



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

Laporan Akhir Praktikum Jaringan Komputer

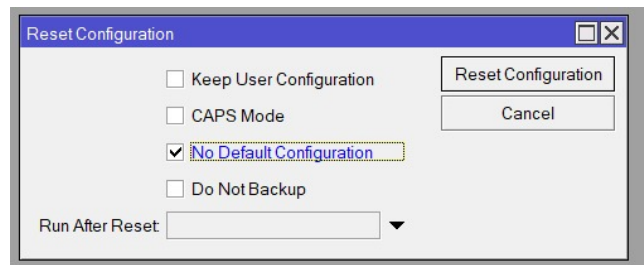
Firewall NAT

Moh. wildan Risqi Maulidi - 5024231056

2025

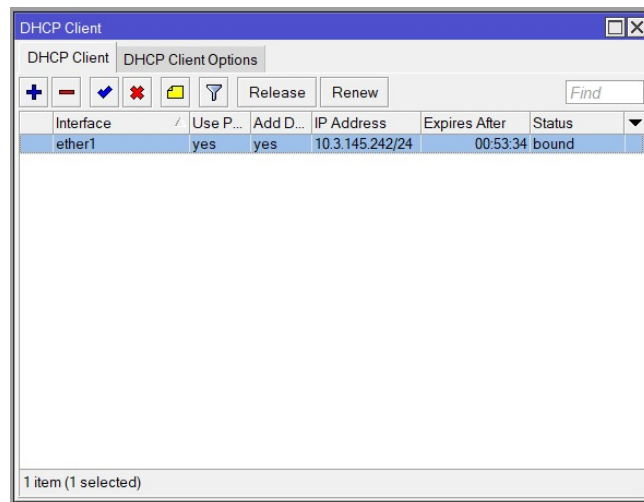
1 Langkah-Langkah Percobaan

- Reset router lalu login kembali

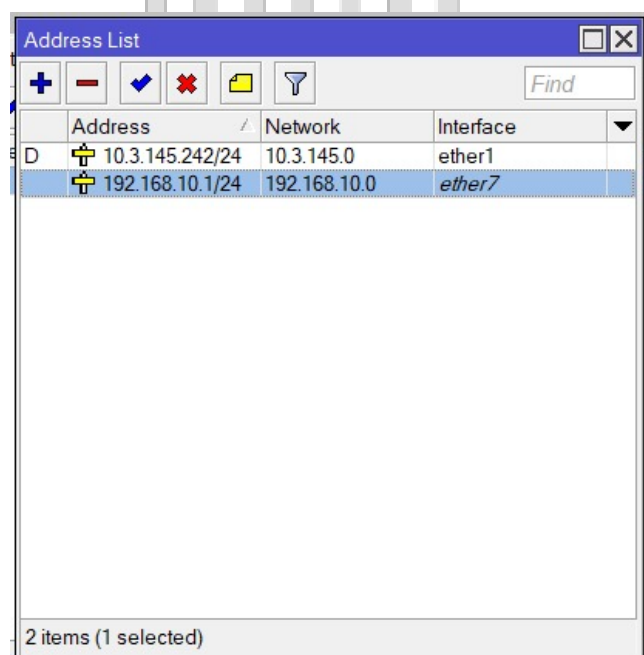


?figurename? 1: Tampilan reset

- Konfigurasi DHCP server pada router Mikrotik, pilih interface yang akan digunakan sebagai DHCP server dengan **ether7** dan pada DHCP Address Space set ip yang digunakan lalu set juga DHCP Client dan pilih **ether1** sebagai interface pastikan status koneksi menunjukkan bound.



?figurename? 2: Tampilan konfigurasi DHCP server dan Client



?figurename? 3: Tampilan Address list

- Konfigurasi NAT pada router Mikrotik, pergi pada menu IP lalu ke Firewall dan ke NAT dan tambah untuk menambahkan aturan baru, pada tab tersebut ke general atur ke **srcnat** dan pada tab action atur ke **masquerade** lalu klik apply.
konfigurasi NAT tersebut untuk menyediakan konektivitas internet pada jaringan lokal.

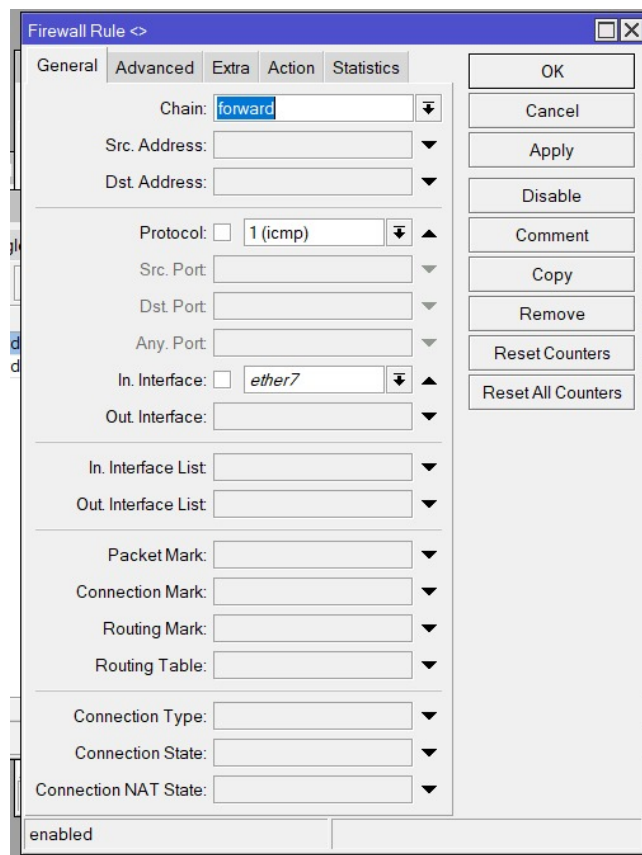
The screenshot shows the 'NAT Rule' configuration window with the 'General' tab selected. The 'Chain' is set to 'srcnat'. The 'Out. Interface' is set to 'ether1'. The 'enabled' checkbox at the bottom is checked. The right sidebar contains buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

figurename? 4: Tampilan konfigurasi NAT bagian general

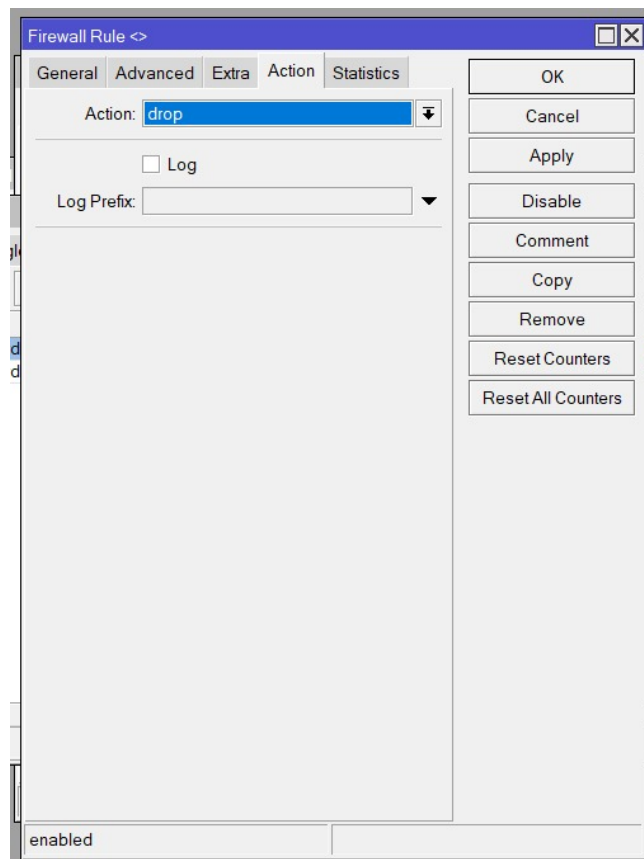
The screenshot shows the 'NAT Rule' configuration window with the 'Action' tab selected. The 'Action' is set to 'masquerade'. The 'Log' checkbox is unchecked. The 'Log Prefix' and 'To Ports' fields are empty. The right sidebar contains buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. The 'enabled' checkbox at the bottom is checked.

?figurename? 5: Tampilan konfigurasi NAT bagian action

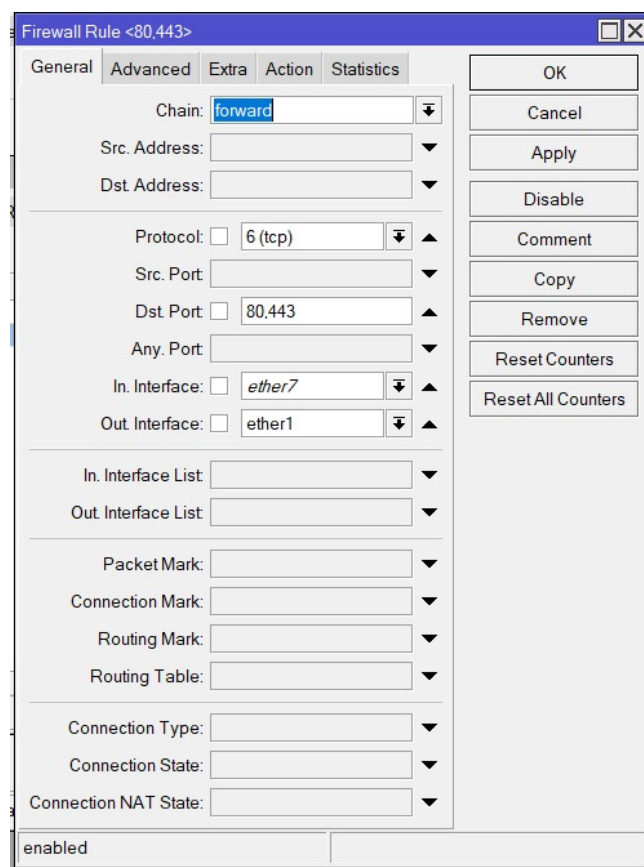
- Konfigurasi firewall pada router Mikrotik, pergi pada menu IP lalu ke Firewall dan ke Filter Rules dan tambah untuk menambahkan aturan baru, pada tab tersebut atur chain ke **forward** dan pada tab general juga atur protocol **icmp** dan general atur in untuk interface "ether7" konfigurasi ini untuk pemblokiran ICMP (Internet Control Message Protocol). dan jika ingin pemblokiran web berdasarkan konten atur pada tab general meliputi chain untuk forward, protocol untuk tcp,dst. port untuk 80,443 ,in. interface untuk ether7 dan yang out untuk ether1. Lalu pergi ke Advance atur content lalu sebagai contoh website yang di blokir adalah speedtest atau youtube ketik "speedtest" atau "youtube" langsung. Dan terakhir pada action atur action ke dalam nilai **drop** untuk memblokir akses ke website tersebut.



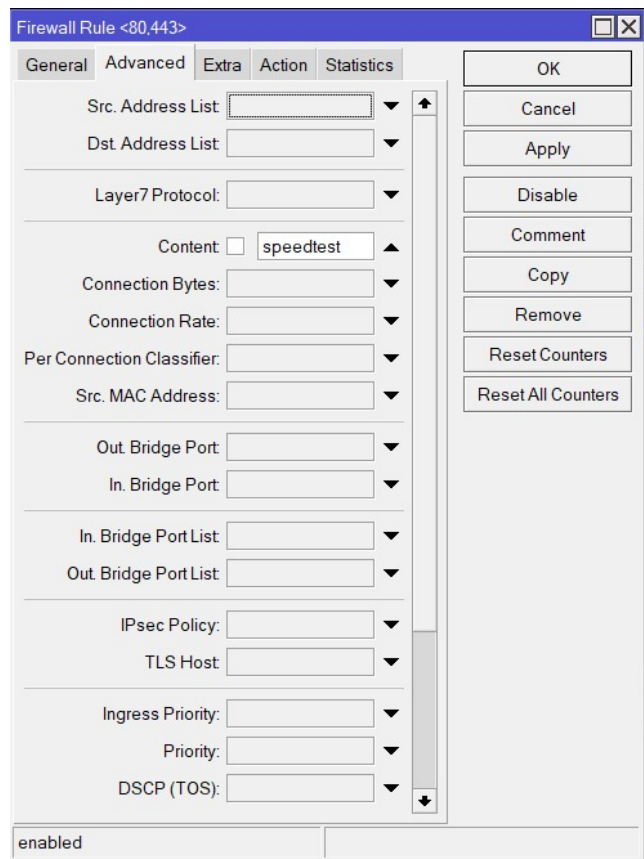
?figurename? 6: Tampilan konfigurasi firewall bagian general



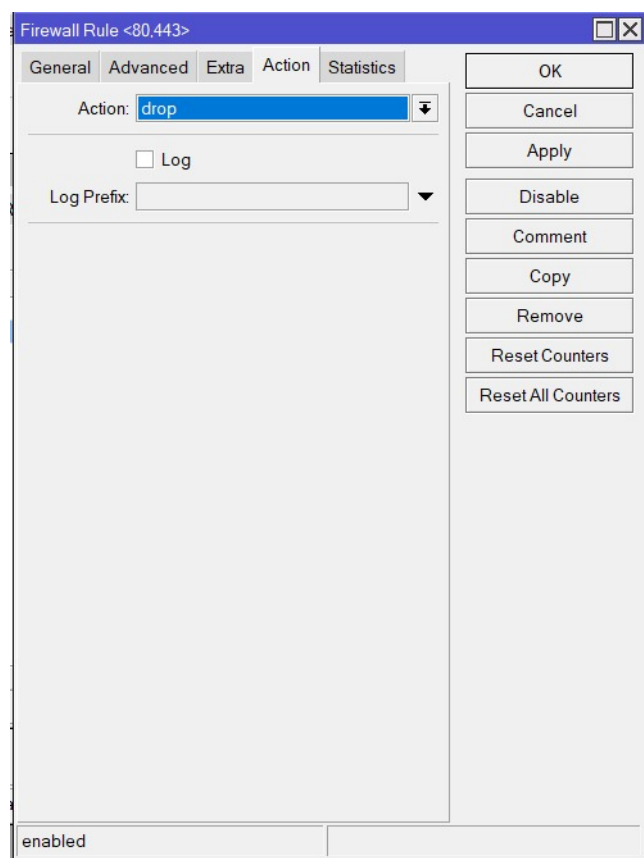
?figurename? 7: Tampilan konfigurasi firewall bagian action



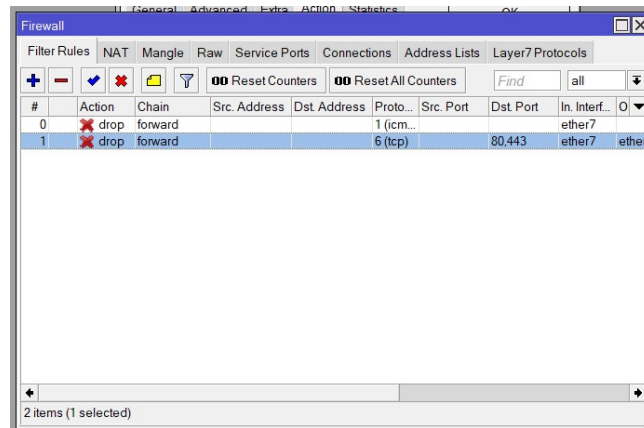
?figurename? 8: Tampilan konfigurasi firewall bagian general untuk port 80,443



?figurename? 9: Tampilan konfigurasi firewall bagian general untuk port 80,443 part 2



?figurename? 10: Tampilan konfigurasi firewall bagian action untuk port 80,443



?figurename? 11: Tampilan konfigurasi firewall filter rules

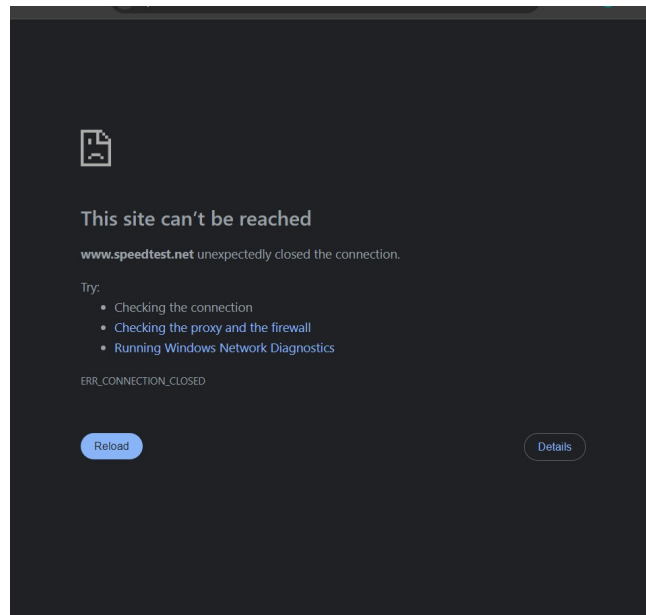
- pertama tes ping untuk firewall dimana mencoba mengaktifkan firewall untuk memblokir google dan nonaktifkan dengan cara **ping 8.8.8.8**, dapat terlihat pada gambar dibawah jika diaktifkan maka hasilnya **Request timed out** yang berarti firewall berhasil memblokir ping ke google. Dan jika dinonaktifkan maka hasilnya **Reply from 8.8.8.8 ...** yang berarti firewall tidak memblokir ping ke google.

```
Ping statistics for 8.8.8.8:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\USER>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
```

?figurename? 12: Tampilan ping ke 8.8.8.8

- Untuk tes blokir web, pertama buka browser dan coba akses ke website yang diblokir seperti speedtest atau youtube, jika berhasil diblokir maka akan muncul tampilan **This site can't be reached**. Dan jika tidak berhasil diblokir maka akan muncul tampilan website tersebut.



?figurename? 13: Tampilan ping ke website

2 Analisis Hasil Percobaan

hasilnya kita dapat memblokir suatu ip untuk masuk ke laptop saya melalui router dan juga kita dapat memblokir website yang kitaset pada firewall pada router yang terhubung dengan PC atau laptop, dan hasil untuk NAT sendiri adalah untuk menerjemahkan alamat IP dari jaringan lokal ke alamat IP jaringan global yang dapat diakses.

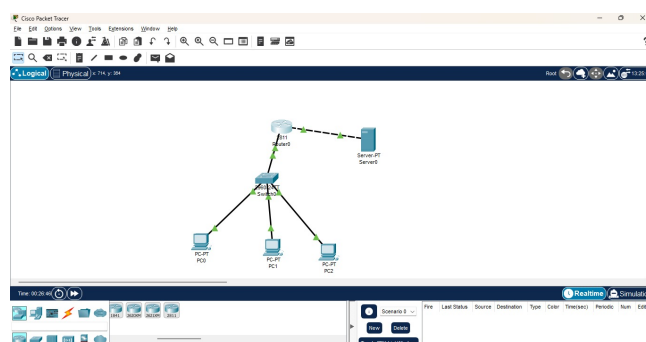
3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:

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

Jawab:

dibawah adalah topologi sederhana yang dibuat di Cisco Packet Tracer:



?figurename? 14: Tampilan topologi sederhana di Cisco Packet Tracer

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

Jawab:

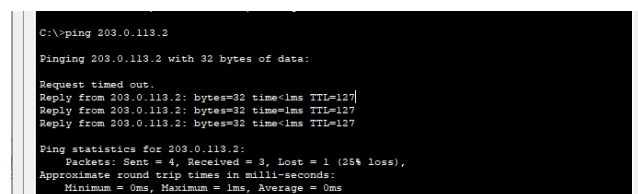
pertama atur CLI router seperti dibawah:

```
1 Router>enable
2 Router#
3 Router#configure terminal
4 Enter configuration commands, one per line. End with CNTL/Z.
5 Router\((config-if)\)#
6 Router\((config-if)\)#access-list 1 permit 192.168.10.0 0.0.0.255
7 Router\((config)\)#
8 Router\((config)\)#ip nat inside source list 1 interface FastEthernet0/1
  overload
9 Router\((config)\)#
10 Router\((config)\)#interface FastEthernet0/0
11 Router\((config-if)\)#ip nat inside
12 Router\((config-if)\)#ex
13 Router\((config)\)#interface FastEthernet0/1
14 Router\((config-if)\)#ip nat outside
15 Router\((config-if)\)#ex
16 Router\((config)\)#end
17 Router#
18 %SYS-5-CONFIG_I: Configured from console by console
19
20 Router#
21
```

Setelah itu atur IP pada PC seperti dibawah:

PC	Ip Address	Subnet Mask	Default Gateway
PC0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	192.168.10.3	255.255.255.0	192.168.10.1
PC2	192.168.10.4	255.255.255.0	192.168.10.1

dan set untuk router adalah : untuk IP Address: 203.0.113.2, Subnet mask: 255.255.255.0, Default Gateway: 203.0.113.1 (konfigurasi ini untuk nomor 1 juga). Lalu uji ping pada PC0, Pc1, dan PC2, didapat hasil pada gambar dibawah:



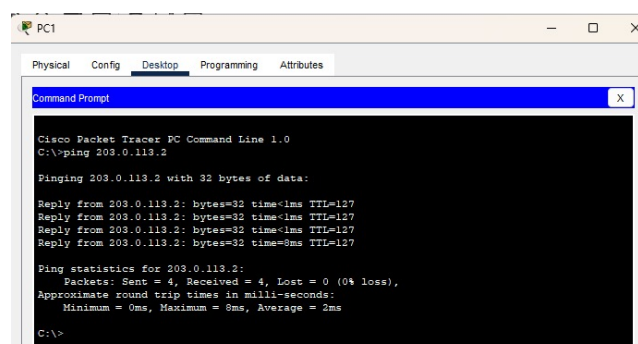
```
C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

?figurename? 15: hasil ping PC0



```
PC1
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=8ms 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 = 8ms, Average = 2ms
C:\>
```

?figurename? 16: hasil ping PC1

```

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=10ms 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 = 10ms, Average = 2ms

C:\>
  
```

?figurename? 17: hasil ping PC2

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.

Jawab:

Atur IPnya seperti ini:	PC	Ip Address	dan pada routeratur pada CLI nya seperti dibawah:
	PC0	192.168.10.10	
	PC1	192.168.10.11	
	PC2	192.168.10.12	

```

1 Router> enable
2 Router# configure terminal
3 Router(config)# access-list 100 deny ip host 192.168.10.10 host 203.0.113.2
4 Router(config)# access-list 100 deny ip host 192.168.10.11 host 203.0.113.2
5 Router(config)# access-list 100 permit ip any any
6 Router(config)# interface FastEthernet0/1
7 Router(config-if)# ip access-group 100 out
8 Router(config-if)# exit
9 Router(config)# end
10
  
```

pada pengujian saya set pc2 saja yang bisa akses tetapi PC1 bisa entah kenapa tetapi pada konfigurasi sebelumnya harusnya PC1 bisa ter blokir dilihat pada gambar dibawah:

```

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=10ms 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 = 10ms, Average = 2ms

C:\>ping 203.0.113.2

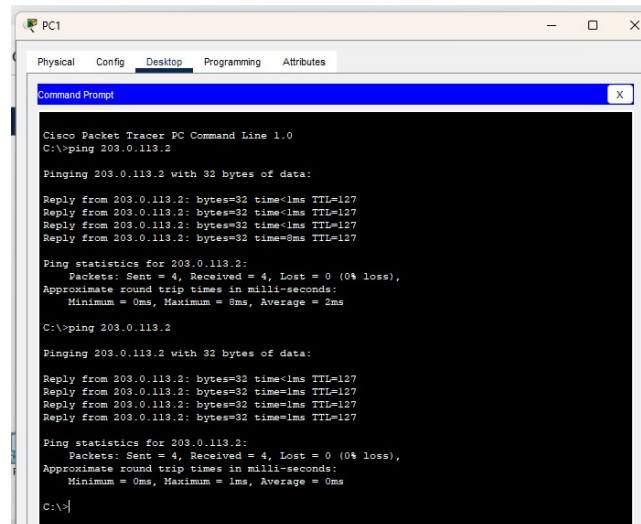
Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time=1ms TTL=127
Reply from 203.0.113.2: bytes=32 time=5ms 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 = 5ms, Average = 1ms

C:\>
  
```

?figurename? 18: Tampilan ping pada PC2



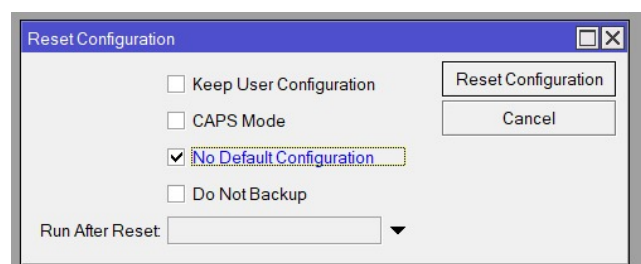
?figurename? 19: Tampilan ping pada PC1

4 Kesimpulan

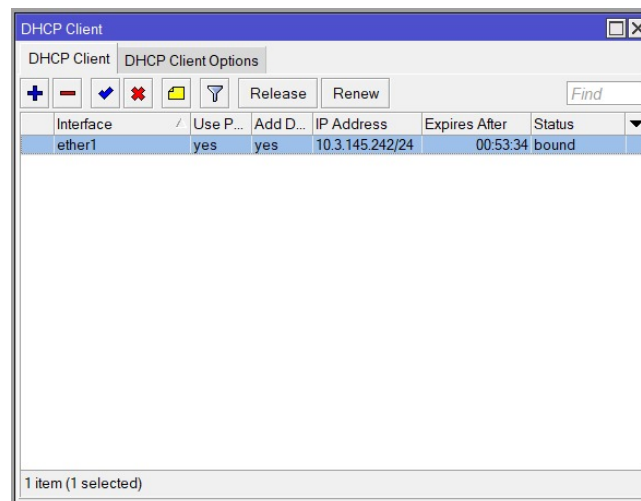
Dari percobaan yang telah dilakukan, dapat disimpulkan bahwa konfigurasi dasar pada router Mikrotik seperti DHCP, NAT, dan Firewall berhasil diterapkan. DHCP memungkinkan otomatisasi pemberian alamat IP kepada perangkat di jaringan lokal. Konfigurasi NAT memungkinkan koneksi perangkat lokal ke internet dengan menerjemahkan IP lokal menjadi IP publik. Sedangkan firewall berhasil digunakan untuk memblokir trafik ICMP (seperti ping) dan akses ke situs tertentu berdasarkan konten. Dalam tugas simulasi menggunakan Cisco Packet Tracer, topologi jaringan berhasil dibangun dan diuji. Konfigurasi NAT berhasil membuat seluruh PC dapat mengakses server menggunakan IP publik router. Selain itu, firewall berbasis ACL berhasil digunakan untuk mengatur akses ke server, termasuk mengizinkan atau memblokir PC tertentu tanpa mengganggu komunikasi antar PC di jaringan lokal. Hal ini menunjukkan pemahaman dasar yang baik dalam pengelolaan jaringan dan keamanan melalui konfigurasi router.

5 Lampiran

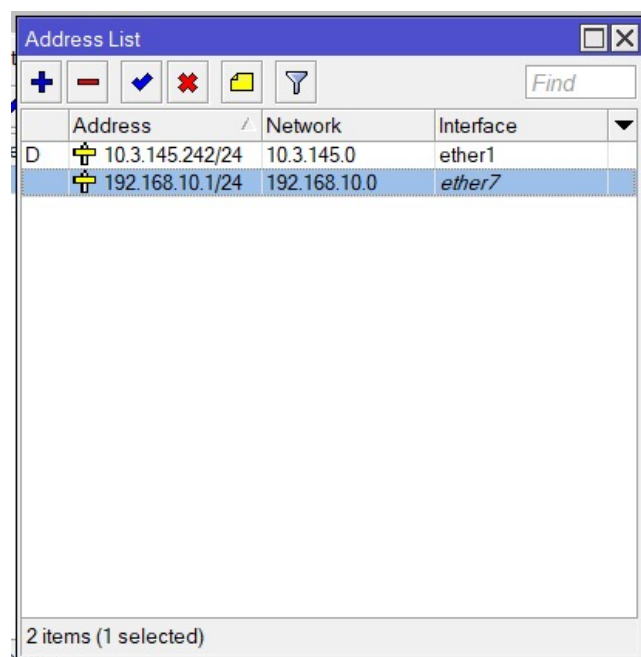
5.1 Dokumentasi saat praktikum



?figurename? 20: Lampiran



?figurename? 21: Lampiran



?figurename? 22: Lampiran

NAT Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ☐

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

?figurename? 23: Lampiran

NAT Rule <>

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

To Ports:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

enabled

?figurename? 24: Lampiran

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol: ☐ 1 (icmp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐ ether7

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

?figurename? 25: Lampiran

Firewall Rule <>

General Advanced Extra Action Statistics

Action: **drop**

☐ Log

Log Prefix:

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

?figurename? 26: Lampiran

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 80,443

Any. Port:

In. Interface: ☐ ether7

Out. Interface: ☐ ether1

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

?figurename? 27: Lampiran

Firewall Rule <80,443>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content: ☐ speedtest

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy:

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

?figurename? 28: Lampiran

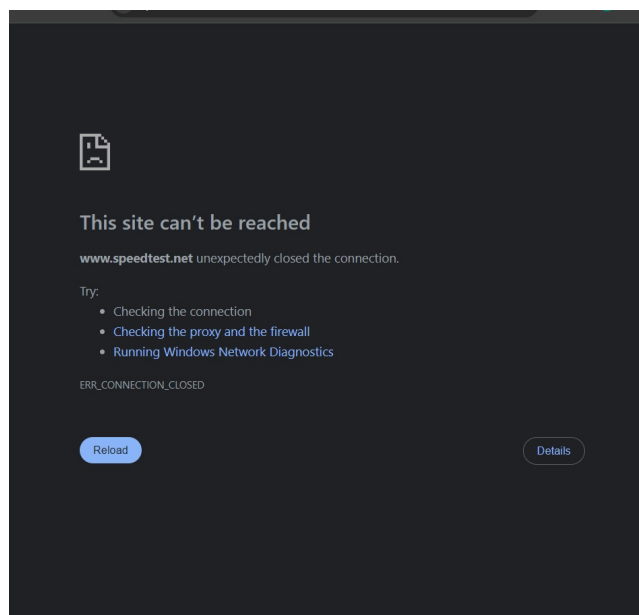

```

Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    ^C
C:\Users\USER>ping 8.8.8.8 -t

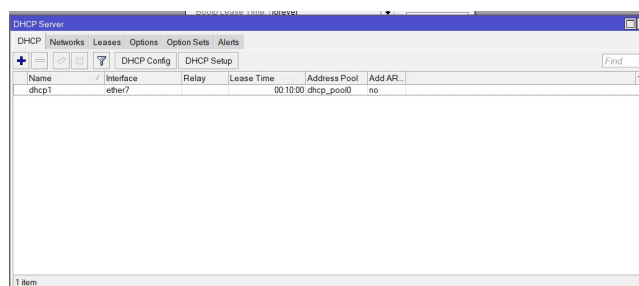
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms 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
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112

```

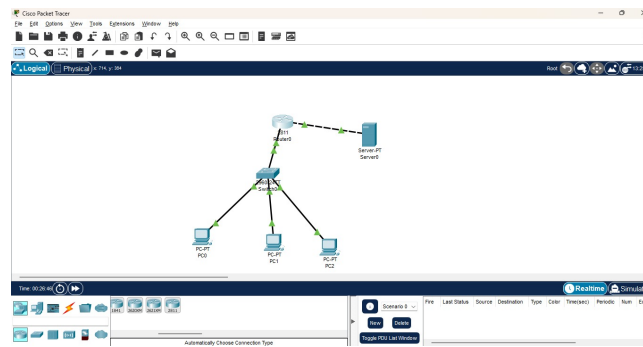
?figurename? 31: Lampiran



?figurename? 32: Lampiran



?figurename? 33: Lampiran



?figurename? 34: Lampiran

```
C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

?figurename? 35: Lampiran

PC1

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=4ms TTL=127
Reply from 203.0.113.2: bytes=32 time=4ms TTL=127
Reply from 203.0.113.2: bytes=32 time=4ms TTL=127
Reply from 203.0.113.2: bytes=32 time=4ms 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 = 4ms, Maximum = 4ms, Average = 4ms

C:\>
```

?figurename? 36: Lampiran

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.2

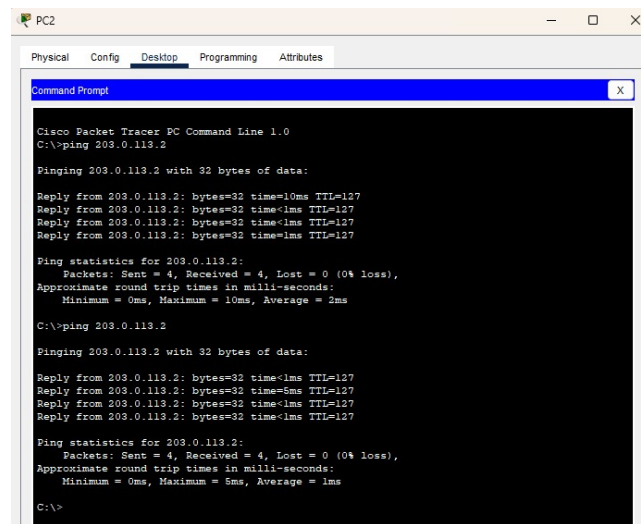
Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time=10ms 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 = 10ms, Average = 2ms

C:\>
```

?figurename? 37: Lampiran



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=10ms 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 = 10ms, Average = 2ms

C:\>ping 203.0.113.2

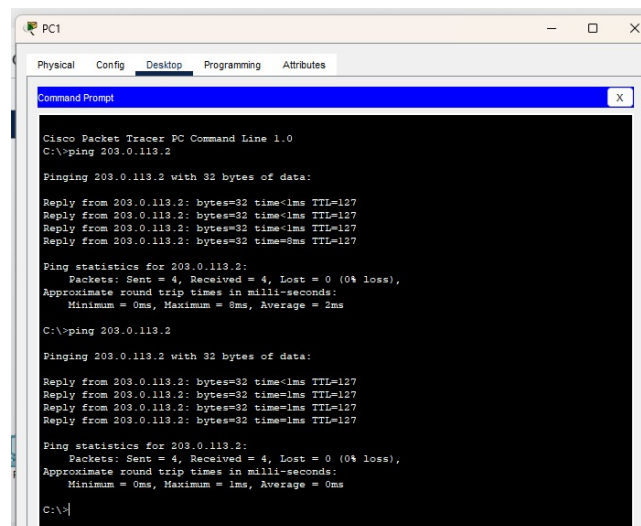
Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time=1ms TTL=127
Reply from 203.0.113.2: bytes=32 time=5ms 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 = 5ms, Average = 1ms

C:\>
```

?figurename? 38: Lampiran



PC1

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=8ms 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 = 8ms, Average = 2ms

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 = 1ms, Average = 0ms

C:\>]
```

?figurename? 39: Lampiran