Praktikum Jaringan Komputer

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

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

2. Dasar Teori

Standard Access Control List (ACL) adalah salah satu metode pengamanan jaringan yang diterapkan pada perangkat jaringan, terutama router, untuk mengatur lalu lintas data berdasarkan alamat IP sumber. ACL bertindak sebagai filter yang menentukan apakah suatu paket data diizinkan (*permit*) atau ditolak (*deny*) untuk melintasi suatu antarmuka jaringan. Standard ACL merupakan jenis ACL yang paling dasar karena hanya mempertimbangkan satu kriteria, yaitu alamat IP asal dari paket yang datang.

Tujuan utama penggunaan Standard ACL adalah untuk mengontrol akses ke jaringan atau segmen jaringan tertentu demi menjaga keamanan dan efisiensi lalu lintas data. Dengan menerapkan Standard ACL, administrator dapat membatasi akses dari alamat IP tertentu, mencegah perangkat tidak sah masuk ke jaringan internal, dan meminimalkan potensi gangguan. ACL ini sering digunakan pada jaringan skala kecil hingga menengah, di mana pengendalian akses tidak memerlukan kompleksitas tinggi.

Standard ACL bekerja dengan mengevaluasi alamat IP sumber dari setiap paket data yang masuk atau keluar pada suatu interface router. Jika alamat IP tersebut cocok dengan entri dalam daftar ACL, maka keputusan untuk mengizinkan atau menolak akses akan dijalankan sesuai perintah (*permit* atau *deny*). Jika tidak ada entri yang cocok, maka secara default paket akan ditolak karena adanya aturan *implicit deny* di akhir setiap ACL. Oleh karena itu, setiap konfigurasi ACL harus memperhatikan urutan dan kelengkapan entri agar tidak menimbulkan pemblokiran tidak sengaja.

Karena hanya memeriksa alamat IP sumber, Standard ACL biasanya diletakkan sedekat mungkin dengan tujuan (*destination*) dari paket data untuk mencegah penyaringan terlalu awal terhadap lalu lintas yang mungkin berguna. Implementasi ACL dilakukan melalui baris perintah pada perangkat jaringan, di mana daftar ACL dibuat terlebih dahulu dan kemudian diaplikasikan ke interface tertentu dalam arah masuk (*inbound*) atau keluar (*outbound*). Hal ini memungkinkan router untuk melakukan pengambilan keputusan terhadap setiap paket yang melintas berdasarkan daftar aturan yang telah ditentukan.

Keunggulan utama Standard ACL terletak pada kesederhanaannya, membuatnya mudah dikonfigurasi dan dikelola, terutama bagi administrator jaringan pemula. Namun, karena hanya dapat mengevaluasi alamat IP sumber, kemampuannya sangat terbatas untuk skenario pengamanan kompleks yang memerlukan kontrol berdasarkan protokol, port, atau alamat tujuan. Untuk kebutuhan yang lebih mendalam, Extended ACL menjadi pilihan yang lebih tepat karena mampu menyaring lalu lintas berdasarkan berbagai parameter tambahan seperti protokol dan nomor port.

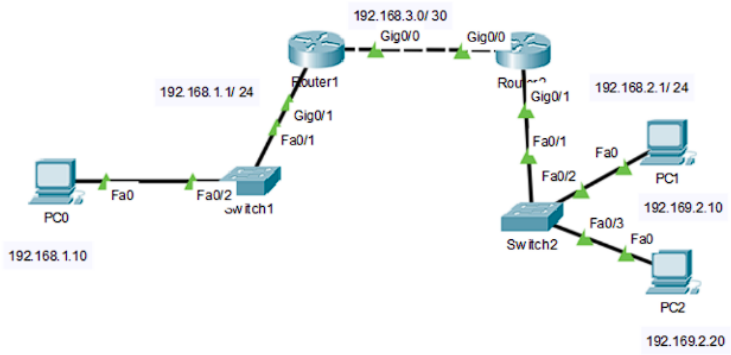
3. Prosedur

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

a. End devices: PC

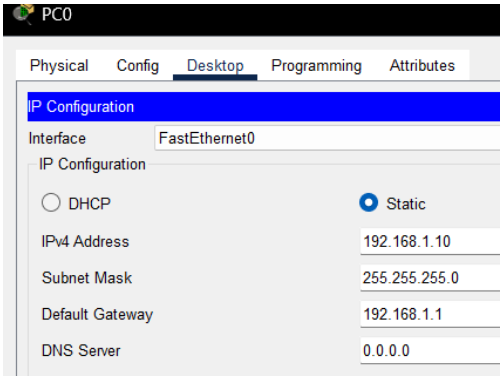
b. Network devices: Switch, Router

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

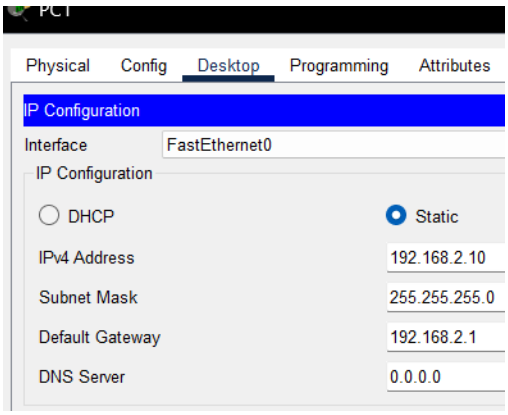


3.2. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

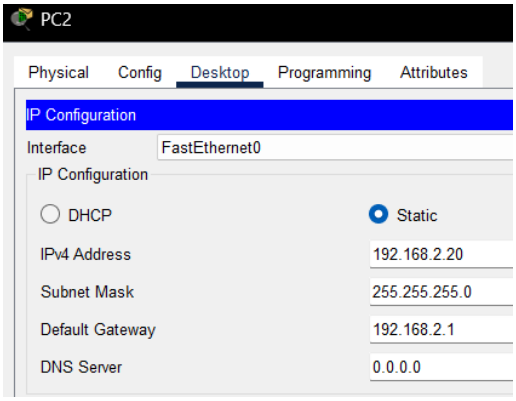
a. PC 0



b. PC 1



c. PC 2



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

a. Konfigurasi Fast Ethernet 0/0 dan Serial 2/0 pada Router 0

```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
% 192.168.1.0 overlaps with GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#ex
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.252
% 192.168.3.0 overlaps with GigabitEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
```

b. Konfigurasi Fast Ethernet 0/0 dan Serial 2/0 pada Router 1

```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
% 192.168.2.0 overlaps with GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#ex
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.3.2 255.255.255.252
% 192.168.3.0 overlaps with GigabitEthernet0/1
```

3.4. Lakukan konfigurasi static routing pada semua router

a. Router 0

```
outer(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
Invalid next hop address (it's this router)
outer(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
outer(config)#ex
outer#
```

b. Router 1

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
ping 192.168.1.1
```

3.5. Jalankan perintah Router# Router IP show pada router 0 dan 1, serta lakukan analisa

a. Router 0

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 [1/0] via 192.168.3.2
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

b. Router 1

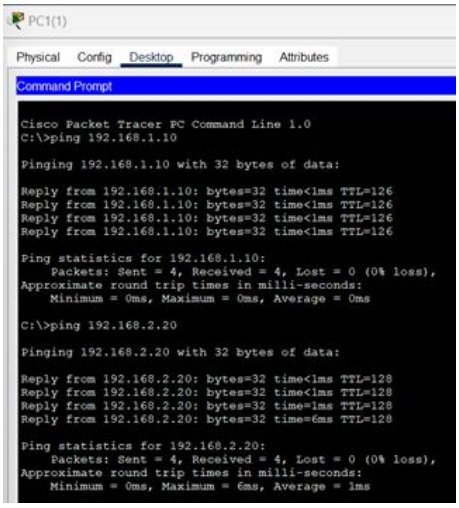
```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

S    192.168.1.0/24 [1/0] via 192.168.3.1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, GigabitEthernet0/0
L       192.168.3.2/32 is directly connected, GigabitEthernet0/0
```

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

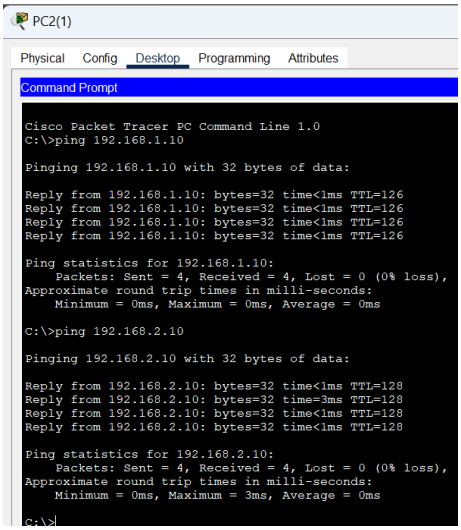
a. PC 0 ke PC lain

```
C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Reply from 192.168.2.20: bytes=32 time=5ms TTL=126
Reply from 192.168.2.20: bytes=32 time<1ms TTL=126
Reply from 192.168.2.20: bytes=32 time<1ms TTL=126
Reply from 192.168.2.20: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. PC 1 ke PC lain



c. PC 2 ke PC lain



3.7. Lakukan Konfigurasi Access Control List (ACL) pada router, analisa perintah tersebut

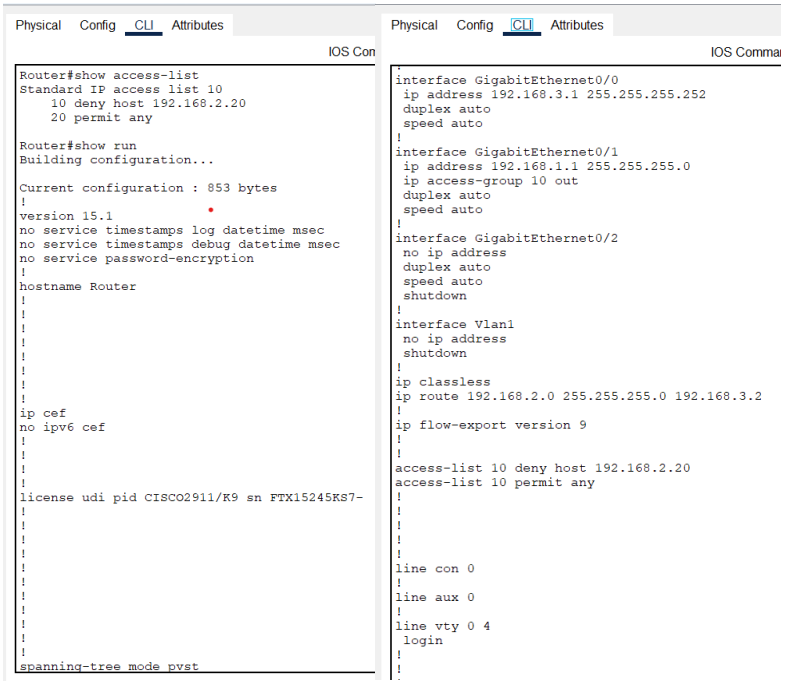
a. Lakukan blocking untuk koneksi single user dari Router1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.2.20 0.0.0.0
Router(config)#access-list 10 permit deny
                                      ^
% Invalid input detected at '^' marker.

Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Terapkan ACL pada interface yang dekat dengan destination

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip access-group 10 out
Router(config-if)#^z
                  ^
% Invalid input detected at '^' marker.
```

3.8. Lihat konfigurasi dengan perintah Router#show access-list dan Router#show run, lalu analisa



Physical Config CLI Attributes

IOS Con

```
Router#show access-list
Standard IP access list 10
    10 deny host 192.168.2.20
    20 permit any

Router#show run
Building configuration...

Current configuration : 853 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX15245KS7-
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
```

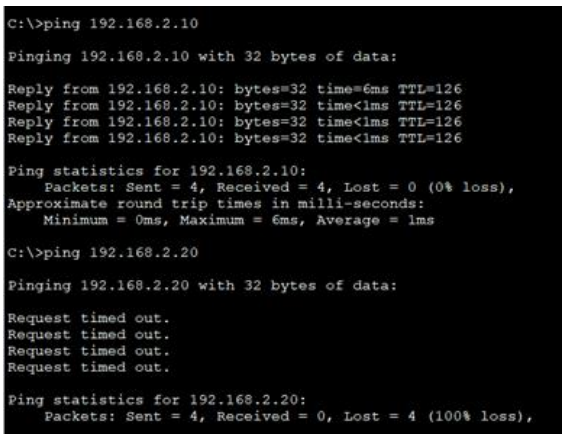
Physical Config CLI Attributes

IOS Comma

```
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 10 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.3.2
!
ip flow-export version 9
!
!
access-list 10 deny host 192.168.2.20
access-list 10 permit any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
```

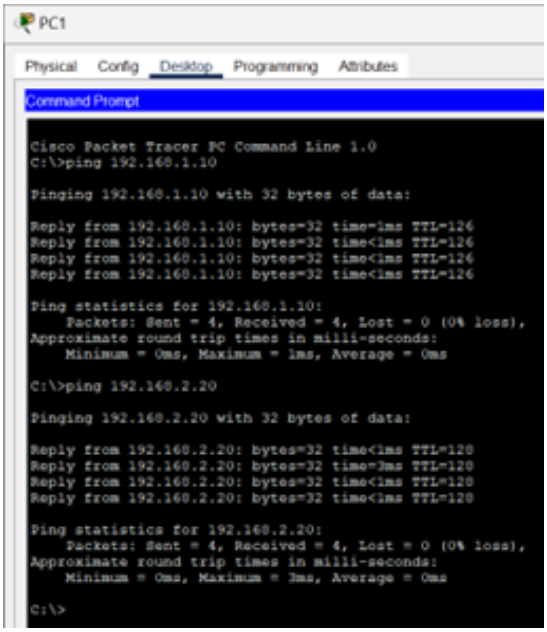
3.9. Gunakan perintah ping dari masing-masing PC ke PC lainnya, tampilkan hasilnya dan analisa, bandingkan dengan hasil percobaan pada Langkah no. 6

a. PC 0

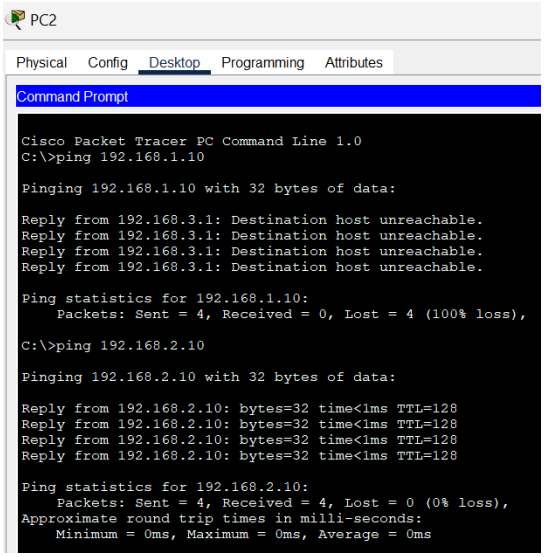


```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=6ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

b. PC 1



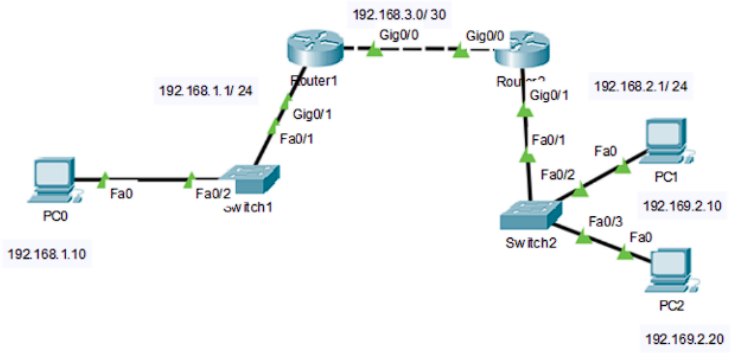
c. PC 2



4. Analisa

Pada Praktikum Kelima ini dilakukan percobaan untuk membuat topologi jaringan komputer dengan menggunakan filter ACL atau Access Control List. ACL ini adalah sekumpulan aturan atau filter yang diterapkan pada router atau switch di layer network untuk mengontrol lalu lintas jaringan. ACL tersebut akan menentukan izin atau permit dan larangan atau deny terhadap paket berdasarkan Alamat IP, protokol, dan port nya dari device pengirim dan device penerimanya. Hal ini untuk meningkatkan keaman jaringan di suatu device yang terhubung dari satu jaringan untuk membatasi aksesnya untuk jaringan diluarnya.

Pada praktikum kali ini akan dilakukan topologi Jaringan Komputer ACL Standart yang mana ini adalah jenis ACL yang paling sederhana. Berikut unutk topologinya:



Dari topologi tersebut terdapat dua router yaitu router 0 dan router 1, lalu tiga end device yaitu PC0, PC1, dan PC2. Router 1 akan menjadi gateaway jaringan 192.168.1.0 dan hostnya adalah PC0 dengan IP 192.168.1.10, lalu Router 0 akan menjadi gateaway jaringan 192.168.2.0 dan hostnya adalah PC1 dengan IP 192.168.2.10 dan PC2 dengan IP 192.168.2.20 agar antar end device bisa berkomunikasi router 1 dan router 0 dihubungkan dengan kabel ethernet di network 192.168.3.0/30.

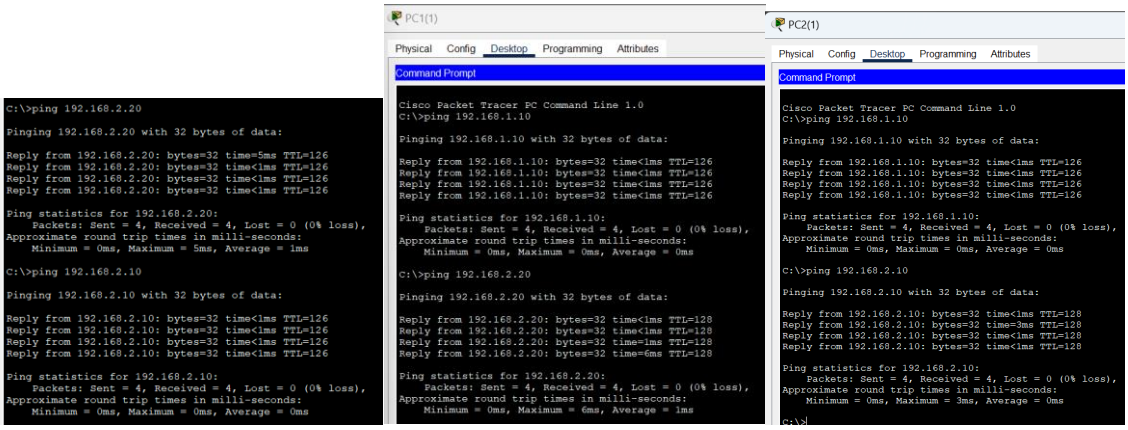
Setelah IP dan interface device di setting, lanjut untuk mengkoneksikan router 0 dan router 1 dengan koneksi static routing. Setelah dua router terkoneksi dengan settingan static routing, maka bisa di cek dahulu koneksi router dengan perintah show ip route. Berikut hasil dari Router 0 dan Router 1

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 [1/0] via 192.168.3.2
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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

S    192.168.1.0/24 [1/0] via 192.168.3.1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, GigabitEthernet0/0
L       192.168.3.2/32 is directly connected, GigabitEthernet0/0
```

Dapat dilihat dari dua gambar tersebut S menandakan bahwa router telah terkoneksi secara static mulai dari via 192.168.3.2 dan 192.168.3.1 yang mana Router 1 akan masuk ke jaringan 192.168.1.0 melalui Router 0 dan Router 0 masuk ke jaringan 192.168.2.0 melalui Router 1. Serta router secara lokal terkoneksi dengan jaringannya di masing-masing port GigabitEthernet.

Setelah semua terkoneksi maka lanjut untuk mengetes ping dari end device ke end device lainnya



Dari sini sudah terlihat static routing terkonfigurasi dengan benar dan seluruh end device sudah terkoneksi dan bisa berkomunikasi satu sama lain.

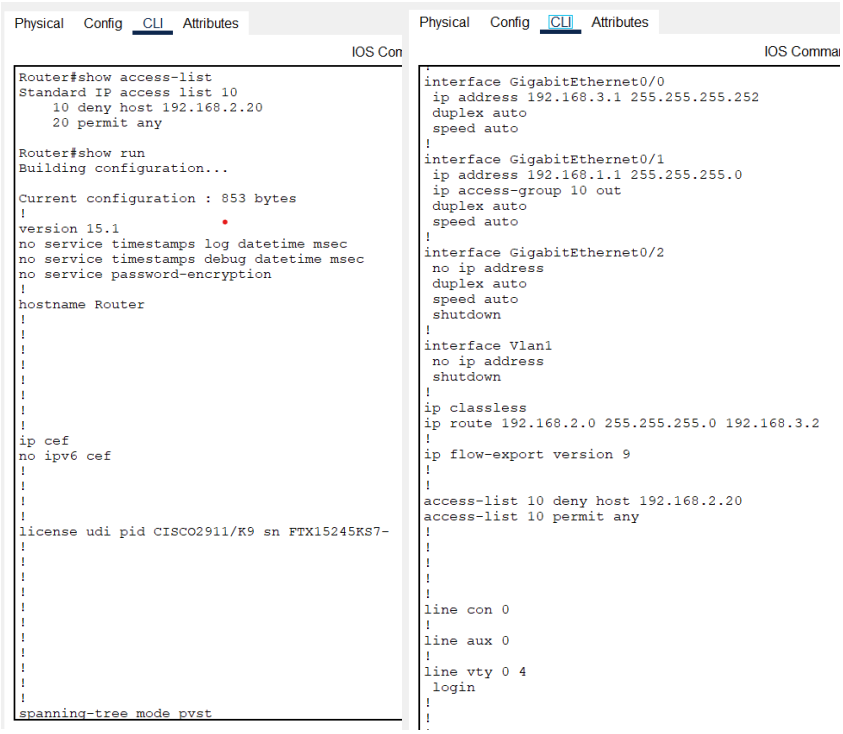
Lalu lanjut untuk memasukkan konfigurasi ACL untuk membatasi koneksi yang masuk ke jaringan Router1. Berikut perintahnya

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.2.20 0.0.0.0
Router(config)#access-list 10 permit deny
                                       ^
% Invalid input detected at '^' marker.

Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip access-group 10 out
Router(config-if)#^z
                  ^
% Invalid input detected at '^' marker.
```

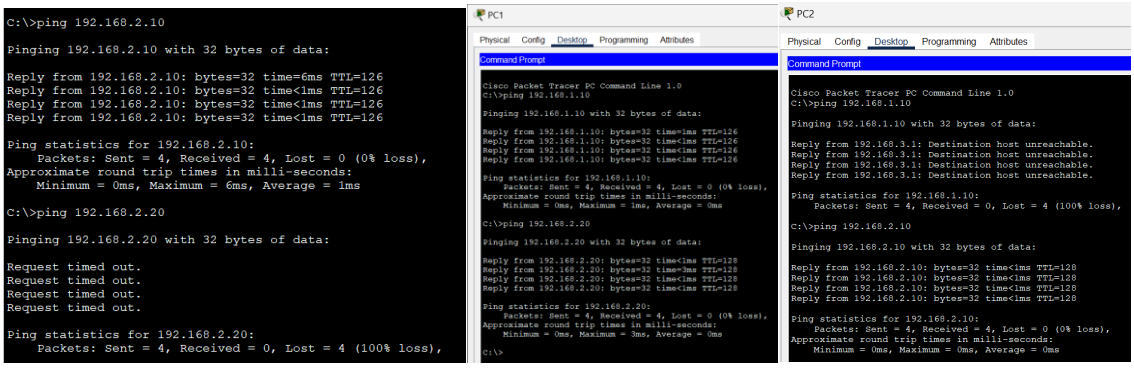
Dari perintah tersebut dapat dilihat ACL Standart hanya menggunakan rentang Access dari 1 hingga 99 dan dalam konfigurasi tersebut digunakan di nomor 10. Dalam perintah tersebut deny yang berarti memblokir IP 192.168.2.20 yang mana itu adalah PC 2. Jadi PC2 akan diblokir oleh router 1 agar tidak masuk kedalam jaringannya yaitu jaringan 192.168.1.1. Lalu setelah perintah deny ada perintah permit any yang mana mengindikasikan bahwa IP selain 192.168.2.20 diperbolehkan untuk masuk network 192.168.1.1 atau melewati router 1. Setelah dikonfigurasi langsung terapkan konfigurasi ACL tersebut ke interface terdekat dengan menggunakan interface atau media hubung port gig0/1 yang mana itu adalah jalan yang menghubungkan router 1 dan router 0. Interface tersebut menggunakan outbound ACL yang mana isi paket yang diterima oleh Router 1 akan diproses dahulu di Router baru dicek apakah IP pengirim berasal dari IP yang di blokir oleh konfigurasi ACL Router 1 nya.

Setelah selesai bisa di cek kebenaran konfigurasi ACL nya di router 0



Dapat dilihat bahwa di perintah access-list tersebut mendeny IP 192.168.2.20 dan mengizinkan IP pengirim selain yang di deny tersebut. Lalu di Show Run dapat dilihat konfigurasi IP dan interface dari Router 1 beserta static routingnya. Lalu juga ada setting dari ACL router 1 tersebut.

Setelah semua telah dikonfigurasi dan diverifikasi ACL nya, maka lanjut untuk mengecek komunikasi antar end devicenya. Berikut hasilnya



Dapat dilihat saat PC 0 mencoba berkomunikasi atau ping PC2 maka langsung RTO hasilnya karena IP pengirim dilihat oleh router 1 dan langsung diblokir karena tidak akan ada koneksi antar network 192.168.1.0 dengan IP 192.168.2.20. Dan juga saat PC 2 mencoba berkomunikasi ke PC 0 hasilnya data tetap terkirim tapi data host unreachable karena data packet tersebut terhenti di proses di router 1 saja dan tidak diteruskan ke host 192.168.1.10 atau PC 0. Tetapi saat PC 1 mencoba mengakses ping ke semua device, semua device dapat menerima keseluruhan ping nya. Hal ini sudah sesuai dengan setting standart ACL untuk memblokir 192.168.2.20 dan mengizinkan IP selain itu mengakses network dari router 1.

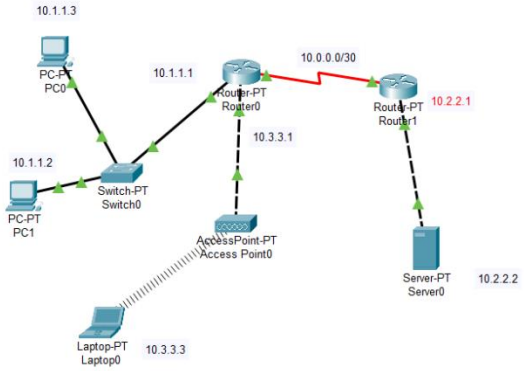
5. Tugas

5.1. 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, wifi



- Lakukan prosedur pengalamatan pada semua end device
- Lakukan prosedur konfigurasi interface pada semua router
- Lakukan konfigurasi static routing
- Lakukan pengujian dan analisa seperti pada prosedur percobaan no. 5 dan 6
- Lakukan konfigurasi ACL seperti berikut pada Router 1

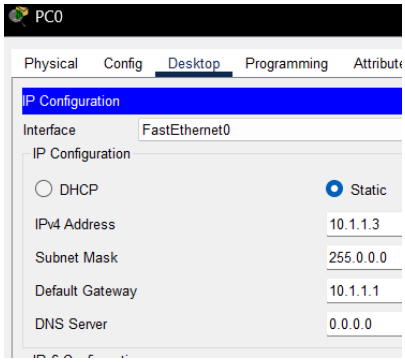
```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 20 permit 10.1.1.2
Router(config)#access-list 20 deny 10.1.1.0 0.0.0.255
Router(config)#access-list 20 permit 10.0.0.0 0.255.255.255
Router(config)#int se2/0
Router(config-if)#ip access-group 20 in
```

- Lakukan pengujian dan analisa seperti pada prosedur percobaan no 8 dan 9

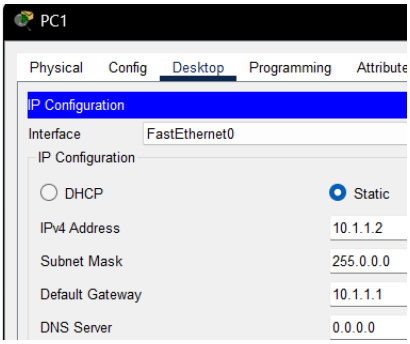
Jawab:

- Pengalamatan end device

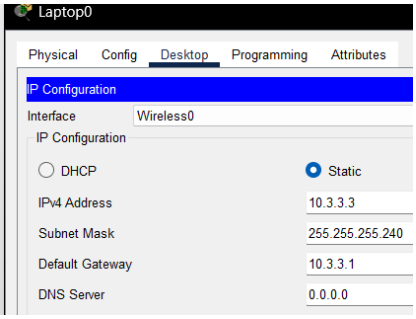
a. PC 0



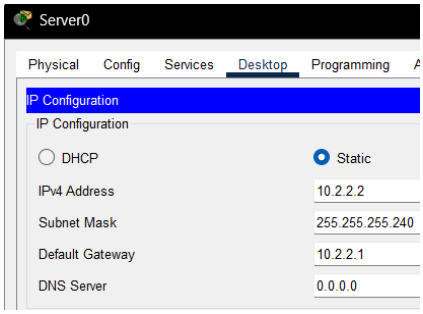
b. PC 1



c. Laptop 0

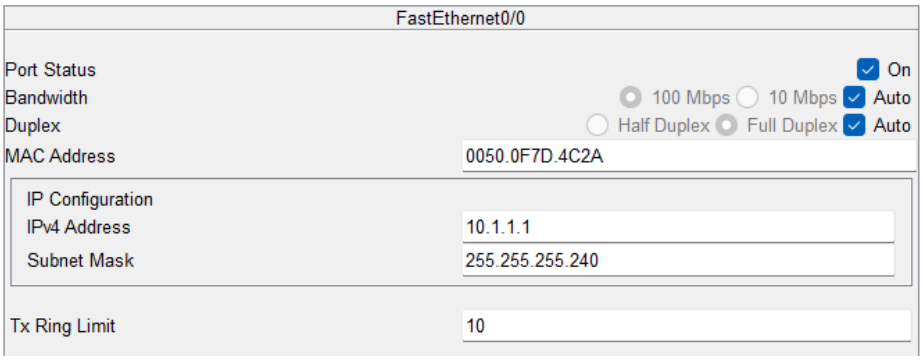


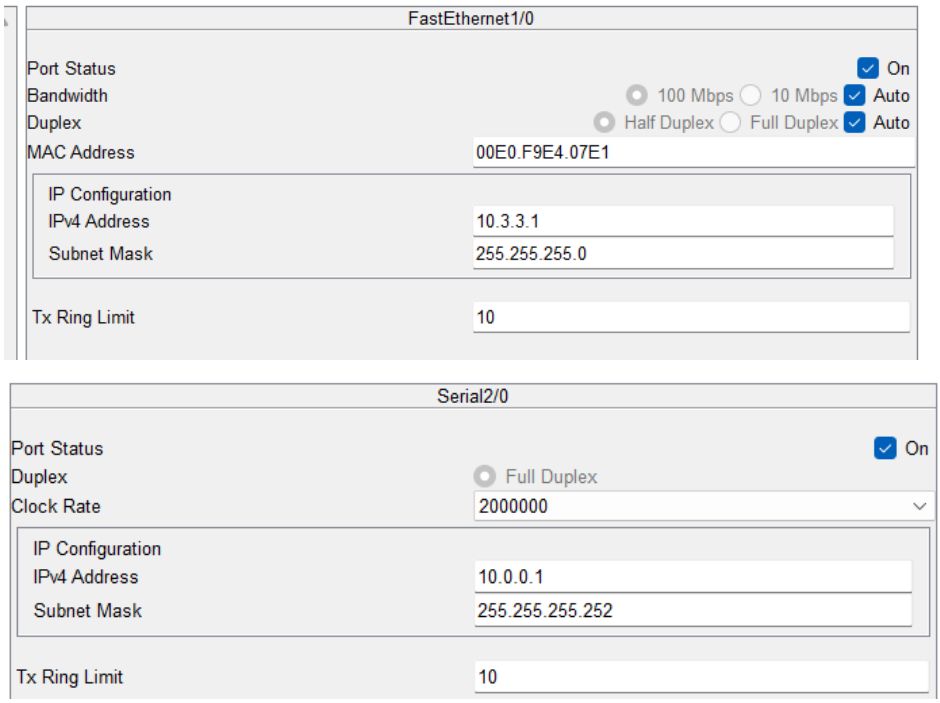
d. Server 0



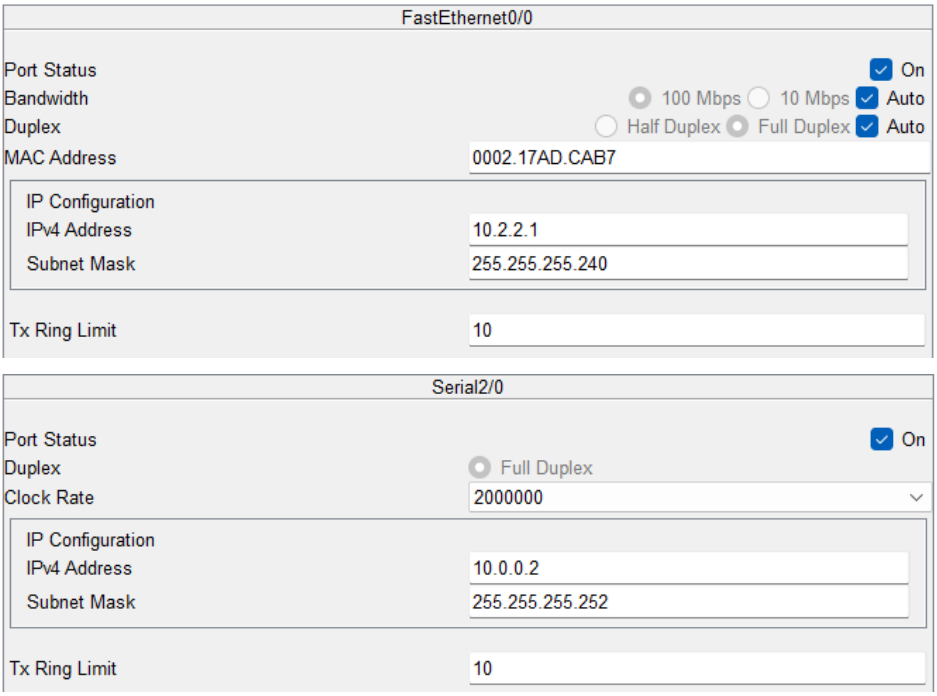
- Konfigurasi Interface Router

a. Router 0

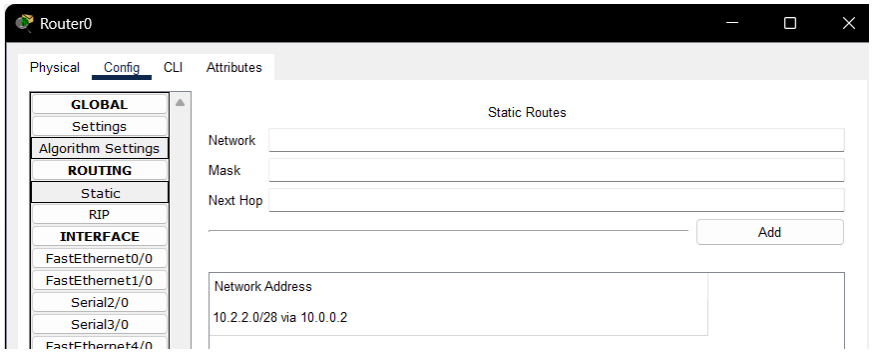



FastEthernet1/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F9E4.07E1
IP Configuration
IPv4 Address
10.3.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.0.0.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10

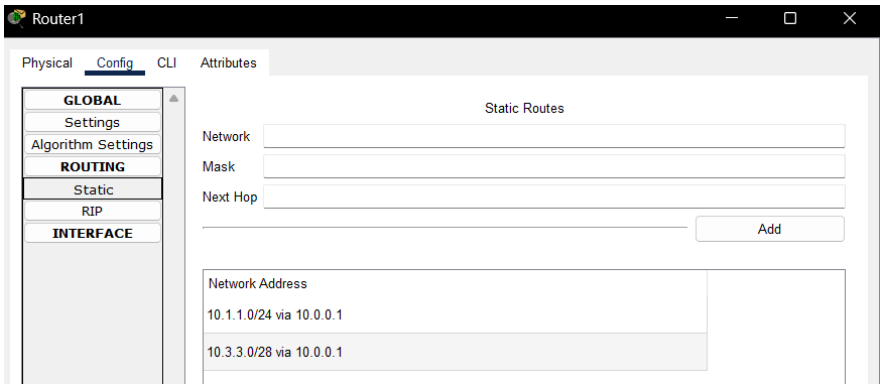
b. Router 1


FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.17AD.CAB7
IP Configuration
IPv4 Address
10.2.2.1
Subnet Mask
255.255.255.240
Tx Ring Limit
10
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.0.0.2
Subnet Mask
255.255.255.252
Tx Ring Limit
10

- Konfigurasi static Routing Router
  a. Router 0



  b. Router 1



- Pengujian Router#show ip route
  a. Router 0

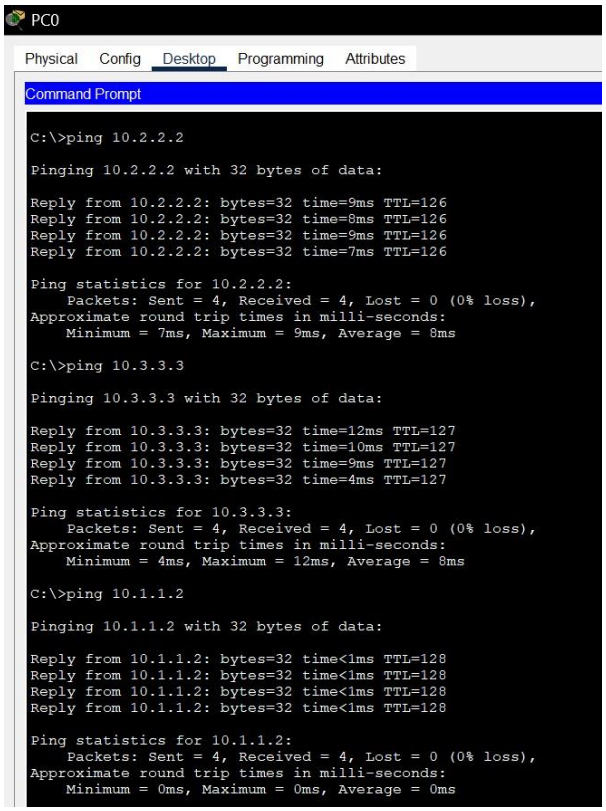
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.0.0.0/30 is directly connected, Serial2/0
C       10.1.1.0/28 is directly connected, FastEthernet0/0
S       10.2.2.0/28 [1/0] via 10.0.0.2
C       10.3.3.0/24 is directly connected, FastEthernet1/0
```

  b. Router 1

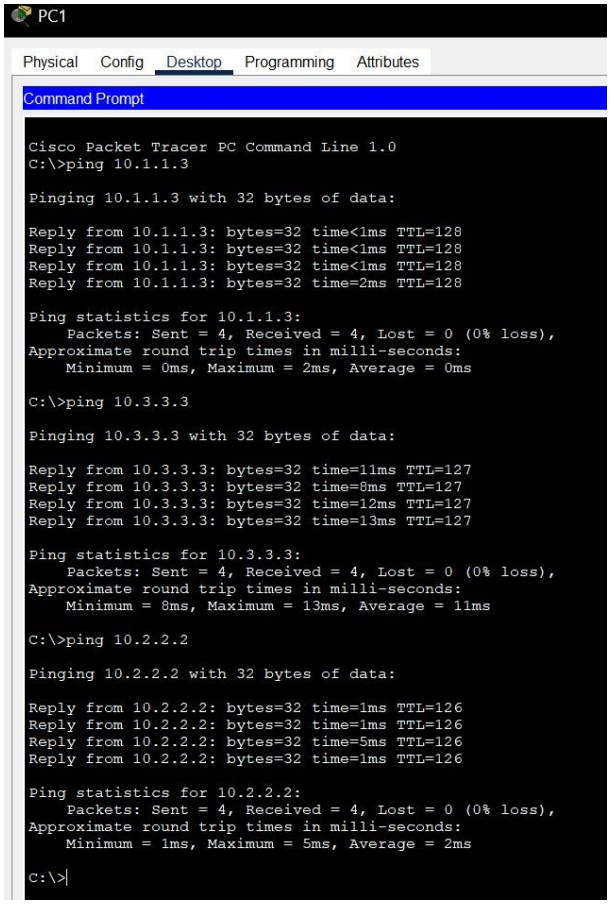
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.0.0.0/30 is directly connected, Serial2/0
S       10.1.1.0/24 [1/0] via 10.0.0.1
C       10.2.2.0/28 is directly connected, FastEthernet0/0
S       10.3.3.0/28 [1/0] via 10.0.0.1
```

- Pengujian tes ping dari masing-masing end device

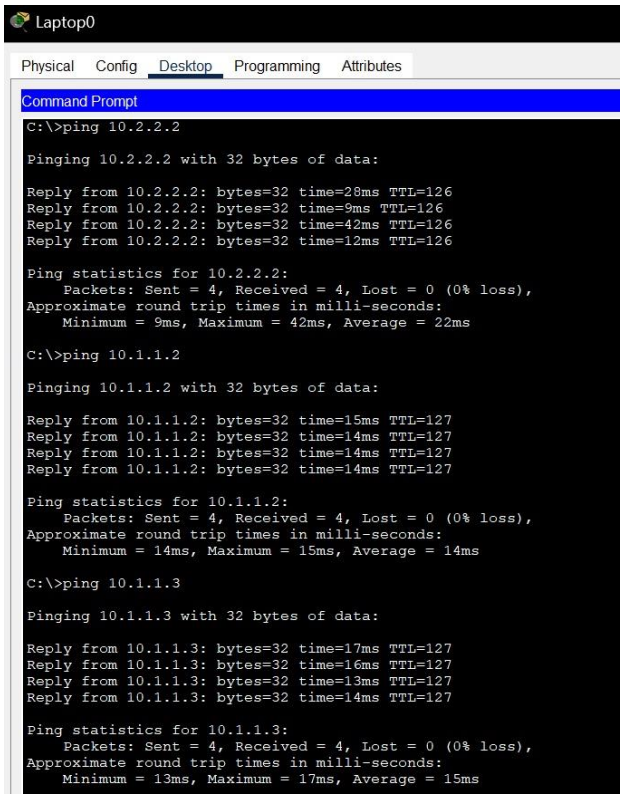
  a. PC 0



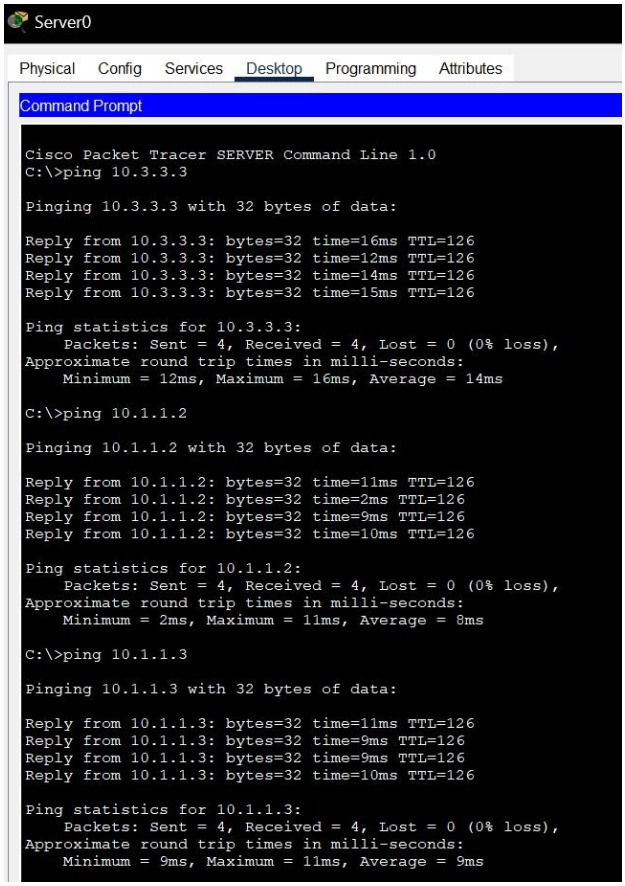
b. PC 1



c. Laptop 0



d. Server 0



- Konfigurasi ACL pada Router 1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 20 permit 10.1.1.2
Router(config)#access-list 20 deny 10.1.1.0 0.0.0.255
Router(config)#access-list 20 permit 10.0.0.0 0.255.255.255
Router(config)#int se2/0
Router(config-if)#ip access-group 20 in
```

- Pengujian Router#show access-list dan Router#show run pada router 1

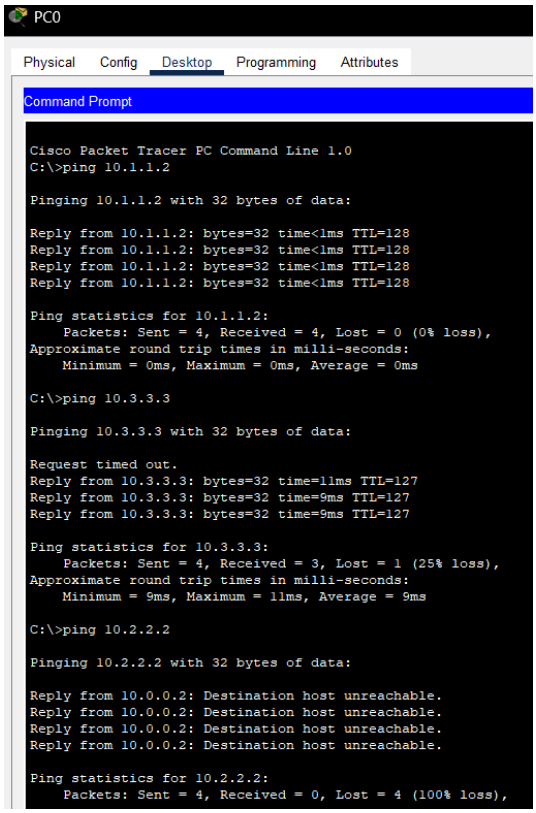
```
Router#show access-list
Standard IP access list 20
    10 permit host 10.1.1.2 (8 match(es))
    20 deny 10.1.1.0 0.0.0.255 (8 match(es))
    30 permit 10.0.0.0 0.255.255.255 (8 match(es))

Router#sh run
Building configuration...

Current configuration : 1108 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
```

```
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.0.0.2 255.255.255.252
 ip access-group 20 in
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
interface FastEthernet6/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet7/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
ip route 10.1.1.0 255.255.255.0 10.0.0.1
ip route 10.3.3.0 255.255.255.240 10.0.0.1
!
```

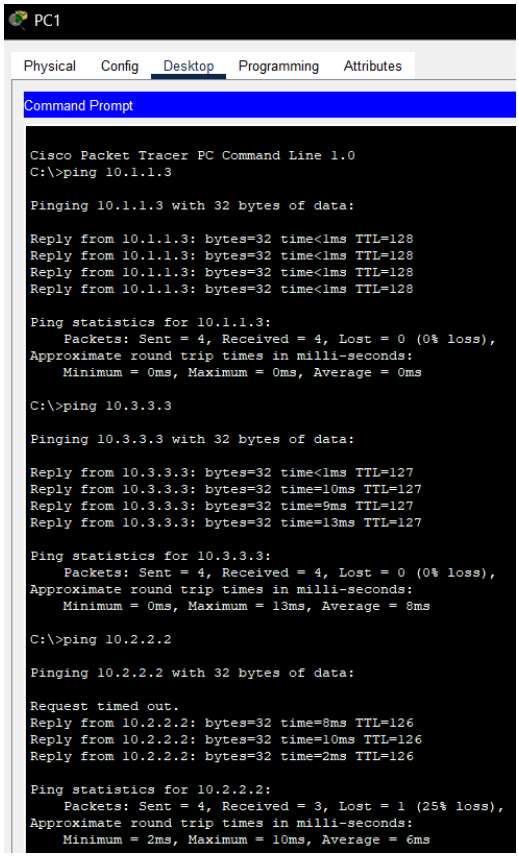
```
ip flow-export version 9
!
!
access-list 20 permit host 10.1.1.2
access-list 20 deny 10.1.1.0 0.0.0.255
access-list 20 permit 10.0.0.0 0.255.255.255
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

- Pengujian tes ping dari masing-masing end device

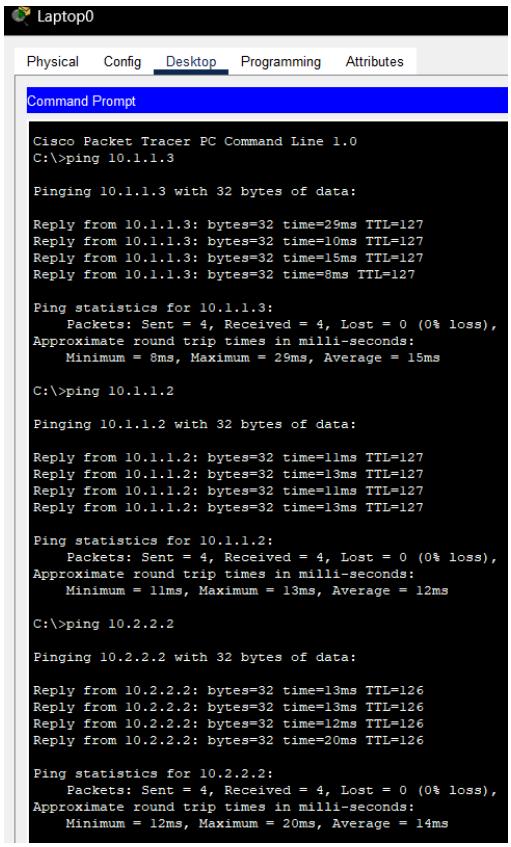
a. PC 0



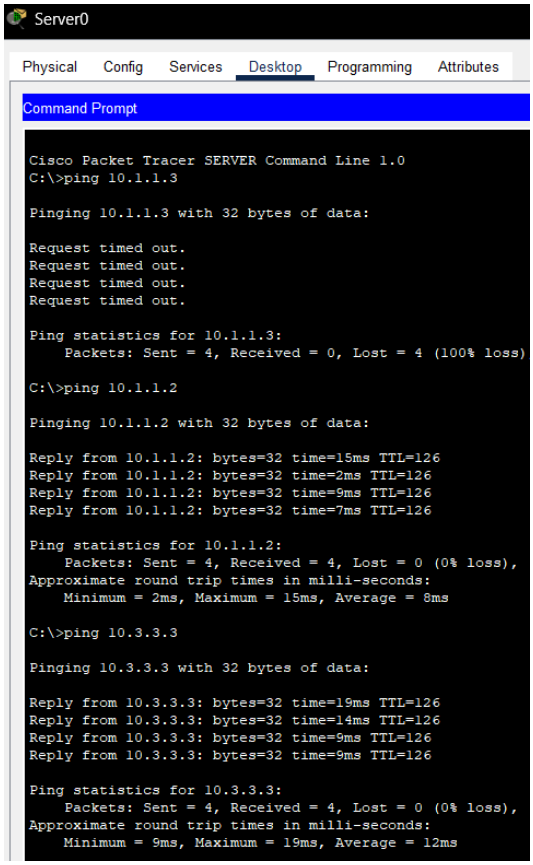
b. PC 1



c. Laptop 0



d. Server 0



Pada bagian tugas ini akan membuat topologi standart ACL tersebut yang mana terdapat 4 end device yaitu PC0, PC1, laptop1, dan Server0 serta ada dua router yaitu Router 1 dan Router 0 untuk menghubungkan dua jaringan tersebut. Semua IP dan interface akan dikonfigurasikan seperti hasilnya diatas.

Lalu hasil awal show ip route sebelum di ACL adalah

```
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

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.0.0.0/30 is directly connected, Serial2/0
C       10.1.1.0/28 is directly connected, FastEthernet0/0
S       10.2.2.0/28 [1/0] via 10.0.0.2
C       10.3.3.0/24 is directly connected, FastEthernet1/0
```

```
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

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.0.0.0/30 is directly connected, Serial2/0
S       10.1.1.0/24 [1/0] via 10.0.0.1
C       10.2.2.0/28 is directly connected, FastEthernet0/0
S       10.3.3.0/28 [1/0] via 10.0.0.1
```

Hasil tersebut menunjukkan Kedua router telah dikonfigurasi static routingnya dan bedanya dengan percobaan adalah tidak ada label Local atau L karena antar router tidak dihubungkan dengan kabel ethernet tapi dihubungkan dengan kebel serial. Hasil dari perintah tersebut adalah network 10.2.2.0 terkoneksi secara static via gerbang 10.0.0.2 lalu network 10.1.10 dan 10.3.3.0 terhubung secara static via gerbang 10.0.0.1.

Lalu hasil dari ping antar end devicenya adalah semuanya terkoneksi dengan baik dan bisa membalas ping nya antar end device satu sama lain.

Lalu setelah semua end device bisa terhubung dan terkoneksi secara static, konfigurasi ACL pada router 1 dilakukan sebagai berikut,

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 20 permit 10.1.1.2
Router(config)#access-list 20 deny 10.1.1.0 0.0.0.255
Router(config)#access-list 20 permit 10.0.0.0 0.255.255.255
Router(config)#int se2/0
Router(config-if)#ip access-group 20 in
```

Di konfigurasi tersebut IP 10.1.1.1 di izinkan untuk melewati router 1, Tetapi end device lainnya di network 10.1.10 dilarang melewati Router 1. Lalu network 10.0.0.0 juga diperbolehkan untuk melewati Router 1 yang mana 10.0.0.0 ini adalah network dari hubungan Router 0 dengan Router 1.

Hasilnya di tes konfigurasi show run dan access-list adalah

```
Router#show access-list
Standard IP access list 20
    10 permit host 10.1.1.2 (8 match(es))
    20 deny 10.1.1.0 0.0.0.255 (8 match(es))
    30 permit 10.0.0.0 0.255.255.255 (8 match(es))

Router#sh run
Building configuration...

Current configuration : 1108 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
```

```
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.0.0.2 255.255.255.252
 ip access-group 20 in
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
interface FastEthernet6/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet7/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
ip route 10.1.1.0 255.255.255.0 10.0.0.1
ip route 10.3.3.0 255.255.255.240 10.0.0.1
!
```

```
ip flow-export version 9
!
!
access-list 20 permit host 10.1.1.2
access-list 20 deny 10.1.1.0 0.0.0.255
access-list 20 permit 10.0.0.0 0.255.255.255
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Dapat dilihat bahwa settingan ACL sudah tersimpan di settingan Router 1 tersebut dan IP seta interface yang terdaftar dalam Router 1 tersebut juga dapat dilihat secara keseluruhan.

Setelah itu dicek untuk hasil komunikasi ping antar devicenya. Dalam gambar tersebut didapatkan bahwa PC0 dapat mengakses semua end device selain end device 10.2.2.2 karena PC 0 termasuk IP device atau network nya di blokir oleh konfigurasi ACL. Sedangkan PC1 masih bisa mengakses end device 10.2.2.2 atau server0, hal ini dikarenakan PC1 dikecualikan untuk masuk dan diizinkan melalui Router 1. Dan Laptop 1 juga diperbolehkan untuk mengakses seluruh end device yang ada. Tetapi, untuk server0 saat mencoba berkomunikasi ping dengan PC0 langsung RTO, hal ini karena saat pengiriman dilihat bahwa terdapat IP 10.1.1.3 yang mana network nya diblokir oleh router 1 sebagai gateaway Server-, alhasil data

packet diblokir dan tidak diteruskan ke Router 0. Lalu untuk Ping lainnya masih bisa terkoneksi dengan baik.

5.2. Jelaskan Perbedaan inbound ACL dan outbound ACL

Jawab:

Inbound ACL adalah kondisi Dimana konfigurasi ACL tersebut mengkonfigurasi bahwa packet atau sistem traffic yang akan masuk ke router akan di cek terlebih dahulu sebelum di proses lebih lanjut oleh router, Jikalau packet ataua sistem trafficnya ditolak maka tidak akan masuk router tersebut sama sekali. Konfigurasi untuk inbound ACL adalah Router(config-if)#ip access-group 10 in.

Outbond ACL adalah kondisi ACL tersebut memperbolehkan packet atau sistem traffic masuk terlebih dahulu ke router untuk diproses lebih lanjut. Traffic atau packet tersebut akan di cek setelah keluar dari interface routernya, jikalau ditolak maka packet atau sistem traffic tidak jadi dikirim keluar router. Lalu konfigurasi outbond ACL nya adalah Router(config-if)#ip access-group 10 out.

Kedua fitur ini memiliki perbedaan di efisiensi nya yaitu untuk Inbound ACL memiliki efisiensi yang lebih tinggi dari pada outbond ACL karena paket data tersebut ditolak sebelum di proses oleh router yang tentunya hal ini akan membuang waktu jika router sudah memproses data tersebut tapi tidak jadi diteruskan keluar. Walaupun Inbound lebih efisien ada bebrapa kondisi outbond ACL tetap digunakan tergantung bagaimana topologi jaringannya.

6. Kesimpulan

Konfigurasi ACL (Access Control List) pada router merupakan metode penting untuk meningkatkan keamanan jaringan dengan cara membatasi akses data berdasarkan alamat IP, protokol, atau port tertentu. Dalam praktikum ini, penggunaan ACL Standar berhasil diterapkan untuk memblokir perangkat tertentu agar tidak dapat mengakses jaringan lain. ACL Standar bekerja dengan cara menetapkan aturan yang diterapkan pada interface router, baik sebagai *inbound* (penyaringan sebelum paket diproses oleh router) maupun *outbound* (penyaringan sebelum paket keluar dari router). Melalui konfigurasi ini, dapat dibuktikan bahwa router mampu menolak paket yang datang dari IP yang diblokir dan hanya mengizinkan paket yang sesuai dengan aturan ACL.

Pengujian menunjukkan bahwa ACL berhasil membatasi akses perangkat tertentu sesuai konfigurasi yang ditentukan. Penggunaan ACL secara tepat tidak hanya mencegah akses yang tidak diinginkan tetapi juga dapat menjaga performa jaringan dengan memfilter lalu lintas lebih awal, terutama jika menggunakan *inbound ACL*. Meskipun begitu, pemilihan antara *inbound* atau *outbound* ACL tetap bergantung pada topologi jaringan dan kebutuhan pengendalian lalu lintas di setiap interface router. Dengan demikian, pemahaman dan penerapan ACL yang tepat sangat krusial dalam manajemen dan keamanan jaringan komputer.