

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

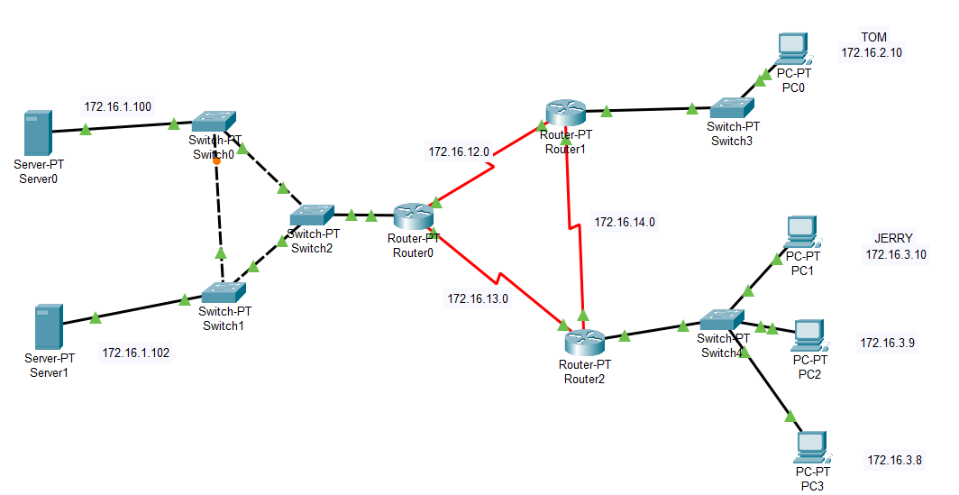
Keunggulan utama Standard ACL adalah kesederhanaan dan kemudahan implementasinya, menjadikannya solusi yang cepat untuk kebutuhan kontrol lalu lintas dasar. Namun, karena hanya berdasarkan IP sumber, penggunaannya menjadi terbatas untuk skenario yang memerlukan kontrol lebih mendalam, seperti membedakan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

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

a. End devices: PC

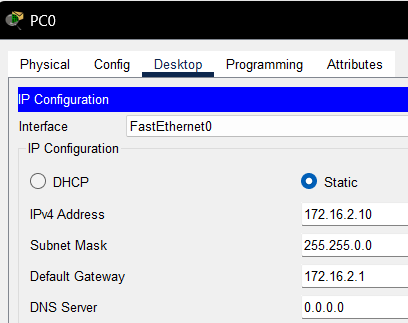
b. Network devices: Switch, Router

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

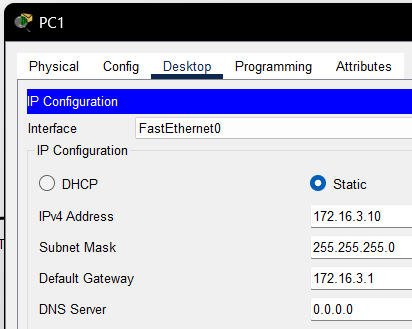


* 1. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

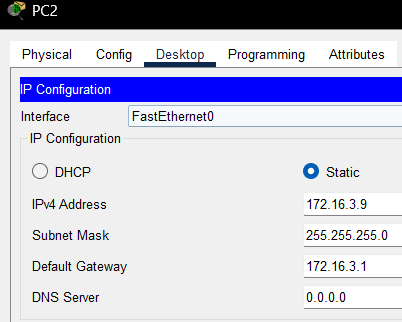
1. PC 0



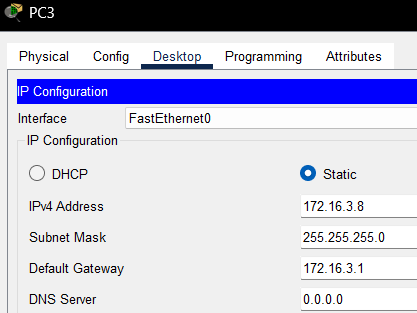
1. PC 1



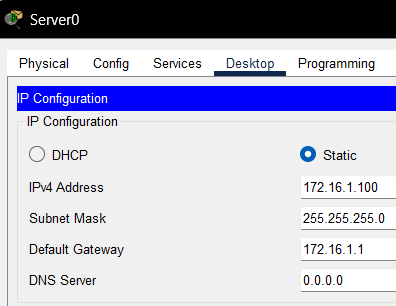
1. PC 2



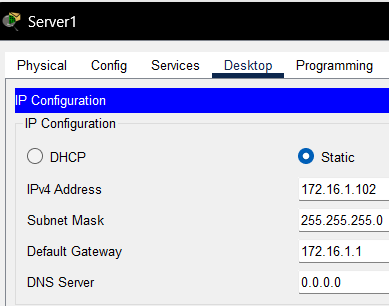
1. PC 3



1. Server 0

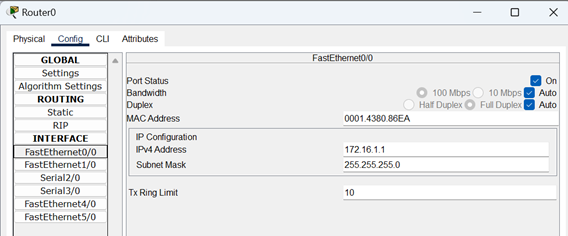


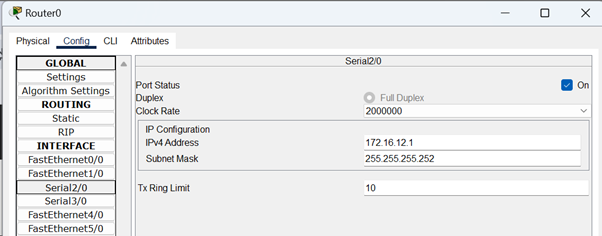
1. Server 1

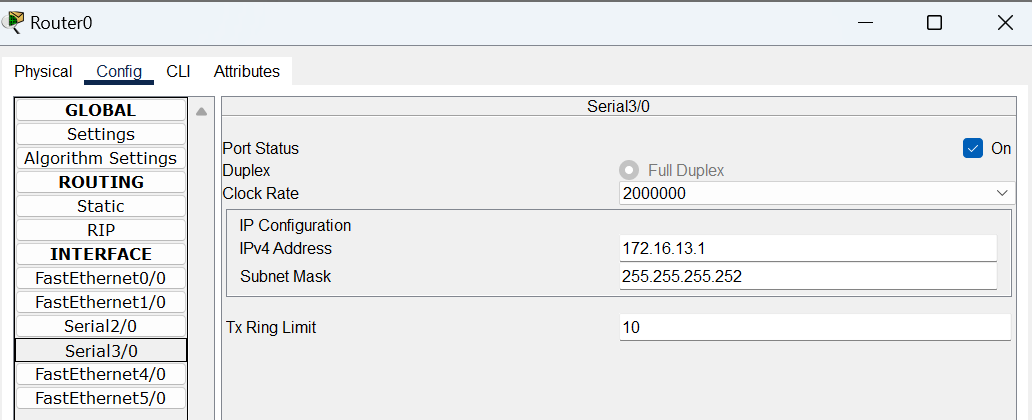


* 1. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

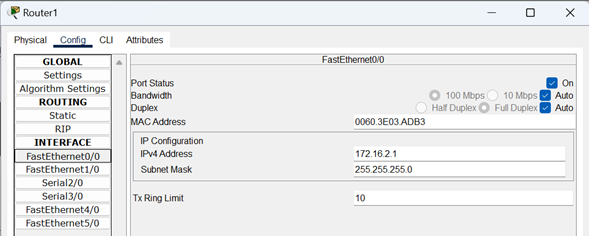
1. Router 0

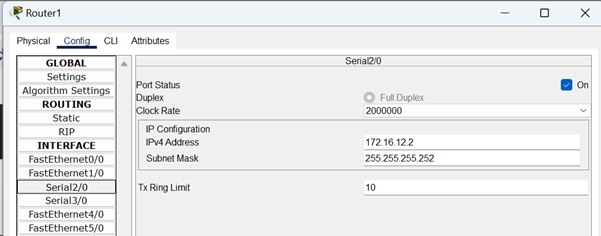


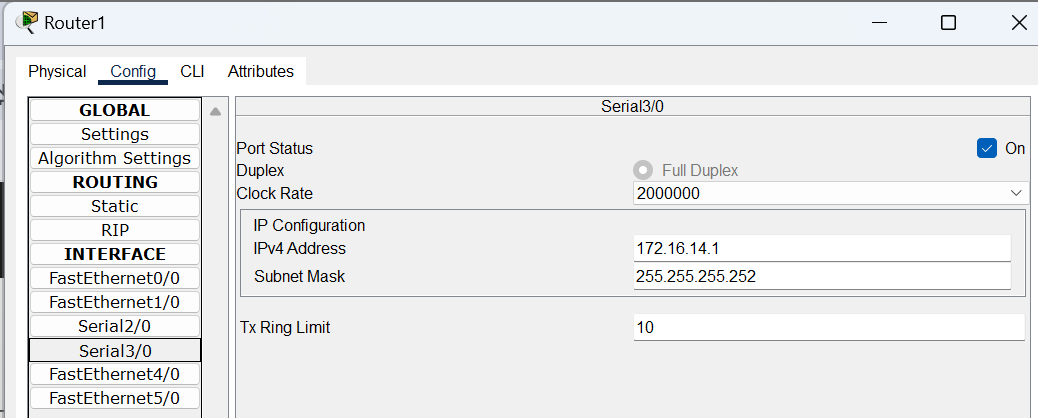




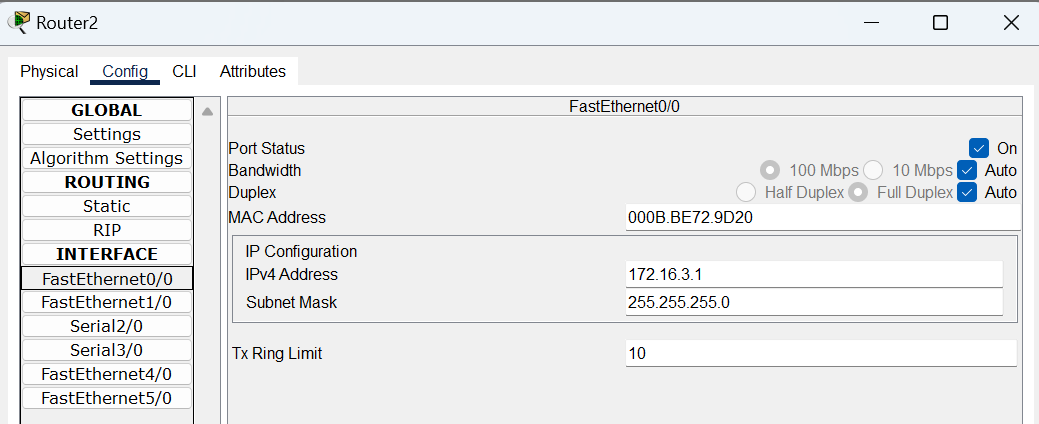
1. Router 1

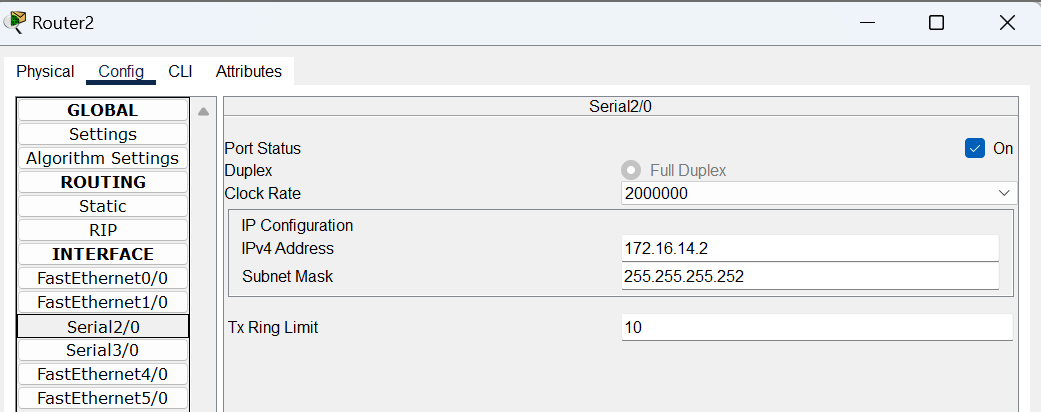


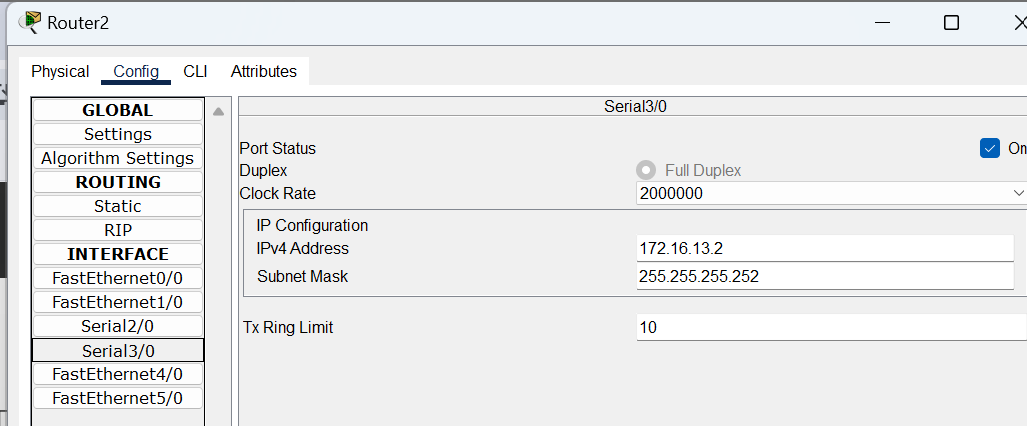




1. Router 2

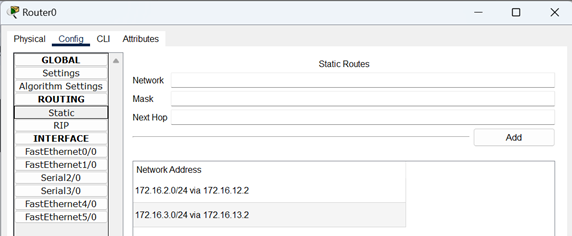




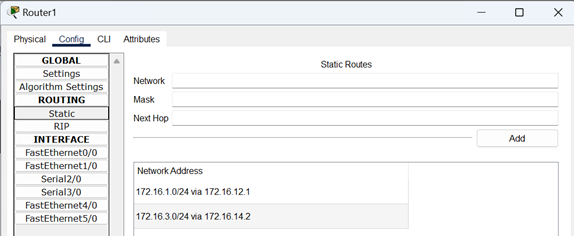


* 1. Lakukan konfigurasi static routing pada Router, seperti berikut:

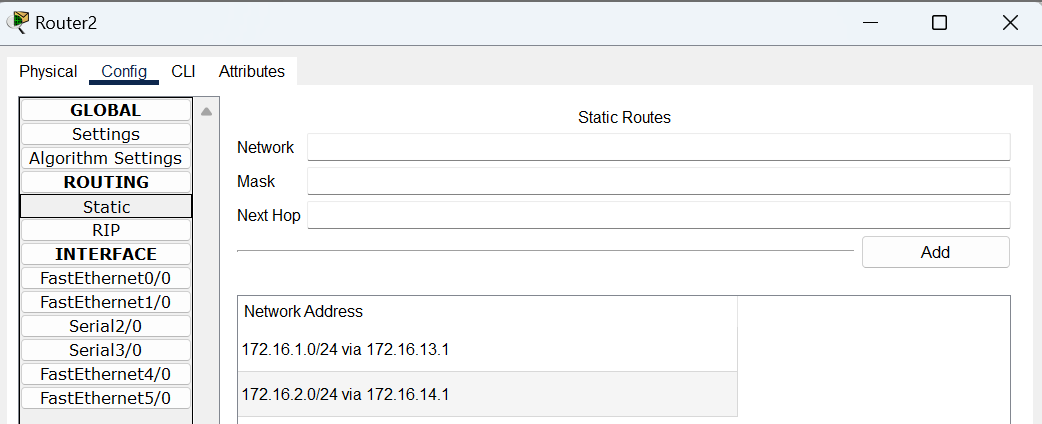
1. Router 0



1. Router 1

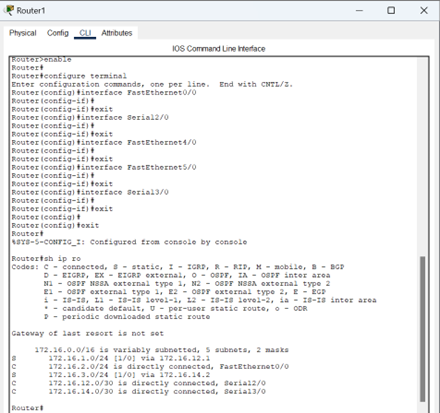


1. Router 2

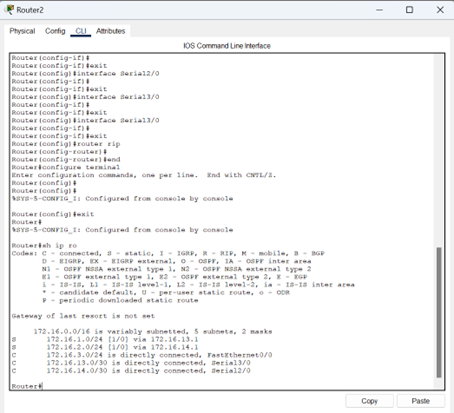


* 1. Jalankan perintah: #show ip route pada router 1 dan 2, serta lakukan analisa

1. Router 1

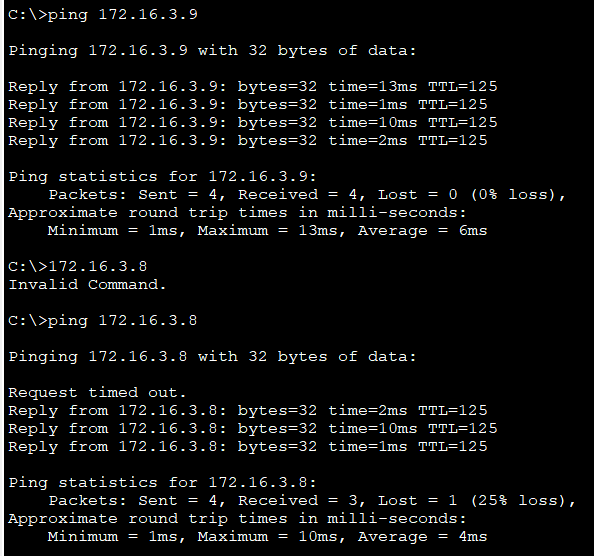
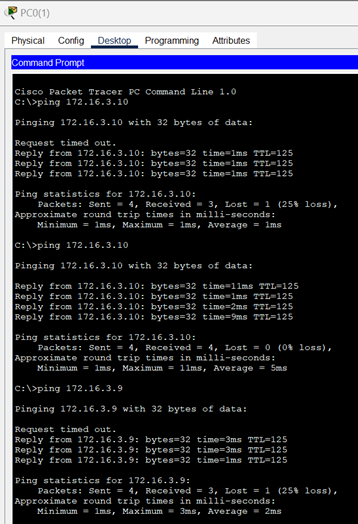


1. Router 1

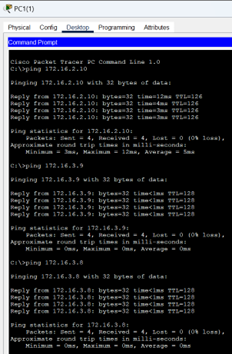


* 1. Lakukan tes ping ke semua PC, kemudian tampilkan hasil percobaan anda dan analisa

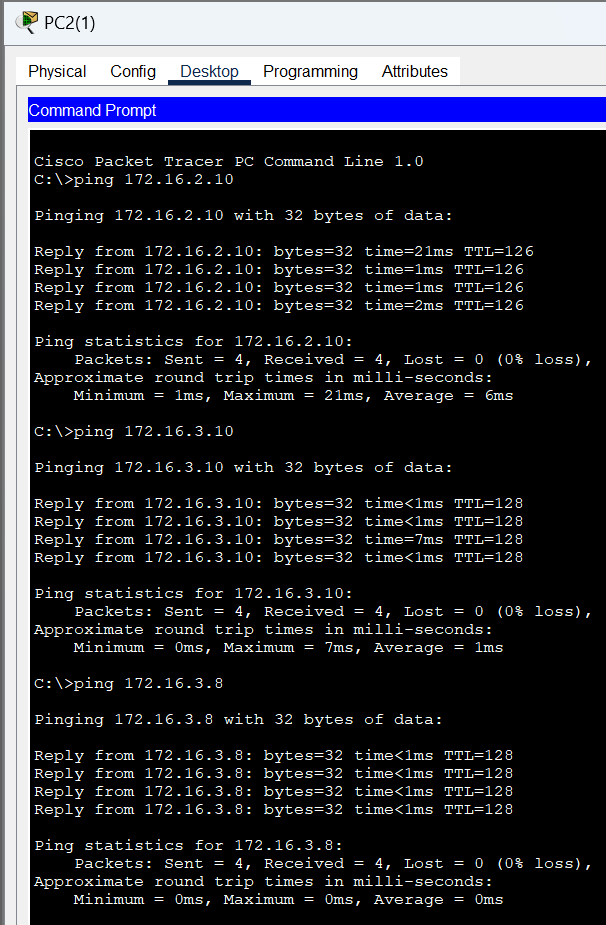
1. PC 0 ke PC lain



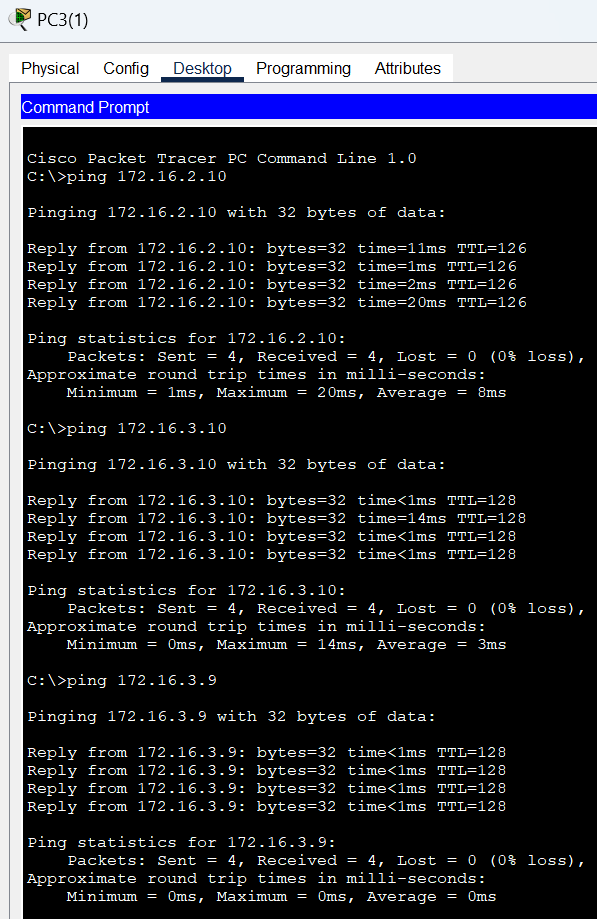
1. PC 1 ke PC lain



1. PC 2 ke PC lain

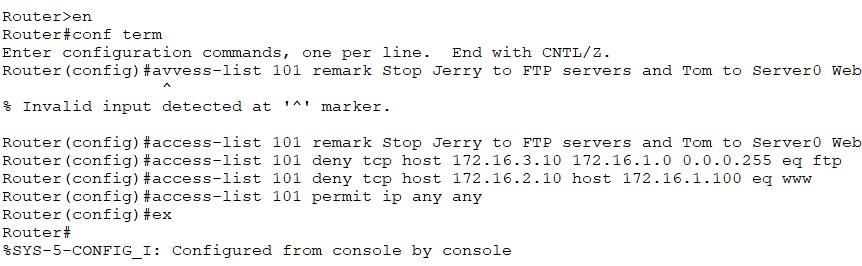


1. PC 3 ke PC lain

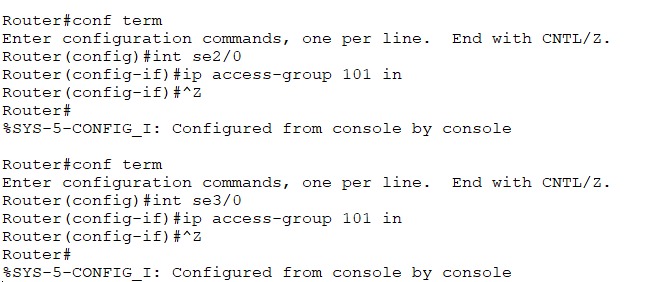


* 1. Lakukan konfigurasi Access Control List (ACL) pada router, analisa perintah konfigurasi yang digunakan berikut ini

1. Lakukan blocking untuk koneksi Tom and Jerry dari Router0

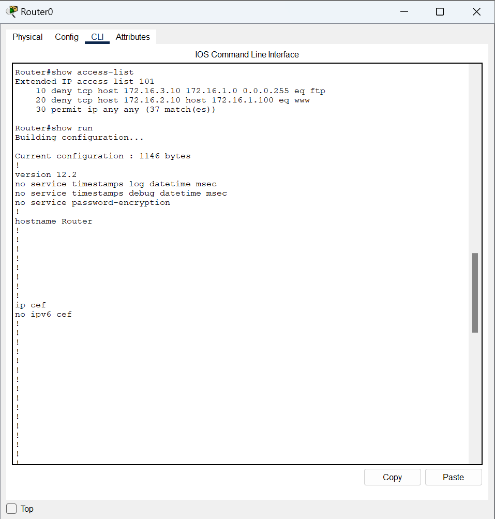


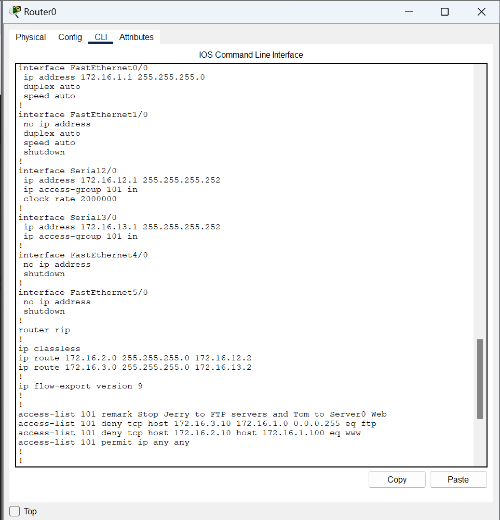
1. Terapkan ACL pada interface yang dekat dengan destination



* 1. Lihat Konfigurasi dengan perintah Router#show run dan analisa

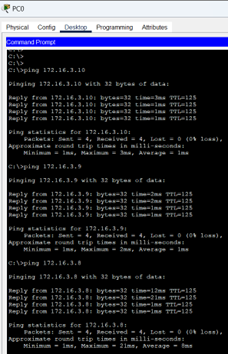
Router 0



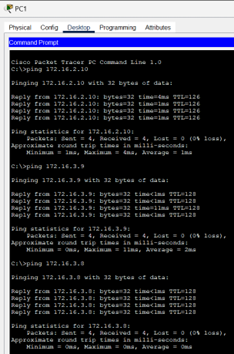


* 1. Gunakan perintah ping dari masing masing PC ke PC lainnya, tampilkan hasilnya dan analisa, bandingkan denan hasil eprcobaan pada Langkah no. 6

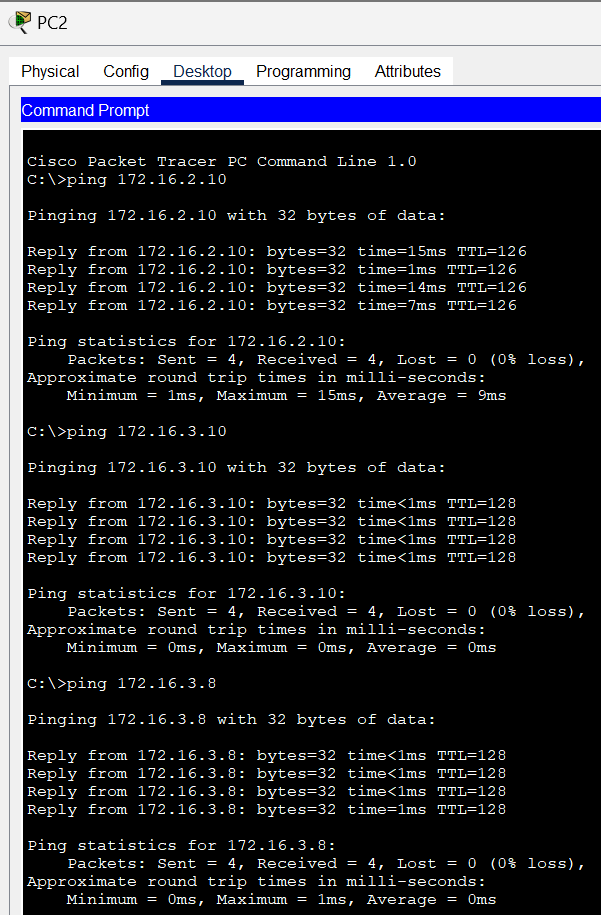
1. PC 0



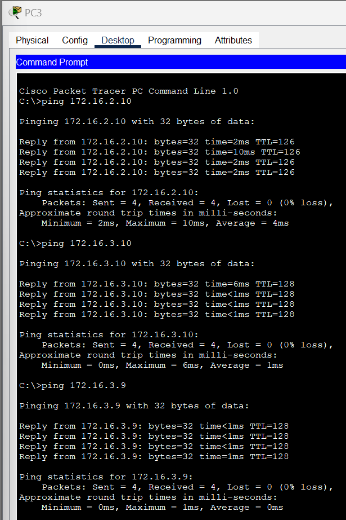
1. PC 1



1. PC 2

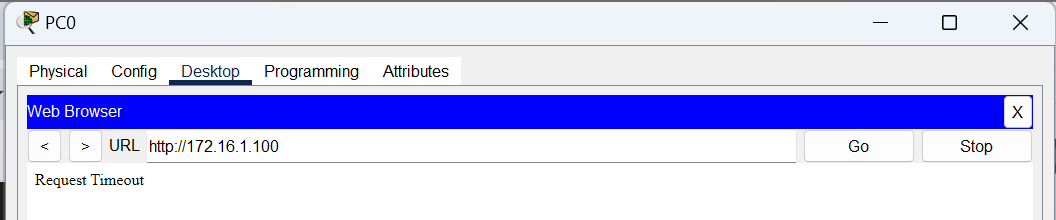


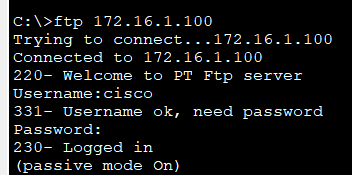
1. PC 3



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

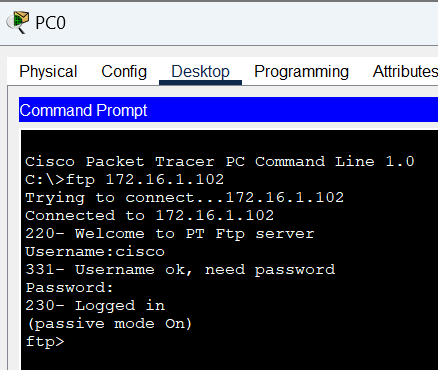
1. Ke Server 0





1. Ke Server 1

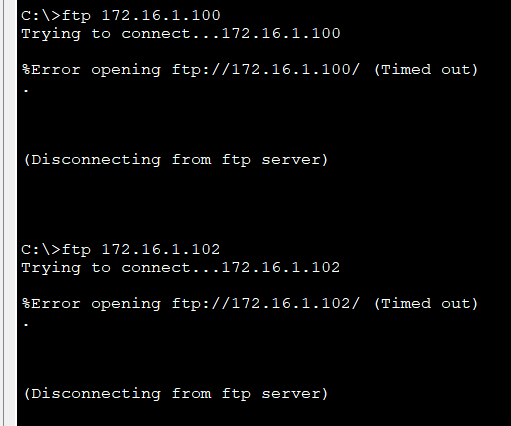




* 1. Lakukan pengujian dari host Jerry pada PC1 dan bandingkan dari PC lain

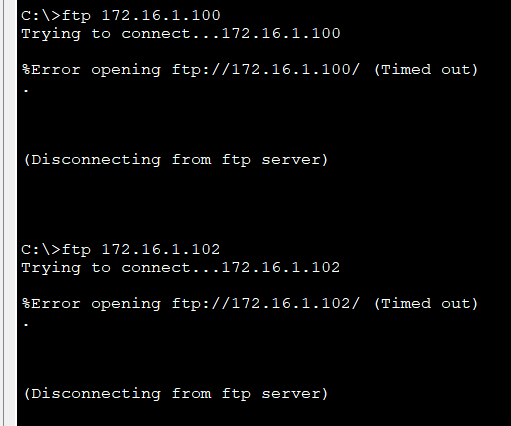
1. Ke Server 0





1. Ke Server 1





1. Analisa

Pada Praktikum Kelima ini dilakukan

.

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. 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.

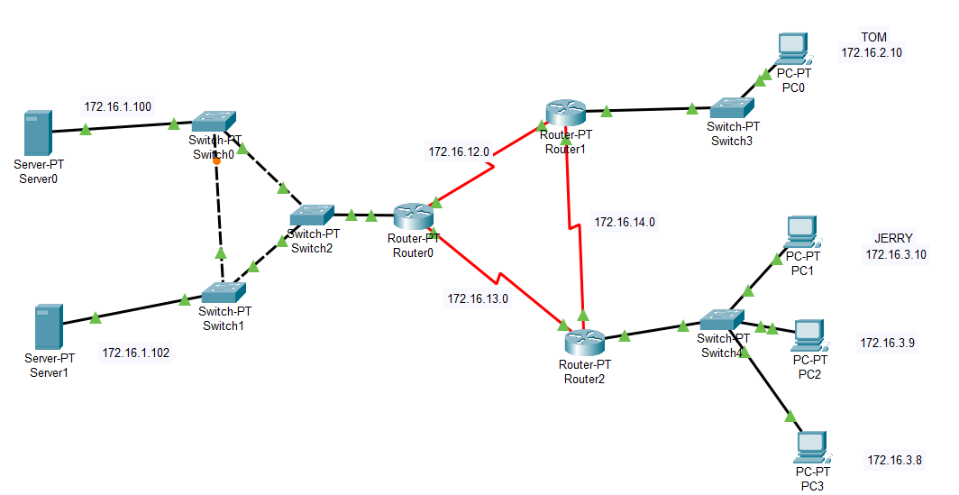
Sedangkan Extended ACL adalah ACL yang menawarkan control yang lebih rinci dan fleksibel dibandingkan Standart ACL. Dimana ACL ini bisa menyaring traffic berdasarkan IP address, tujuan IP address, jenis protokolnya, hingga nomor port seperti FTP dan www. Jadi Extended ACL bisa menyaring admin Jaringan 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.

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

Jawab:

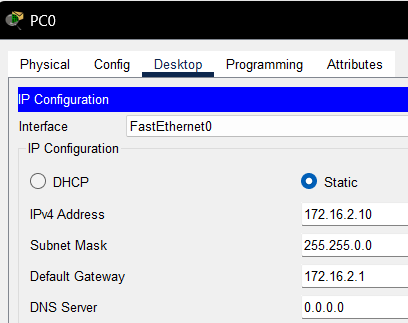
* 1. Lakukan modifikasi ACL pada percobaan, sehinhha host Jerry hanya bisa mengakses FTP server, PC1 dan PC2 tidak bisa mengakses Web Server0, serta PC3 tidak bisa mengakses Web Server1.

Jawab:

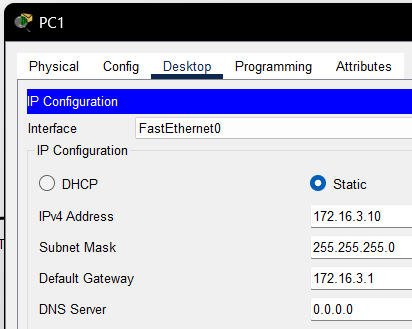


* Konfigurasi Alamat End Device

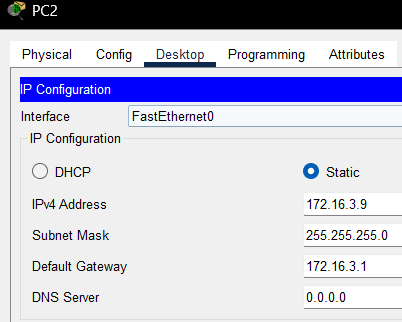
1. PC 0



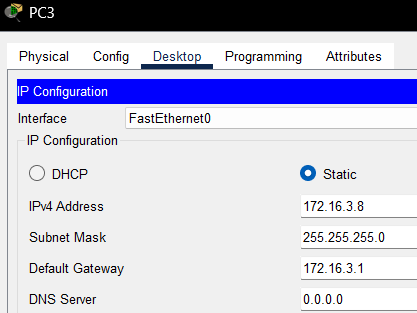
1. PC 1



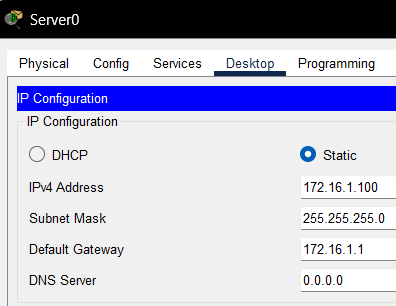
1. PC 2



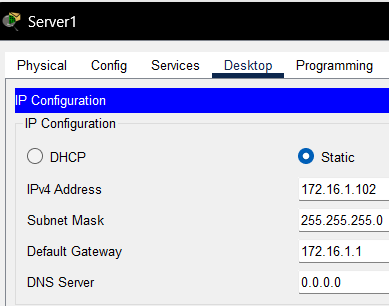
1. PC 3



1. Server 0

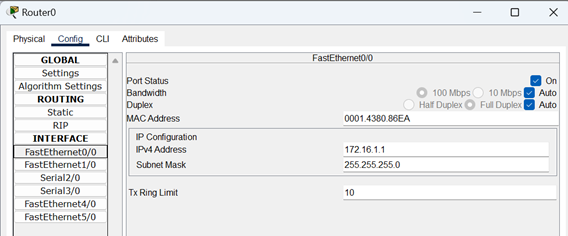


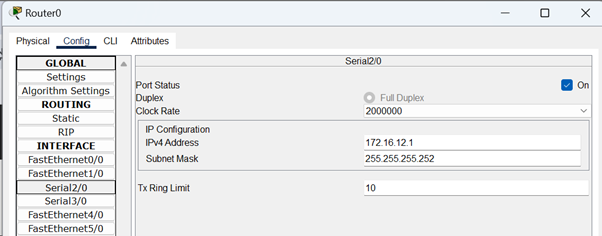
1. Server 1

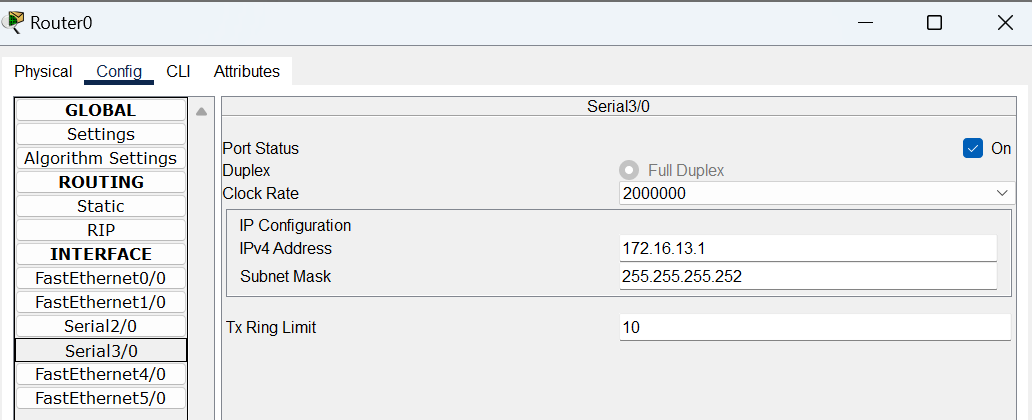


* Konfigurasi Interface Router

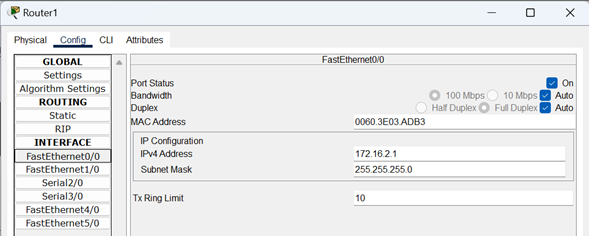
1. Router 0

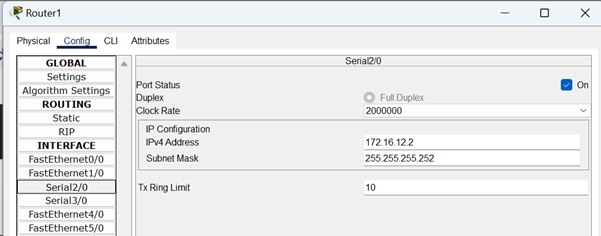


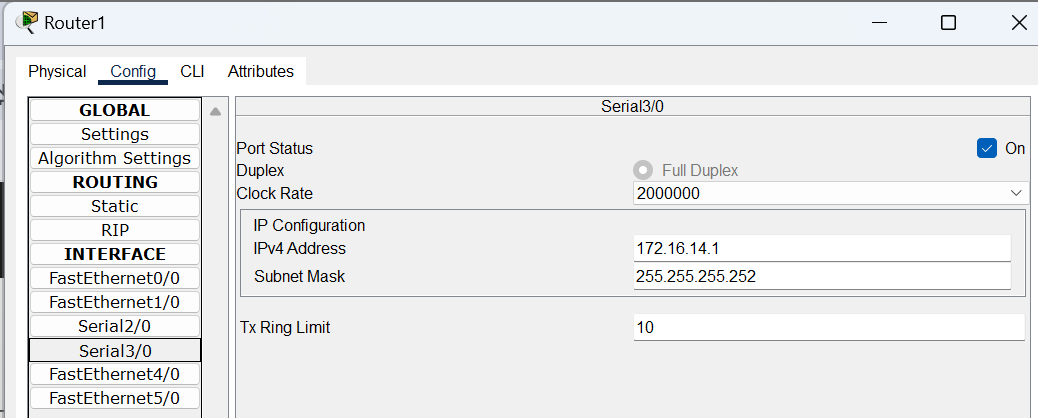




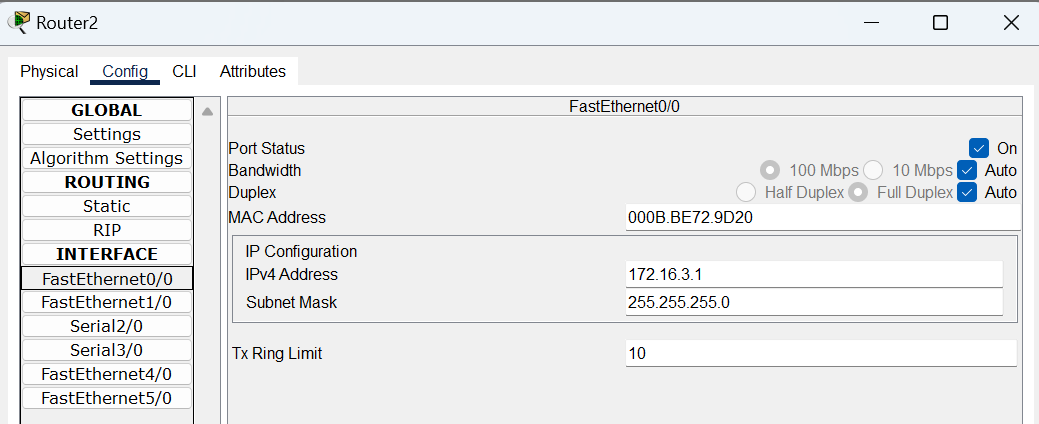
b. Router 1

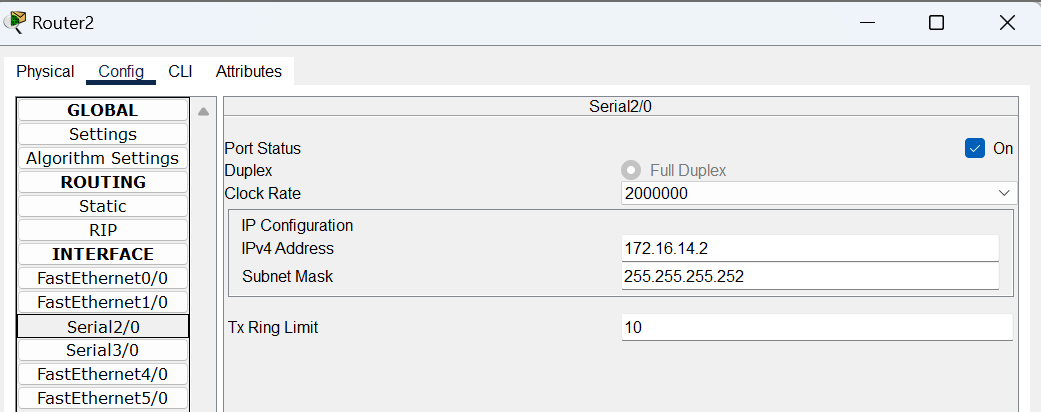


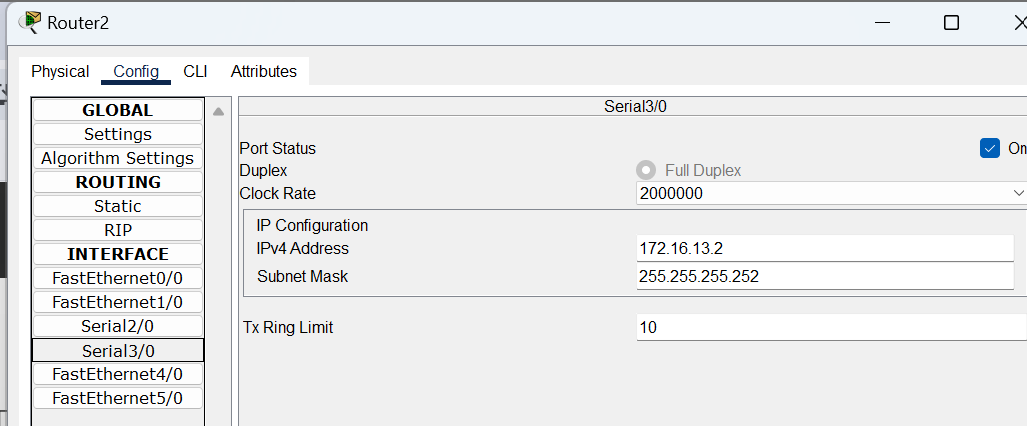




c. Router 2

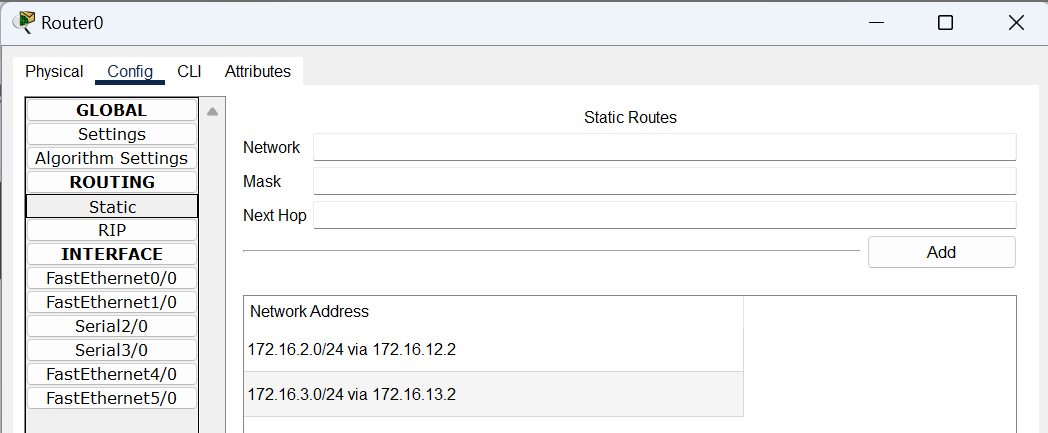




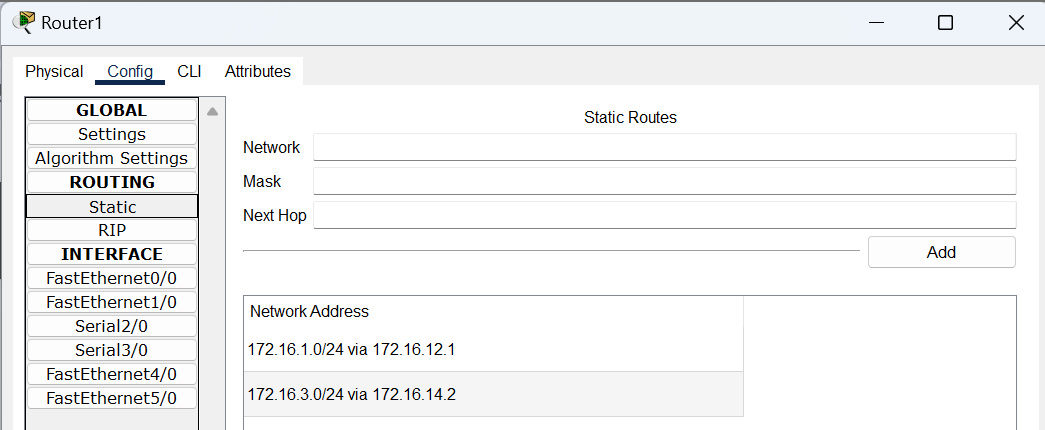


* Konfigurasi static Routing

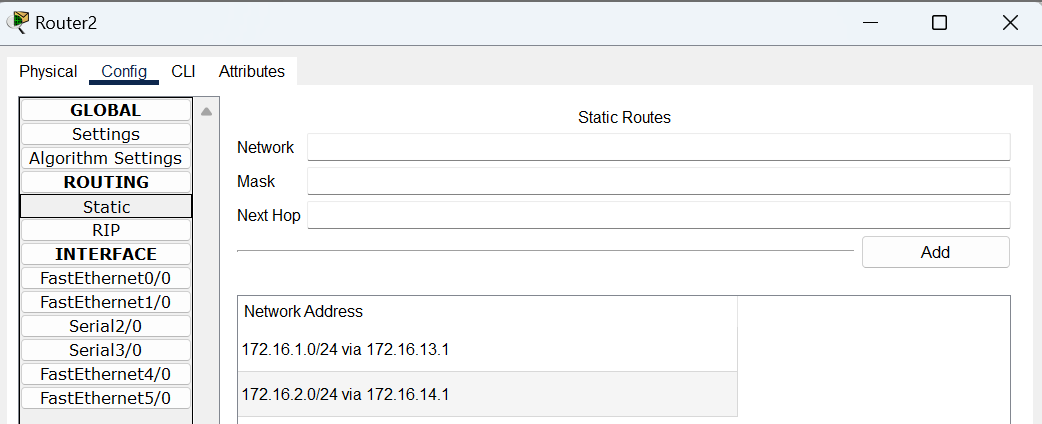
1. Router 0



1. Router 1

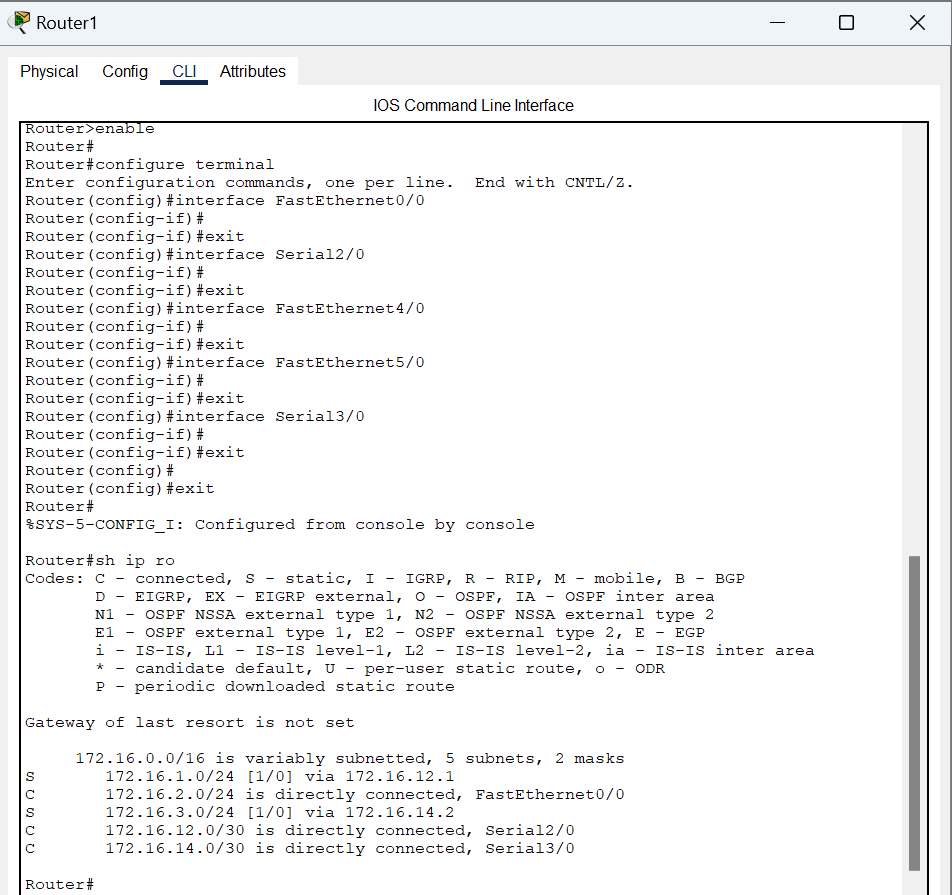


1. Router 2

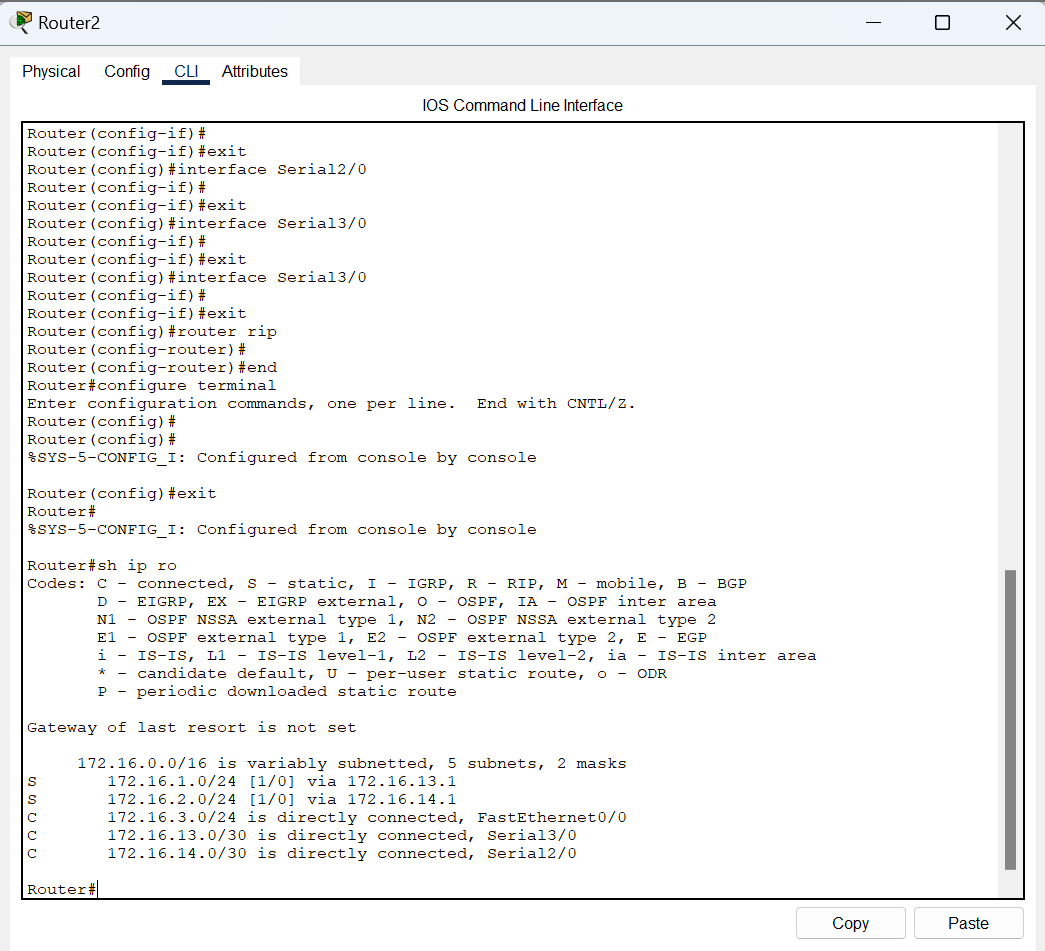


* Pengujian Router#show ip route

1. Router 1

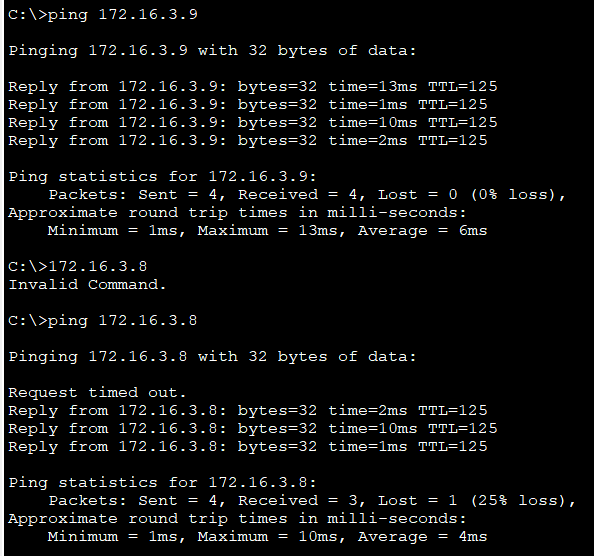
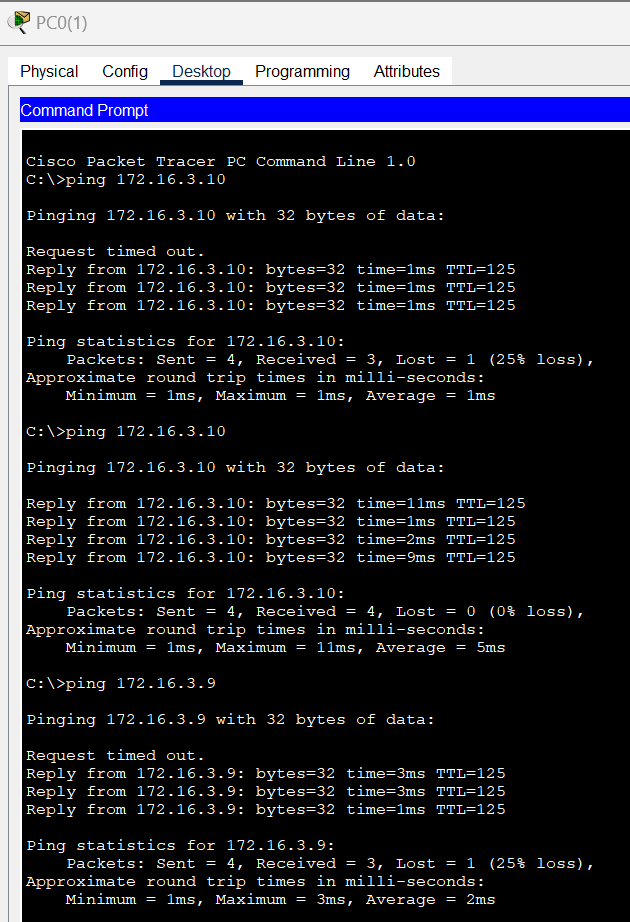


1. Router 2

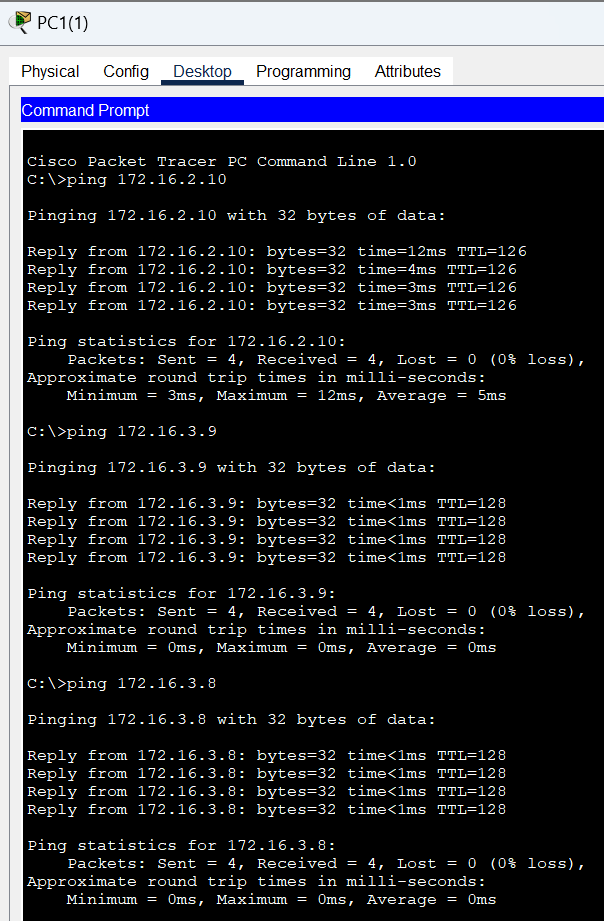


* Pengujian tes ping dari masing-masing PC

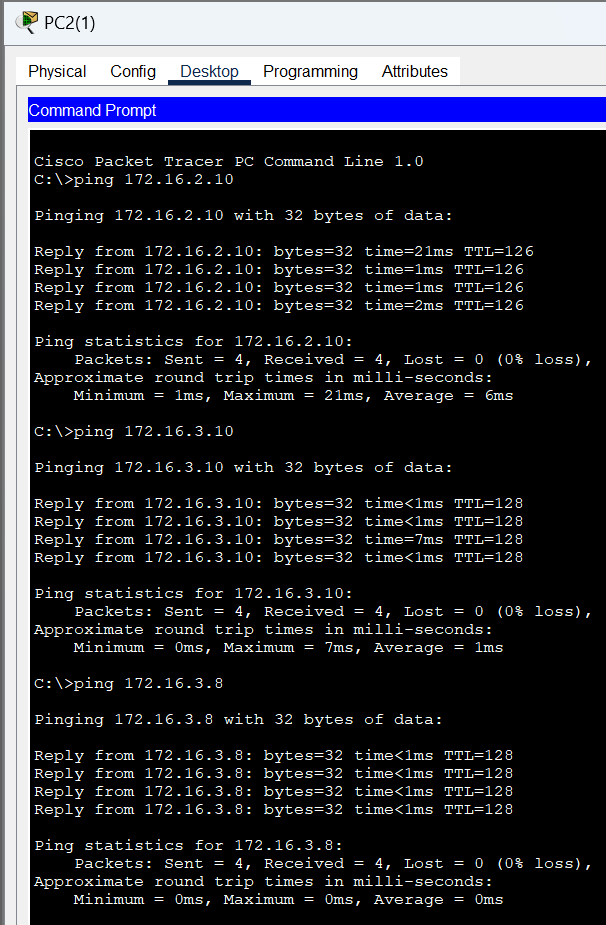
1. PC 0



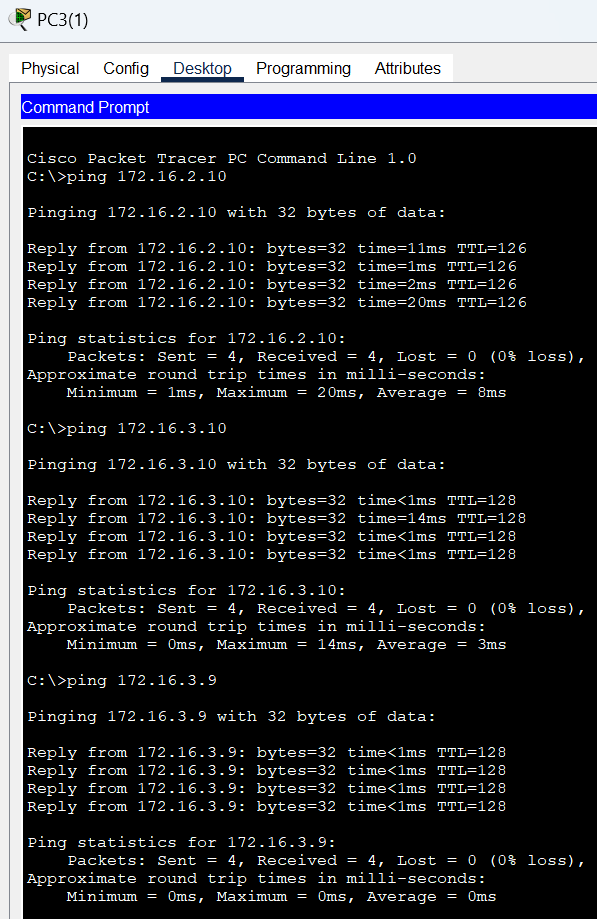
1. PC 1



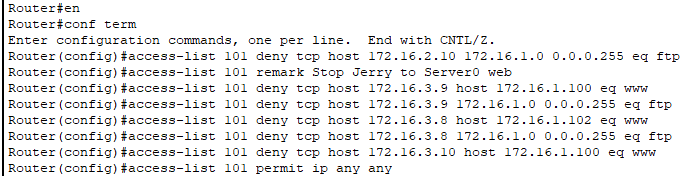
1. PC 2



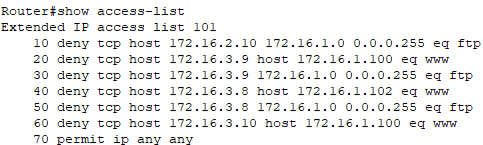
1. PC 3

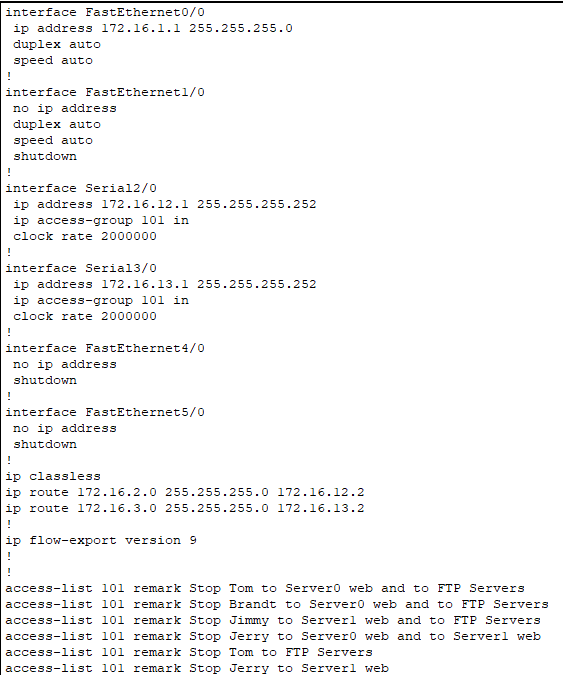
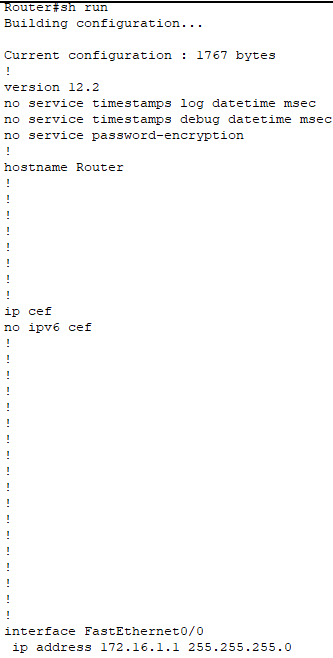


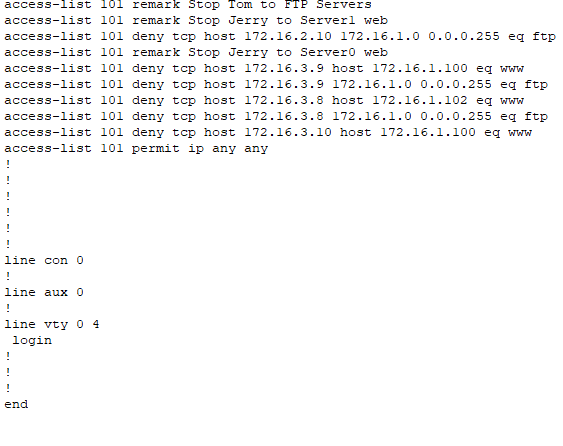
* Konfigurasi Extended ACL



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

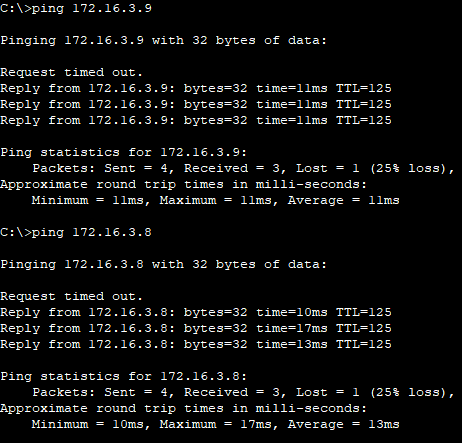
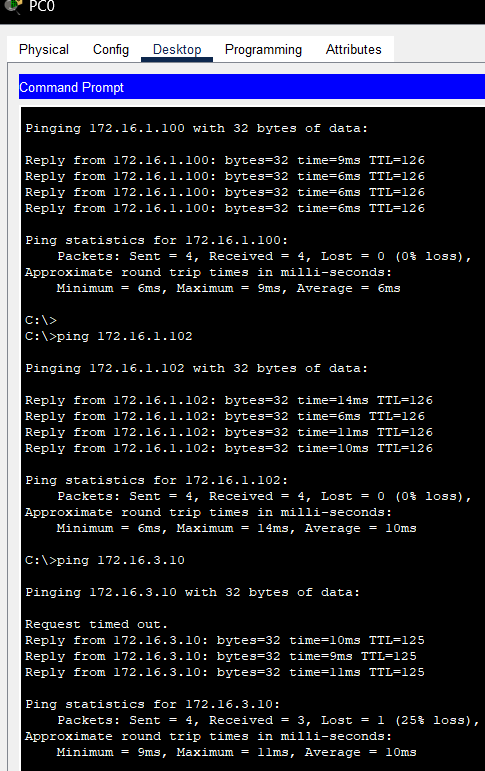




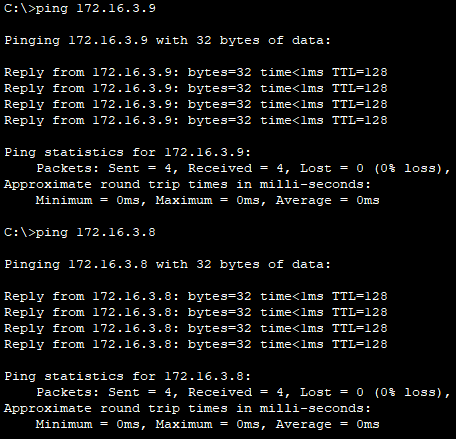
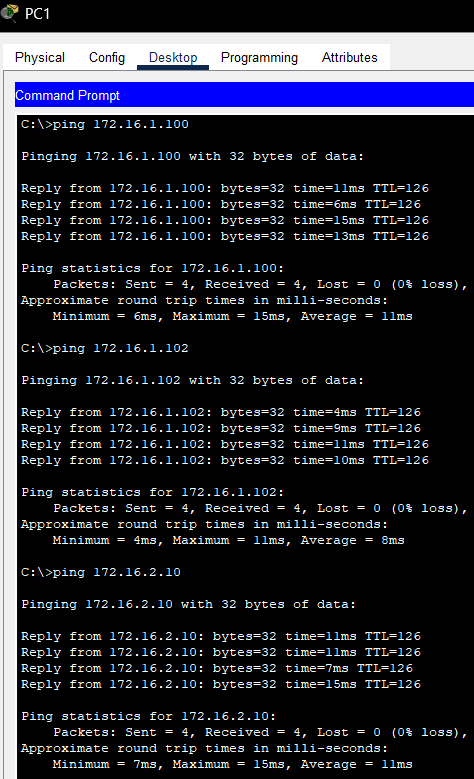


* Pengujian tes ping dari masing-masing PC

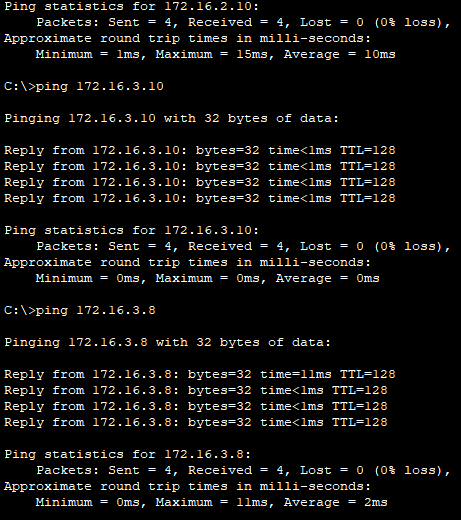
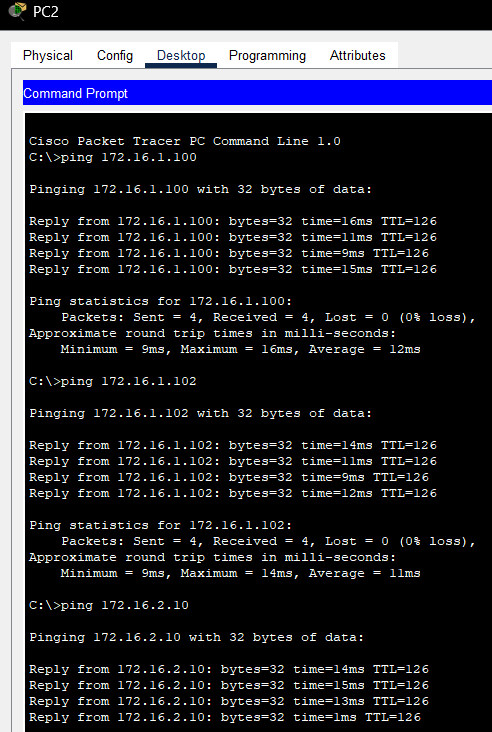
1. PC 0



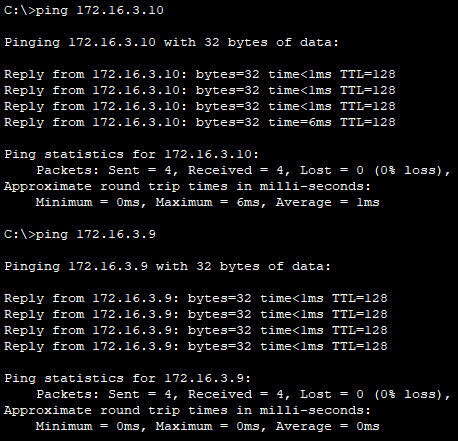
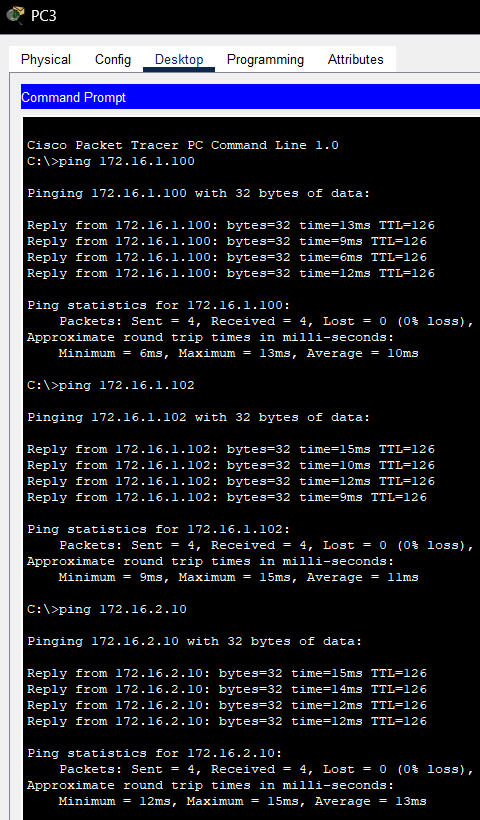
1. PC 1



1. PC 2



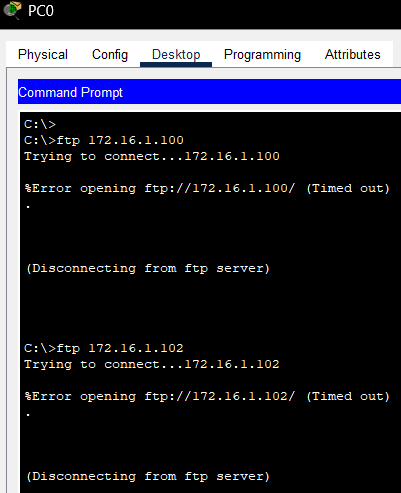
1. PC 3



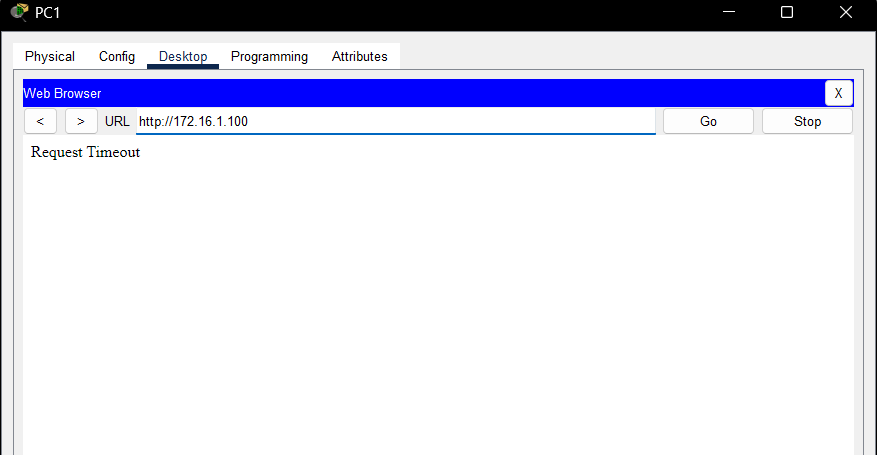
* Pengujian perintah FTP dan akses web di masing-masing PC ke Server

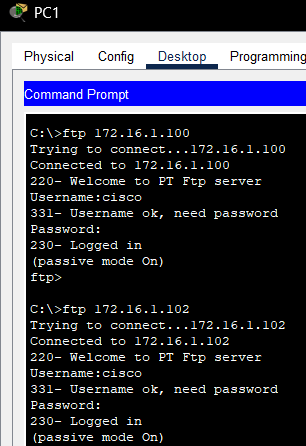
1. PC 0



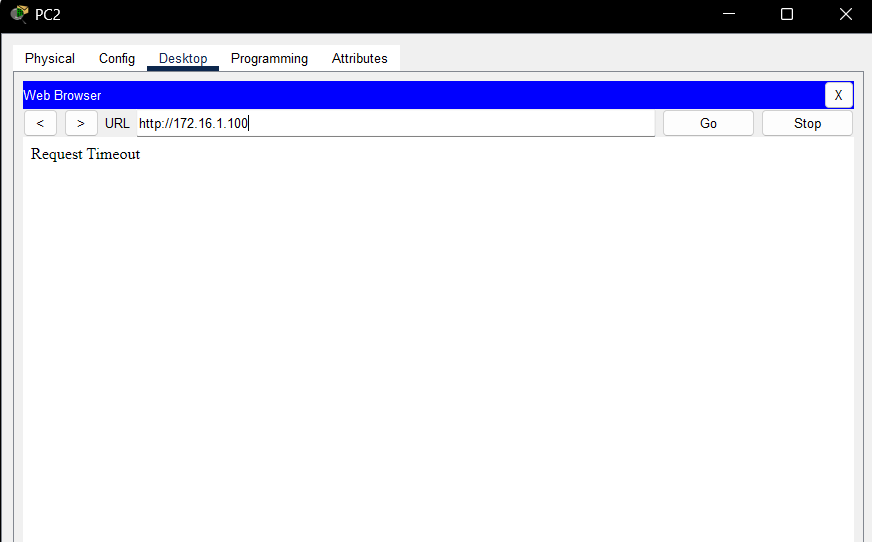


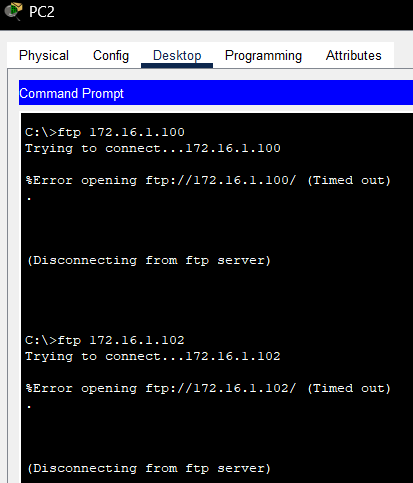
1. PC 1





1. PC 2





1. PC 3

