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

Laporan Akhir
Praktikum Jaringan Komputer

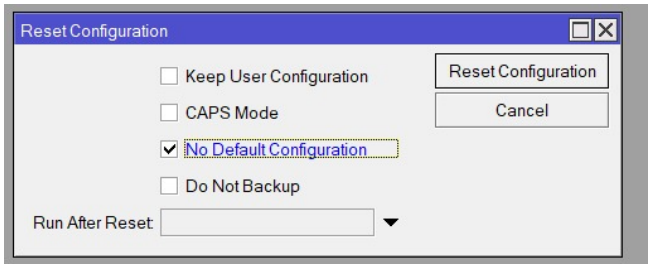
Firewall NAT

Moh. wildan Risqi Maulidi - 5024231056

2025

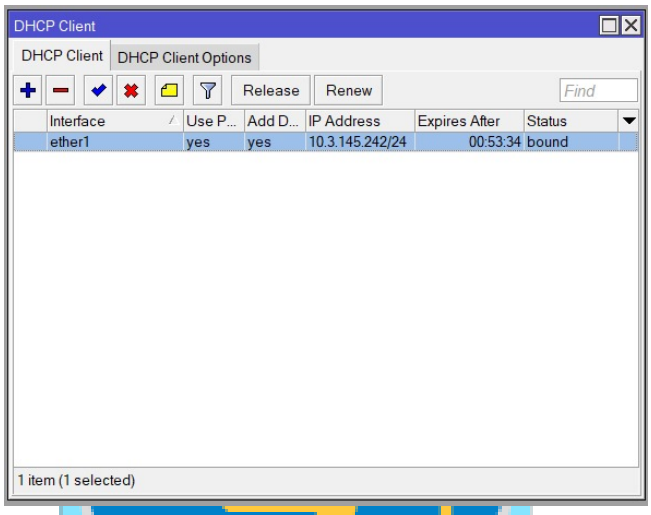
1 Langkah-Langkah Percobaan

- Reset router lalu login kembali

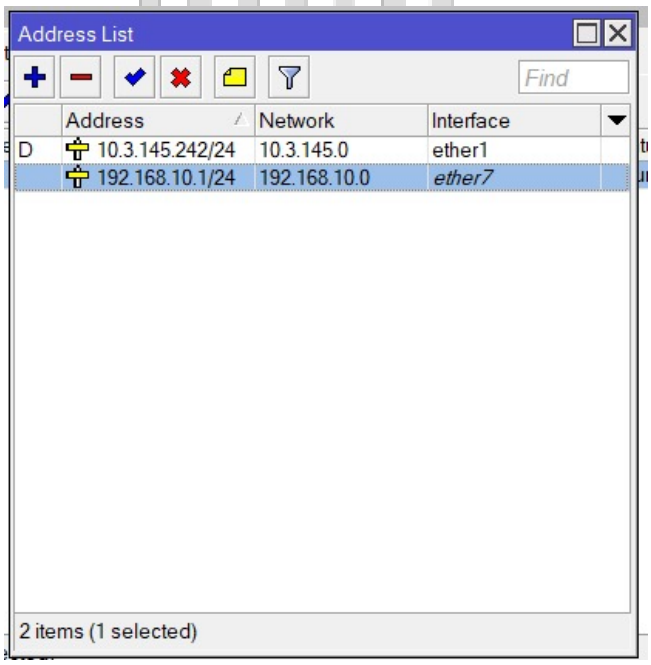


?figurename? 1: Tampilan reset

- 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 konesi menunjukkan bound.

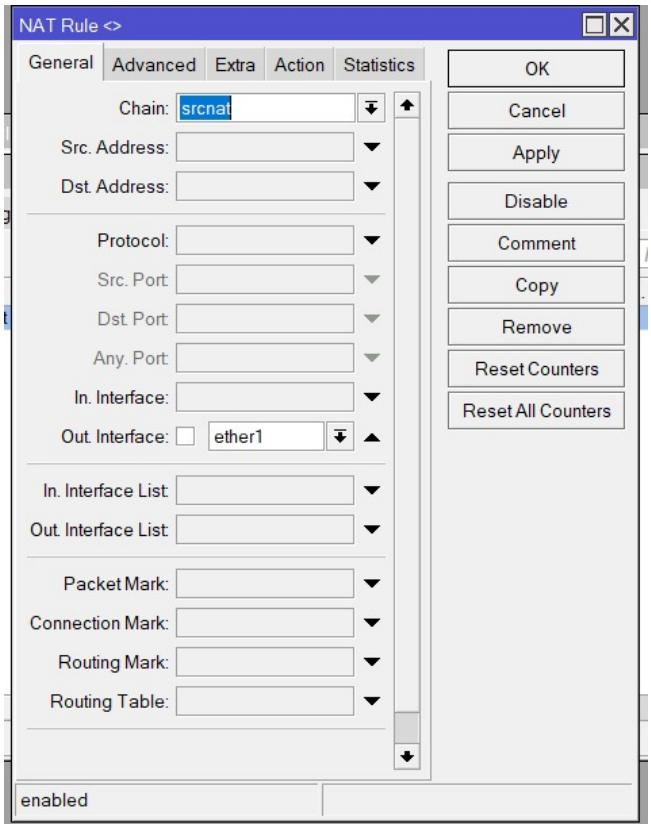


?figurename? 2: Tampilan konfigurasi DHCP server dan Client

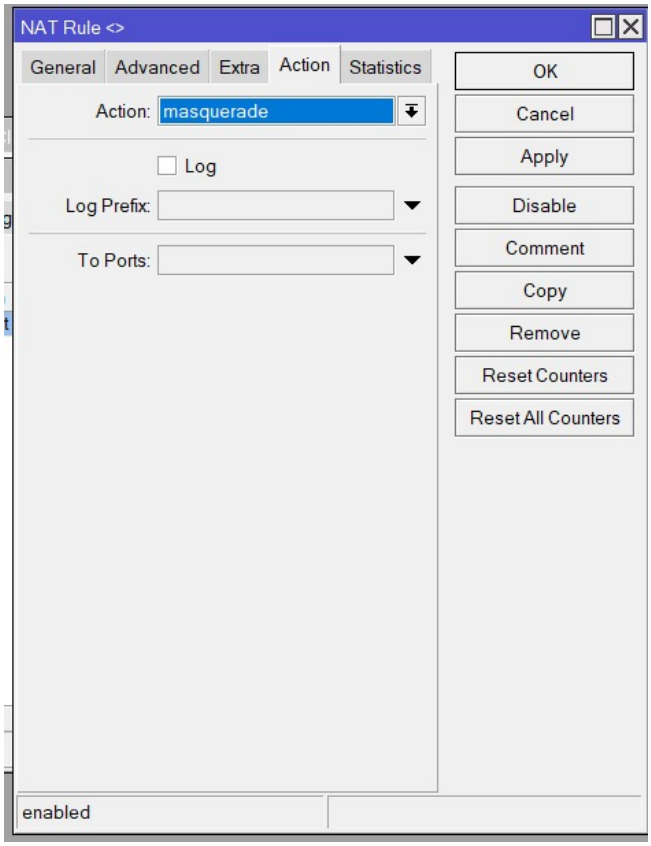


?figurename? 3: Tampilan Address list

- 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.

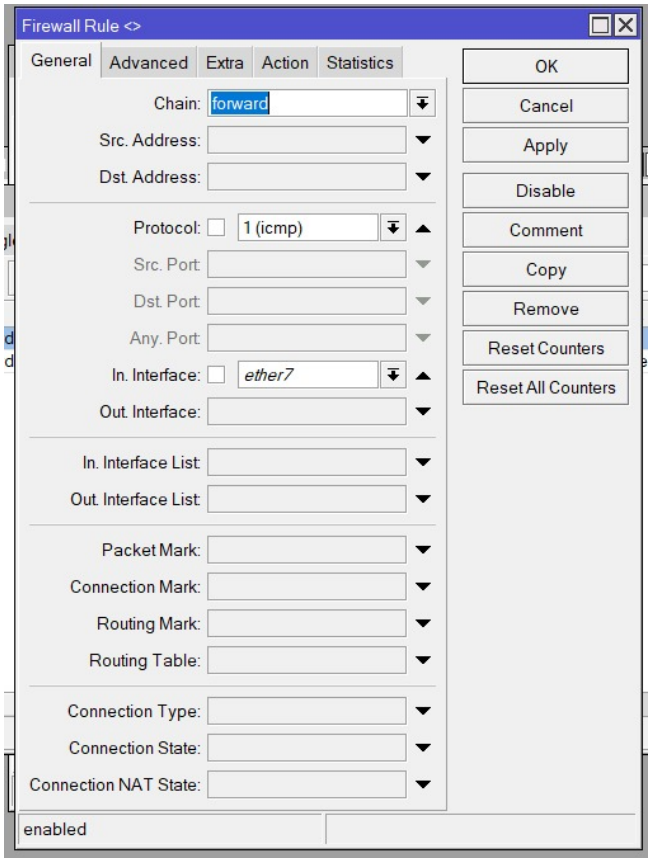


?figurename? 4: Tampilan konfigurasi NAT bagiam general

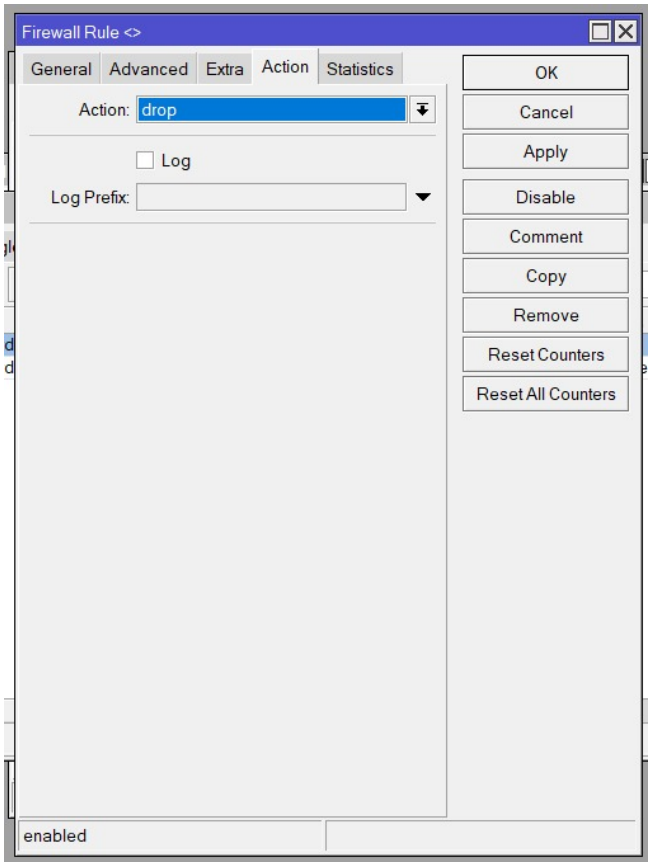


?figurename? 5: Tampilan konfigurasi NAT bagian action

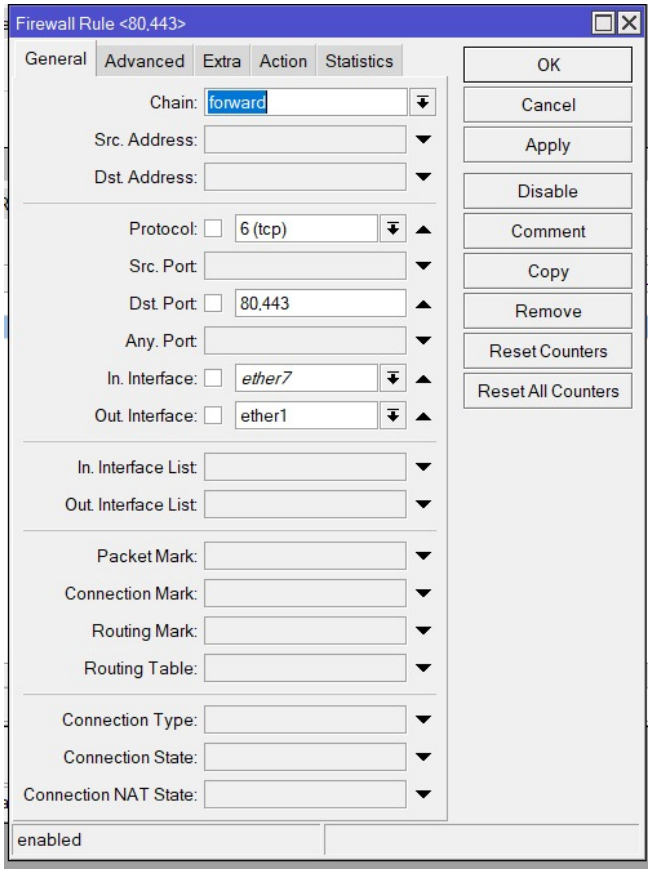
- Konfigurasi firewall pada router Mikrotik, pergi pada menu IP lalu ke Firewall dan ke Filter Rules dan tambah untuk menambahkan aturan baru, pada tab tersebut atur chain ke **forward** dan pada tab general juga atur protocol **icmp** dan general atur in untuk interface "ether7" konfigurasi ini untuk 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.



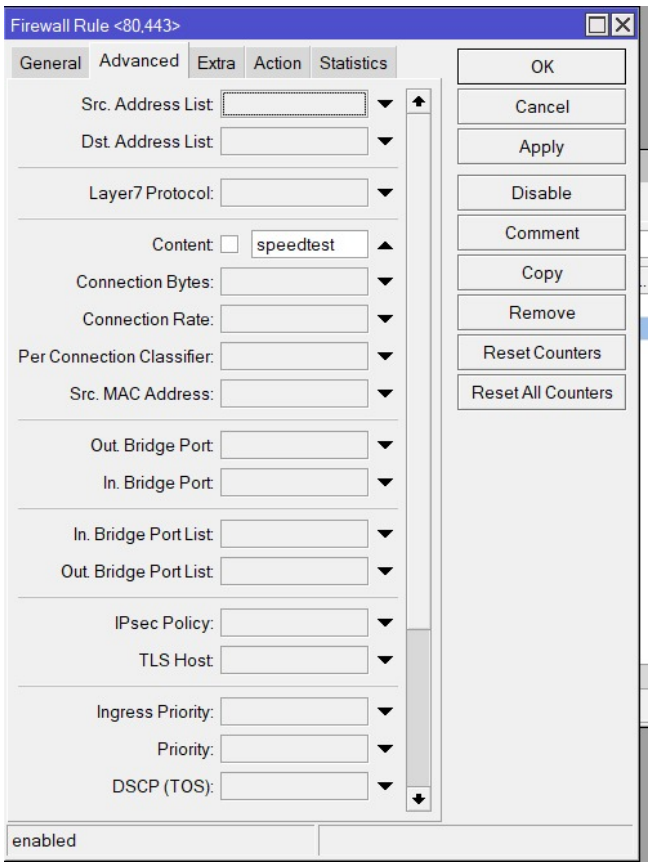
?figurename? 6: Tampilan konfigurasi firewall bagian general



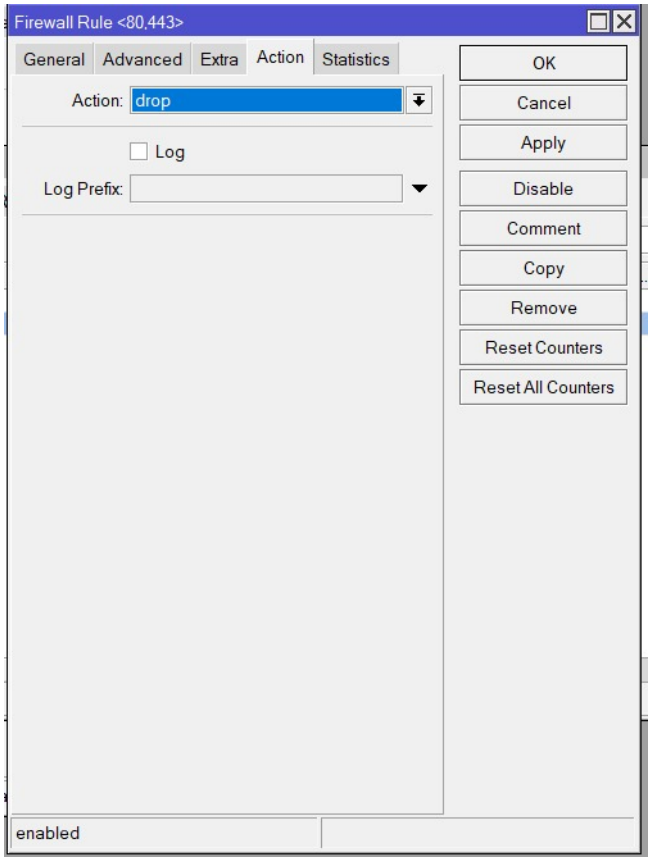
?figurename? 7: Tampilan konfigurasi firewall bagian action



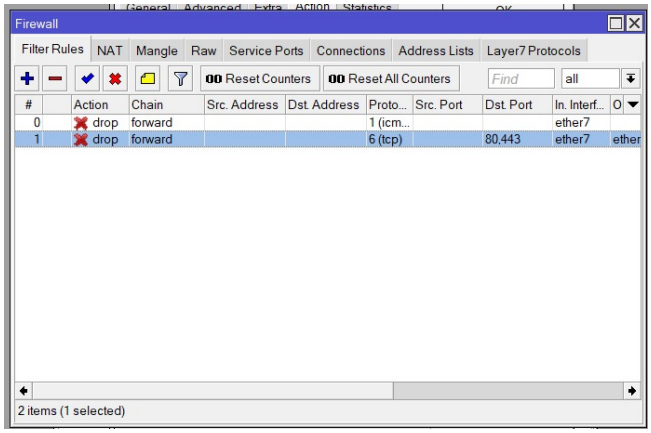
?figurename? 8: Tampilan konfigurasi firewall bagian general untuk port 80,443



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

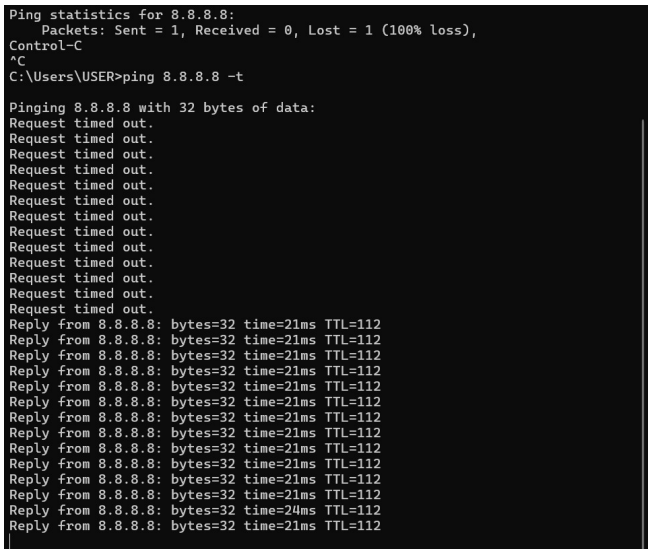


?figurename? 10: Tampilan konfigurasi firewall bagian action untuk port 80,443



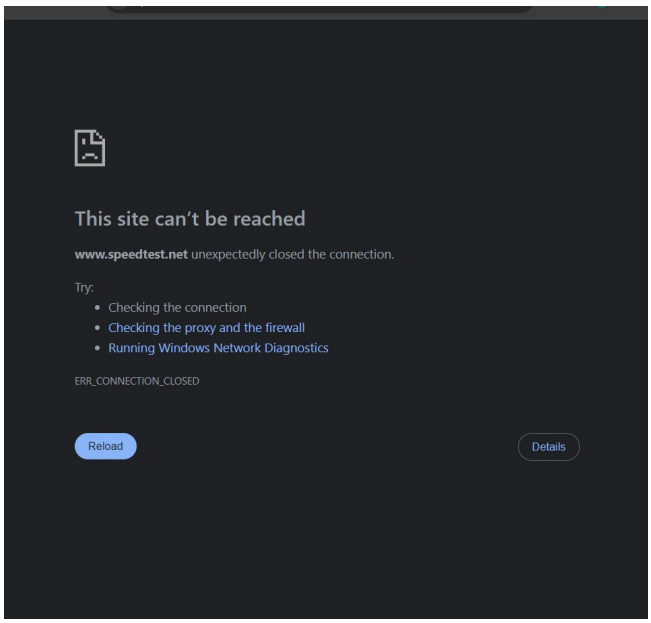
?figurename? 11: Tampilan konfigurasi firewall filter rules

- 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.



?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

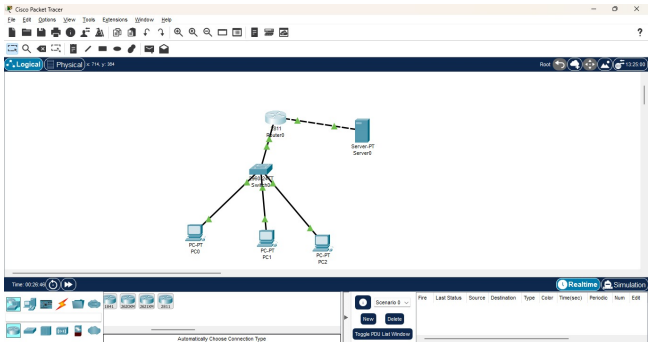
2 Analisis Hasil Percobaan

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 hasul untukNAT sendiri adalah untuk menerjemahkan alamat IP dari jaringan lokal ke alamatIP 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

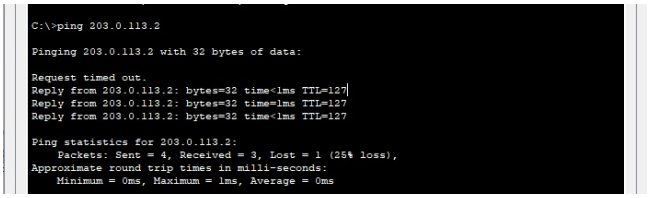
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
   Jawab:
   pertama atur CLI router seperti dibawah:

```
        Router>enable
        Router#
        Router#configure terminal
        Enter configuration commands, one per line.  End with CNTL/Z.
        Router\(config-if\)#
        Router\(config-if\)#access-list 1 permit 192.168.10.0 0.0.0.255
        Router\(config\)#
        Router\(config\)#ip nat inside source list 1 interface FastEthernet0/1
    overload
        Router\(config\)#
        Router\(config\)#interface FastEthernet0/0
        Router\(config-if\)#ip nat inside
        Router\(config-if\)#ex
        Router\(config\)#interface FastEthernet0/1
        Router\(config-if\)#ip nat outside
        Router\(config-if\)#ex
        Router\(config\)#end
        Router#
        %SYS-5-CONFIG_I: Configured from console by console

        Router#

```

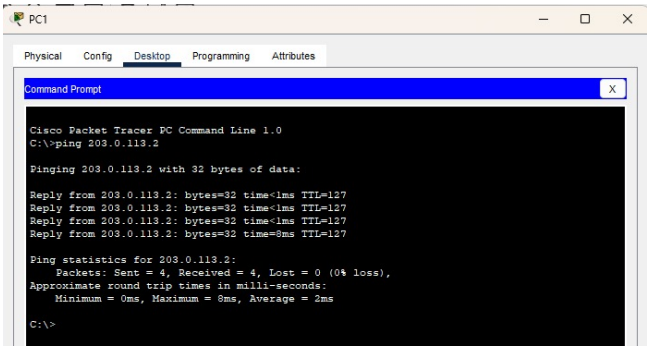
Setelah itu atur IP pada PC seperti dibawah:

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

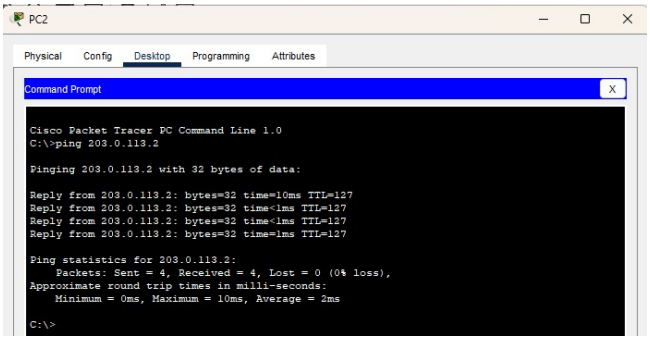
dan set untuk router adalah : untuk IP Address: 203.0.113.2, Subnet mask: 255.255.255.0, Default Gateway: 203.0.113.1 (konfigurasi ini untuk nomor 1 juga). Lalu uji ping pada PC0, Pc1, dan PC2, didapat hasil pada gambar dibawah:



?figurename? 15: hasil ping PC0



?figurename? 16: hasil ping PC1



?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:

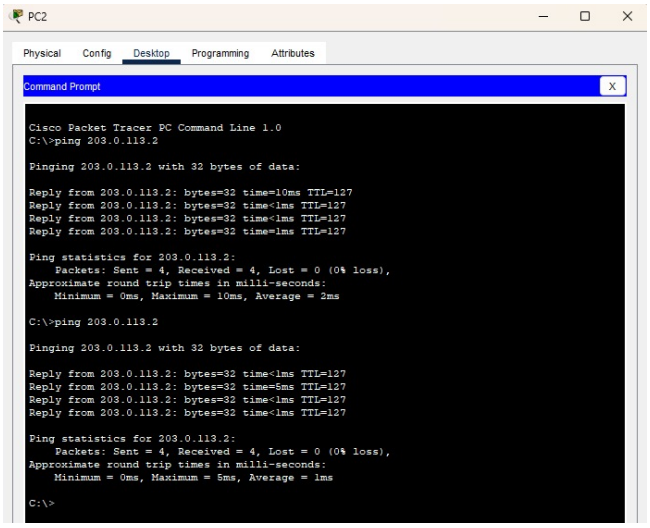
Atur IPnya seperti ini:

PC	Ip Address
PC0	192.168.10.10
PC1	192.168.10.11
PC2	192.168.10.12

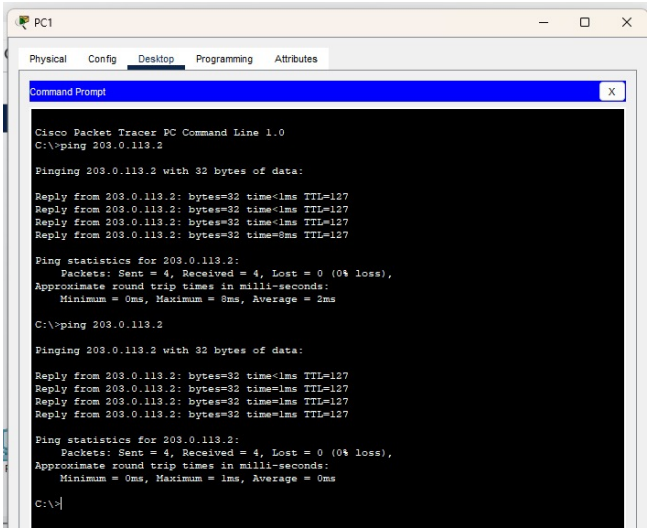
dan pada routeratur pada CLI nya seperti dibawah:

```
Router> enable
Router# configure terminal
Router(config)# access-list 100 deny ip host 192.168.10.10 host 203.0.113.2
Router(config)# access-list 100 deny ip host 192.168.10.11 host 203.0.113.2
Router(config)# access-list 100 permit ip any any
Router(config)# interface FastEthernet0/1
Router(config-if)# ip access-group 100 out
Router(config-if)# exit
Router(config)# end

```

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:



?figurename? 18: Tampilan ping pada PC2



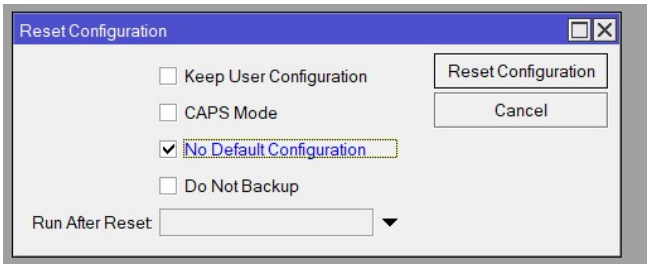
?figurename? 19: Tampilan ping pada PC1

4 Kesimpulan

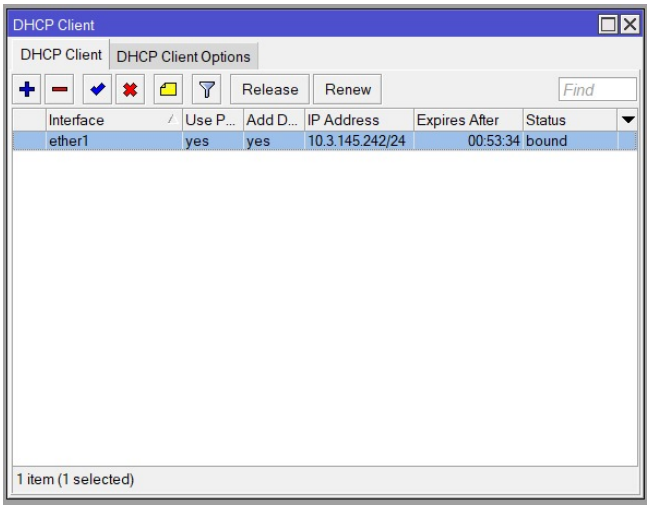
Dari percobaan yang telah dilakukan, dapat disimpulkan bahwa konfigurasi dasar pada router Mikrotik seperti DHCP, NAT, dan Firewall berhasil diterapkan. DHCP memungkinkan otomatisasi pemberian alamat IP kepada perangkat di jaringan lokal. Konfigurasi NAT memungkinkan koneksi perangkat lokal ke internet 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

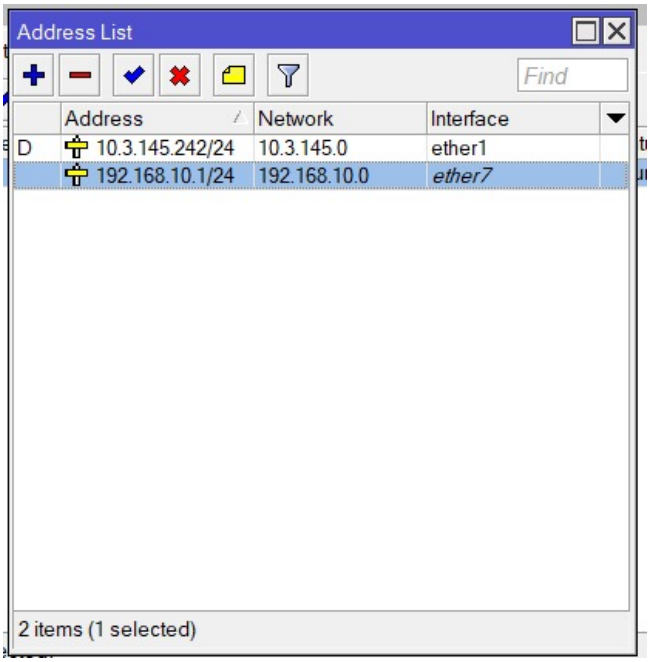
5.1 Dokumentasi saat praktikum



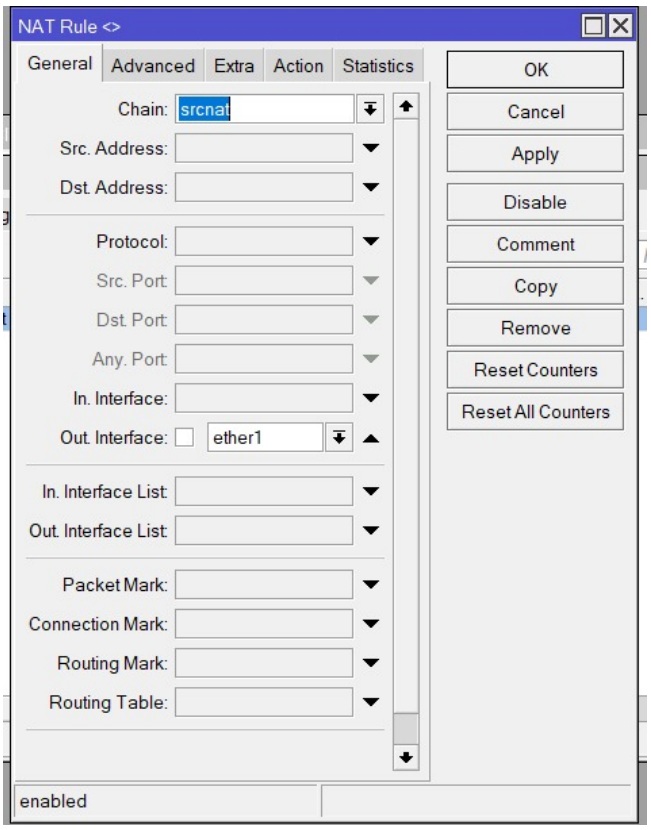
?figurename? 20: Lampiran



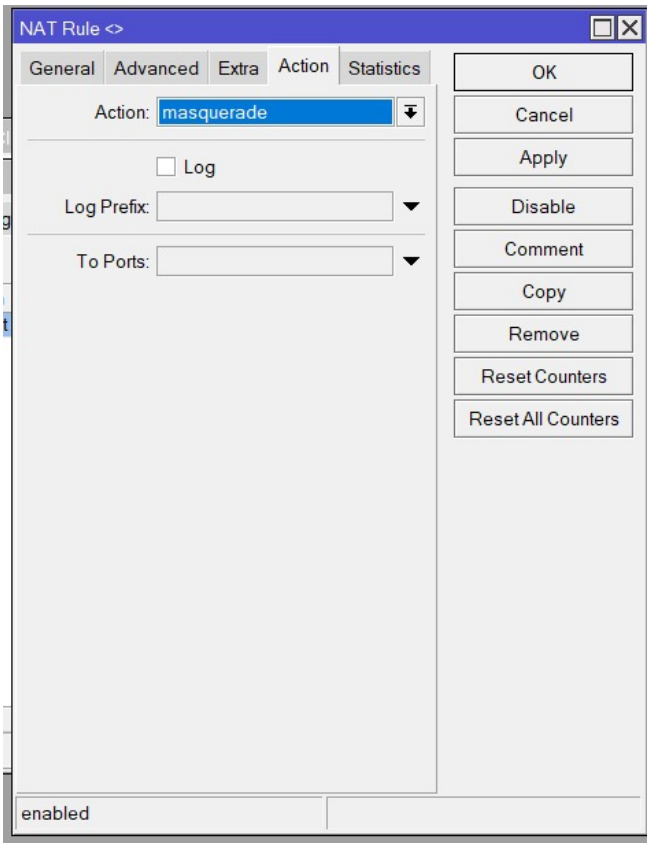
?figurename? 21: Lampiran



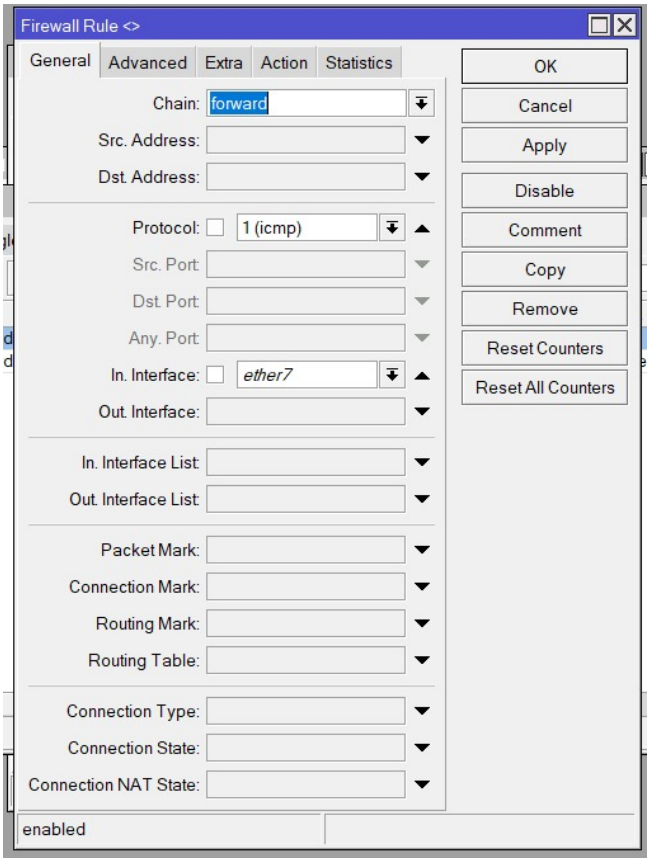
?figurename? 22: Lampiran



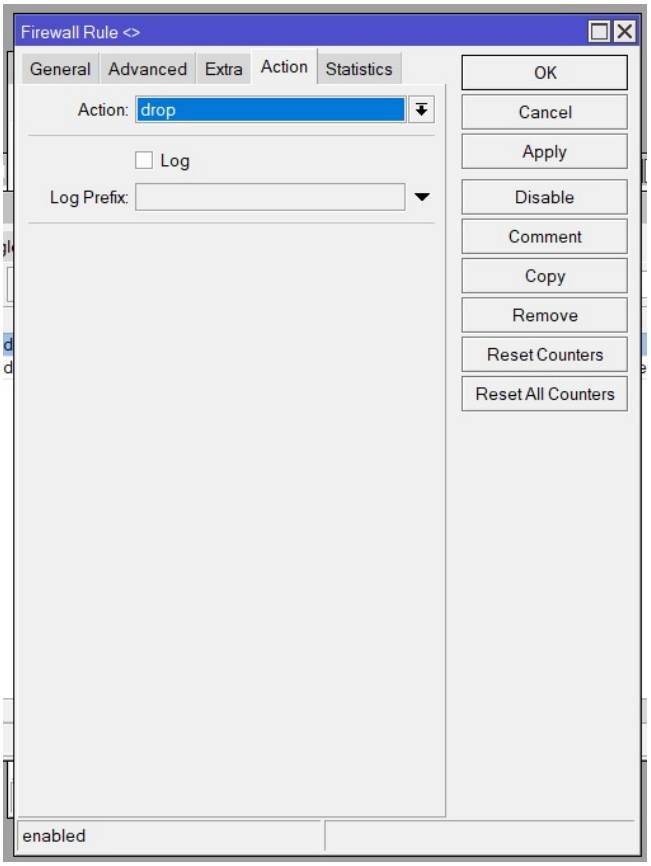
?figurename? 23: Lampiran



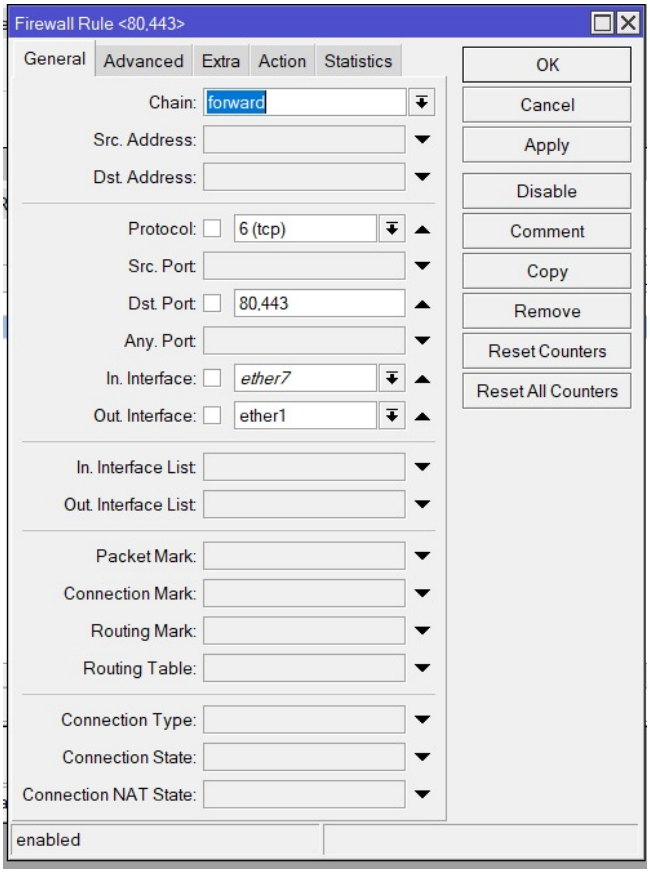
?figurename? 24: Lampiran



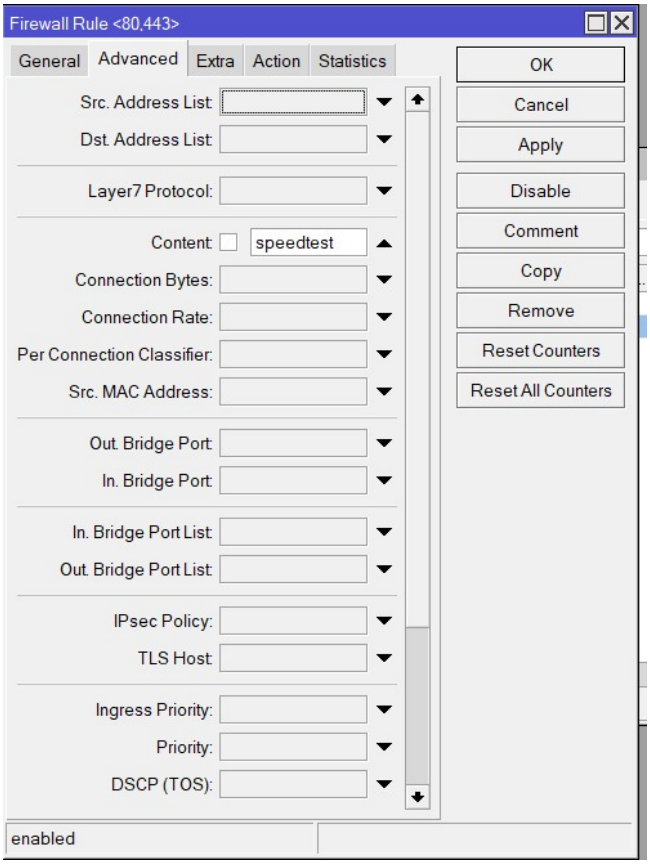
?figurename? 25: Lampiran



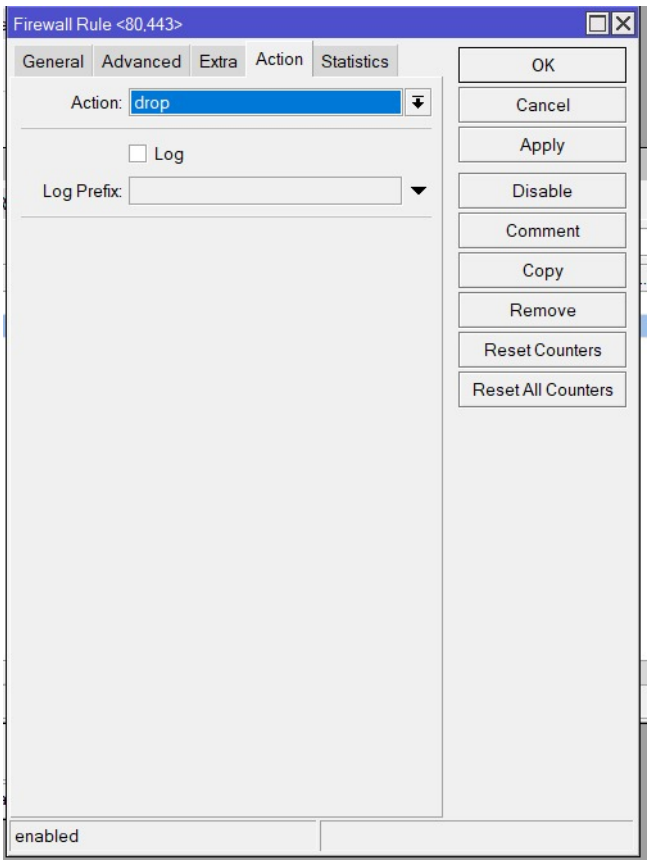
?figurename? 26: Lampiran



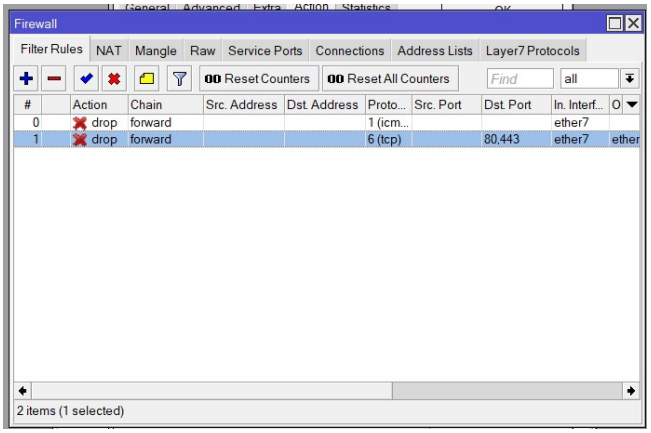
?figurename? 27: Lampiran



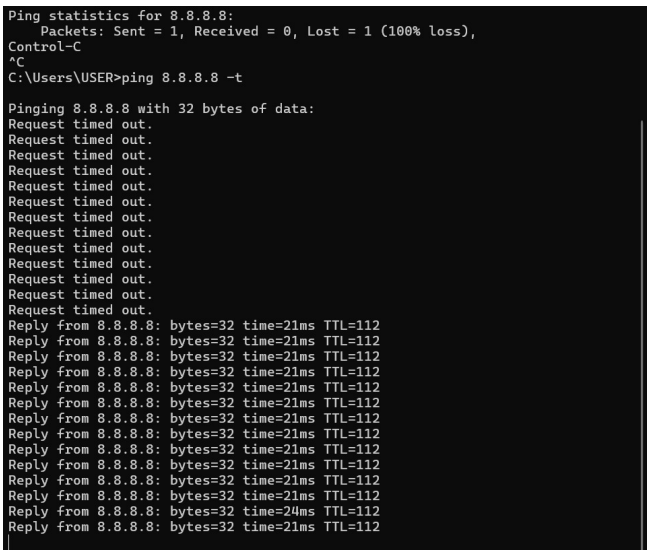
?figurename? 28: Lampiran



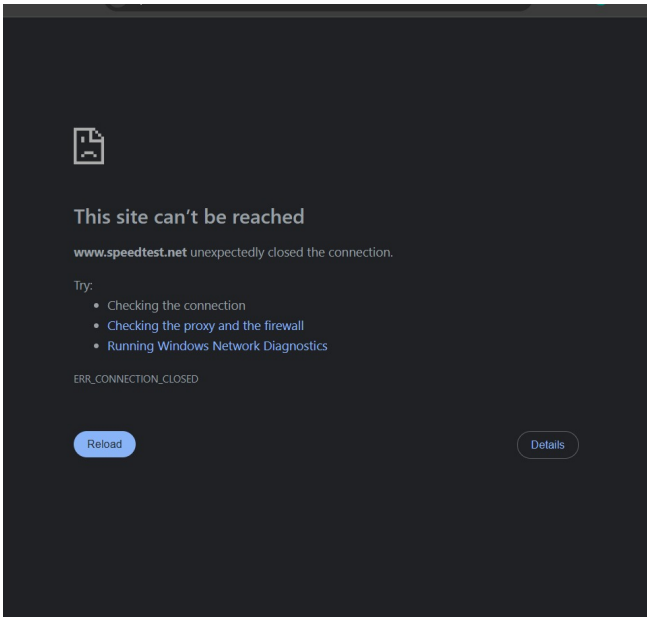
?figurename? 29: Lampiran



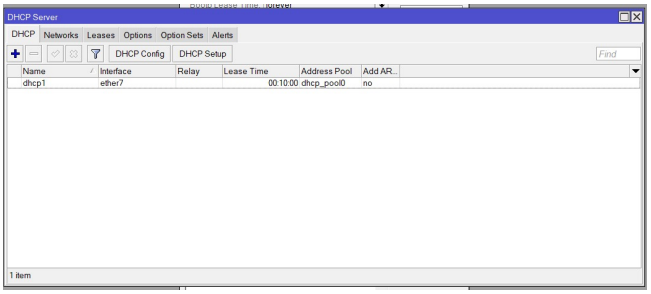
?figurename? 30: Lampiran



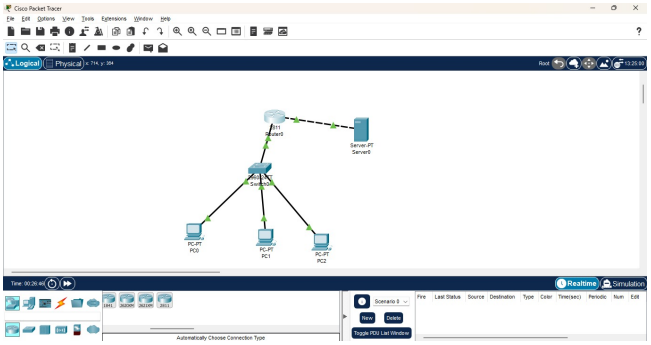
?figurename? 31: Lampiran



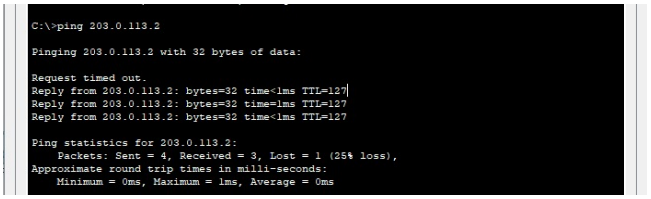
?figurename? 32: Lampiran



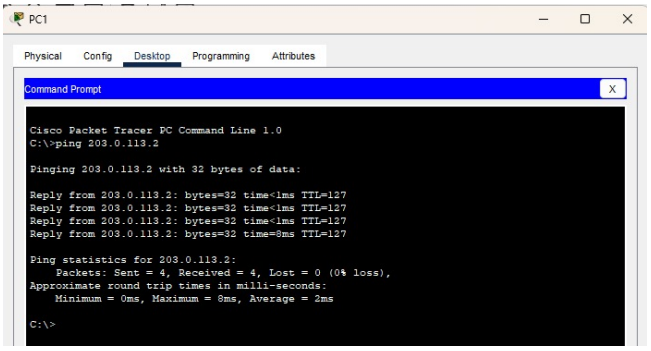
?figurename? 33: Lampiran



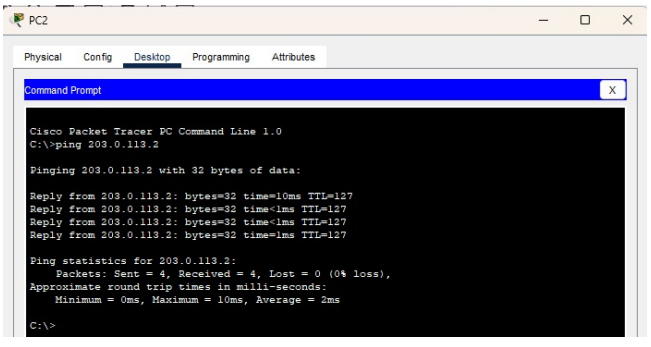
?figurename? 34: Lampiran



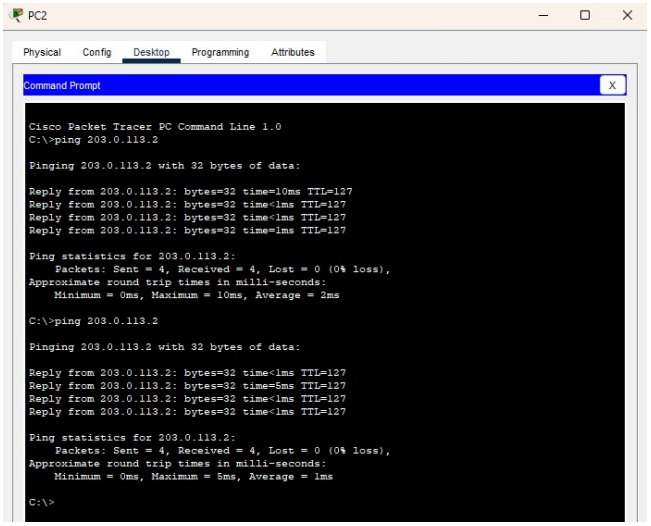
?figurename? 35: Lampiran



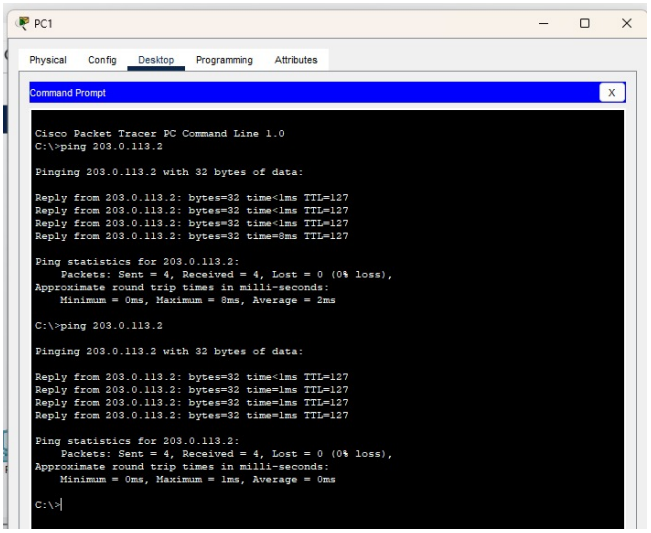
?figurename? 36: Lampiran



?figurename? 37: Lampiran



?figurename? 38: Lampiran



?figurename? 39: Lampiran