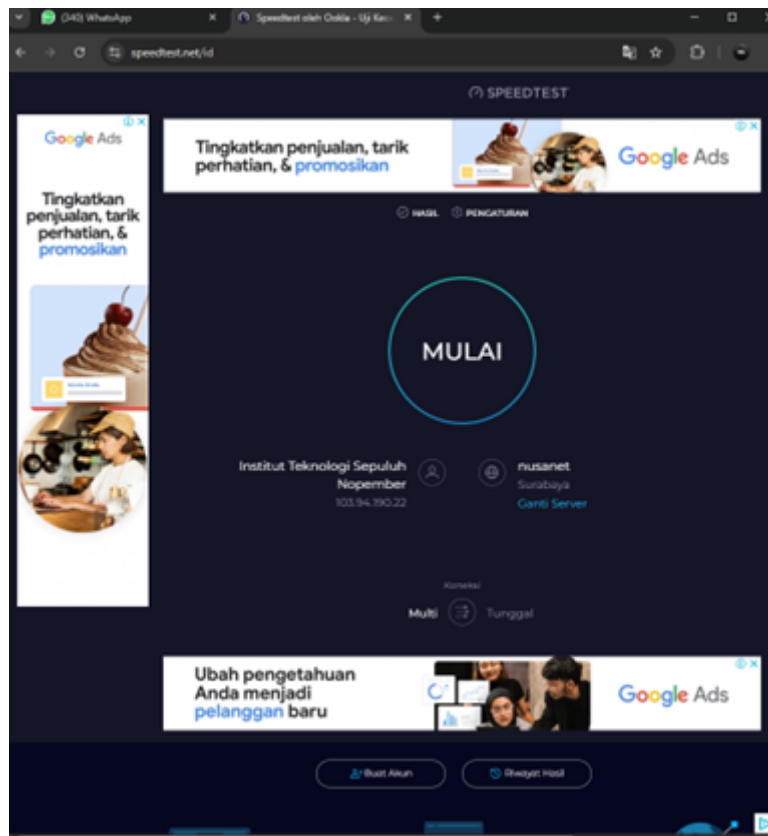
11. Untuk uji pemblokiran konten, coba akses situs yang mengandung kata kunci tertentu dan pastikan situs tersebut terblokir



**Gambar 24:** Cek website speedtest (Saat Firewall Nyala)



**Gambar 25:** Firewall Dalam Keadaan Disable



**Gambar 26:** Cek website speedtest (Saat Firewall Mati)

## 2 Analisis Hasil Percobaan

Secara keseluruhan, praktikum ini berhasil dilakukan dengan baik, sesuai dengan tujuan yang telah ditetapkan. Konfigurasi router dan pengaturan jaringan yang dilakukan berhasil menunjukkan penerapan teori dalam praktik.

Pada tahap pertama, konfigurasi DHCP Client pada Router A berhasil menghubungkan router ke ISP dan mendapatkan alamat IP secara otomatis. Hal ini sesuai dengan teori DHCP yang mempermudah pengalokasian alamat IP. Selanjutnya, penambahan alamat IP pada ether7 untuk memastikan konektivitas dengan switch berjalan lancar dan mendukung teori subnetting untuk pembagian jaringan yang efisien.

Konfigurasi DHCP Server pada Router MikroTik juga berhasil mendistribusikan alamat IP ke perangkat yang terhubung, sesuai dengan teori bahwa DHCP Server memungkinkan pengalokasian IP secara otomatis dan efisien. Konfigurasi NAT yang dilakukan berhasil memungkinkan perangkat dalam jaringan lokal menggunakan satu IP publik untuk mengakses internet, sesuai dengan fungsi NAT dalam menghemat alamat IP publik yang terbatas.

Terakhir, pengujian firewall berhasil membuktikan bahwa aturan yang diterapkan dapat memblokir trafik yang tidak diinginkan, seperti pemblokiran ICMP dan konten web tertentu, yang sesuai dengan teori firewall sebagai pengaman lalu lintas data jaringan.

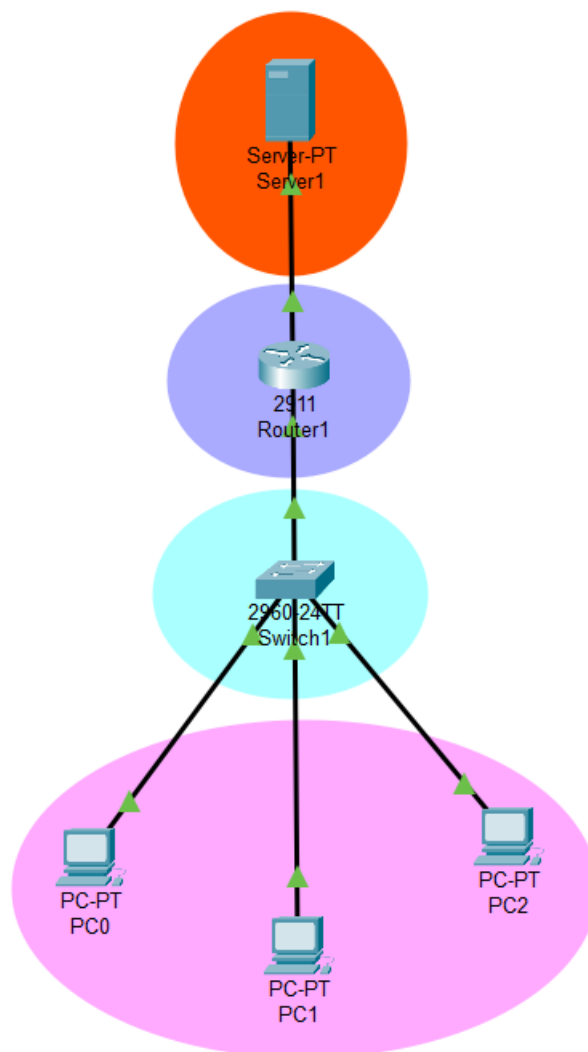
Secara umum, percobaan ini menunjukkan pemahaman yang baik terkait teori dan penerapannya. Tidak ada kesalahan besar dalam pelaksanaan praktikum, meskipun kesalahan kecil dalam pengaturan atau konfigurasi sehingga sempat menghambat praktikum. Namun, hasil percobaan menunjukkan bahwa konsep-konsep dasar dalam manajemen jaringan, seperti DHCP, NAT, dan firewall,

diterapkan dengan benar dan berhasil mencapai tujuannya.

### 3 Hasil Tugas Modul

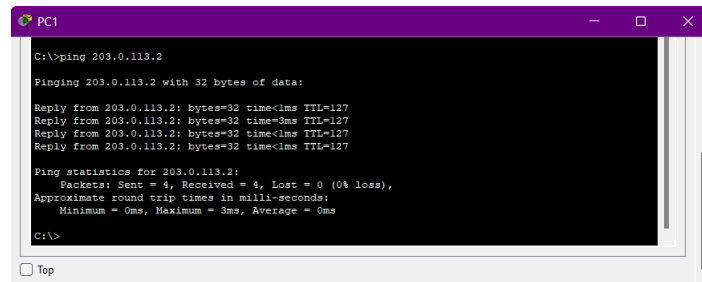
1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:

- 1 Router
- 1 Switch
- 3 PC (LAN)
- 1 Server (Internet/Public)



**Gambar 27:** Topologi Pada Cisco Packet Tracer

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



```
C:\>ping 203.0.113.2

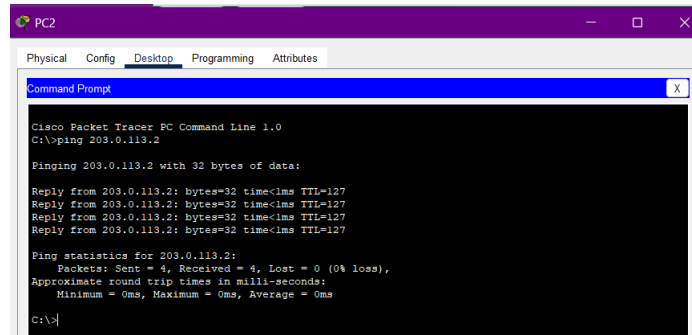
Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>
```

**Gambar 28:** Uji Ping Pada PC 1



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.2

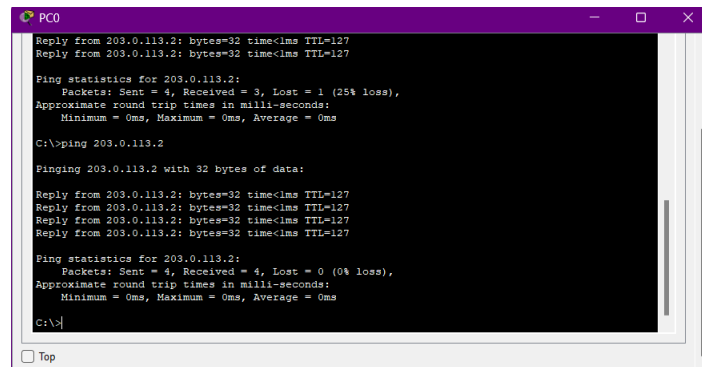
Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Gambar 29:** Uji Ping Pada PC 2



```
PC0
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127
Reply from 203.0.113.2: bytes=32 time<1ms TTL=127

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

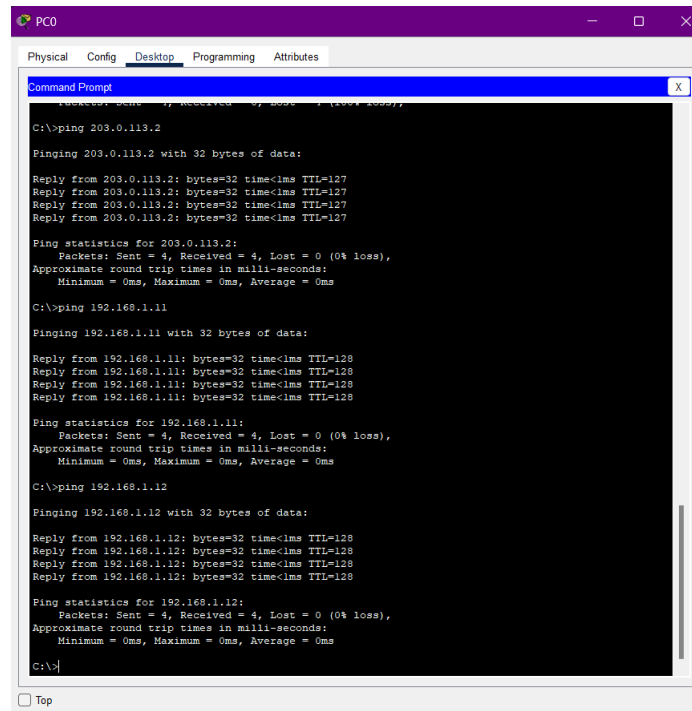
C:\>
```

**Gambar 30:** Uji Ping Pada PC 0

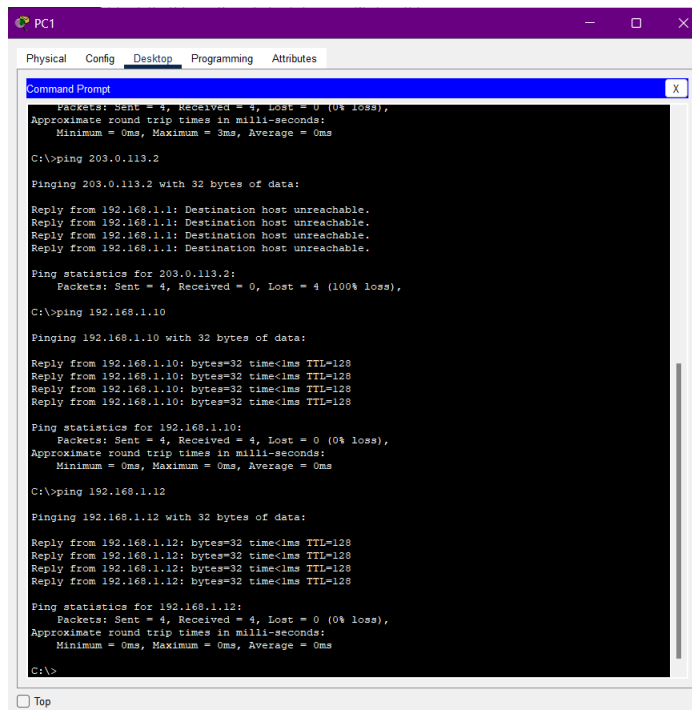
### 3. Konfigurasi Firewall (ACL):

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

Uji koneksi menggunakan ping dan dokumentasikan hasilnya.

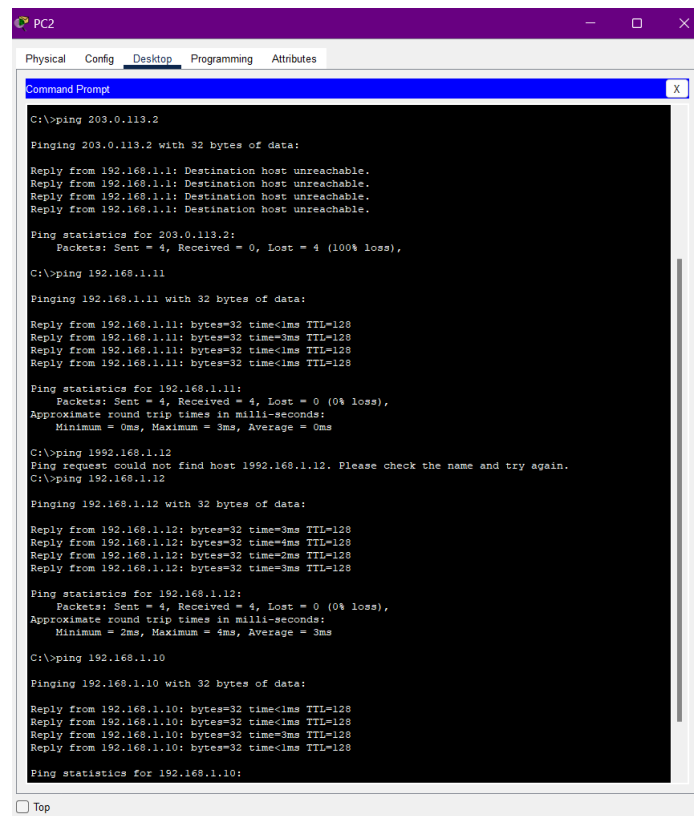


**Gambar 31:** Uji Ping Pada PC 0



**Gambar 32:** Uji Ping Pada PC 1





The screenshot shows a Windows PC2 desktop environment. The 'Desktop' tab is selected in the top navigation bar. A 'Command Prompt' window is open, displaying the results of several ping tests. The tests are as follows:

- Test 1:** `C:\>ping 203.0.113.2`  
Pinging 203.0.113.2 with 32 bytes of data:  
Reply from 192.168.1.1: Destination host unreachable.  
Reply from 192.168.1.1: Destination host unreachable.  
Reply from 192.168.1.1: Destination host unreachable.  
Reply from 192.168.1.1: Destination host unreachable.  
Ping statistics for 203.0.113.2:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
- Test 2:** `C:\>ping 192.168.1.11`  
Pinging 192.168.1.11 with 32 bytes of data:  
Reply from 192.168.1.11: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.11: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.11: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.11: bytes=32 time=3ms TTL=128  
Ping statistics for 192.168.1.11:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 3ms, Average = 0ms
- Test 3:** `C:\>ping 1992.168.1.12`  
Ping request could not find host 1992.168.1.12. Please check the name and try again.  
`C:\>ping 192.168.1.12`  
Pinging 192.168.1.12 with 32 bytes of data:  
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.12: bytes=32 time=4ms TTL=128  
Reply from 192.168.1.12: bytes=32 time=2ms TTL=128  
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128  
Ping statistics for 192.168.1.12:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 4ms, Average = 3ms
- Test 4:** `C:\>ping 192.168.1.10`  
Pinging 192.168.1.10 with 32 bytes of data:  
Reply from 192.168.1.10: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.10: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.10: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.10: bytes=32 time=3ms TTL=128  
Ping statistics for 192.168.1.10:

**Gambar 33:** Uji Ping Pada PC 2

## 4 Kesimpulan

Praktikum ini berhasil mencapai tujuannya dalam mengonfigurasi router dan pengaturan jaringan. Hasil yang diperoleh menunjukkan bahwa langkah-langkah yang diambil sesuai dengan teori yang ada. Konfigurasi DHCP Client pada Router A berhasil memberikan alamat IP otomatis dari ISP, sesuai dengan teori DHCP yang memungkinkan perangkat memperoleh IP secara dinamis. Penambahan alamat IP pada ether7 berjalan lancar, mendukung teori subnetting yang digunakan untuk membagi jaringan agar lebih efisien.

Konfigurasi DHCP Server pada Router MikroTik berhasil mendistribusikan alamat IP ke perangkat yang terhubung, seperti yang dijelaskan dalam teori tentang bagaimana DHCP Server bekerja untuk mengalokasikan IP secara otomatis. Selain itu, konfigurasi NAT yang memungkinkan banyak perangkat menggunakan satu IP publik sesuai dengan prinsip efisiensi alamat IP yang terbatas. Pengujian firewall juga berhasil, dengan aturan yang diterapkan mampu memblokir trafik yang tidak diinginkan, sesuai dengan teori firewall yang berfungsi untuk mengamankan jaringan.

Pembelajaran utama yang diperoleh dari praktikum ini adalah pentingnya pengaturan yang tepat pada setiap tahap konfigurasi untuk memastikan konektivitas yang stabil dan aman dalam jaringan. Terjadi beberapa kesalahan dari praktikan seperti salah memasukkan ip router namun secara keseluruhan, praktikum ini berhasil memperkuat pemahaman tentang konsep-konsep dasar dalam manajemen jaringan dan aplikasi teknisnya.

## 5 Lampiran

### 5.1 Dokumentasi saat praktikum

