

1. Tujuan
   1. Mahasiswa mampu menjelaskan konsep standard Access Control List (ACL)
   2. Mahasiswa mampu melakukan konfigurasi ACL pada router
   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.

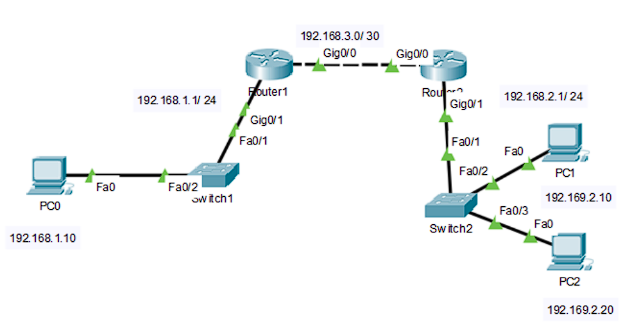
Keunggulan utama Standard ACL terletak pada kesederhanaannya, membuatnya mudah dikonfigurasi dan dikelola, terutama bagi administrator jaringan pemula. Namun, karena hanya dapat mengevaluasi alamat IP sumber, kemampuannya sangat terbatas untuk skenario pengamanan kompleks yang memerlukan kontrol berdasarkan 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.

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

a. End devices: PC

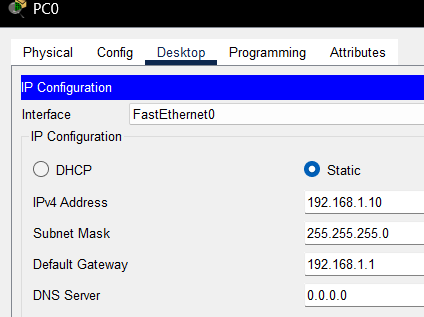
b. Network devices: Switch, Router

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

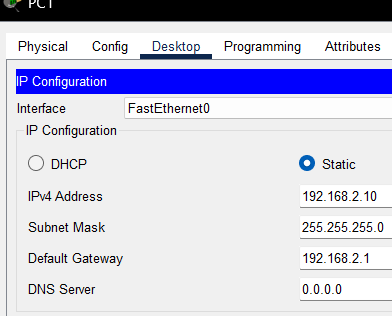


* 1. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

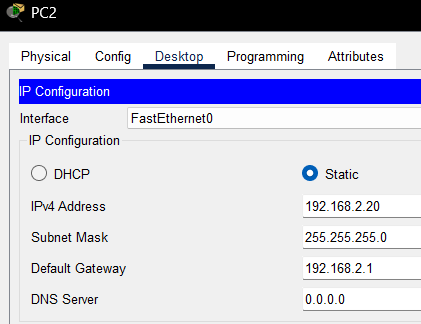
1. PC 0



1. PC 1

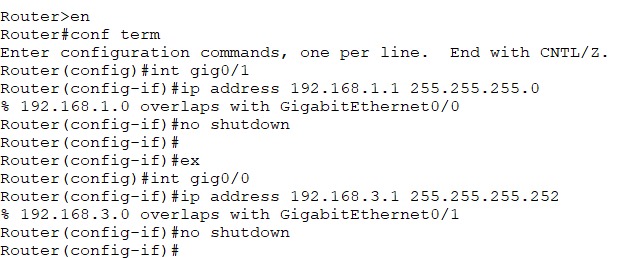


1. PC 2

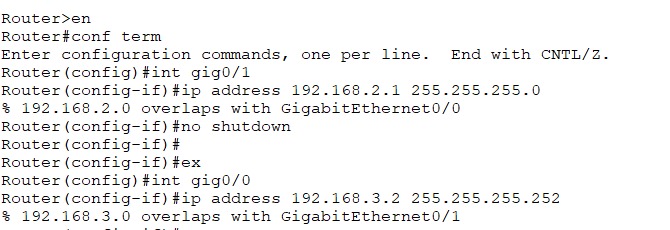


* 1. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

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

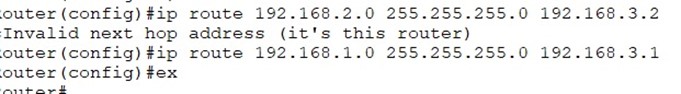


1. Konfigurasi Fast Ethernet 0/0 dan Serial 2/0 pada Router 1

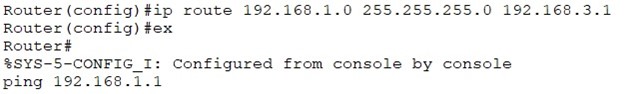


* 1. Lakukan konfigurasi static routing pada semua router

1. Router 0

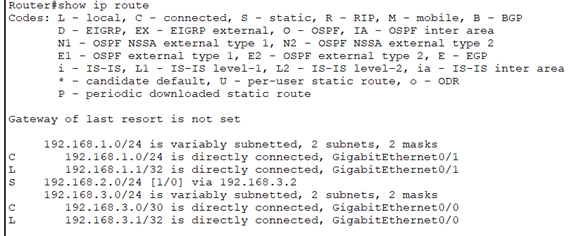


1. Router 1

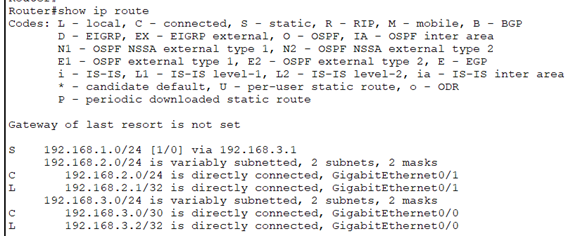


* 1. Jalankan perintah Router# Router IP show pada router 0 dan 1, serta lakukan analisa

1. Router 0

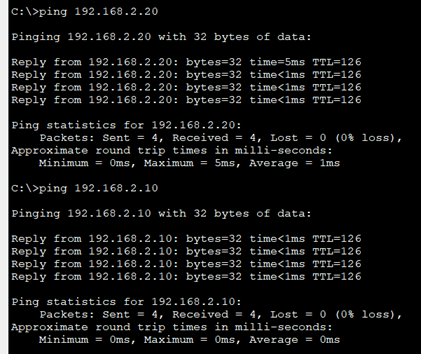


1. Router 1

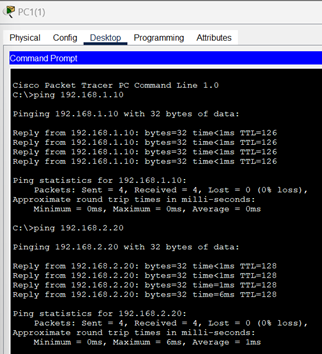


* 1. Lakukan tes ping ke semua PC, kemudian tampilkan hasil percobaan dan analisa anda.

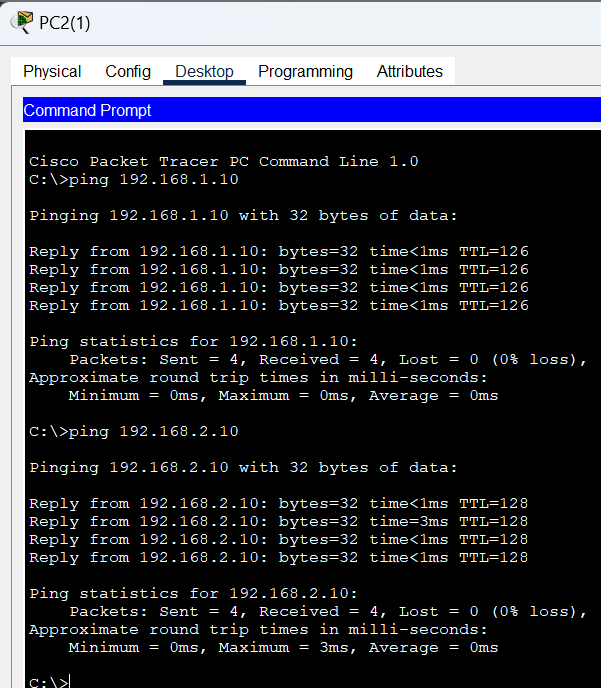
1. PC 0 ke PC lain



1. PC 1 ke PC lain

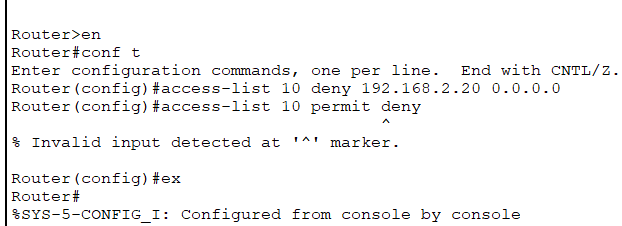


1. PC 2 ke PC lain

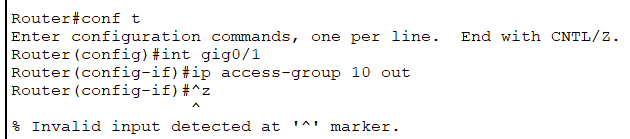


* 1. Lakukan Konfigurasi Access Control List (ACL) pada router, analisa perintah tersebut

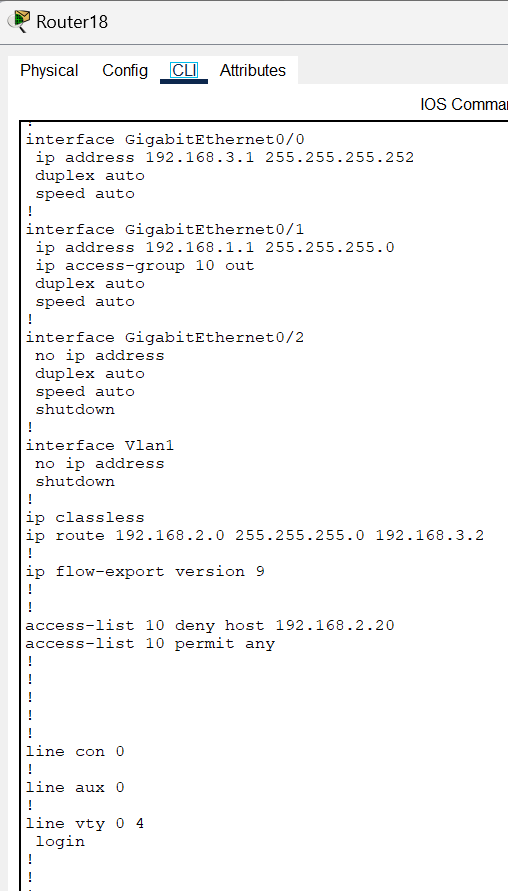
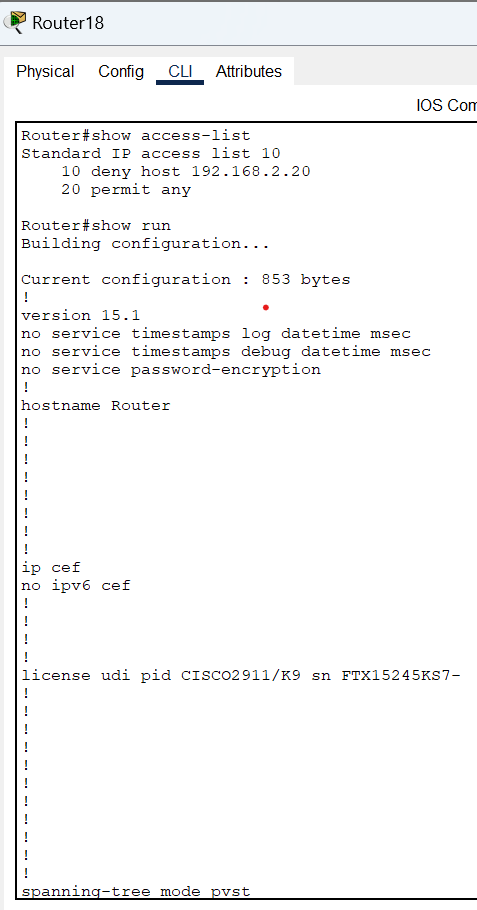
1. Lakukan blocking untuk koneksi single user dari Router1



1. Terapkan ACL pada interface yang dekat dengan destination

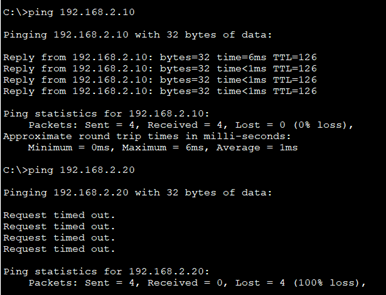


* 1. Lihat konfigurasi dengan perintah Router#show access-list dan Router#show run, lalu analisa

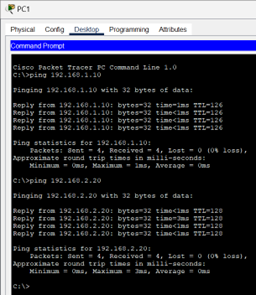


* 1. Gunakan perintah ping dari masing-masing PC ke PC lainnya, tampilkan hasilnya dan analisa, bandingkan dengan hasil percobaan pada Langkah no. 6

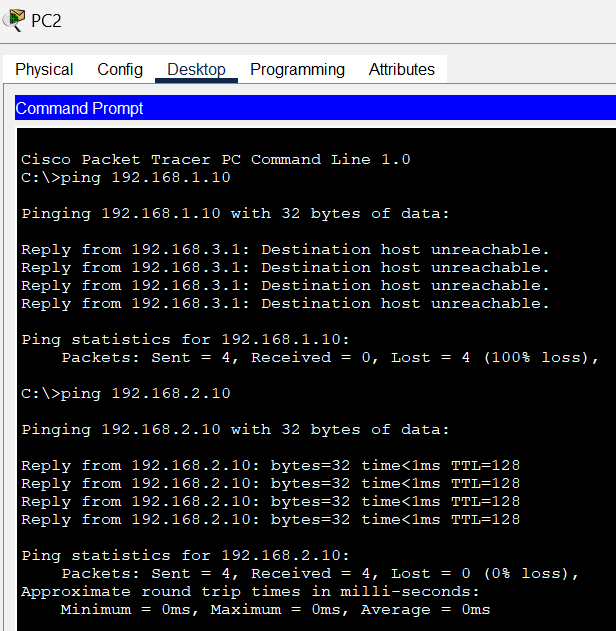
1. PC 0



1. PC 1



1. PC 2



1. Analisa

Pada Praktikum Kelima ini

1. Kesimpulan

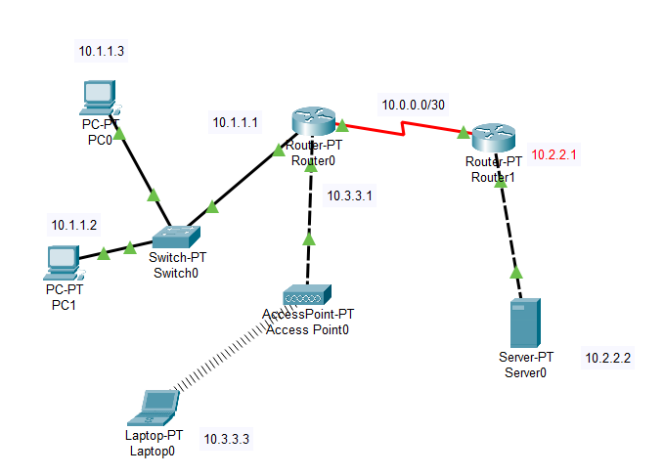
Pada praktikum ini berhasil dilakukan konfigurasi dynamic routing menggunakan BGP (Border Gateway Protocol) sebagai protokol Exterior Gateway Protocol (EGP) untuk komunikasi antar Autonomous System (AS), dan OSPF sebagai Interior Gateway Protocol (IGP) untuk komunikasi routing di dalam satu AS. Praktikum menunjukkan bahwa BGP memungkinkan pertukaran informasi rute antar jaringan yang dikelola oleh entitas berbeda, seperti antar ISP, sementara OSPF berfungsi untuk mendistribusikan rute secara efisien dalam satu organisasi atau AS. Dengan menggunakan perintah redistribute, integrasi antara BGP dan OSPF juga berhasil diterapkan sehingga jaringan dari dua domain routing berbeda dapat saling terhubung dan saling bertukar rute, memungkinkan komunikasi end-to-end antar seluruh perangkat di jaringan. Hasilnya, semua perangkat bisa saling ping dan berkomunikasi meskipun berasal dari domain yang berbeda baik dari sisi BGP maupun OSPF.

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

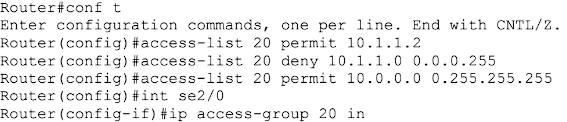
a. End devices: PC

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

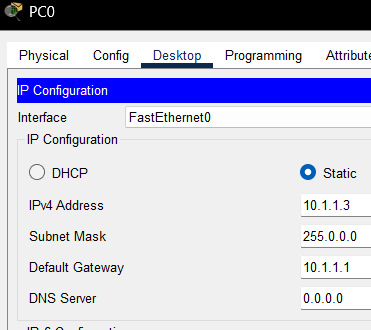


* Lakukan pengujian dan analisa seperti pada prosedur percobaan no 8 dan 9

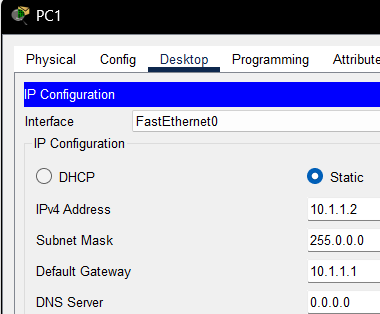
Jawab:

* Pengalamatan end device

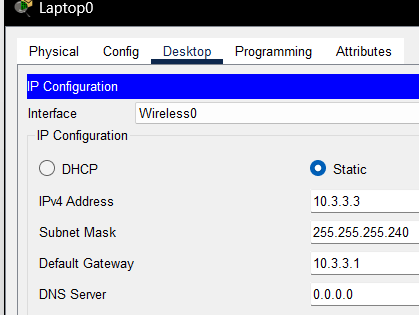
1. PC 0



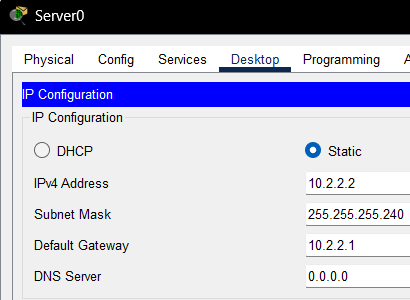
1. PC 1



1. Laptop 0

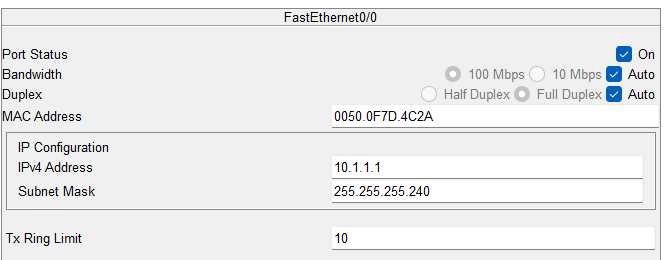


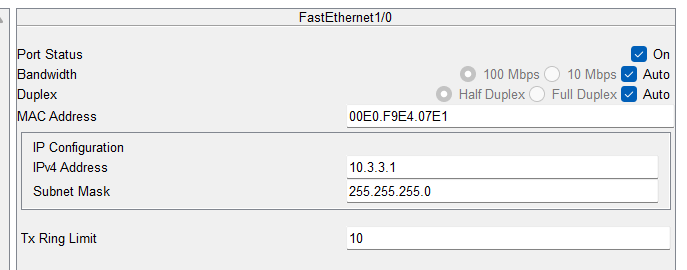
1. Server 0

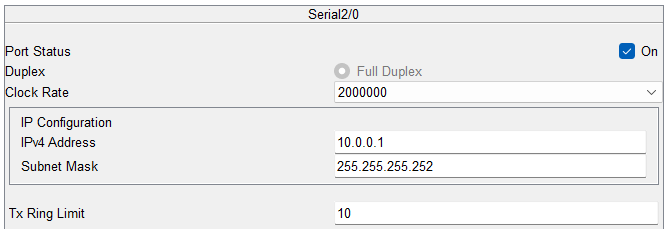


* Konfigurasi Interface Router

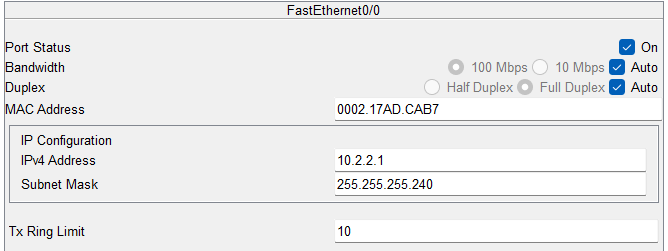
1. Router 0

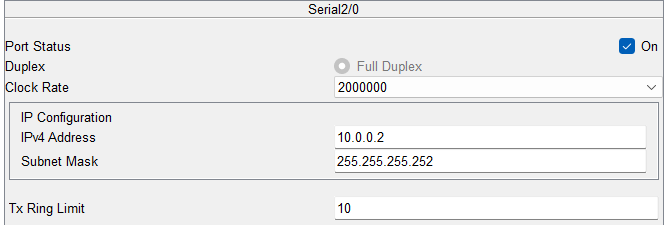






1. Router 1



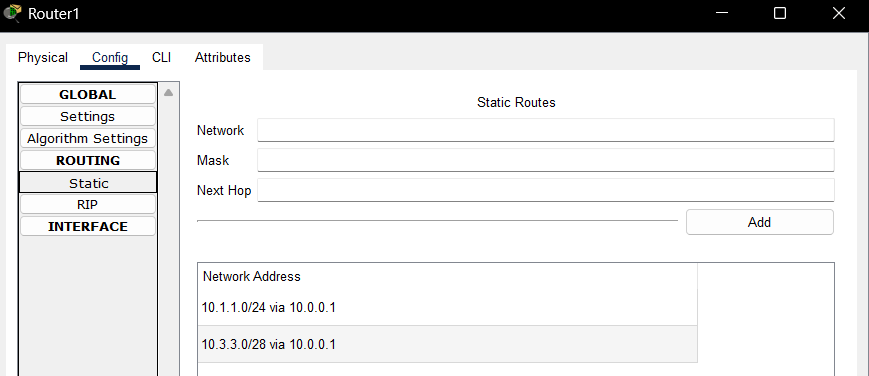


* Konfigurasi static Routing Router

1. Router 0

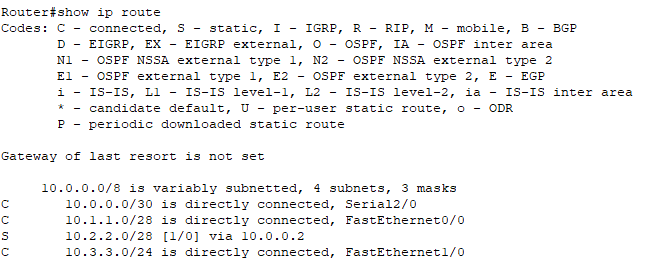


1. Router 1

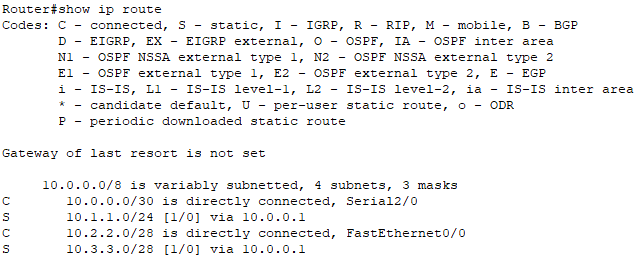


* Pengujian Router#show ip route

1. Router 0

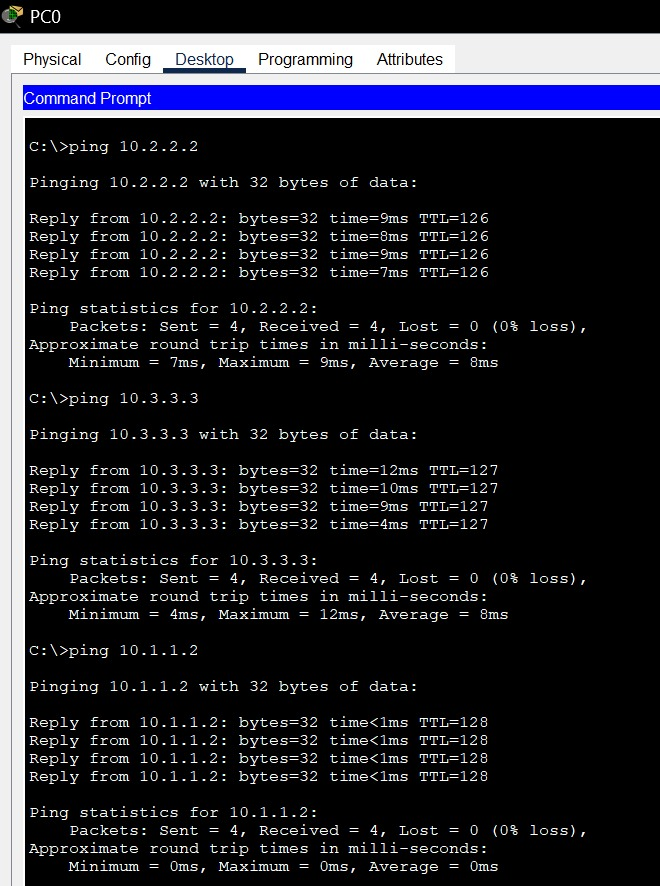


1. Router 1

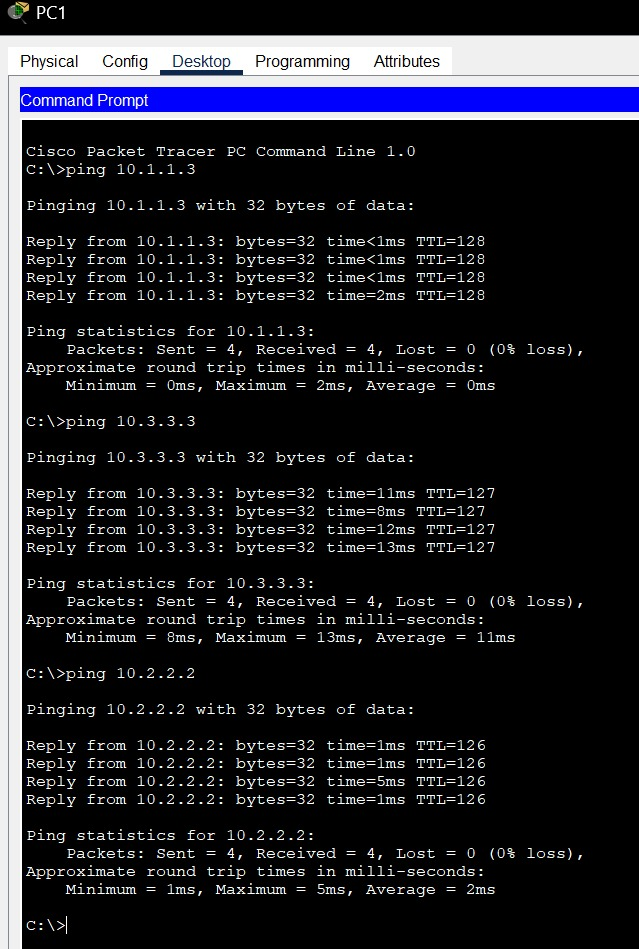


* Pengujian tes ping dari masing-masing end device

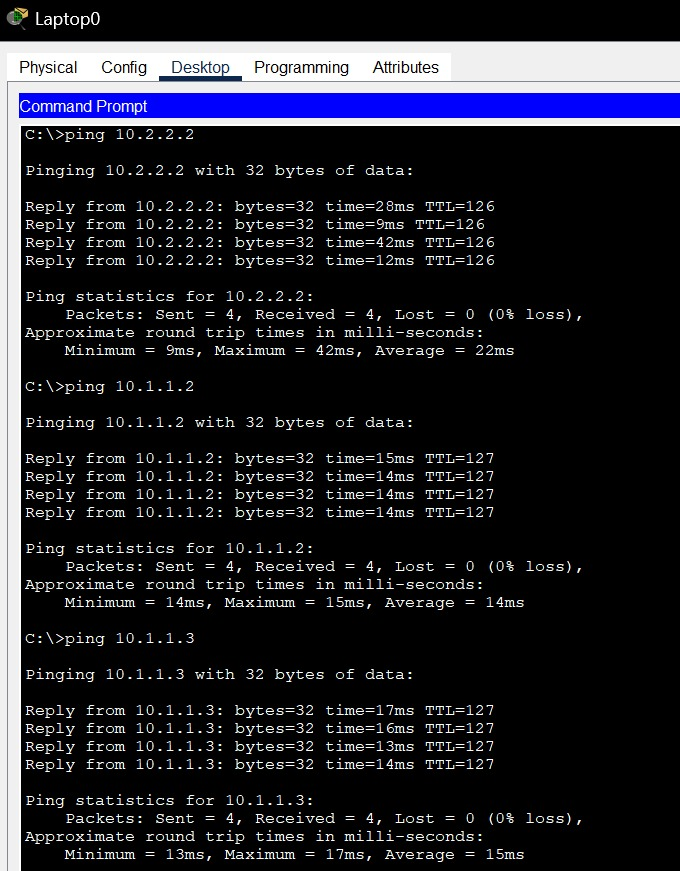
1. PC 0



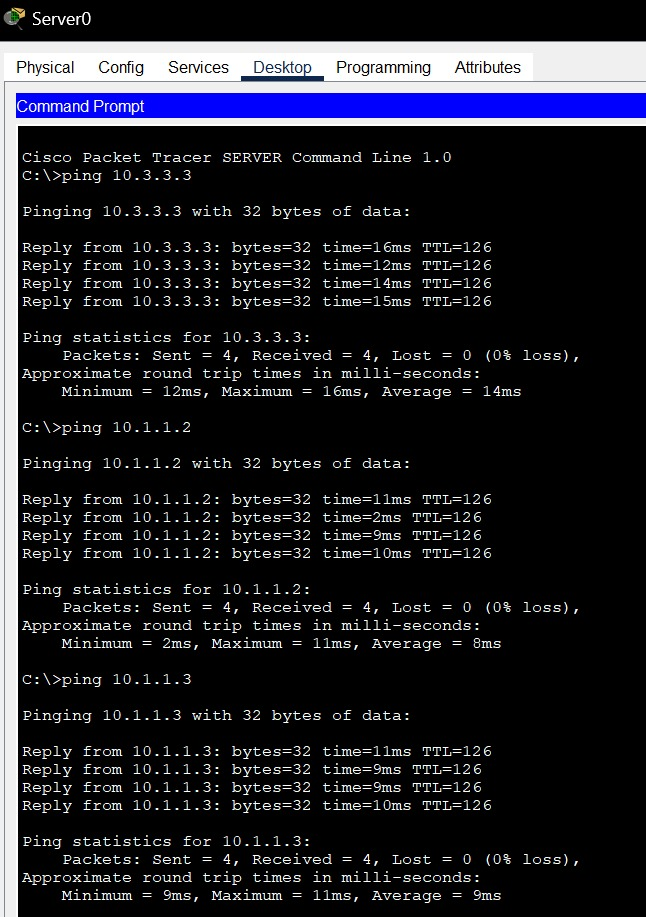
1. PC 1



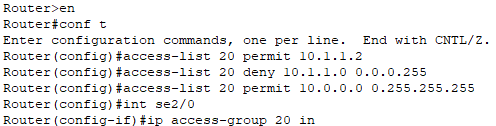
1. Laptop 0



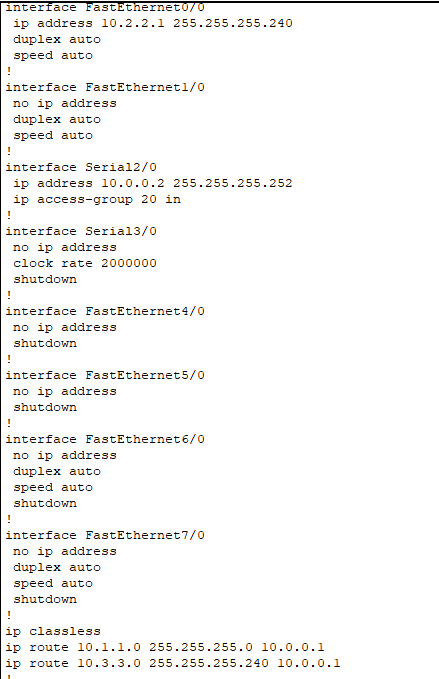
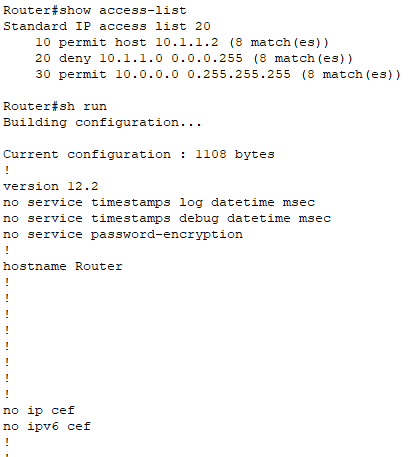
1. Server 0

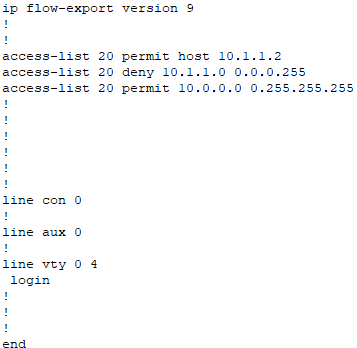


* Konfigurasi ACL pada Router 1



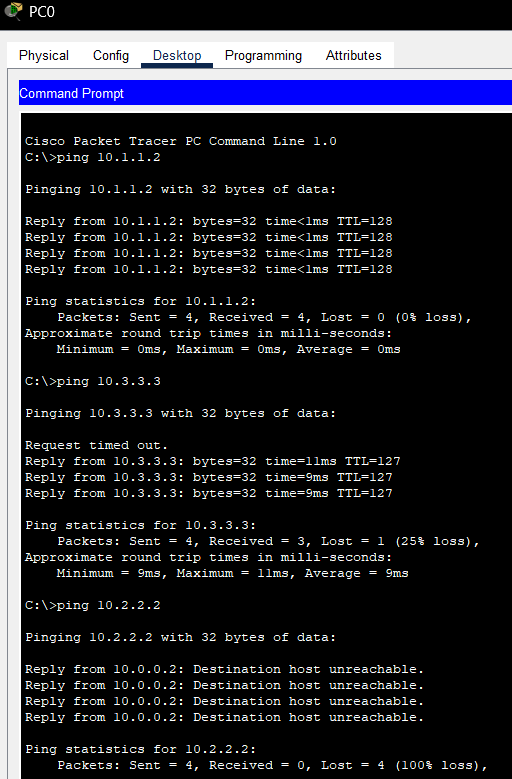
* Pengujian Router#show access-list dan Router#show run pada router 1



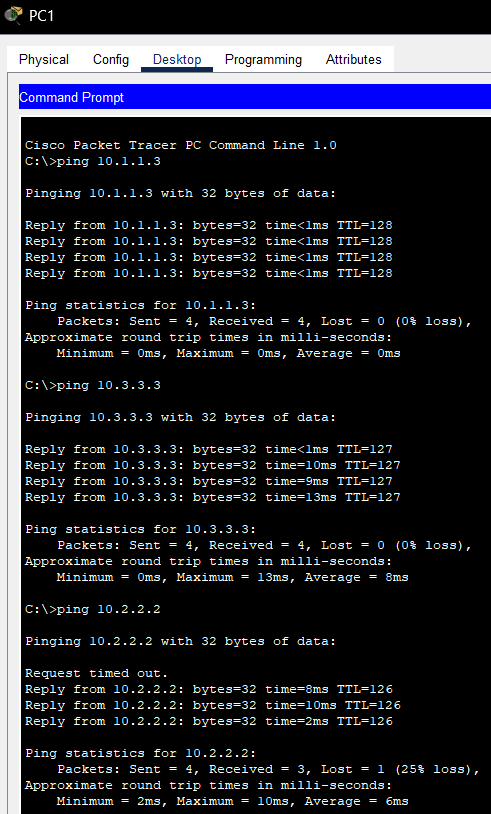


* Pengujian tes ping dari masing-masing end device

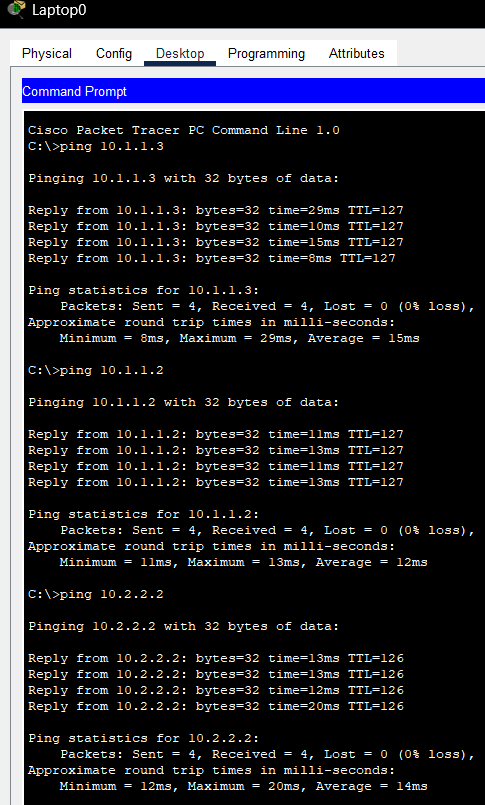
1. PC 0



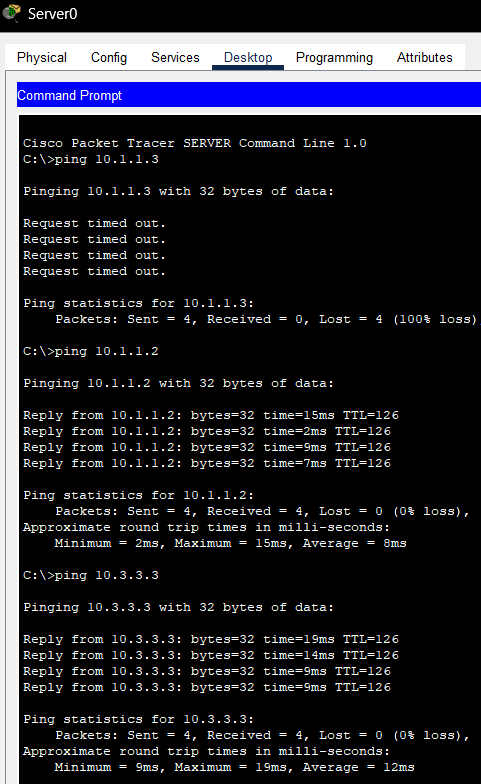
1. PC 1



1. Laptop 0



1. Server 0



* 1. 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.