Praktikum Jaringan Komputer

NRP	:	3223600017
Nama	:	Muhammad Alfarrel Arya Mahardika
Materi	:	Extended Access Control List
Tanggal	:	16 April 2025

1. Tujuan
   1.1. Mahasiswa mampu melakukan konfigurasi extended Access Control List (ACL) pada router
   1.2. Mahasiswa mampu menjelaskan konsep extended Access Control List (ACL)
   1.3. Mahasiswa mampu menerapkan ACL pada suatu jaringan

2. Dasar Teori

Standard Access Control List (ACL) adalah salah satu jenis kontrol akses yang digunakan dalam pengelolaan jaringan komputer, khususnya pada perangkat router. ACL berfungsi sebagai filter lalu lintas jaringan yang bekerja berdasarkan alamat IP sumber (*source IP address*). Dengan menggunakan ACL, administrator jaringan dapat mengizinkan atau menolak paket data untuk melewati suatu antarmuka jaringan, bergantung pada kebijakan keamanan atau kebutuhan pengelolaan lalu lintas.

Standard ACL tergolong paling sederhana dibandingkan jenis ACL lainnya, karena hanya mempertimbangkan alamat IP sumber tanpa melihat jenis protokol atau port tujuan. Biasanya, ACL jenis ini diberi nomor dari 1 hingga 99 dalam sistem penomoran standar, atau 1300 hingga 1999 dalam format yang diperluas (*expanded range*). Karena keterbatasan ini, standard ACL biasanya ditempatkan sedekat mungkin dengan *destination* (tujuan) untuk menghindari pemblokiran awal terhadap trafik yang mungkin dibutuhkan oleh jaringan.

Saat sebuah paket data melewati router yang memiliki ACL, router akan mencocokkan alamat IP sumber dari paket tersebut dengan entri-entri yang ada dalam ACL. Jika ditemukan kecocokan dan perintahnya adalah *permit*, maka paket akan diteruskan; sebaliknya, jika perintahnya *deny*, maka paket dibuang. Jika tidak ada kecocokan sama sekali, maka router akan menerapkan *implicit deny*, yaitu secara otomatis menolak paket tersebut.

Standard ACL biasanya digunakan untuk aplikasi dasar seperti membatasi akses ke jaringan internal dari IP tertentu atau mengatur lalu lintas yang boleh keluar dari suatu subnet. Implementasi Standard ACL dilakukan melalui konfigurasi pada router menggunakan perintah di mode konfigurasi global, kemudian diaktifkan pada interface tertentu dalam mode *inbound* atau *outbound*. Contohnya, ACL bisa digunakan untuk memblokir akses dari IP tertentu ke jaringan administratif.

Keunggulan utama Standard ACL adalah kesederhanaan dan kemudahan implementasinya, menjadikannya solusi yang cepat untuk kebutuhan kontrol lalu lintas dasar. Namun, karena hanya berdasarkan IP sumber, penggunaannya menjadi terbatas untuk skenario yang memerlukan kontrol lebih mendalam, seperti membedakan jenis layanan (web, email, FTP). Untuk kebutuhan tersebut, Extended ACL lebih direkomendasikan karena memiliki fleksibilitas yang lebih tinggi dalam menyaring trafik berdasarkan banyak parameter.

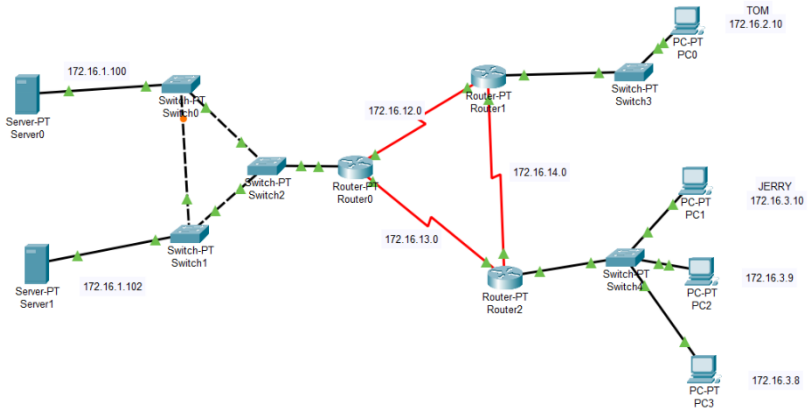
3. Prosedur

3.1. Buatlah topologi BGP menggunakan simulator Packet Tracer, dimana perangkat yang dibutuhkan yaitu:

a. End devices: PC

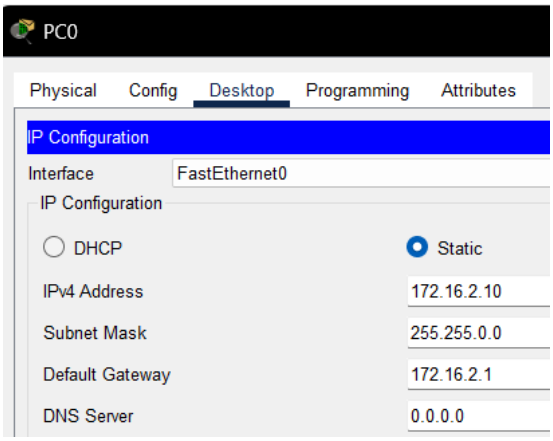
b. Network devices: Switch, Router

c. Connections: Copper Straight-Through, Copper Cross-Over, Serial DCE

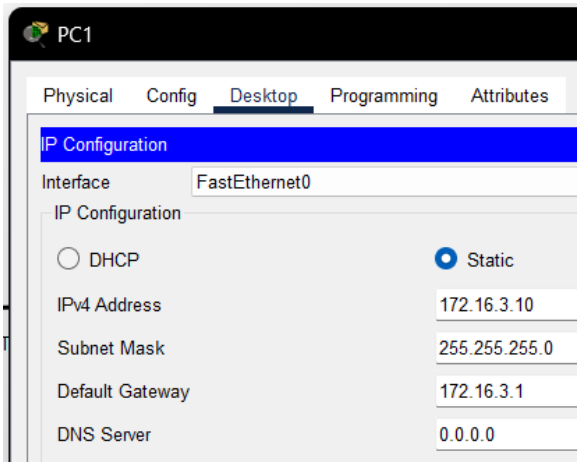


3.2. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

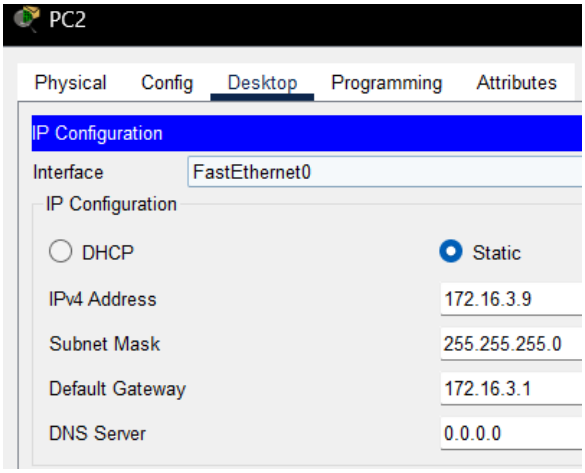
a. PC 0



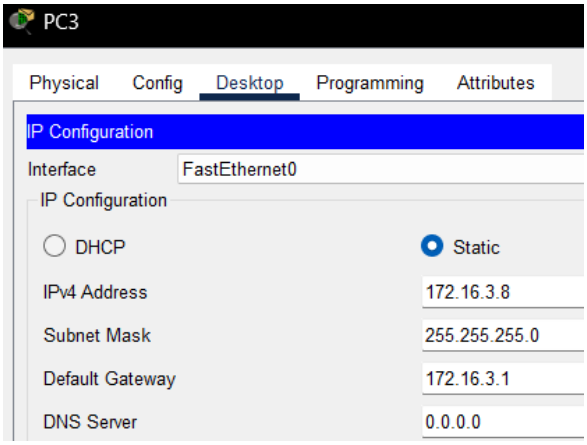
b. PC 1



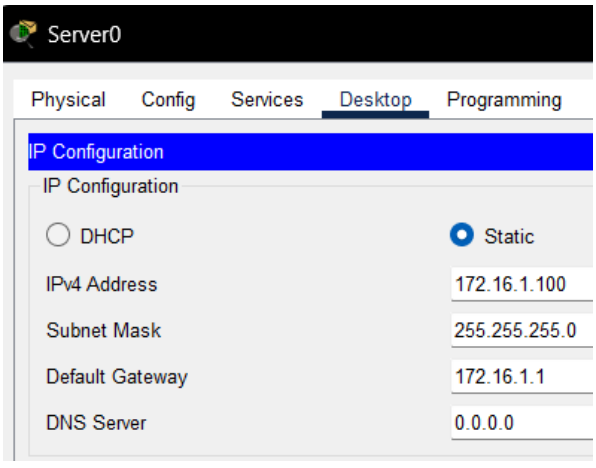
c. PC 2



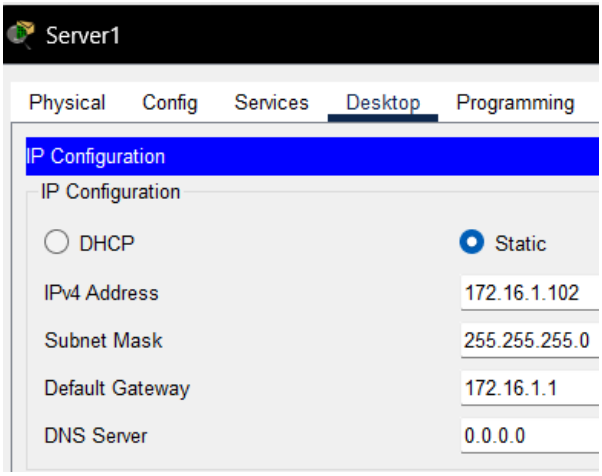
d. PC 3



e. Server 0

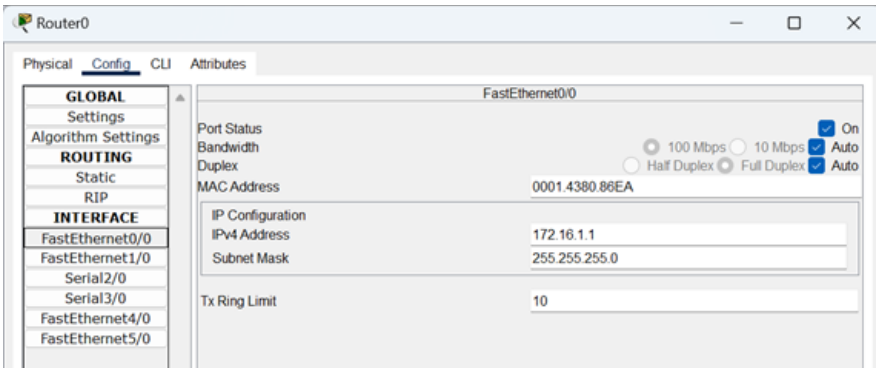


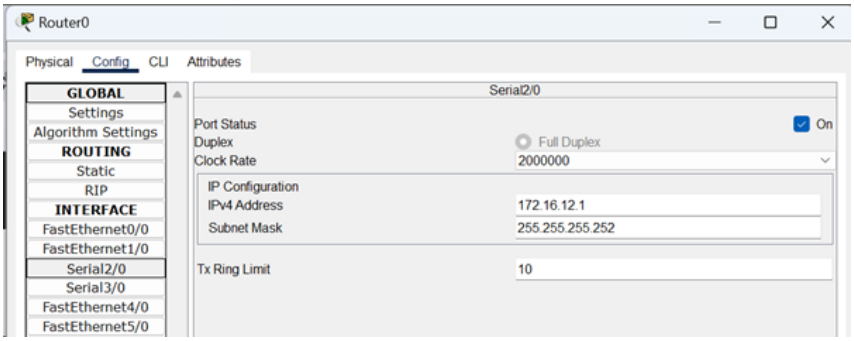
f. Server 1

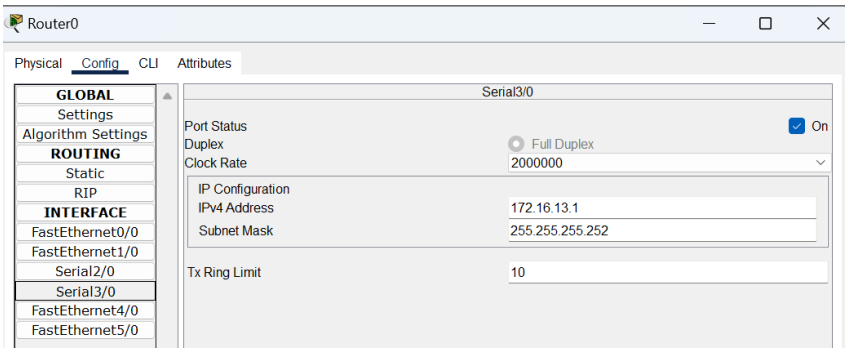


3.3. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

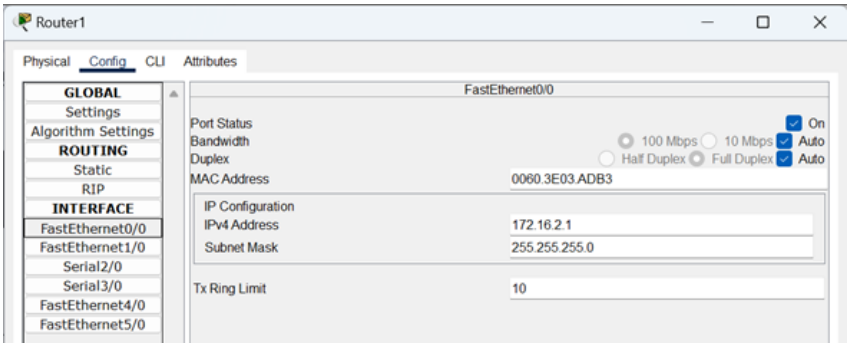
a. Router 0

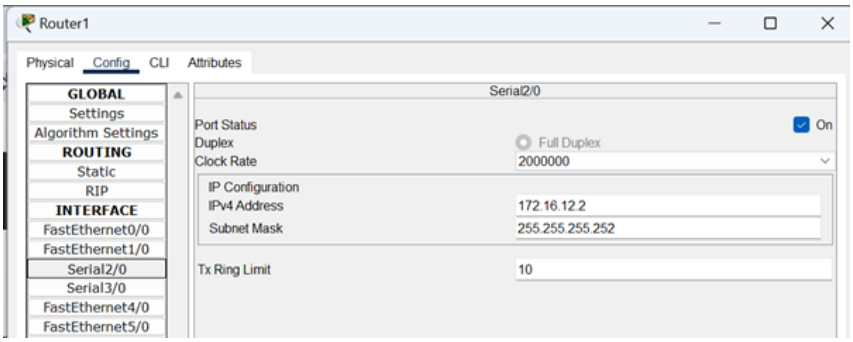


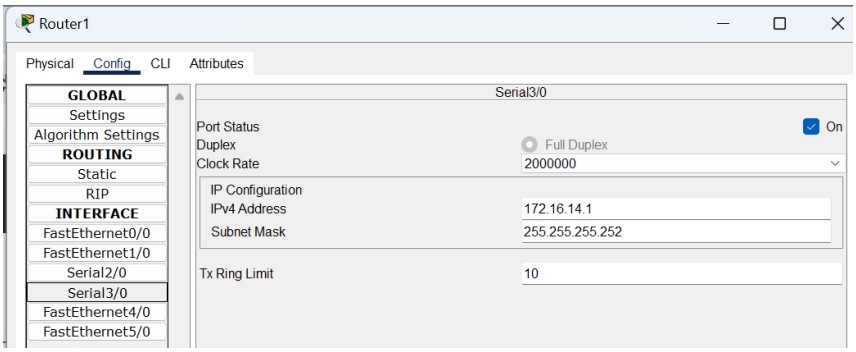




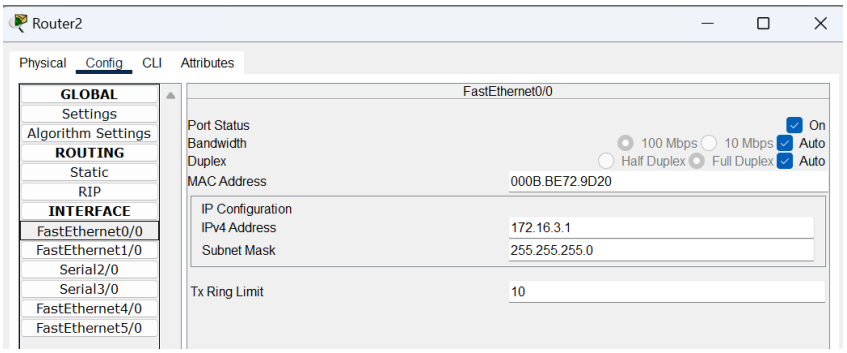
b. Router 1

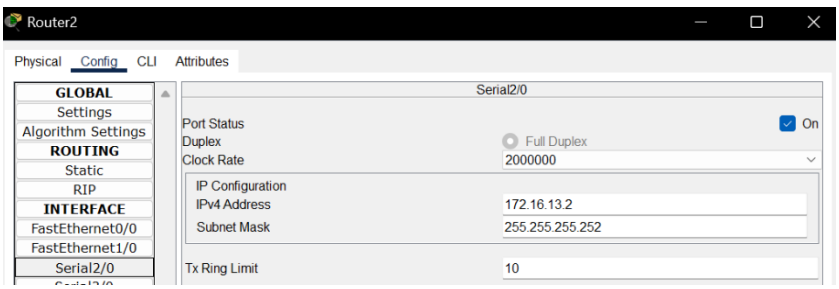


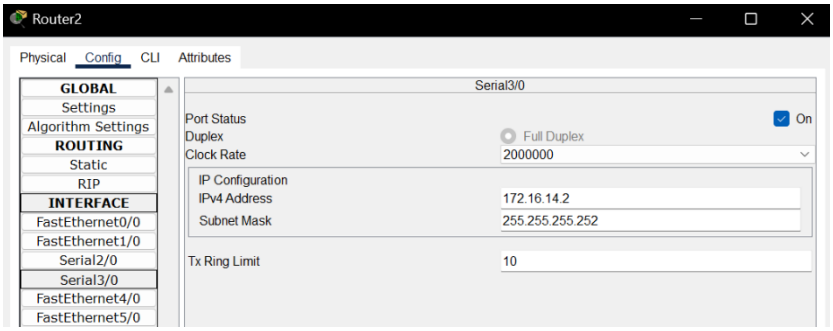




c. Router 2

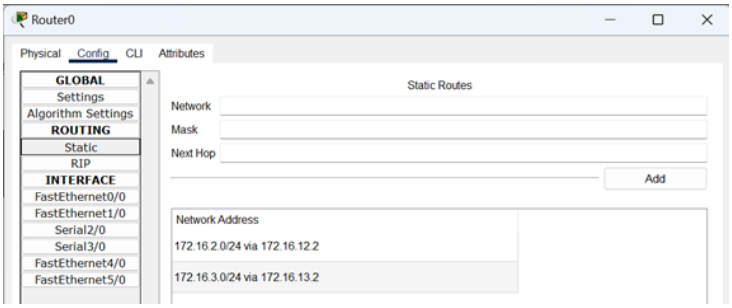




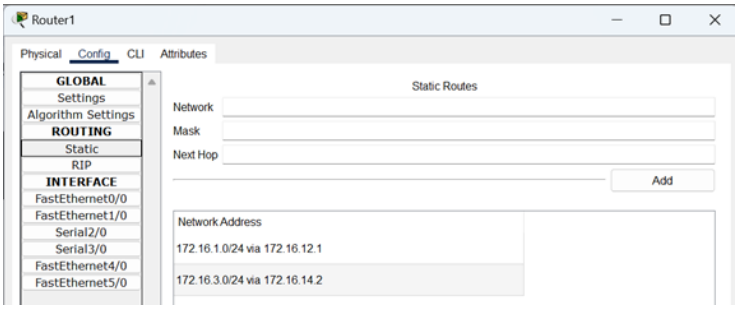


3.4. Lakukan konfigurasi static routing pada Router, seperti berikut:

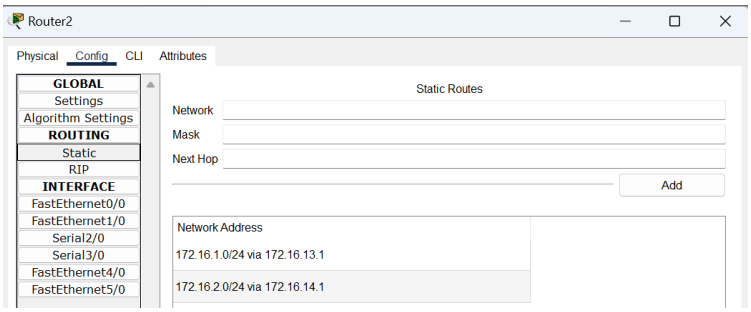
a. Router 0



b. Router 1



c. Router 2



3.5. Jalankan perintah: #show ip route pada router 1 dan 2, serta lakukan analisa

a. Router 1

```
Router#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.12.1
C       172.16.2.0/24 is directly connected, FastEthernet0/0
S       172.16.3.0/24 [1/0] via 172.16.14.2
C       172.16.12.0/30 is directly connected, Serial2/0
C       172.16.14.0/30 is directly connected, Serial3/0

Router#
```

b. Router 1

```
Router#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.13.1
S       172.16.2.0/24 [1/0] via 172.16.14.1
C       172.16.3.0/24 is directly connected, FastEthernet0/0
C       172.16.13.0/30 is directly connected, Serial3/0
C       172.16.14.0/30 is directly connected, Serial2/0

Router#
```

Copy Paste

3.6. Lakukan tes ping ke semua PC, kemudian tampilkan hasil percobaan anda dan analisa

a. PC 0 ke PC lain

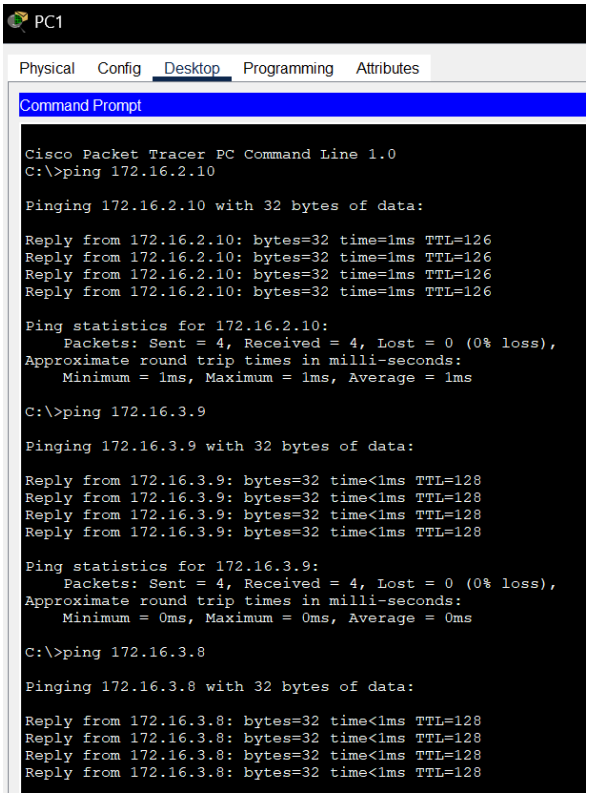
PC0

Physical Config Desktop Programming Attributes

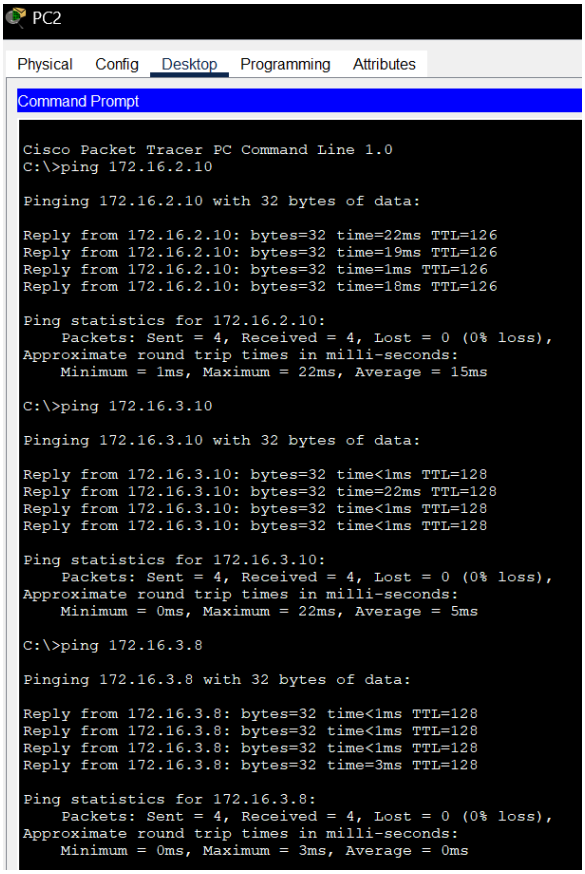
Command Prompt

```
C:\>ping 172.16.3.10

Pinging 172.16.3.10 with 32 bytes of data:

Reply from 172.16.3.10: bytes=32 time=1ms TTL=126
Reply from 172.16.3.10: bytes=32 time=1ms TTL=126
Reply from 172.16.3.10: bytes=32 time=1ms TTL=126
Reply from 172.16.3.10: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 4ms

C:\>ping 172.16.3.9

Pinging 172.16.3.9 with 32 bytes of data:

Reply from 172.16.3.9: bytes=32 time=23ms TTL=126
Reply from 172.16.3.9: bytes=32 time=1ms TTL=126
Reply from 172.16.3.9: bytes=32 time=15ms TTL=126
Reply from 172.16.3.9: bytes=32 time=15ms TTL=126

Ping statistics for 172.16.3.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 23ms, Average = 13ms

C:\>ping 172.16.3.8

Pinging 172.16.3.8 with 32 bytes of data:

Reply from 172.16.3.8: bytes=32 time=23ms TTL=126
Reply from 172.16.3.8: bytes=32 time=16ms TTL=126
Reply from 172.16.3.8: bytes=32 time=29ms TTL=126
Reply from 172.16.3.8: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 29ms, Average = 21ms
```

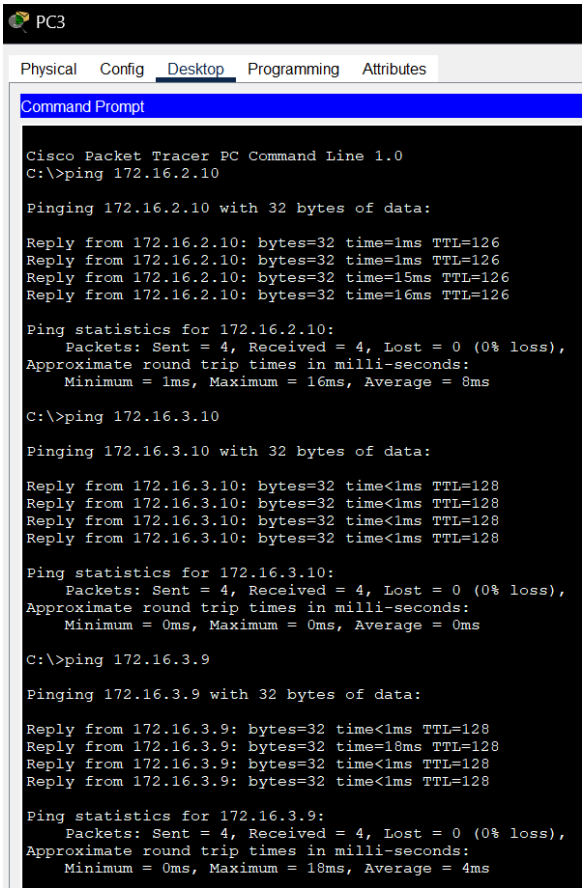
b. PC 1 ke PC lain



c. PC 2 ke PC lain



d. PC 3 ke PC lain



3.7. Lakukan konfigurasi Access Control List (ACL) pada router, analisa perintah konfigurasi yang digunakan berikut ini

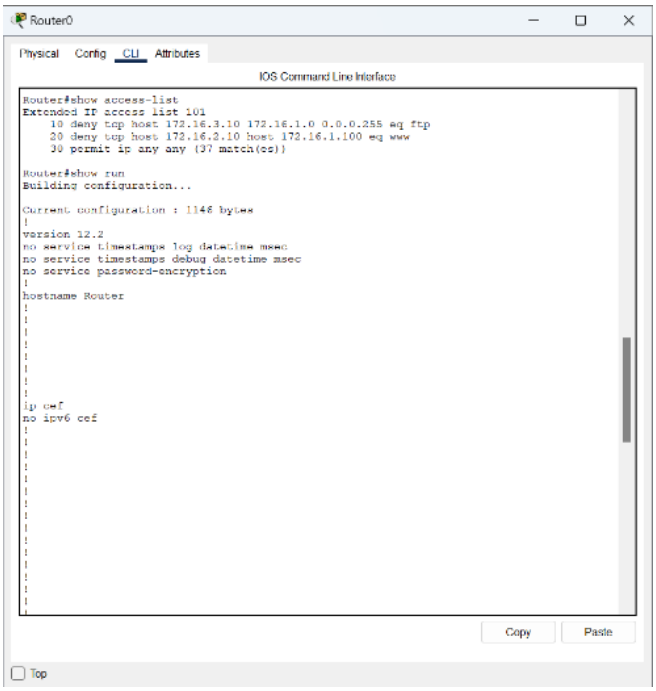
a. Lakukan blocking untuk koneksi Tom and Jerry dari Router0

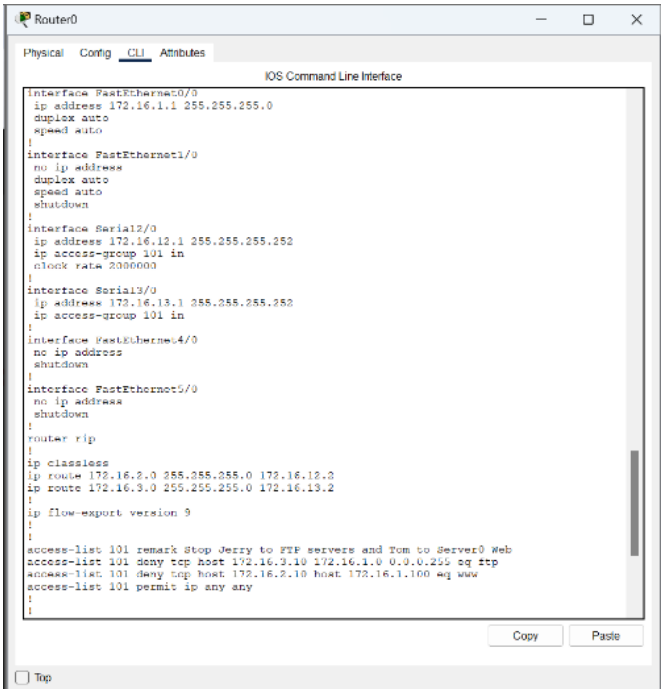
```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#avvess-list 101 remark Stop Jerry to FTP servers and Tom to Server0 Web
               ^
% Invalid input detected at '^' marker.

Router(config)#access-list 101 remark Stop Jerry to FTP servers and Tom to Server0 Web
Router(config)#access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
Router(config)#access-list 101 permit ip any any
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Terapkan ACL pada interface yang dekat dengan destination

```
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se2/0
Router(config-if)#ip access-group 101 in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se3/0
Router(config-if)#ip access-group 101 in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

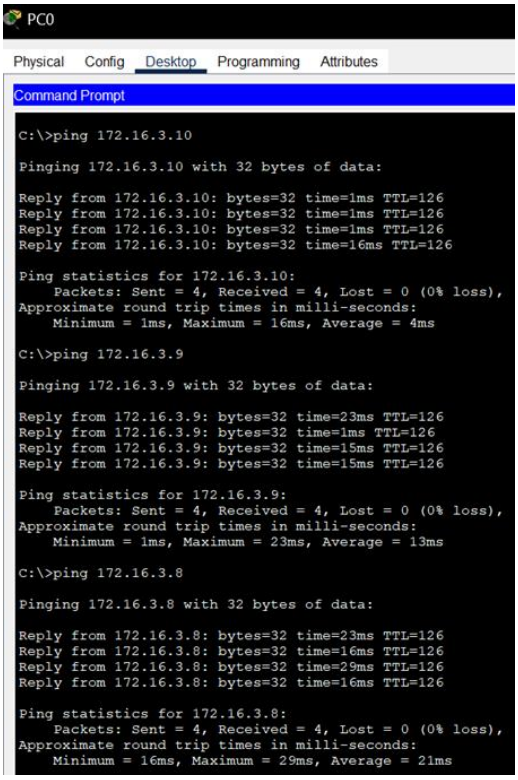
3.8. Lihat Konfigurasi dengan perintah Router#show run dan analisa Router 0



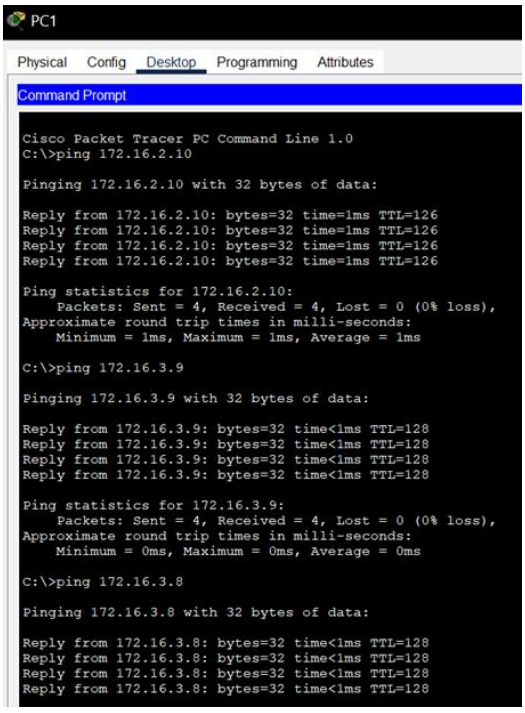


3.9. Gunakan perintah ping dari masing masing PC ke PC lainnya, tampilkan hasilnya dan analisa, bandingkan dengan hasil percobaan pada Langkah no. 6

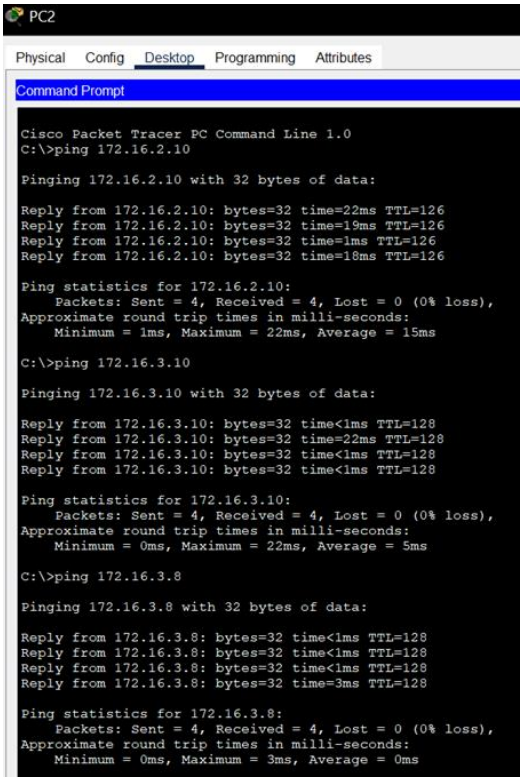
a. PC 0



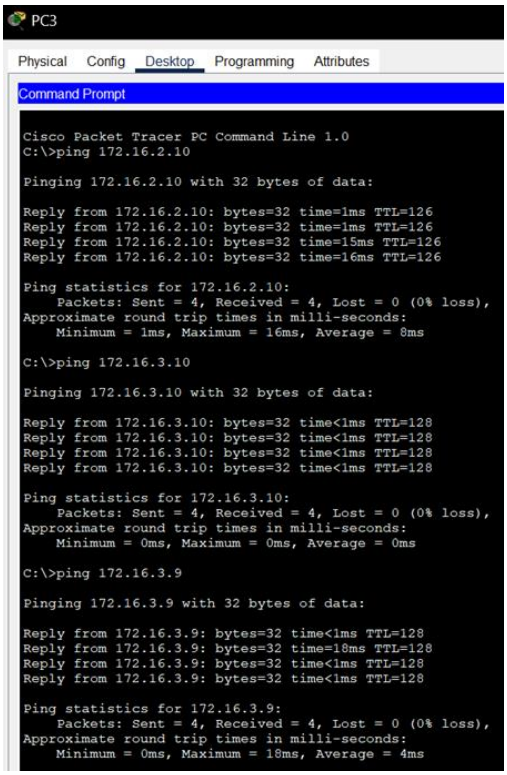
b. PC 1



c. PC 2

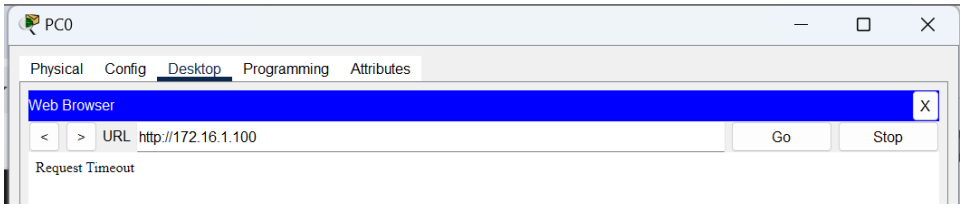

PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.10
Pinging 172.16.2.10 with 32 bytes of data:
Reply from 172.16.2.10: bytes=32 time=22ms TTL=126
Reply from 172.16.2.10: bytes=32 time=19ms TTL=126
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=18ms TTL=126
Ping statistics for 172.16.2.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 22ms, Average = 15ms
C:\>ping 172.16.3.10
Pinging 172.16.3.10 with 32 bytes of data:
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time=22ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.3.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 22ms, Average = 5ms
C:\>ping 172.16.3.8
Pinging 172.16.3.8 with 32 bytes of data:
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time=3ms TTL=128
Ping statistics for 172.16.3.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 0ms

d. PC 3


PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.10
Pinging 172.16.2.10 with 32 bytes of data:
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=15ms TTL=126
Reply from 172.16.2.10: bytes=32 time=16ms TTL=126
Ping statistics for 172.16.2.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 16ms, Average = 8ms
C:\>ping 172.16.3.10
Pinging 172.16.3.10 with 32 bytes of data:
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.3.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.16.3.9
Pinging 172.16.3.9 with 32 bytes of data:
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time=18ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.3.9:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 18ms, Average = 4ms

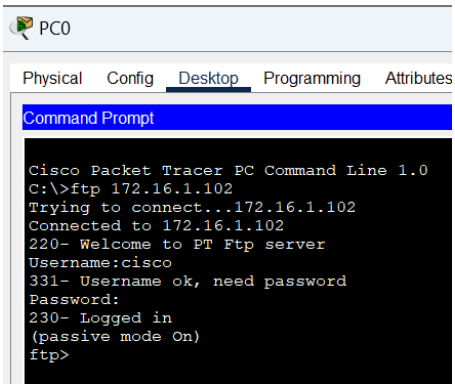
3.10. Lakukan pengujian dari host Tom pada PC 0 dan bandingkan dari PC lain

a. Ke Server 0



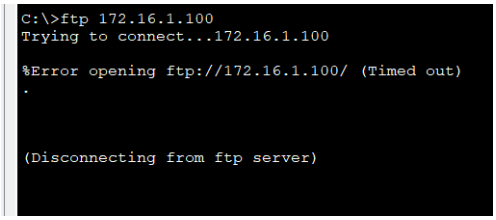

```
C:\>ftp 172.16.1.100
Trying to connect...172.16.1.100
Connected to 172.16.1.100
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

b. Ke Server 1

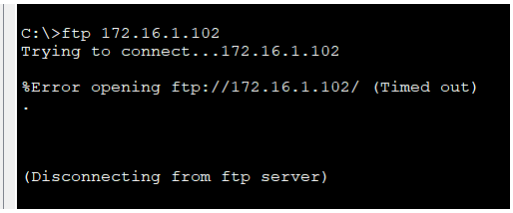


3.11. Lakukan pengujian dari host Jerry pada PC1 dan bandingkan dari PC lain

a. Ke Server 0



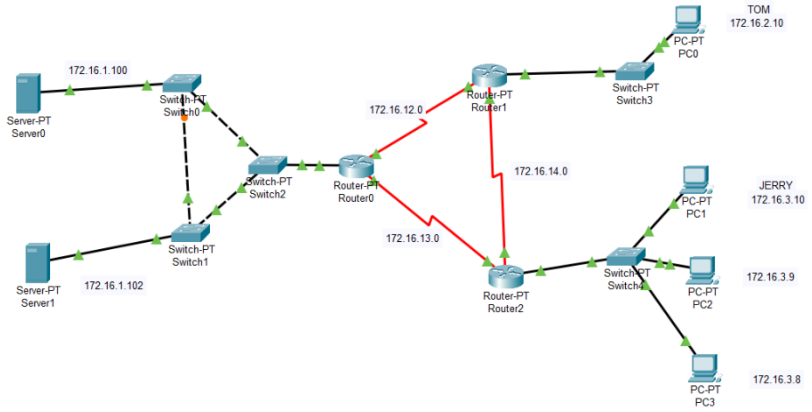
b. Ke Server 1



4. Analisa

Pada Praktikum Kelima ini dilakukan Extended ACL. ACL ini tentunya fungsinya sama seperti praktikum sebelumnya dimana ACL sebagai fitur untuk mengatur lalu lintas data berdasarkan Alamat IP sumber. ACL ini bertindak sebagai filter yang menentukan suatu paket data didizinkan (permit) atau ditolak (deny) untuk melintas suatu antarmuka jaringan. Karena ini adalah Extended ACL yang mana memiliki fitur yang lebih banyak dari pada Standart ACL. Extended ACL bisa memfilter paket yang masuk berdasarkan Alamat ip sumber, ip tujuan, protokol yang digunakan, dan portnya.

Untuk percobaanya akan dibuat topologi jaringan sebagai berikut:



Dalam topologi tersebut terdapat tiga jaringan yaitu 172.16.1.0 yang mencakup Server0 dan Server1 sebagai end device dan Router 0 sebagai gateawaynya, lalu 172.16.2.0 yng terdapat PC0 dan Router 1 sebagai gateawaynya, dan yang terakhir adalah jaringan 172.16.3.0 yang terdapat PC1, PC2, dan PC3 sebagai end device serta Router 2 sebagai gateawaynya. Lalu untuk koneksi serial antar Router menggunakan network 172.16.12.0, 172.16.13.0, dan 172.16.14.0. Khusus untuk PC0 memiliki inisialisasi nama Tom dan PC1 memiliki inisialisassi nama Jerry.

Setelah diketahui networknya, semua device akan di konfigurasi sesuai dengan networknya dan hasilnya sesuai dengan foto topologi diatas. Lalu antar ketiga Router di routing dengan static routing agar antar end device secara keseluruhan bisa saling terkoneksi. Berikut hasil konfigurasi static routing jika dilihat menggunakan perintah #show ip route untuk Router 1 dan Router 2

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#ip sh ro
          ^
% Invalid input detected at '^' marker.

Router#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.12.1
C       172.16.2.0/24 is directly connected, FastEthernet0/0
S       172.16.3.0/24 [1/0] via 172.16.14.2
C       172.16.12.0/30 is directly connected, Serial2/0
C       172.16.14.0/30 is directly connected, Serial3/0
```

Router2

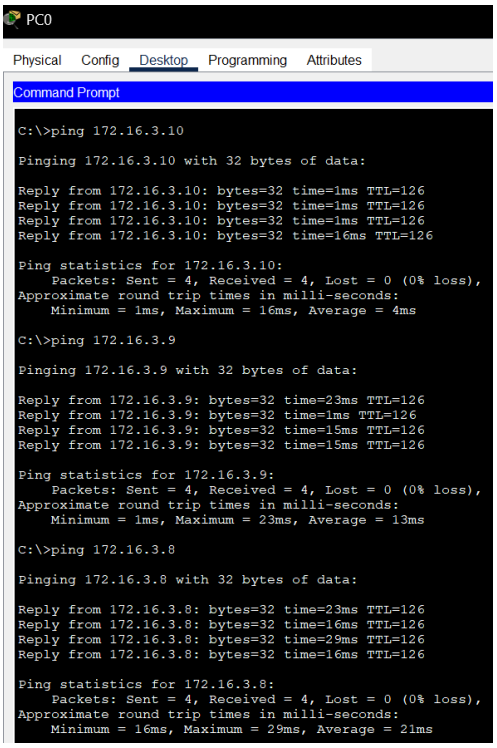
Physical Config CLI Attributes

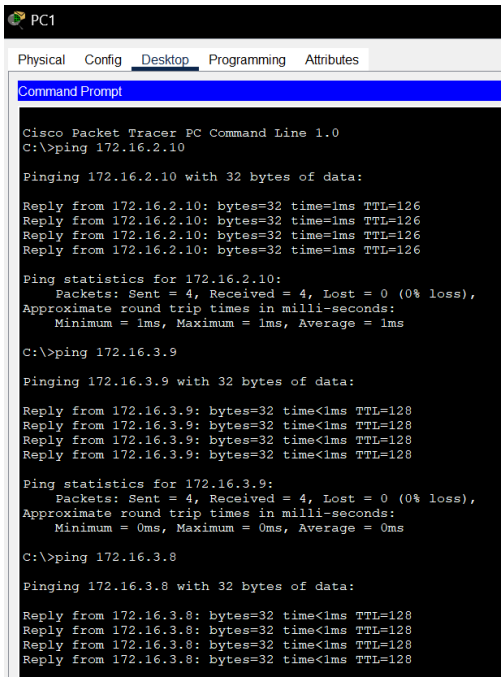
IOS Command Line Interface

```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.13.1
S       172.16.2.0/24 [1/0] via 172.16.14.1
C       172.16.3.0/24 is directly connected, FastEthernet0/0
C       172.16.13.0/30 is directly connected, Serial3/0
C       172.16.14.0/30 is directly connected, Serial2/0
```

Dari kedua gambar CLI Router 1 dan Router 2 menunjukkan adanya koneksi dengan jaringan diseluruh router ada. Pada Router 1 sudah terkoneksi secara static dengan network 172.16.1.0 via ip port 172.16.12.1 dan network 172.16.3.0 via ip port 172.16.14.2. Pada Router 2 sudah terkoneksi secara static dengan 172.16.1.0 via ip port 172.16.13.1 dan network 172.16.2.0 via ip port 172.16.14.1.

Setelah seluruh router saling terkoneksi satu sama lain dengan static routing, maka bisa mengetes untuk masing-masing PC untuk saling berkomunikasi dan terkoneksi satu sama lain. Berikut hasil ping dari PC0 hingga PC3





PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.10

Pinging 172.16.2.10 with 32 bytes of data:

Reply from 172.16.2.10: bytes=32 time=22ms TTL=126
Reply from 172.16.2.10: bytes=32 time=19ms TTL=126
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=18ms TTL=126

Ping statistics for 172.16.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 22ms, Average = 15ms

C:\>ping 172.16.3.10

Pinging 172.16.3.10 with 32 bytes of data:

Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time=22ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 5ms

C:\>ping 172.16.3.8

Pinging 172.16.3.8 with 32 bytes of data:

Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time=3ms TTL=128

Ping statistics for 172.16.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.10

Pinging 172.16.2.10 with 32 bytes of data:

Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126
Reply from 172.16.2.10: bytes=32 time=15ms TTL=126
Reply from 172.16.2.10: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 8ms

C:\>ping 172.16.3.10

Pinging 172.16.3.10 with 32 bytes of data:

Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.3.9

Pinging 172.16.3.9 with 32 bytes of data:

Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time=18ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms
```

Terlihat bahwasannya antar satu dan lain PC sudah bisa menerima pesan ping yang dikirimkan. Ini menandakan static routing berhasil dikonfigurasi di masing-masing router. Lalu pesan yang disampaikan oleh TTL memiliki arti saat TTL= 128 itu berarti pengiriman paket berada di satu network dan saat TTL= 126 berarti paket melewati 2 router untuk mengirim paket data ke sumber end device tujuan.

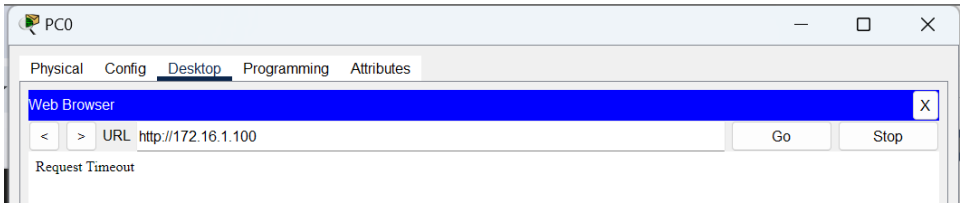
Lalu dilakukan untuk mengkonfigurasi ACL dengan Extended ACL dalam Router 0 untuk membatasi koneksi yang masuk jaringan Router 0. Berikut perintahnya

```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#avvess-list 101 remark Stop Jerry to FTP servers and Tom to Server0 Web
               ^
% Invalid input detected at '^' marker.

Router(config)#access-list 101 remark Stop Jerry to FTP servers and Tom to Server0 Web
Router(config)#access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
Router(config)#access-list 101 permit ip any any
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

          Router#conf term
          Enter configuration commands, one per line.  End with CNTL/Z.
          Router(config)#int se2/0
          Router(config-if)#ip access-group 101 in
          Router(config-if)#^Z
          Router#
          %SYS-5-CONFIG_I: Configured from console by console

          Router#conf term
          Enter configuration commands, one per line.  End with CNTL/Z.
          Router(config)#int se3/0
          Router(config-if)#ip access-group 101 in
          Router(config-if)#^Z
          Router#
          %SYS-5-CONFIG_I: Configured from console by console
```

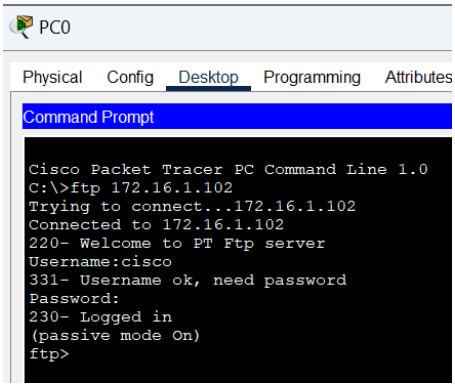
Dari perintah tersebut dapat dilihat ACL Extended menggunakan rentang ACL dari 100 hingga 199 yang aman disitu menggunakan nomor 101. Dalam perintah tersebut terdapat perintah untuk menandai atau menamai Stop PC Jerry mengakses FTP serve dan PC Tom untuk mengakses web dari Server0. Tapi tentunya hal tersebut hanya untuk penamaan detailnya harus di susun dengan perintah deny protokol tcp dari host 172.16.3.10 untuk mengakses ftp server dan deny protokol tcp dari host 172.16.2.10 ke server0 untuk mengakses bagian port webnya. Hal ini menjadi bukti banyaknya fitur konfigurasi seperti protokol yang digunakan, port yang digunakan seperti web atau ftp, dan juga ip tujuannya. Sedangkan, ACL Standart hanya bisa memblokir atau mengizinkan berdasarkan ip nya saja.

Lalu bisa dicoba untuk ping antar end device PC. Yang mana bisa dilihat di prosedur diatas, hasilnya tetap sama, hal ini dikarenakan router yang ada ACL nya hanya router 0 sedangkan end device PC masih bisa berkomunikasi satu sama lain lewat Router 1 dan Router 2 saja.

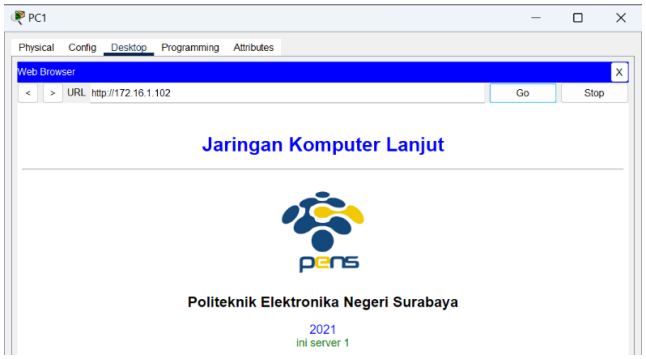
Lalu setelah itu karena poin aturan dari Router 0 lebih banyak merujuk ke PC Tom dan PC Jerry, maka dicobalah kedua PC tersebut untuk mengakses server 0 dan server 1. Berikut hasilnya

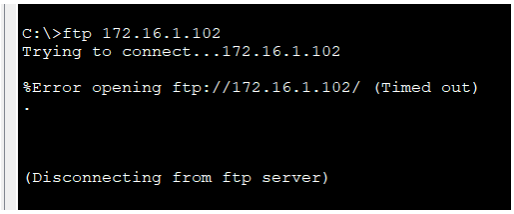


```
C:\>ftp 172.16.1.100
Trying to connect...172.16.1.100
Connected to 172.16.1.100
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```




```
C:\>ftp 172.16.1.100
Trying to connect...172.16.1.100

%Error opening ftp://172.16.1.100/ (Timed out)
.


(Disconnecting from ftp server)
```





Bisa dilihat hasilnya saat PC 0 mengakses port web atau laman web server 0 atau IP 172.16.1.100 hasilnya adalah request time out. Hal ini mengindikasikan bahwa ACL yang terkonfigurasi sudah bisa terpakai dengan baik, karena perintah yang dikeluarkan tadi di CLI Router 0 adalah untuk memblokir akses PC0 ke port web server 0. Maka dari itu, selain port web server0, PC0 masih bisa untuk mengaksesnya.

Sedangkan untuk di PC1 atau Jerry, dikkonfigurasi hanya bisa mengakses port web saja dan port ftp dari kedua server akan diblokir. Hal tersebut benar adanya, karena dalam percobaan mengkases ftp kedua server hasilnya adalah disconnecting yaitu network tidak mau atau memblokir packet data dari PC1 atau Jerry untuk mengakses isi ftp di masing-masing server network 172.16.1.0.

5. Tugas

5.1. Menurut anda, apa saja perbedaan standart ACL dan extended ACL?

Jawab:

Standart ACL adalah jenis ACL yang paling sederhana karena hanya memeriksa dan menyaring packet data berdasarkan IP address nya saja. Oleh karena itu, peraturan atau konfigurasi yang dibuat dari standart ACL ini tidak akan memperhatikan ke mana tujuan packet dikirim, protocol yang digunakan, bahkan jenis layanannya. Standart ACL biasanya digunakan untuk control akses seperti memlokir traffic yang berasal dari subnet atau IP tertentu. Lalu rentang nomor standart ACL umumnya berkisar dari 1 hingga 99 dan 1300 hingga 1999.

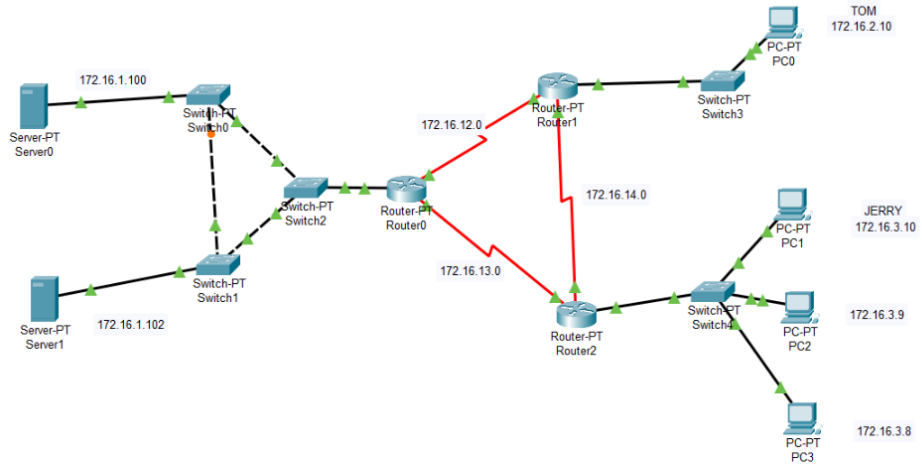
Sedangkan Extended ACL adalah ACL yang menawarkan control yang lebih rinci dan fleksibel dibandingkan Standart ACL. Dimana ACL ini bisa menyaring traffic berdasarkan IP address, tujuan IP address, jenis protokolnya, hingga nomor port seperti FTP dan www. Jadi Extended ACL bisa menyaring admin Jaringan untuk memblokir akses FTP tetapi masih mengizinkan akses web dari IP server tertentu. Lalu rentang nomor extended ACL umumnya berkisar dari rentang nomor 100-199 dan 200- 2699.

5.2. Berdasarkan percobaan di atas, bila ACL diterapkan bukan di Router0, tetapi hanya di terapkan di Router2, jelaskan apa yang terjadi?

Jawab:

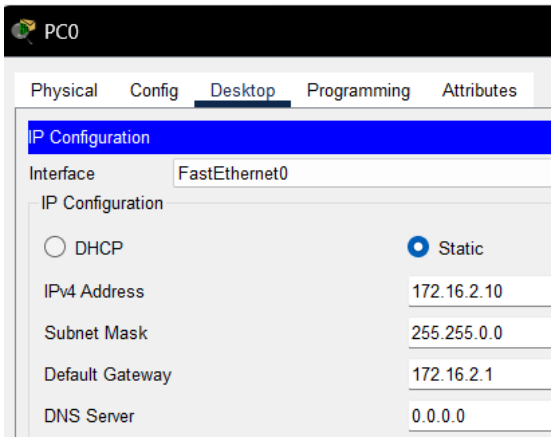
Jika ACL hanya diterapkan di Router 2, amka proses traffic yang akan diatur adalah keluar masuk ke network 172.16.3.0 atau yang berkaitan dengan router 2. Hal ini dikarenakan, satu ACL hanya mengkonfigurasi satu router untuk network yang terhubung dalam router tersebut, missal untuk Router 2 itu hanya network 172.16.3.0 saja. Jadi disitu kitab isa membatasi untuk emngakses data-data atau port yang ada di PC1 hingga PC3. Bisa nanti berdasarkan port ftpnya atau webnya atau keseluruhan port yang ada dalam masing-masing PC tersebut. Jadi akses server ke PC0 bisa dilakukan dengan bebas, atau PC0 bisa mengakses kedua server tersebut open source selaman tersambung dalam jaringan. Sedangkan untuk berhubungkan dengan PC1 sampai PC3 nya harus berdasarkan aturan ACL yang di setting di Router 2.

5.3. Lakukan modifikasi ACL pada percobaan, sehingga host Jerry hanya bisa mengakses FTP server, PC1 dan PC2 tidak bisa mengakses Web Server0, serta PC3 tidak bisa mengakses Web Server1.
Jawab:

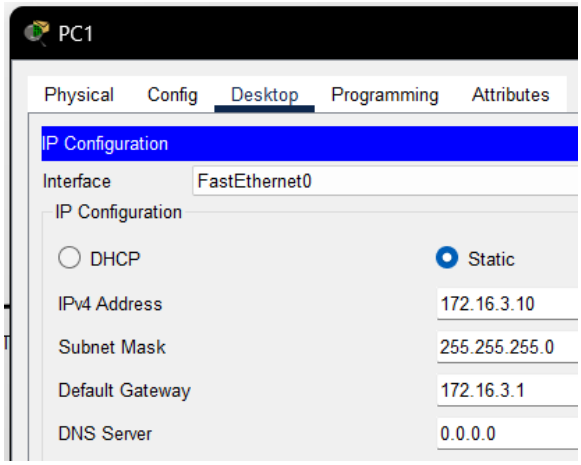


- Konfigurasi Alamat End Device

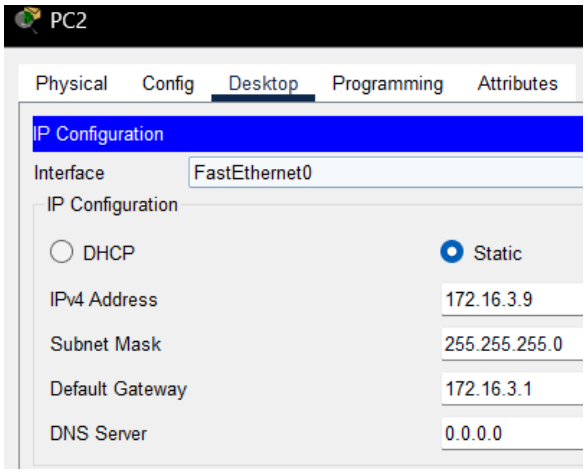
  a. PC 0



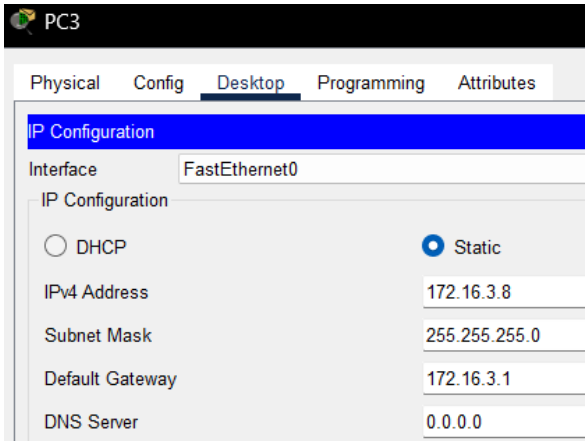
b. PC 1



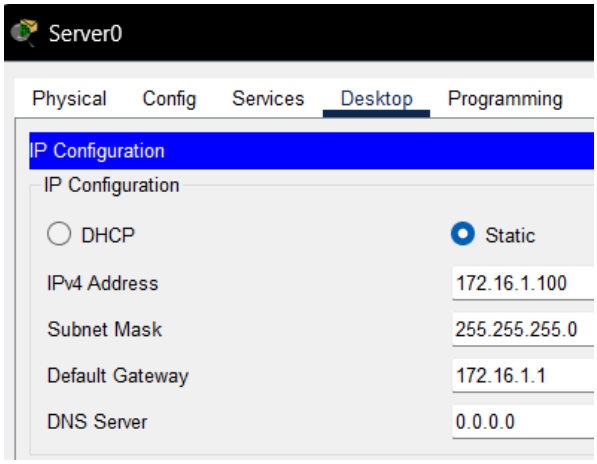
c. PC 2



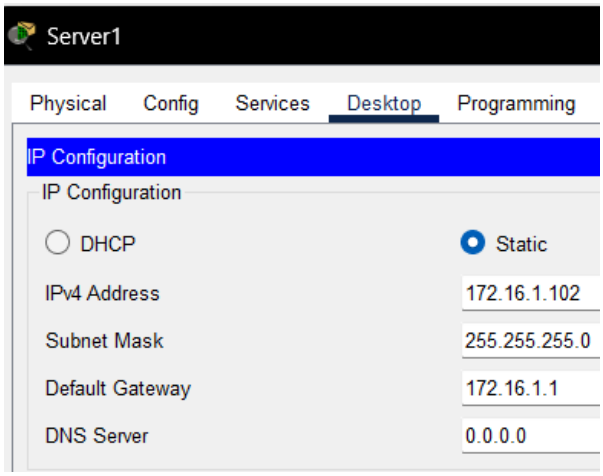
d. PC 3



e. Server 0

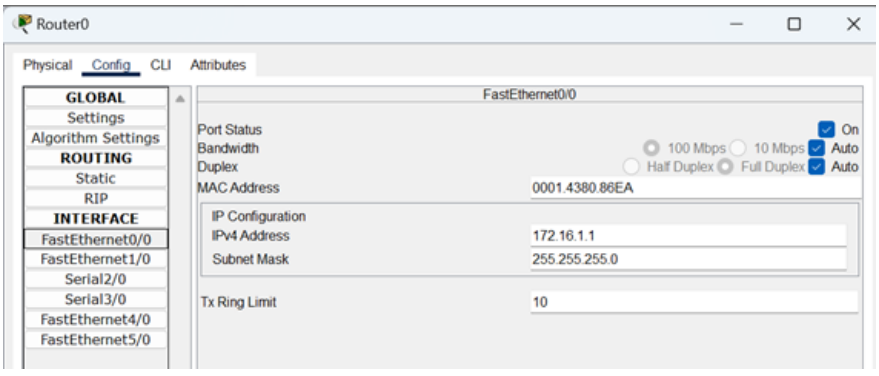


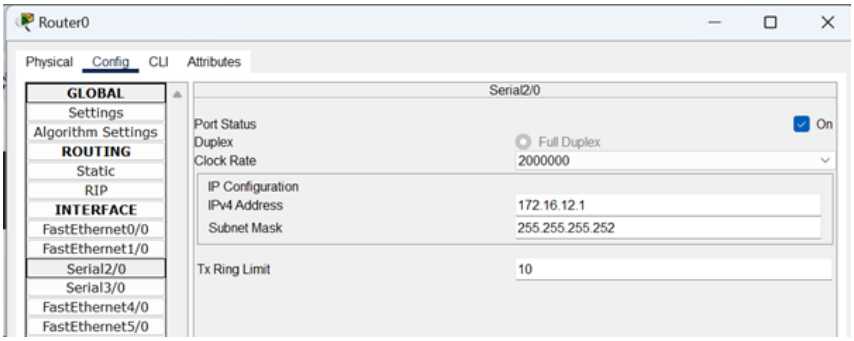
f. Server 1

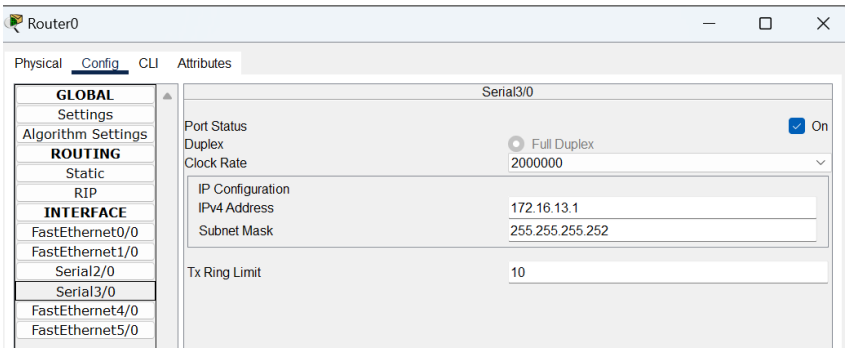


- Konfigurasi Interface Router

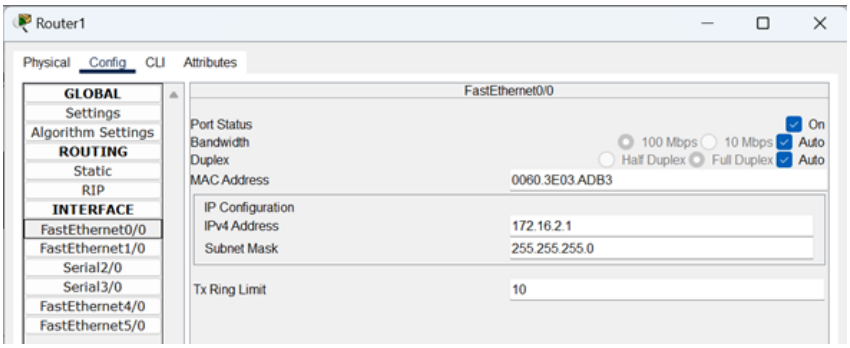
a. Router 0

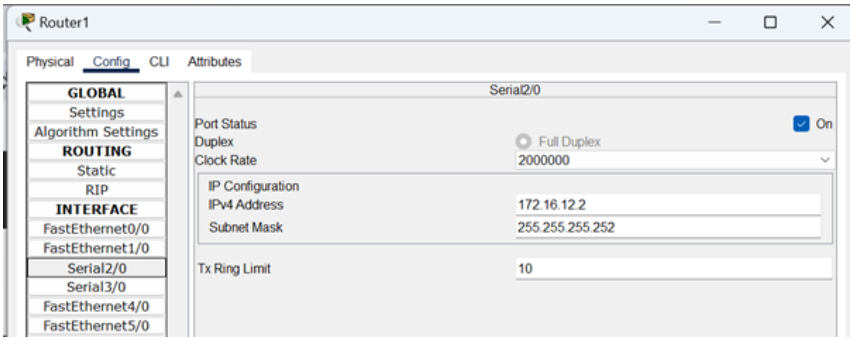


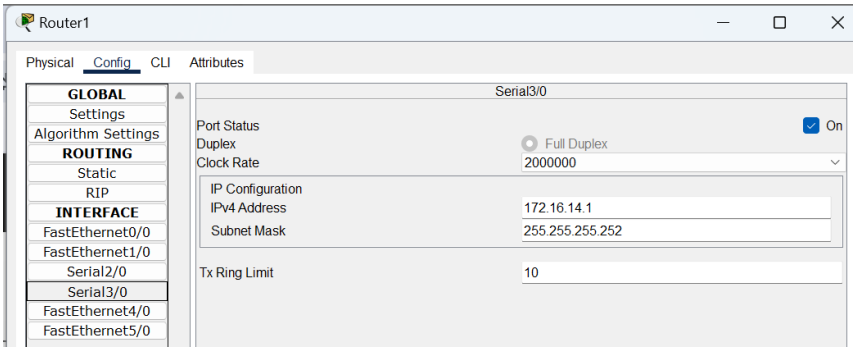

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
172.16.12.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
172.16.13.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10

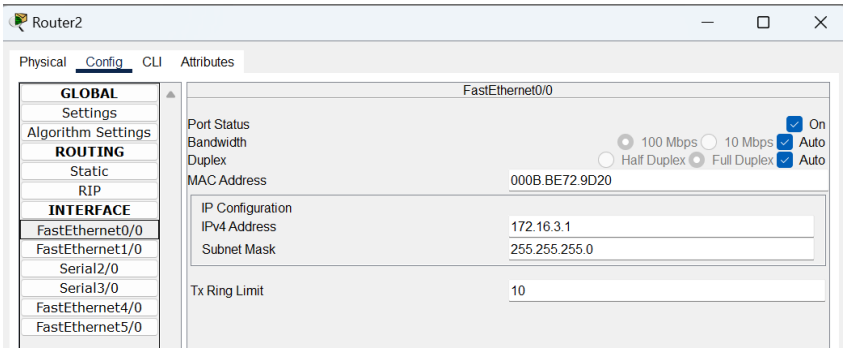
b. Router 1

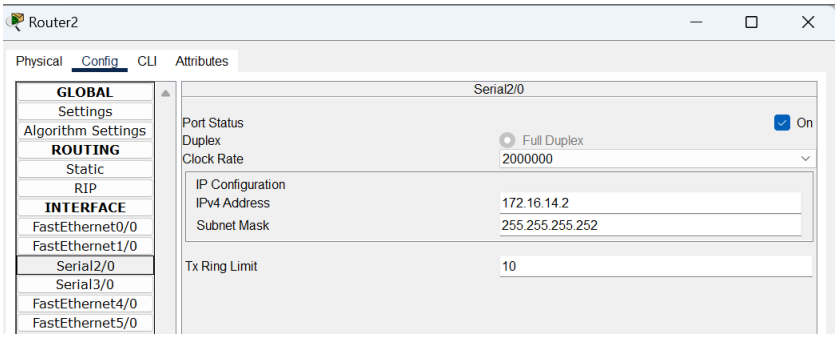

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.3E03.ADB3
IP Configuration
IPv4 Address
172.16.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

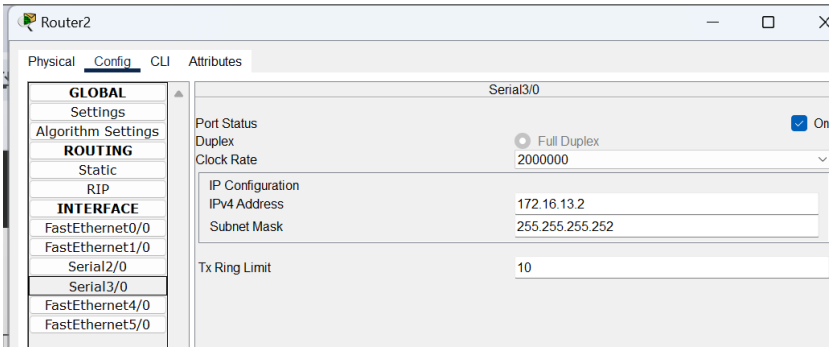

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
172.16.12.2
Subnet Mask
255.255.255.252
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
172.16.14.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10

c. Router 2

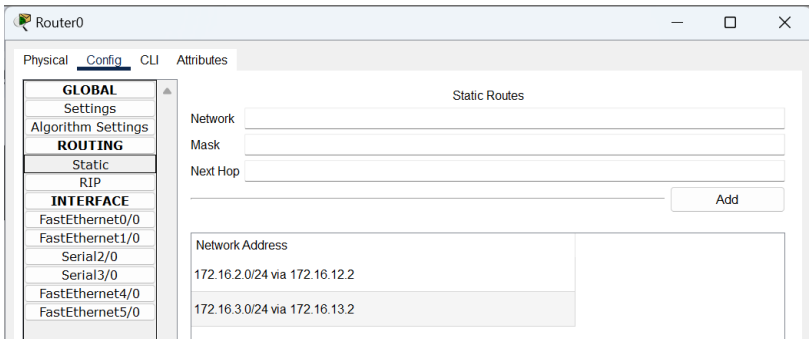




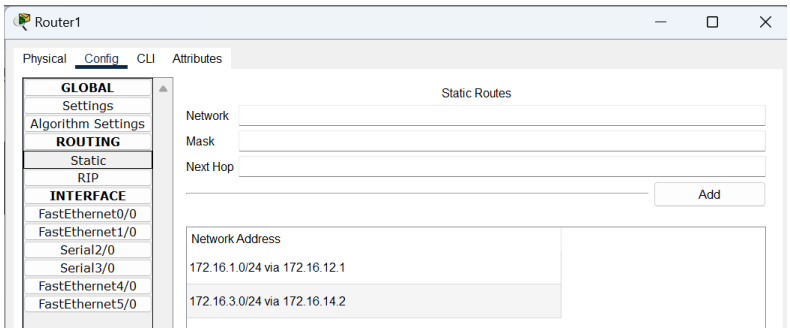


- Konfigurasi static Routing

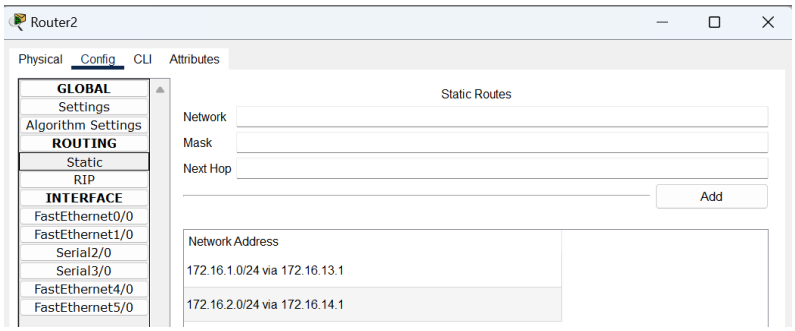
a. Router 0



b. Router 1

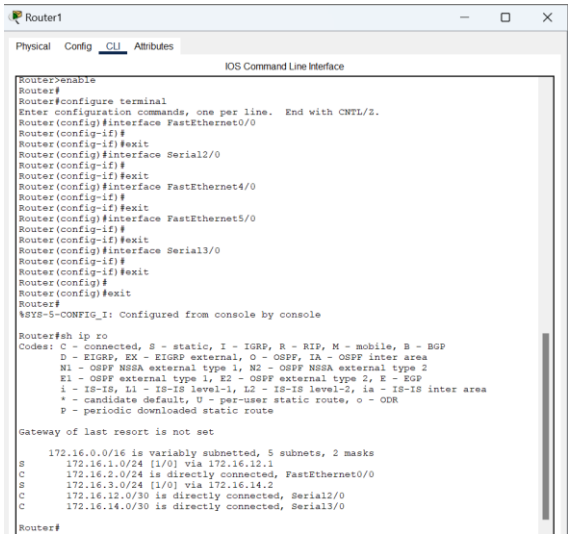


c. Router 2

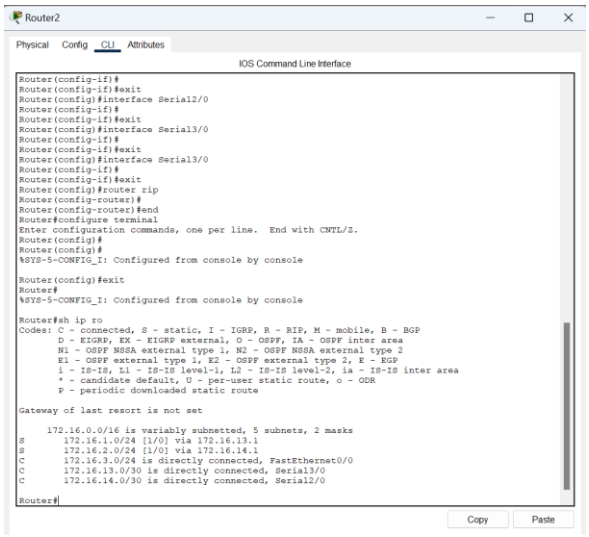


- Pengujian Router#show ip route

a. Router 1

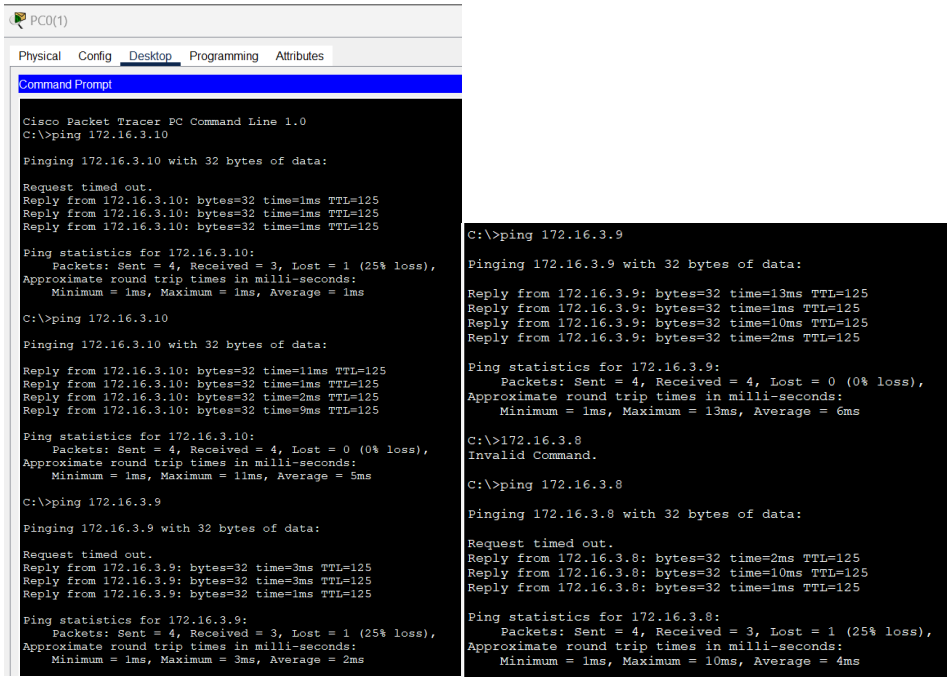


b. Router 2

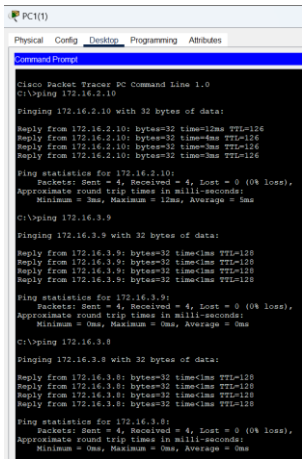


- Pengujian tes ping dari masing-masing PC

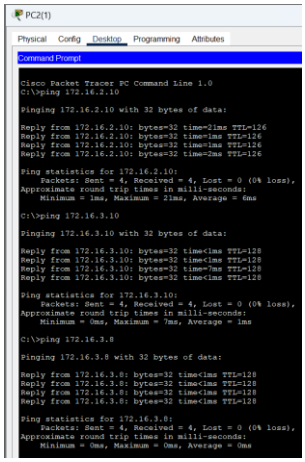
a. PC 0



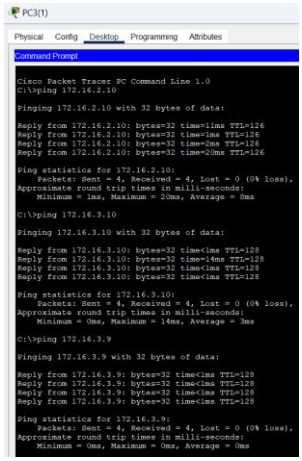
b. PC 1



c. PC 2



d. PC 3



- Konfigurasi Extended ACL

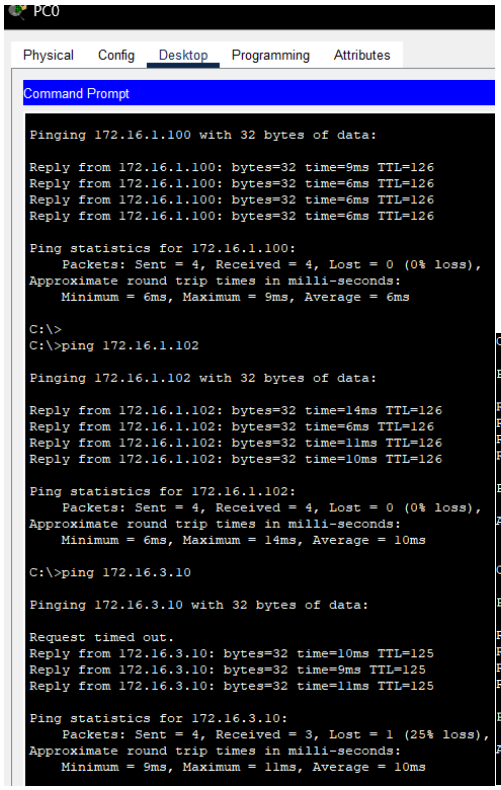
```
Router#en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 remark Stop Jerry to Server0 web
Router(config)#access-list 101 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
Router(config)#access-list 101 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
Router(config)#access-list 101 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
Router(config)#access-list 101 permit ip any any
```

- Pengujian Router#show access-list dan Router#show run pada router 0

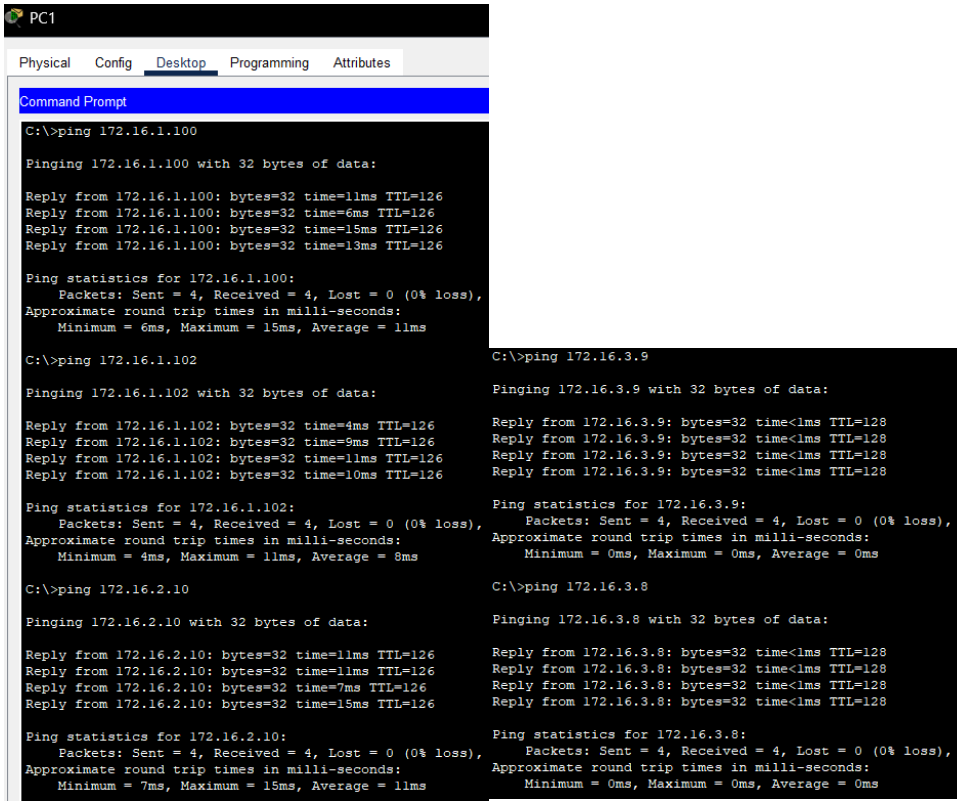
```
Router#show access-list
Extended IP access list 101
    10 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
    20 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
    30 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
    40 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
    50 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
    60 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
    70 permit ip any any
```

```
Router#sh run
Building configuration...

Current configuration : 1767 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 172.16.12.1 255.255.255.252
 ip access-group 101 in
 clock rate 2000000
!
interface Serial3/0
 ip address 172.16.13.1 255.255.255.252
 ip access-group 101 in
 clock rate 2000000
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip classless
ip route 172.16.2.0 255.255.255.0 172.16.12.2
ip route 172.16.3.0 255.255.255.0 172.16.13.2
!
ip flow-export version 9
!
!
access-list 101 remark Stop Tom to Server0 web and to FTP Servers
access-list 101 remark Stop Brandt to Server0 web and to FTP Servers
access-list 101 remark Stop Jimmy to Server1 web and to FTP Servers
access-list 101 remark Stop Jerry to Server0 web and to Server1 web
access-list 101 remark Stop Tom to FTP Servers
access-list 101 remark Stop Jerry to Server1 web
access-list 101 remark Stop Tom to FTP Servers
access-list 101 remark Stop Jerry to Server1 web
access-list 101 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 remark Stop Jerry to Server0 web
access-list 101 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
access-list 101 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
access-list 101 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

- Pengujian tes ping dari masing-masing PC
  a. PC 0



  b. PC 1



c. PC 2

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=16ms TTL=126
Reply from 172.16.1.100: bytes=32 time=11ms TTL=126
Reply from 172.16.1.100: bytes=32 time=9ms TTL=126
Reply from 172.16.1.100: bytes=32 time=15ms TTL=126

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 16ms, Average = 12ms

C:\>ping 172.16.1.102

Pinging 172.16.1.102 with 32 bytes of data:

Reply from 172.16.1.102: bytes=32 time=14ms TTL=126
Reply from 172.16.1.102: bytes=32 time=11ms TTL=126
Reply from 172.16.1.102: bytes=32 time=9ms TTL=126
Reply from 172.16.1.102: bytes=32 time=12ms TTL=126

Ping statistics for 172.16.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 14ms, Average = 11ms

C:\>ping 172.16.2.10

Pinging 172.16.2.10 with 32 bytes of data:

Reply from 172.16.2.10: bytes=32 time=14ms TTL=126
Reply from 172.16.2.10: bytes=32 time=15ms TTL=126
Reply from 172.16.2.10: bytes=32 time=13ms TTL=126
Reply from 172.16.2.10: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 10ms

C:\>ping 172.16.3.10

Pinging 172.16.3.10 with 32 bytes of data:

Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.3.8

Pinging 172.16.3.8 with 32 bytes of data:

Reply from 172.16.3.8: bytes=32 time=11ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128
Reply from 172.16.3.8: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

d. PC 3

PC3

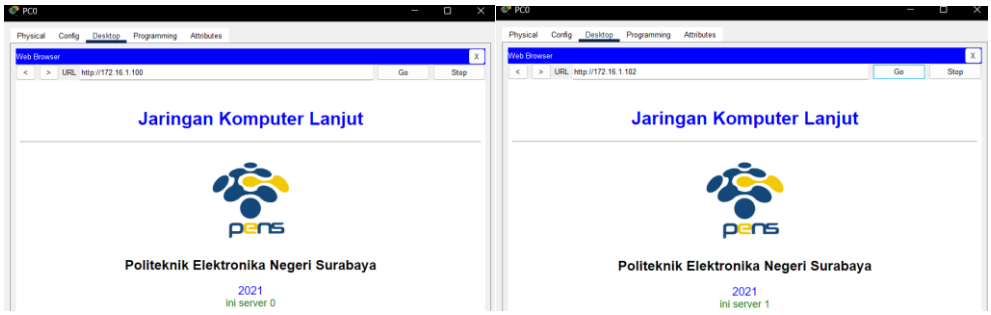
Physical Config Desktop Programming Attributes

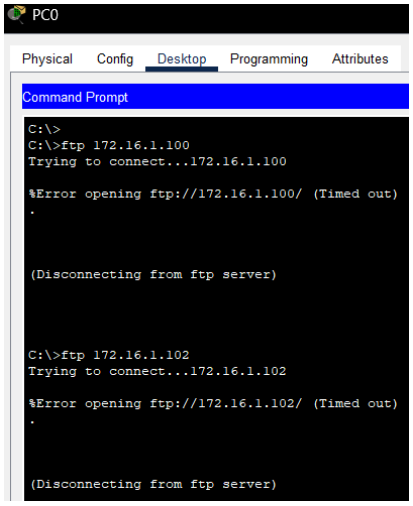
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=13ms TTL=126
Reply from 172.16.1.100: bytes=32 time=9ms TTL=126
Reply from 172.16.1.100: bytes=32 time=6ms TTL=126
Reply from 172.16.1.100: bytes=32 time=12ms TTL=126

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 13ms, Average = 10ms

C:\>ping 172.16.1.102

Pinging 172.16.1.102 with 32 bytes of data:

Reply from 172.16.1.102: bytes=32 time=15ms TTL=126
Reply from 172.16.1.102: bytes=32 time=10ms TTL=126
Reply from 172.16.1.102: bytes=32 time=12ms TTL=126
Reply from 172.16.1.102: bytes=32 time=9ms TTL=126

Ping statistics for 172.16.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 11ms

C:\>ping 172.16.2.10

Pinging 172.16.2.10 with 32 bytes of data:

Reply from 172.16.2.10: bytes=32 time=15ms TTL=126
Reply from 172.16.2.10: bytes=32 time=14ms TTL=126
Reply from 172.16.2.10: bytes=32 time=12ms TTL=126
Reply from 172.16.2.10: bytes=32 time=12ms TTL=126

Ping statistics for 172.16.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 15ms, Average = 13ms

C:\>ping 172.16.3.10

Pinging 172.16.3.10 with 32 bytes of data:

Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time<1ms TTL=128
Reply from 172.16.3.10: bytes=32 time=6ms TTL=128

Ping statistics for 172.16.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>ping 172.16.3.9

Pinging 172.16.3.9 with 32 bytes of data:

Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128
Reply from 172.16.3.9: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

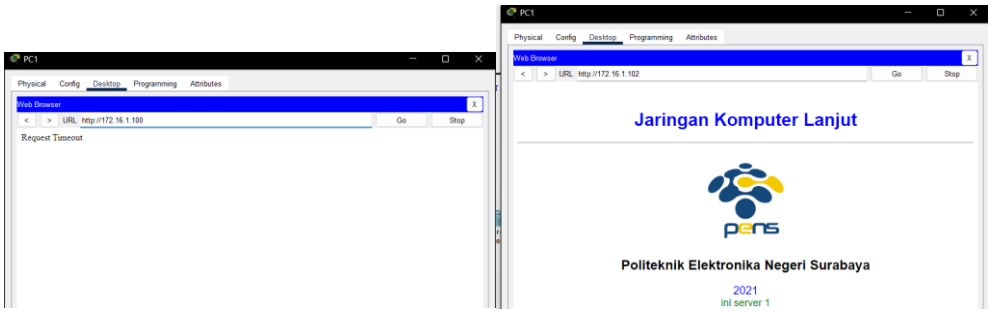
- Pengujian perintah FTP dan akses web di masing-masing PC ke Server

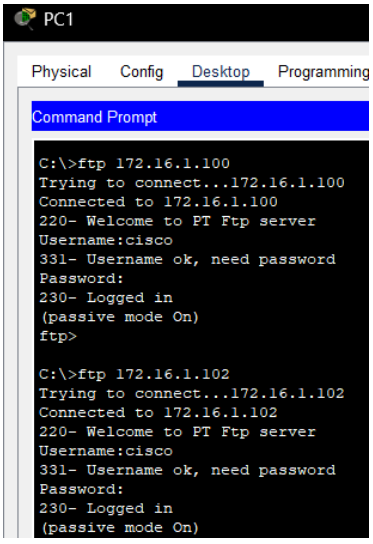
a. PC 0



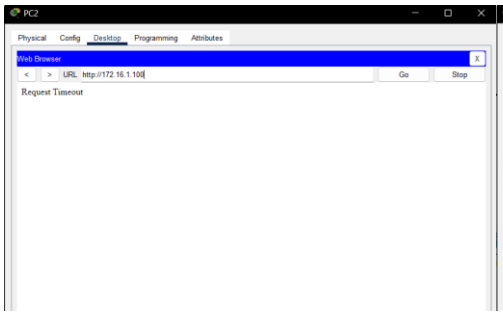


b. PC 1

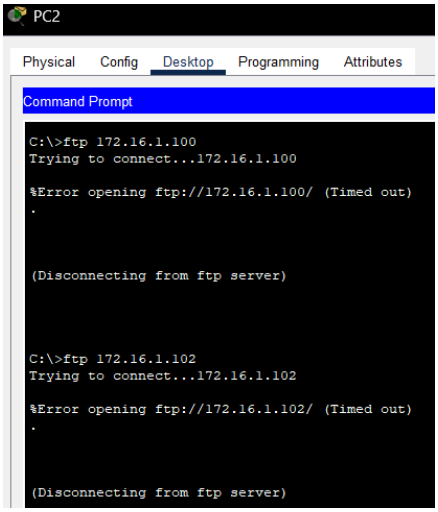




c. PC 2

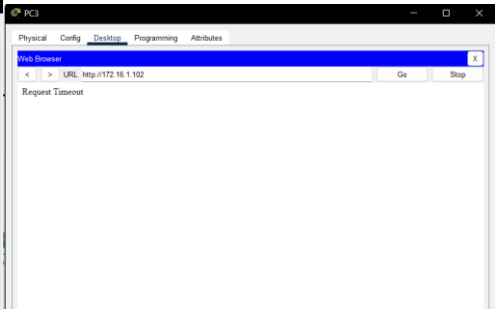

PC2
Physical Config Desktop Programming Attributes
Web Browser
URL http://172.16.1.100
Go Stop
Request Timeout

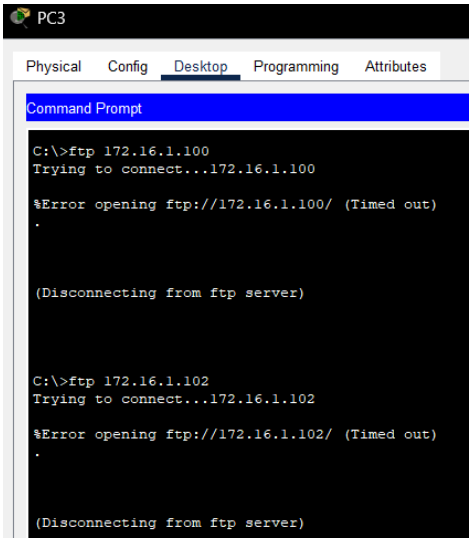

PC2
Physical Config Desktop Programming Attributes
Web Browser
URL http://172.16.1.102
Go Stop
Jaringan Komputer Lanjut
pens
Politeknik Elektronika Negeri Surabaya
2021
ini server 1


PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ftp 172.16.1.100
Trying to connect...172.16.1.100
%Error opening ftp://172.16.1.100/ (Timed out)
.
(Disconnecting from ftp server)
C:\>ftp 172.16.1.102
Trying to connect...172.16.1.102
%Error opening ftp://172.16.1.102/ (Timed out)
.
(Disconnecting from ftp server)

d. PC 3


PC3
Physical Config Desktop Programming Attributes
Web Browser
URL http://172.16.1.100
Go Stop
Jaringan Komputer Lanjut
pens
Politeknik Elektronika Negeri Surabaya
2021
ini server 0


PC3
Physical Config Desktop Programming Attributes
Web Browser
URL http://172.16.1.102
Go Stop
Request Timeout


PC3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ftp 172.16.1.100
Trying to connect...172.16.1.100
%Error opening ftp://172.16.1.100/ (Timed out)
.
(Disconnecting from ftp server)
C:\>ftp 172.16.1.102
Trying to connect...172.16.1.102
%Error opening ftp://172.16.1.102/ (Timed out)
.
(Disconnecting from ftp server)

Dari perubahan konfigurasi Extended ACL dari percobaan menjadi seperti ini

```
Router#en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 remark Stop Jerry to Server0 web
Router(config)#access-list 101 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
Router(config)#access-list 101 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
Router(config)#access-list 101 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
Router(config)#access-list 101 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
Router(config)#access-list 101 permit ip any any
```

Hal ini berarti memblokir akses PC2 untuk mengakses port web server 0 dan port ftp kedua server, PC3 di blokir aksesnya untuk mengakses port web server1 dan port ftp kedua server, PC1 juga diblokir aksesnya untuk mengakses port web server 0 saja, dan PC0 diblokir aksesnya untuk mengakses port ftp kedua server saja. Selain itu, host bisa mengakses apapun di server network 172.16.1.0

Hasil testing atau verifikasi konfigurasi di Router 0 nya adalah

```
Router#show access-list
Extended IP access list 101
    10 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
    20 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
    30 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
    40 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
    50 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
    60 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
    70 permit ip any any
```

```
Router#sh run
Building configuration...

Current configuration : 1767 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 172.16.12.1 255.255.255.252
 ip access-group 101 in
 clock rate 2000000
!
interface Serial3/0
 ip address 172.16.13.1 255.255.255.252
 ip access-group 101 in
 clock rate 2000000
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip classless
ip route 172.16.2.0 255.255.255.0 172.16.12.2
ip route 172.16.3.0 255.255.255.0 172.16.13.2
!
ip flow-export version 9
!
!
access-list 101 remark Stop Tom to Server0 web and to FTP Servers
access-list 101 remark Stop Brandt to Server0 web and to FTP Servers
access-list 101 remark Stop Jimmy to Server1 web and to FTP Servers
access-list 101 remark Stop Jerry to Server0 web and to Server1 web
access-list 101 remark Stop Tom to FTP Servers
access-list 101 remark Stop Jerry to Server1 web
```

```
access-list 101 remark Stop Tom to FTP Servers
access-list 101 remark Stop Jerry to Server1 web
access-list 101 deny tcp host 172.16.2.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 remark Stop Jerry to Server0 web
access-list 101 deny tcp host 172.16.3.9 host 172.16.1.100 eq www
access-list 101 deny tcp host 172.16.3.9 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.3.8 host 172.16.1.102 eq www
access-list 101 deny tcp host 172.16.3.8 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.3.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Ini menunjukkan bahwasannya konfigurasi yang ditulis tadi sudah masuk kedalam access-list 101 dan masuk di konfigurasi show run atau konfigurasi yang sedang dijalankan oleh Router 0.

Lalu Hasil ping nya karena hanya beberapa port saja yang di blokir oleh Router 0, maka tiap PC ke server atau PC ke PC maish bisa berkomunikasi atau berkoneksi dengan perintah ping tersebut. Hal terseubt menandakan bahwa tiap server dan pc masih bisa merespon apa yang di terima kecuali packet data tersebut portnya sama dengan port ftp atau port web nya, maka hal itu akan berurusan dengan aturan ACL yang berlaku, karena di ACL yang sudah disusun hanya Menyusun bagian port FTP dan port Web saja yang dblokir.

Tetapi saat hasil akses masing-masing PC ke port ftp dan web nya tentu hasilnya berbeda. Untuk PC0, akan RTO saat mengakses port ftp, tetapi akan terkoneksi saat mengakses port web. Unutk PC1, akan RTO saat mengakses port Web server 0, tetapi bisa mengakses port web server 1 dan port FTP kedua server. Untuk PC2, akan RTO saat mengakses web server0 dan ftp di kedua server, tetapi bisa mengakses port web server 1. Untuk PC 3, hanya bisa mengakses port web server 1 saja, selain untuk port ftp dan web lainnnya tidak bisa.

6. Kesimpulan

Konfigurasi Extended ACL pada praktikum ini menunjukkan bahwa dengan menggunakan ACL bertipe extended, administrator jaringan memiliki kontrol yang lebih spesifik terhadap lalu lintas data yang diizinkan atau diblokir berdasarkan alamat IP sumber dan tujuan, protokol, serta nomor port tertentu seperti FTP (port 21) dan Web (port 80). Extended ACL ini berhasil diterapkan di Router 0 untuk membatasi akses dari host-host tertentu terhadap layanan tertentu di Server0 dan Server1, seperti membatasi PC1 (Jerry) hanya dapat mengakses layanan FTP, memblokir PC2 dari seluruh akses ke FTP dan Web Server0, serta membatasi PC3 dari Web Server1.

Hasil uji coba menunjukkan bahwa aturan ACL yang diterapkan bekerja dengan baik. Paket yang diarahkan ke layanan tertentu sesuai dengan konfigurasi akan diblokir (Request Time Out), sementara paket lainnya tetap diteruskan. Dengan konfigurasi ini, jaringan menjadi lebih aman karena lalu lintas dapat dikontrol secara presisi, sesuai dengan kebutuhan dan peran tiap host dalam jaringan. Extended ACL terbukti lebih fleksibel dan efektif dibandingkan Standart ACL untuk pengaturan trafik yang kompleks.