

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.

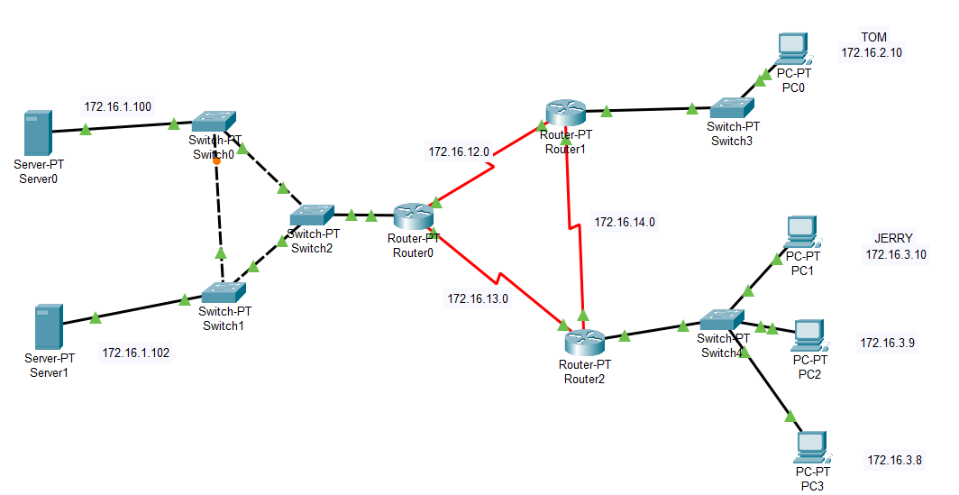
Keunggulan utama Standard ACL adalah kesederhanaan dan kemudahan implementasinya, menjadikannya solusi yang cepat untuk kebutuhan kontrol lalu lintas dasar. Namun, karena hanya berdasarkan IP sumber, penggunaannya menjadi terbatas untuk skenario yang memerlukan kontrol lebih mendalam, seperti membedakan 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

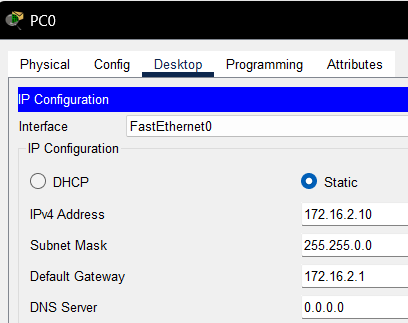
b. Network devices: Switch, Router

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

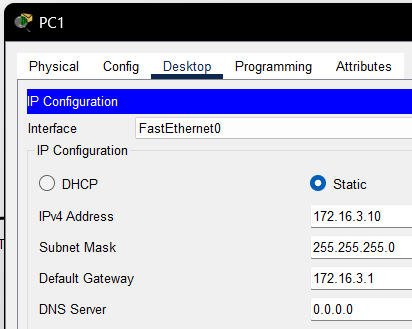


* 1. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

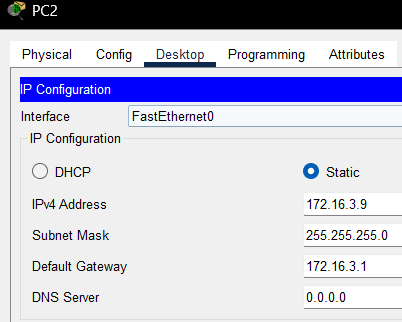
1. PC 0



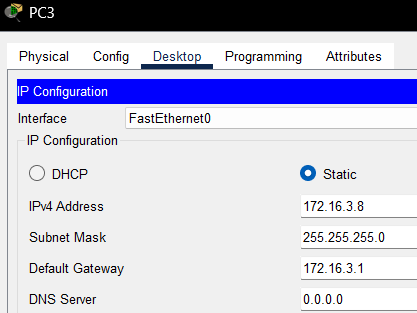
1. PC 1



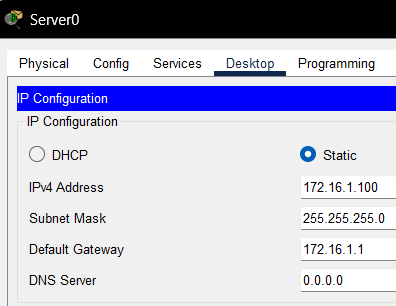
1. PC 2



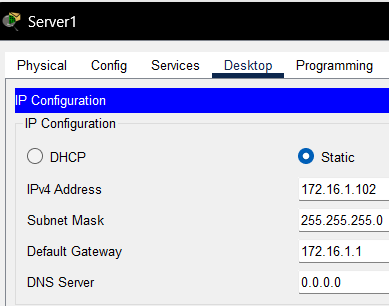
1. PC 3



1. Server 0

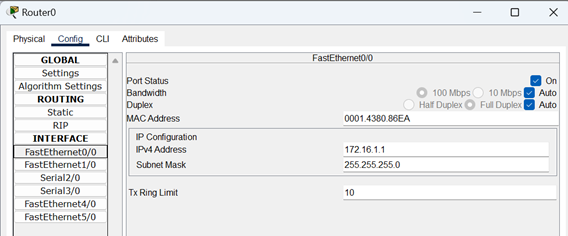


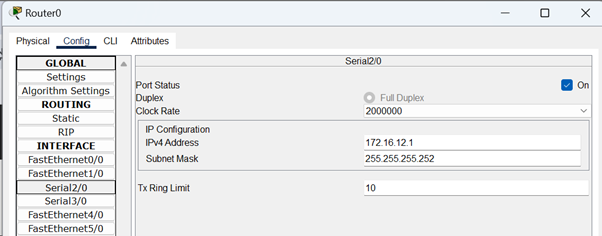
1. Server 1

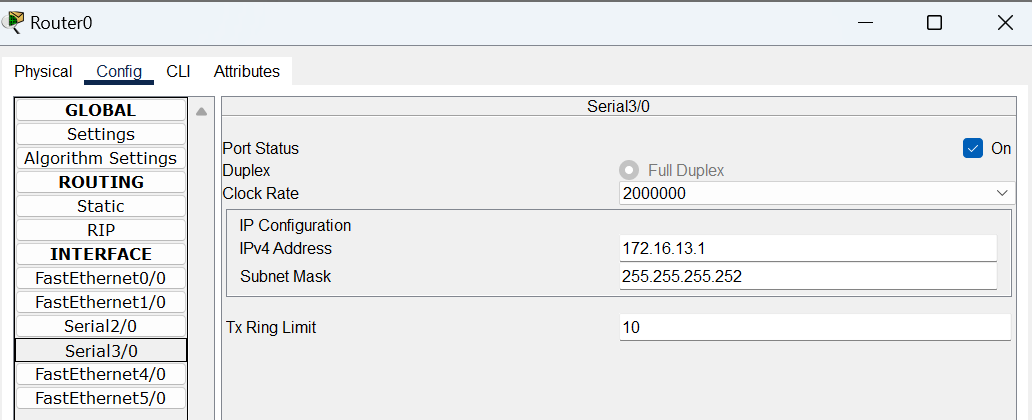


* 1. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

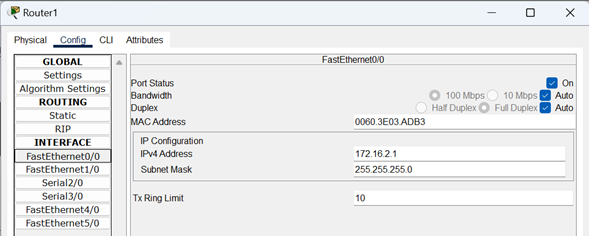
1. Router 0

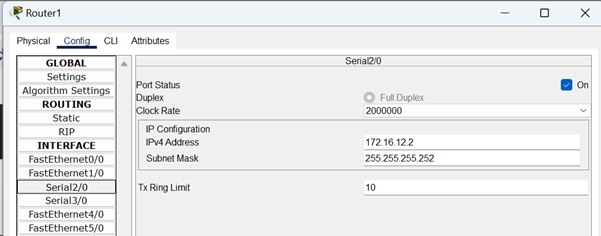


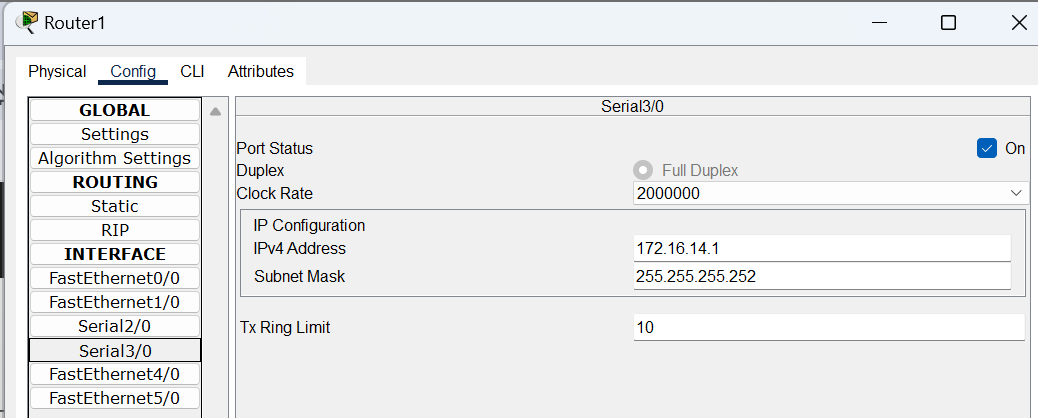




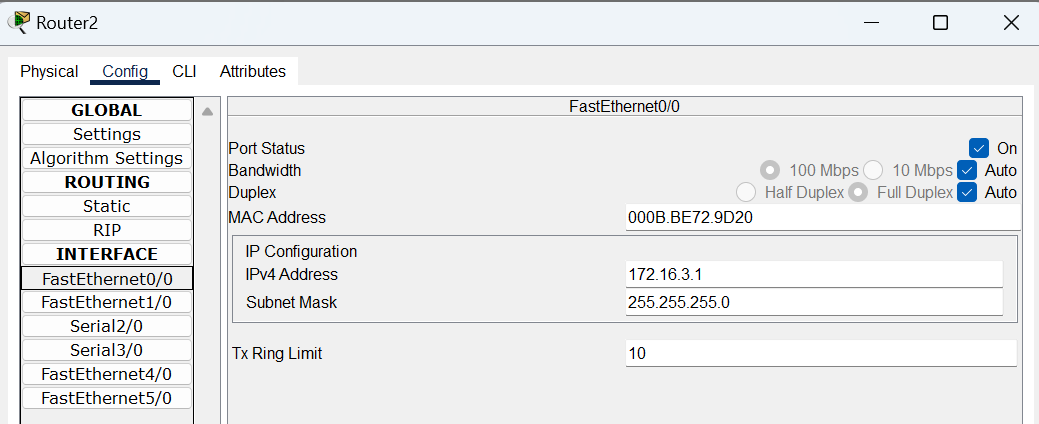
1. Router 1

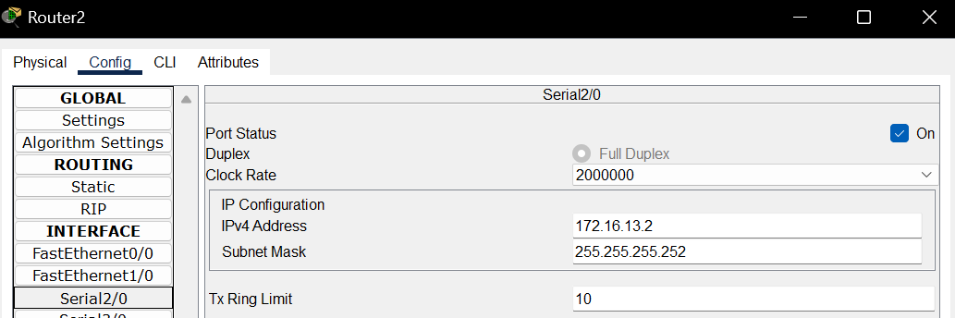


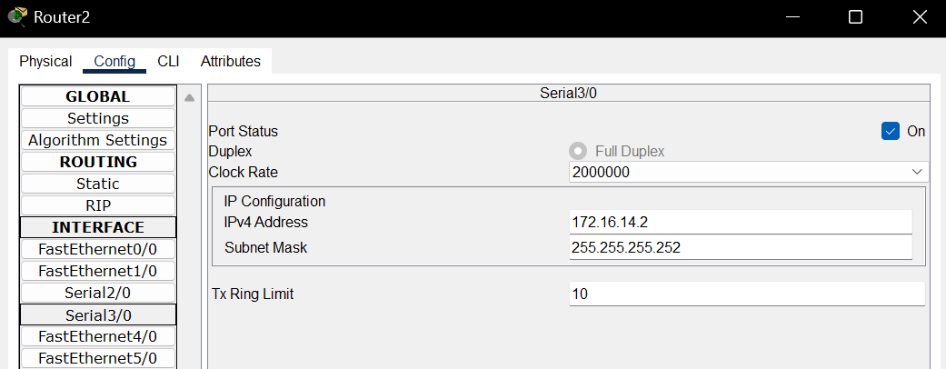




1. Router 2

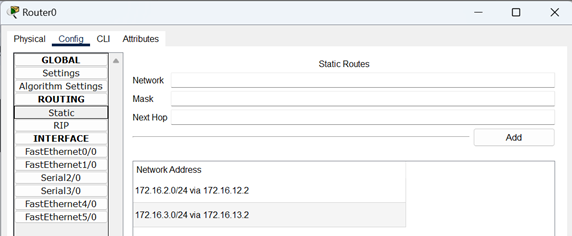




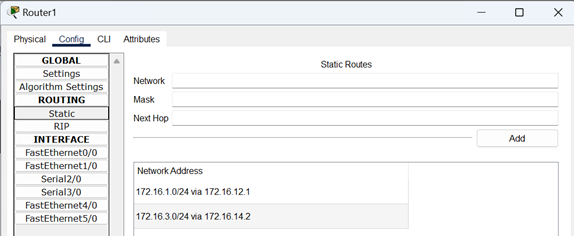


* 1. Lakukan konfigurasi static routing pada Router, seperti berikut:

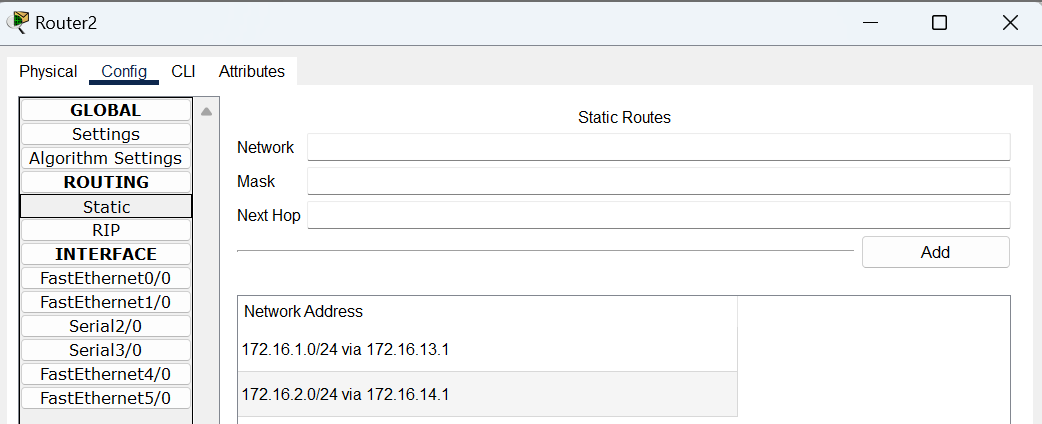
1. Router 0



1. Router 1

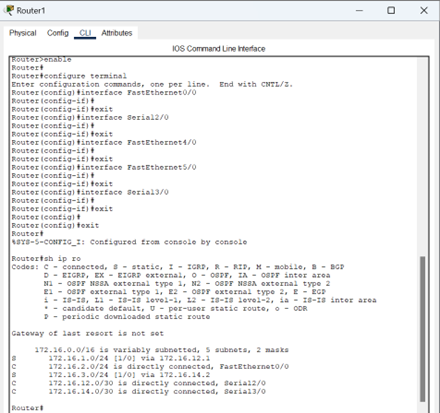


1. Router 2

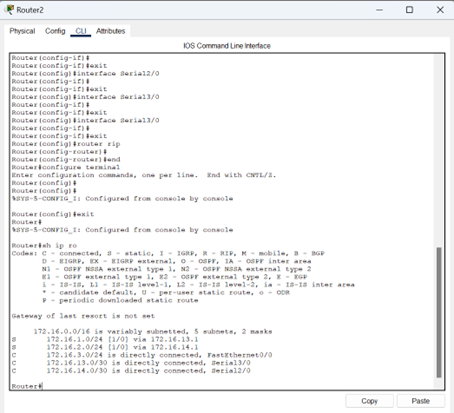


* 1. Jalankan perintah: #show ip route pada router 1 dan 2, serta lakukan analisa

1. Router 1

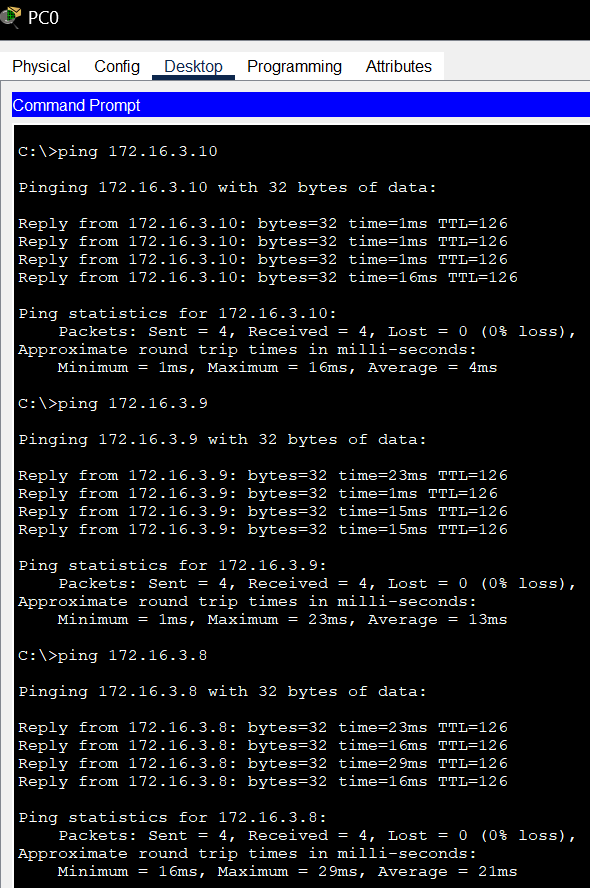


1. Router 1

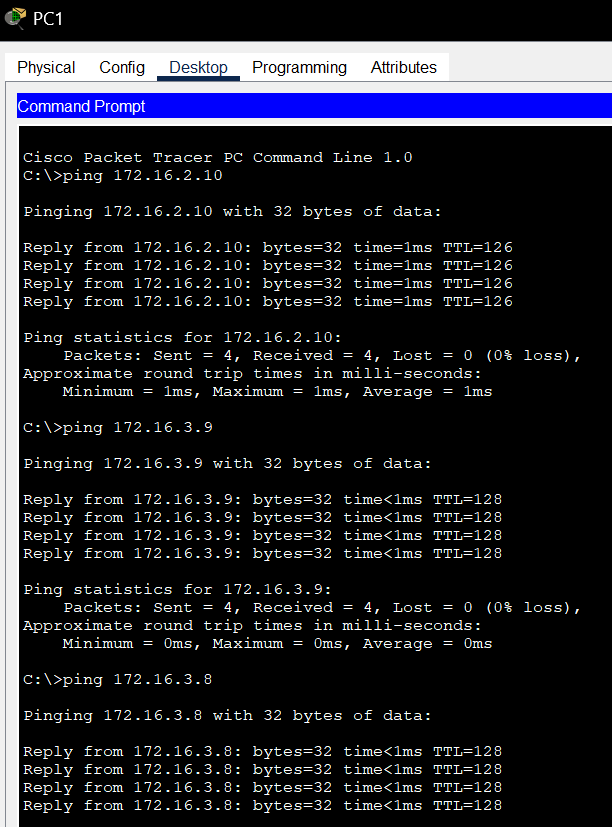


* 1. Lakukan tes ping ke semua PC, kemudian tampilkan hasil percobaan anda dan analisa

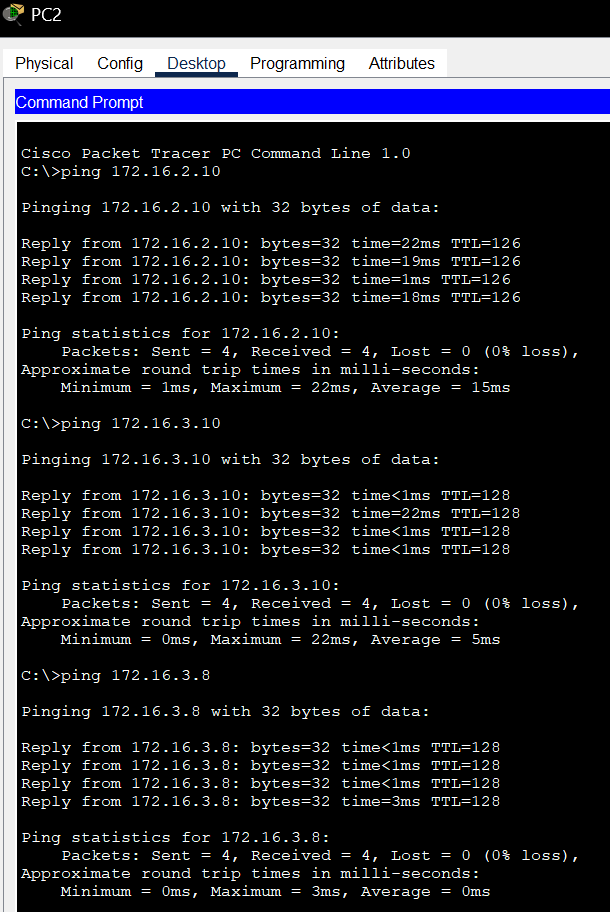
1. PC 0 ke PC lain



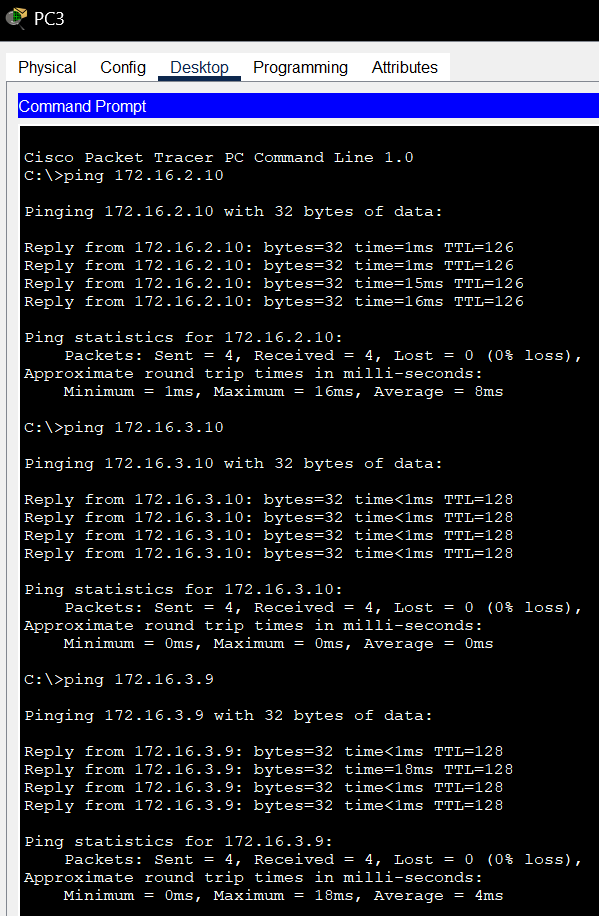
1. PC 1 ke PC lain



1. PC 2 ke PC lain

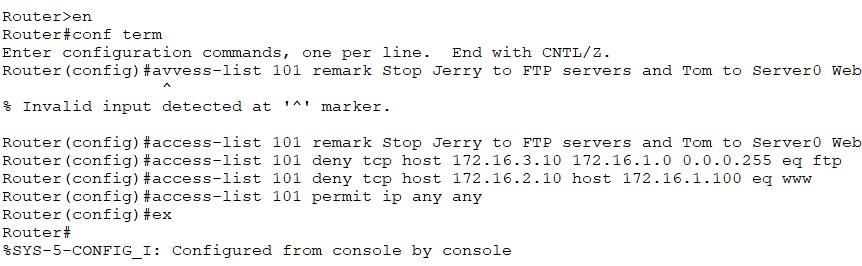


1. PC 3 ke PC lain

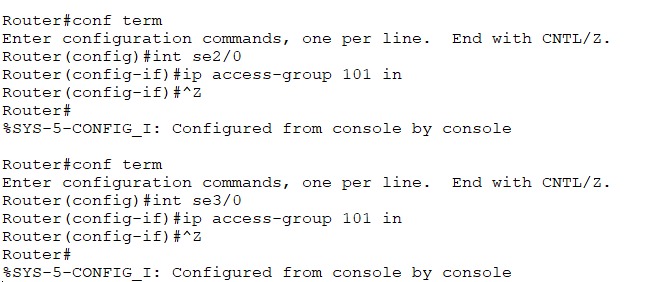


* 1. Lakukan konfigurasi Access Control List (ACL) pada router, analisa perintah konfigurasi yang digunakan berikut ini

1. Lakukan blocking untuk koneksi Tom and Jerry dari Router0

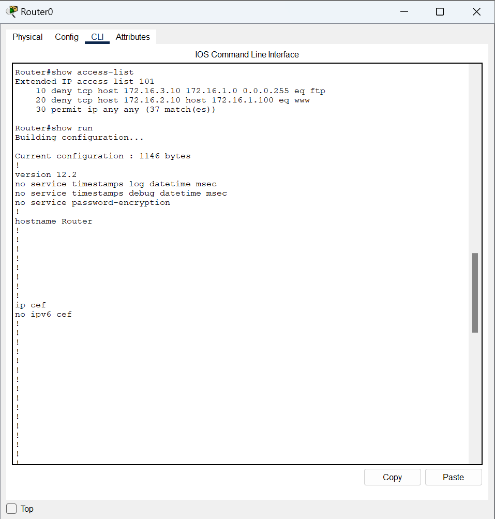


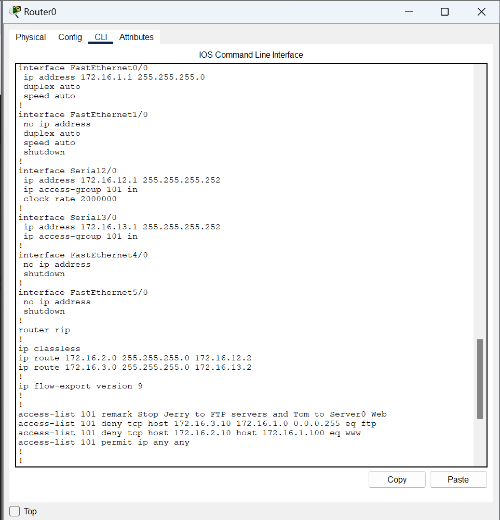
1. Terapkan ACL pada interface yang dekat dengan destination



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

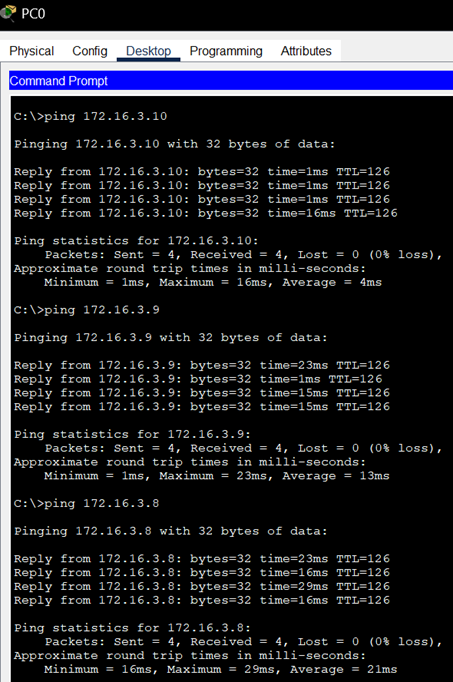
Router 0



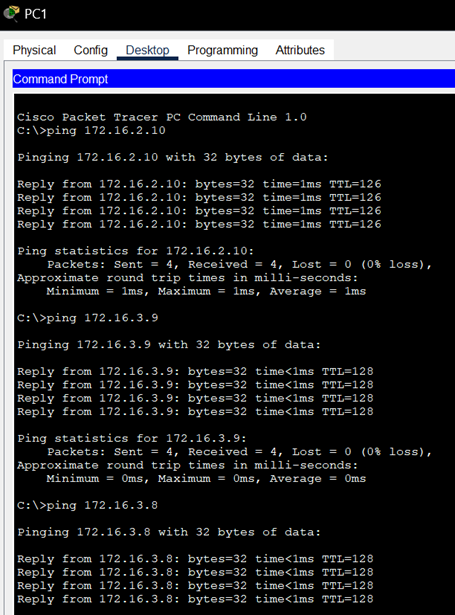


* 1. Gunakan perintah ping dari masing masing PC ke PC lainnya, tampilkan hasilnya dan analisa, bandingkan dengan hasil percobaan pada Langkah no. 6

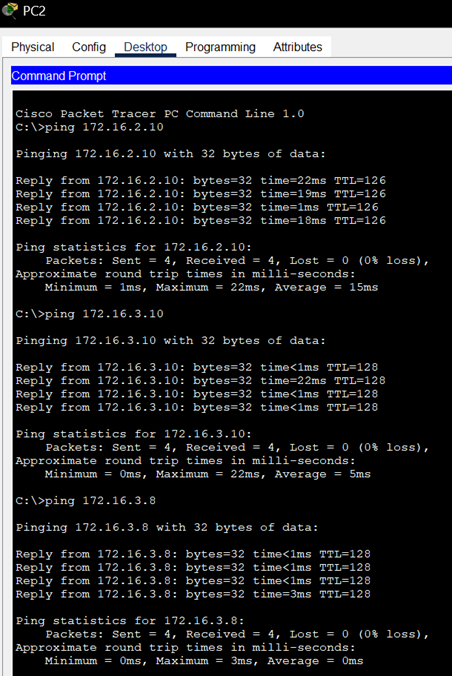
1. PC 0



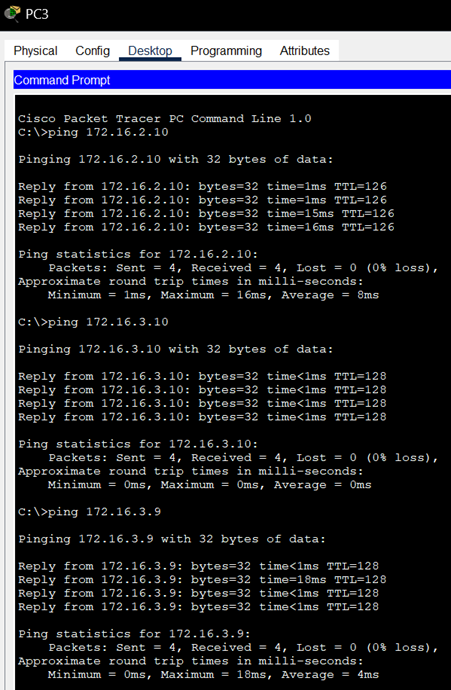
1. PC 1



1. PC 2

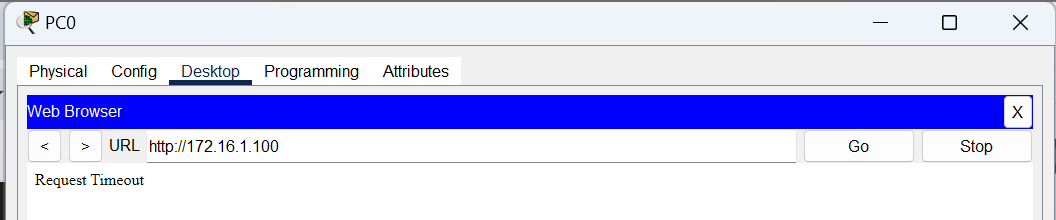


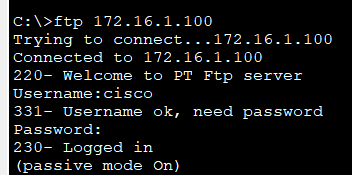
1. PC 3



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

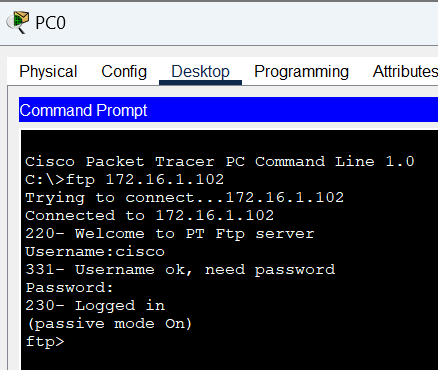
1. Ke Server 0





1. Ke Server 1

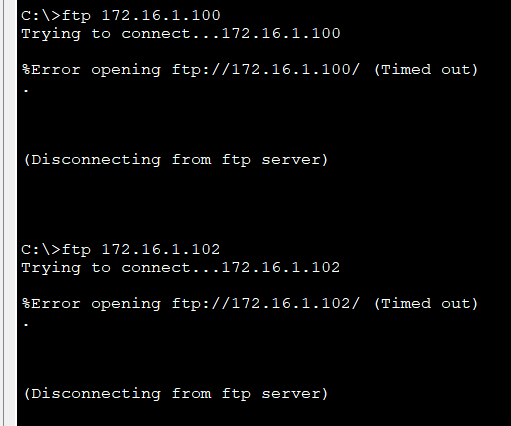




* 1. Lakukan pengujian dari host Jerry pada PC1 dan bandingkan dari PC lain

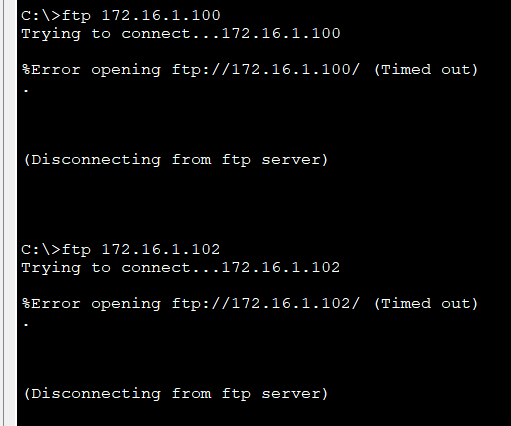
1. Ke Server 0





1. Ke Server 1

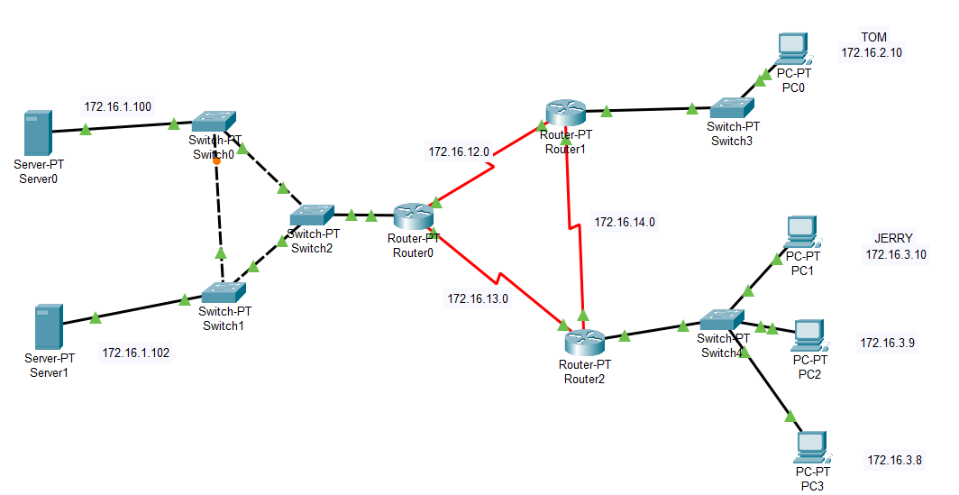




1. Analisa

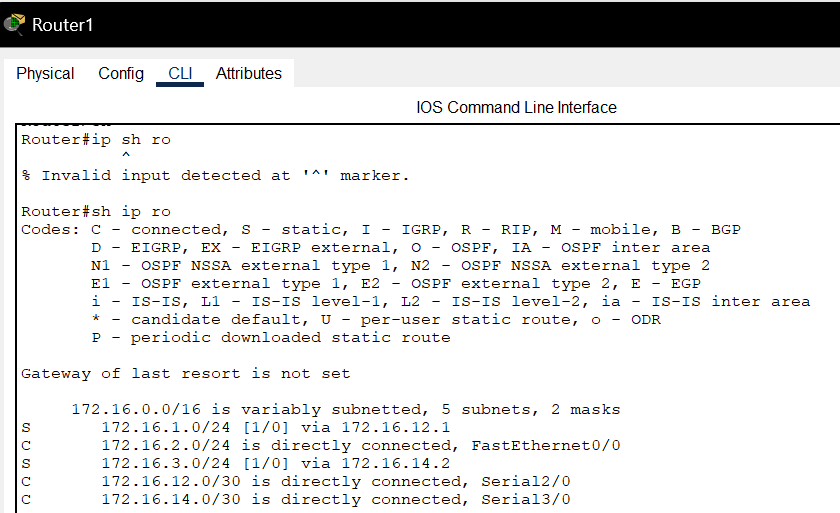
Pada Praktikum Kelima ini dilakukan Extended ACL. ACL ini tentunya fungsinya sama seperti praktikum sebelumnya dimana ACL sebagai fitur untuk mengatur lalu lintas data berdasarkan Alamat IP sumber. ACL ini bertindak sebagai filter yang menentukan suatu paket data didizinkan (permit) atau ditolak (deny) 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.

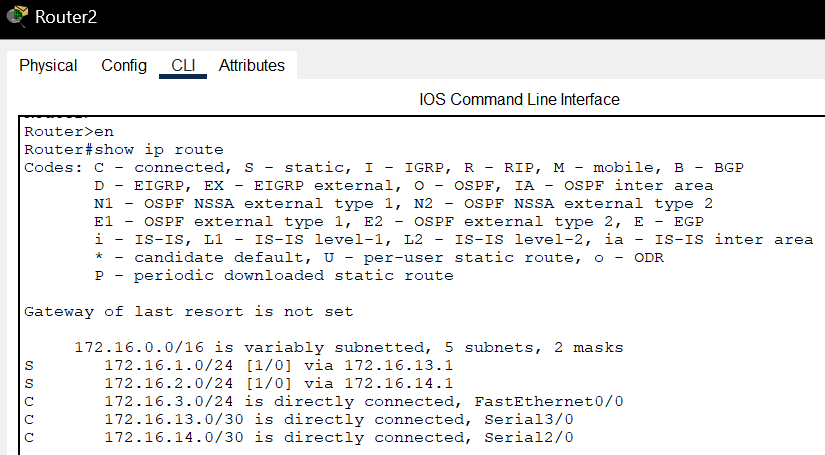
Untuk percobaanya akan dibuat topologi jaringan sebagai berikut:



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.

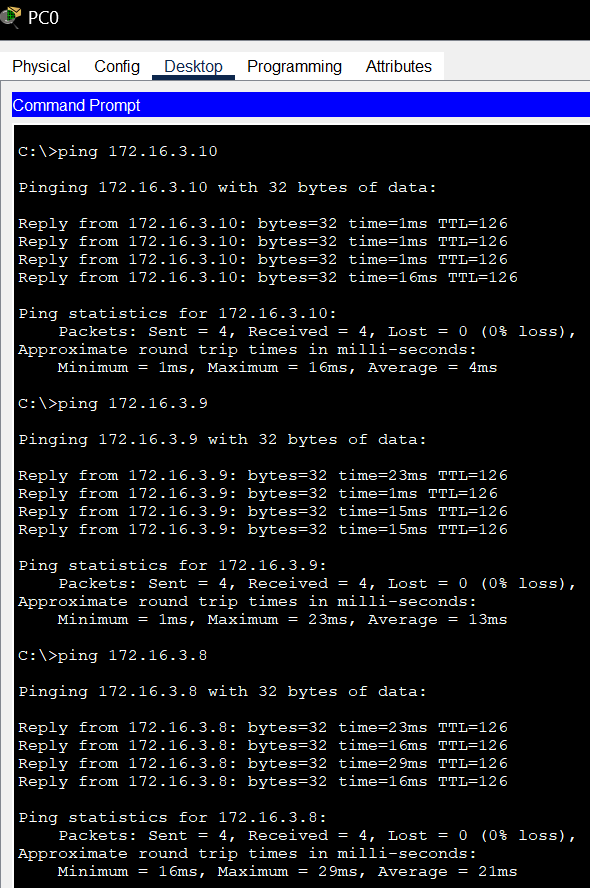
Setelah diketahui networknya, semua device akan di konfigurasi sesuai dengan networknya dan hasilnya sesuai dengan foto topologi diatas. Lalu antar ketiga Router di routing dengan static routing agar antar end device secara keseluruhan bisa saling terkoneksi. Berikut hasil konfigurasi static routing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

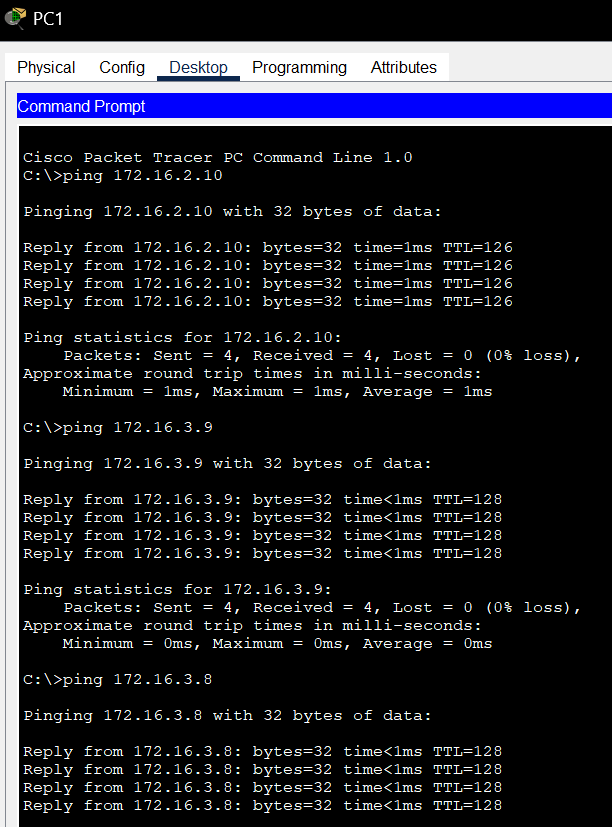


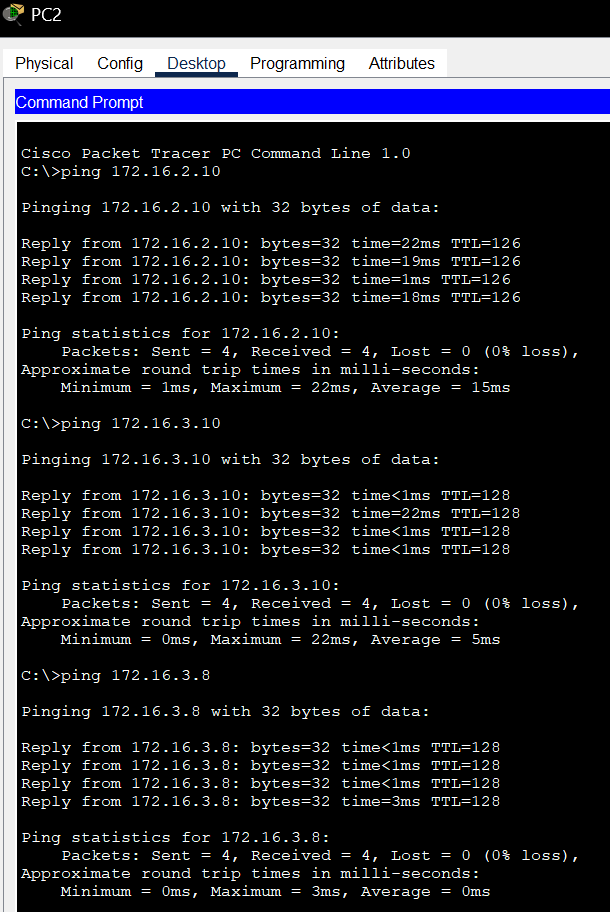


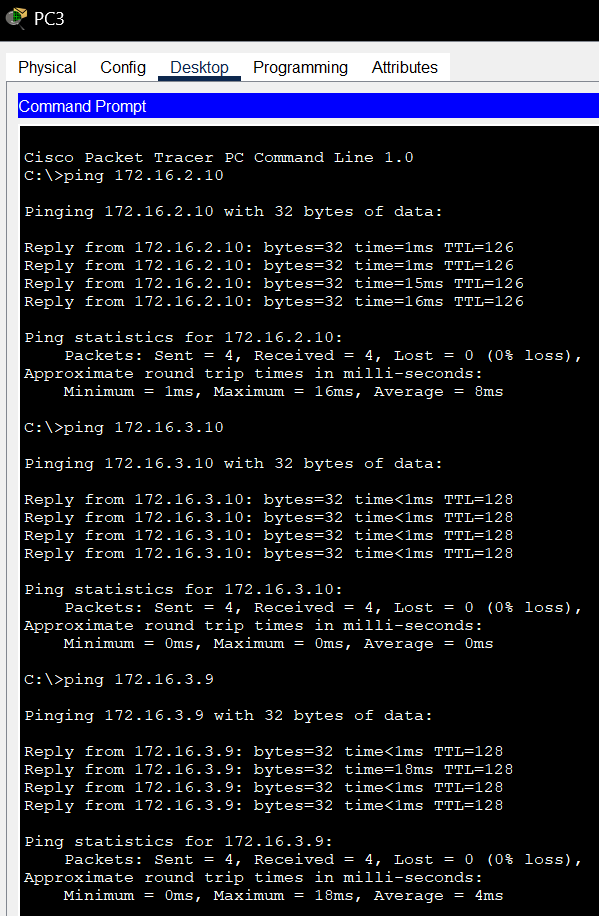
Dari kedua gambar CLI Router 1 dan Router 2 menunjukkan adanya koneksi dengan jaringan diseluruh router ada. Pada Router 1 sudah terkoneksi secara static dengan network 172.16.1.0 via ip port 172.16.12.1 dan network 172.16.3.0 via ip port 172.16.14.2. Pada Router 2 sudah terkoneksi secara static dengan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



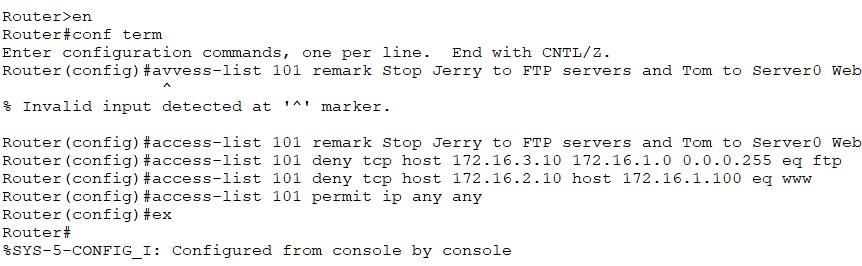


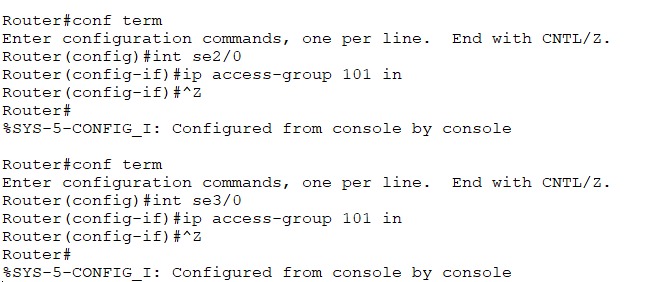




Terlihat bahwasannya antar satu dan lain PC sudah bisa menerima pesan ping yang dikirimkan. Ini menandakan static routing berhasil dikonfigurasi di masing-masing router. Lalu pesan yang disampaikan oleh TTL memiliki arti saat TTL= 128 itu berarti pengiriman paket berada di satu network dan saat TTL= 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

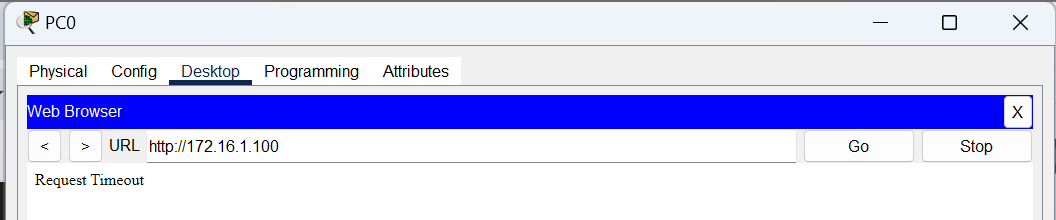


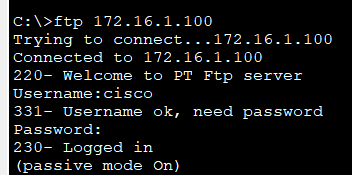


Dari perintah tersebut dapat dilihat ACL Extended menggunakan rentang ACL dari 100 hingga 199 yang aman disitu menggunakan nomor 101. Dalam perintah tersebut terdapat perintah untuk menandai atau menamai Stop PC Jerry mengakses FTP serve dan PC Tom untuk mengakses web dari Server0. Tapi tentunya hal 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.

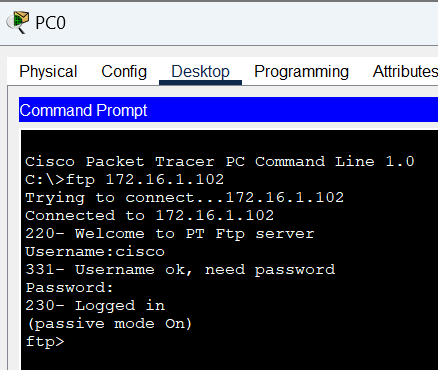
Lalu bisa dicoba untuk ping antar end device PC. Yang mana bisa dilihat di prosedur diatas, hasilnya tetap sama, hal ini dikarenakan router yang ada ACL nya hanya router 0 sedangkan end device PC masih bisa berkomunikasi satu sama lain lewat Router 1 dan Router 2 saja.

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

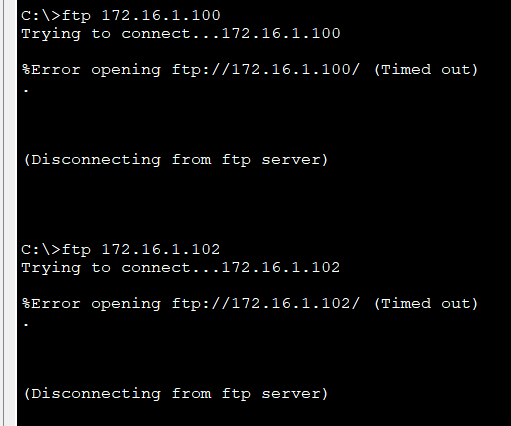




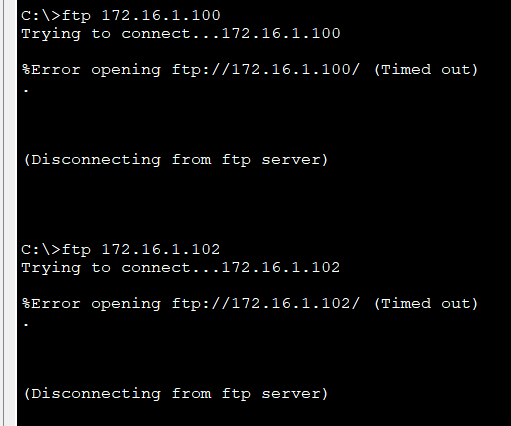












Bisa dilihat hasilnya saat PC 0 mengakses port web atau laman web server 0 atau IP 172.16.1.100 hasilnya adalah request time out. Hal ini mengindikasikan bahwa ACL yang terkonfigurasi sudah bisa terpakai dengan baik, karena perintah yang dikeluarkan tadi di CLI Router 0 adalah untuk memblokir akses PC0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

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.

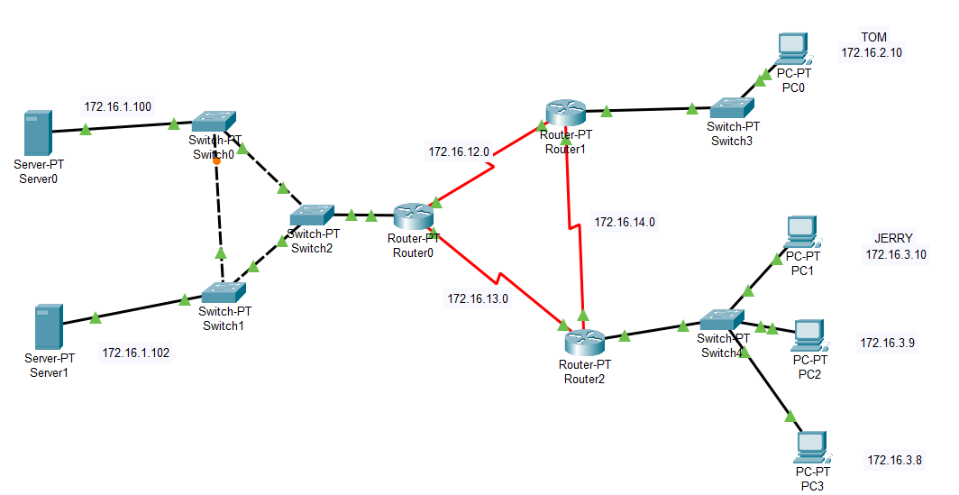
* 1. Berdasarkan percobaan di atas, bila ACL diterapkan bukan di Router0, tetapi hanya di terapkan di Router2, jelaskan apa yang terjadi?

Jawab:

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.

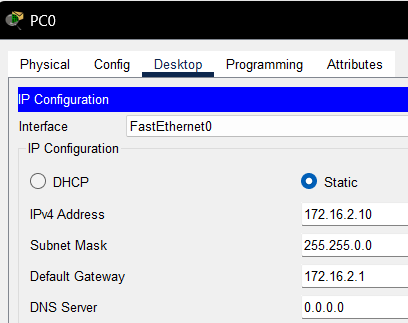
* 1. Lakukan modifikasi ACL pada percobaan, sehingga host Jerry hanya bisa mengakses FTP server, PC1 dan PC2 tidak bisa mengakses Web Server0, serta PC3 tidak bisa mengakses Web Server1.

Jawab:

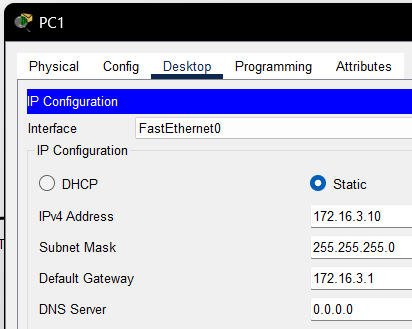


* Konfigurasi Alamat End Device

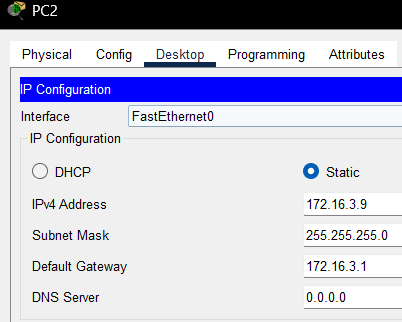
1. PC 0



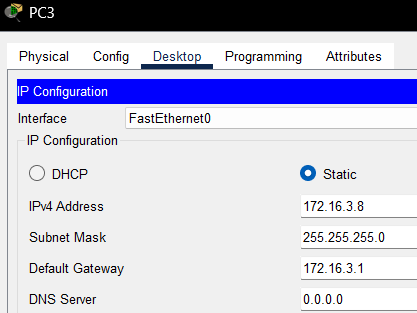
1. PC 1



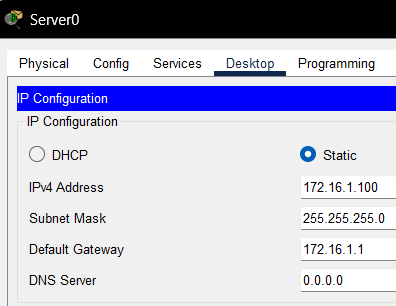
1. PC 2



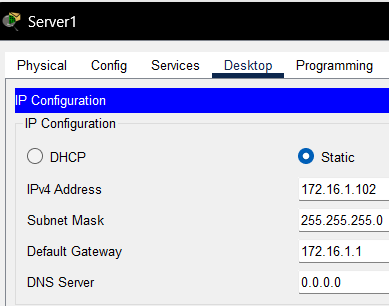
1. PC 3



1. Server 0

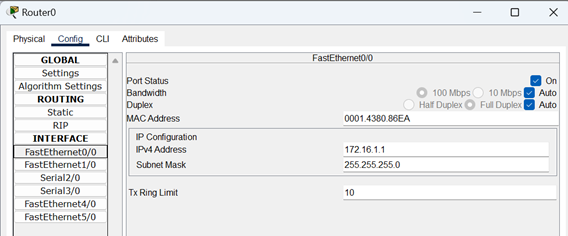


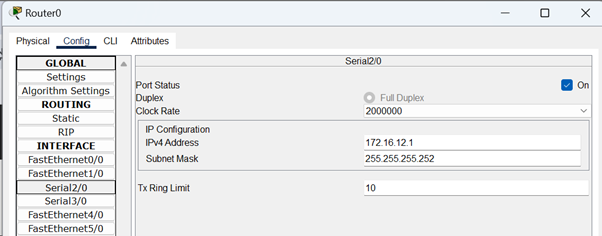
1. Server 1

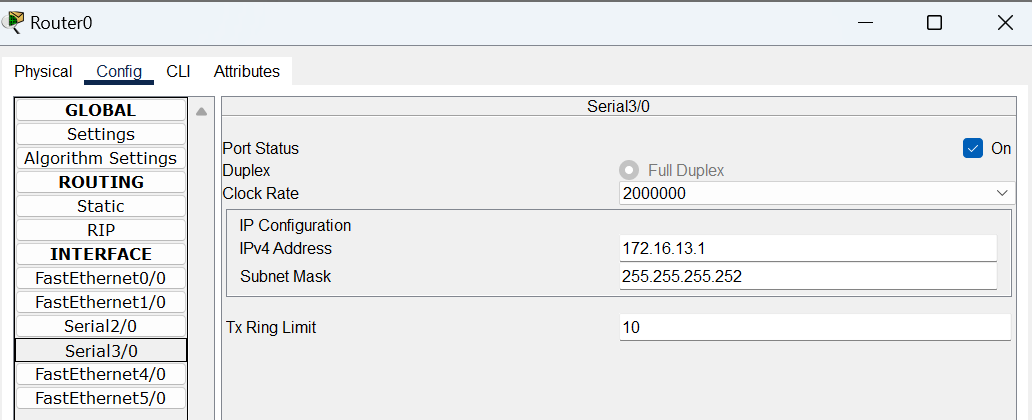


* Konfigurasi Interface Router

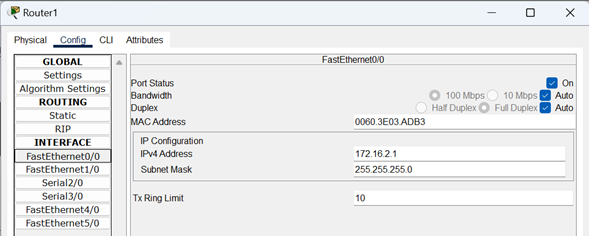
1. Router 0

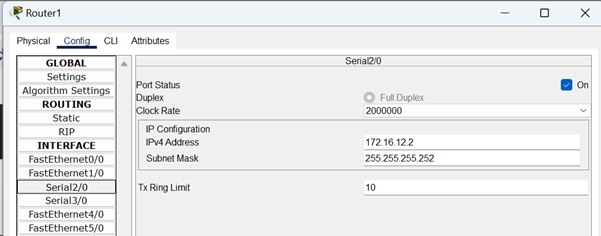


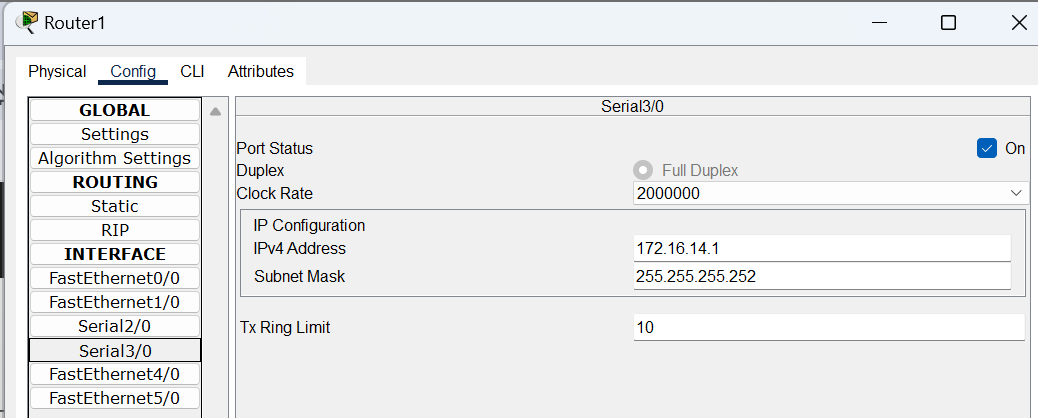




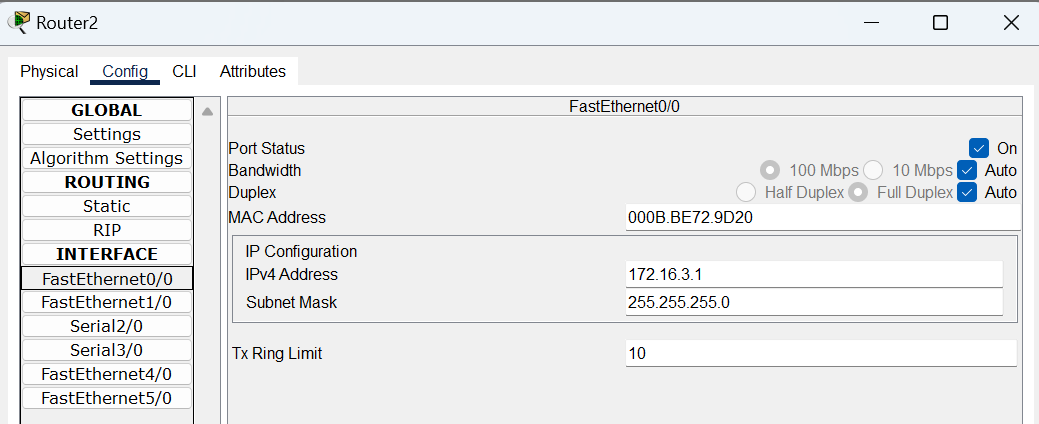
b. Router 1

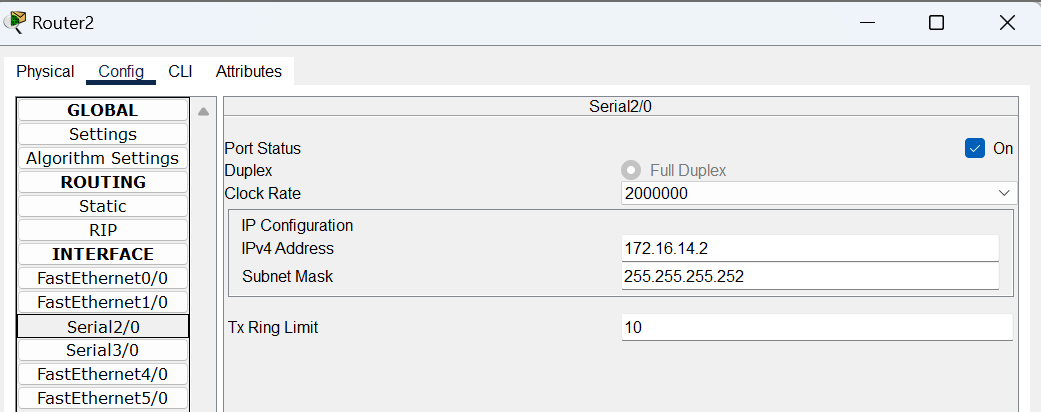


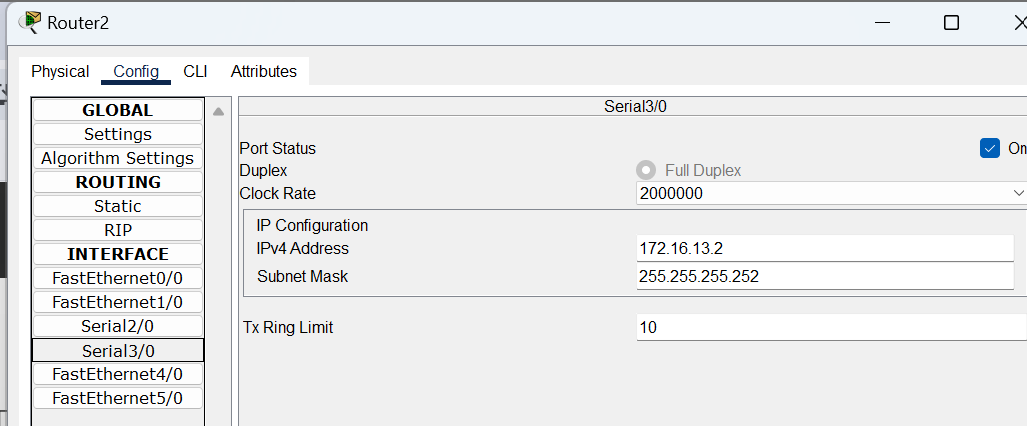




c. Router 2

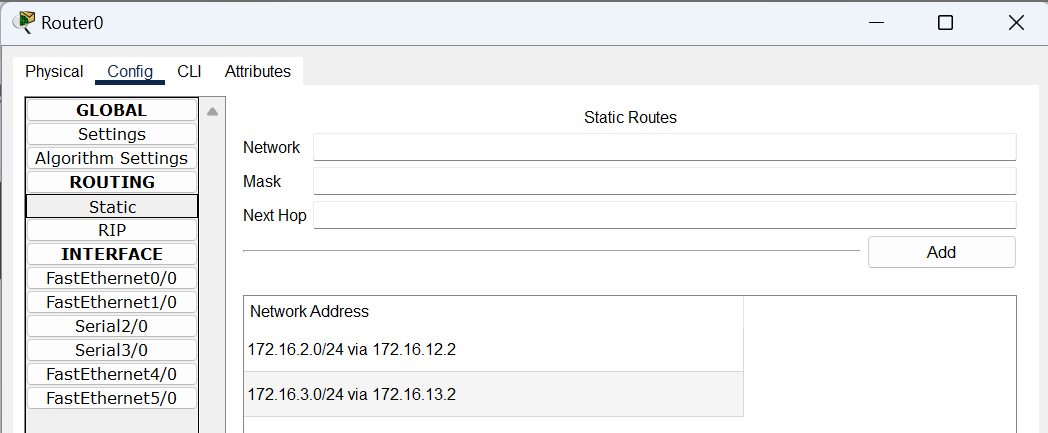




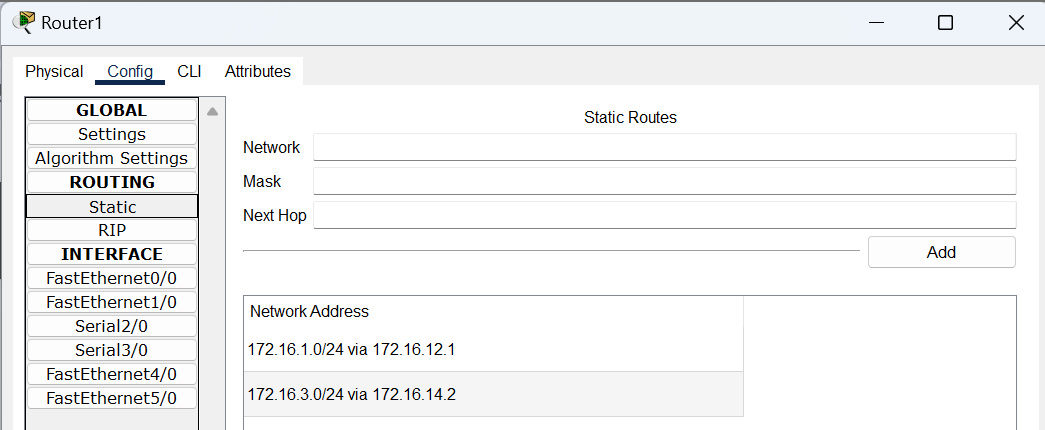


* Konfigurasi static Routing

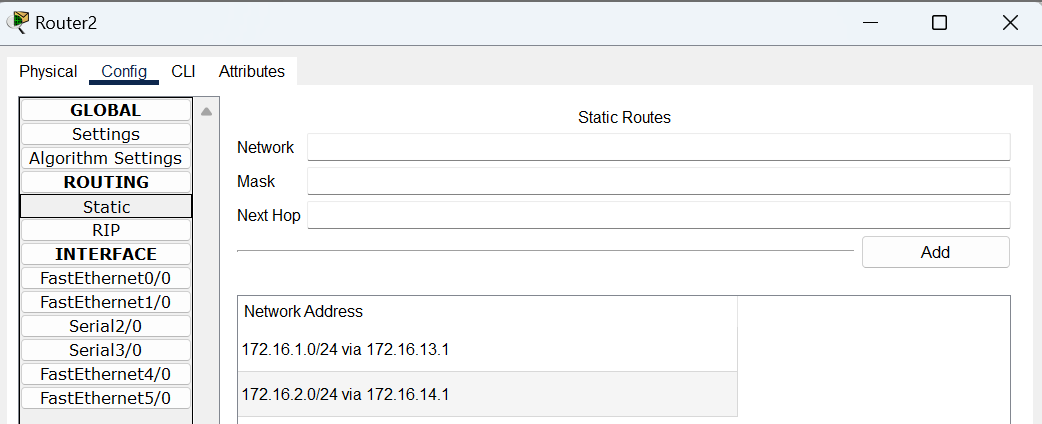
1. Router 0



1. Router 1

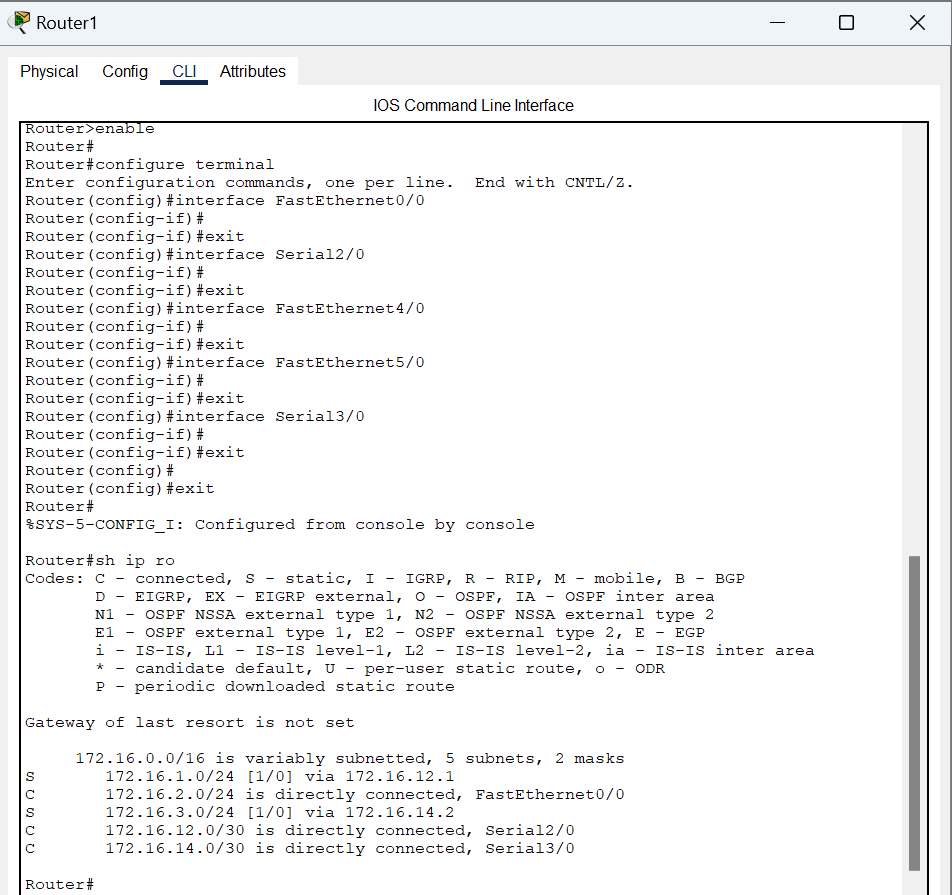


1. Router 2

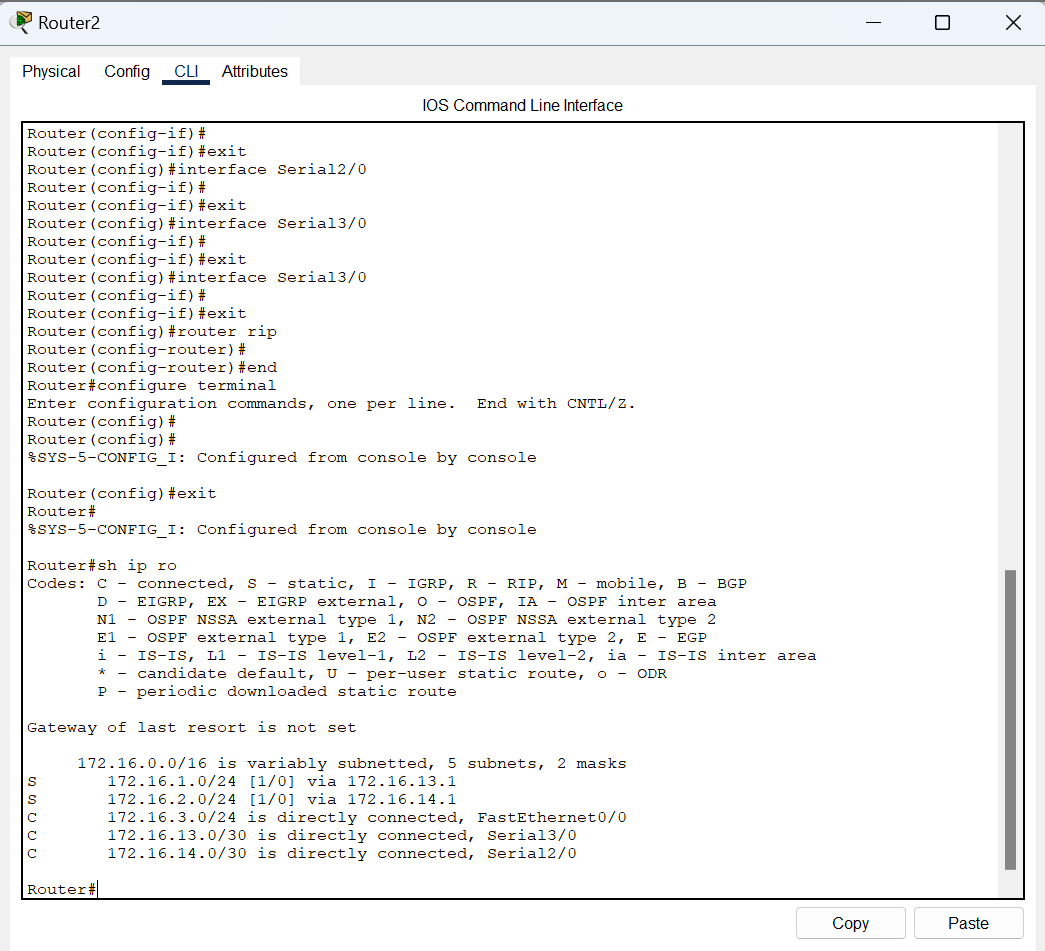


* Pengujian Router#show ip route

1. Router 1

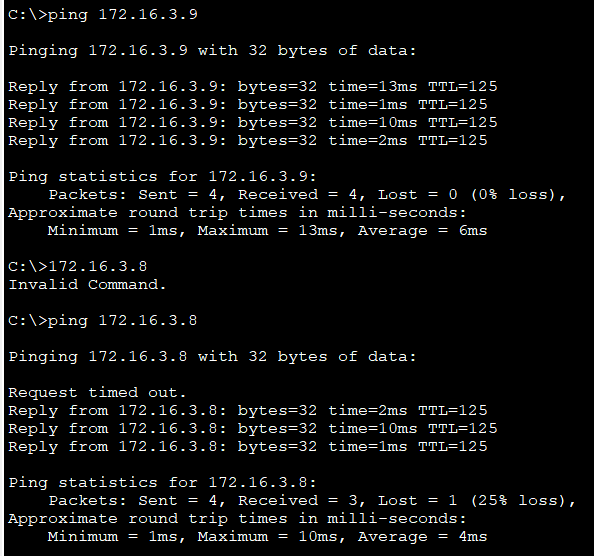
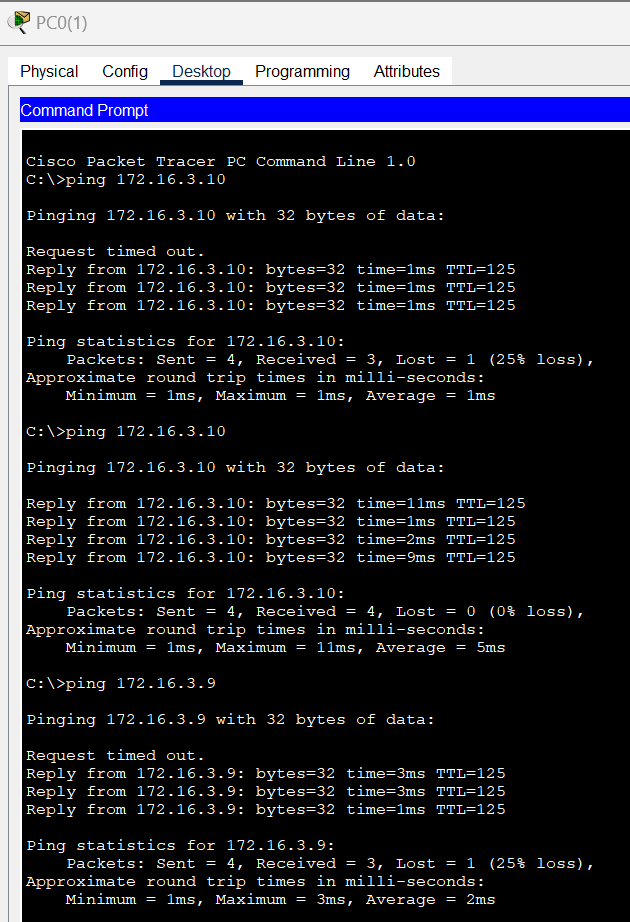


1. Router 2

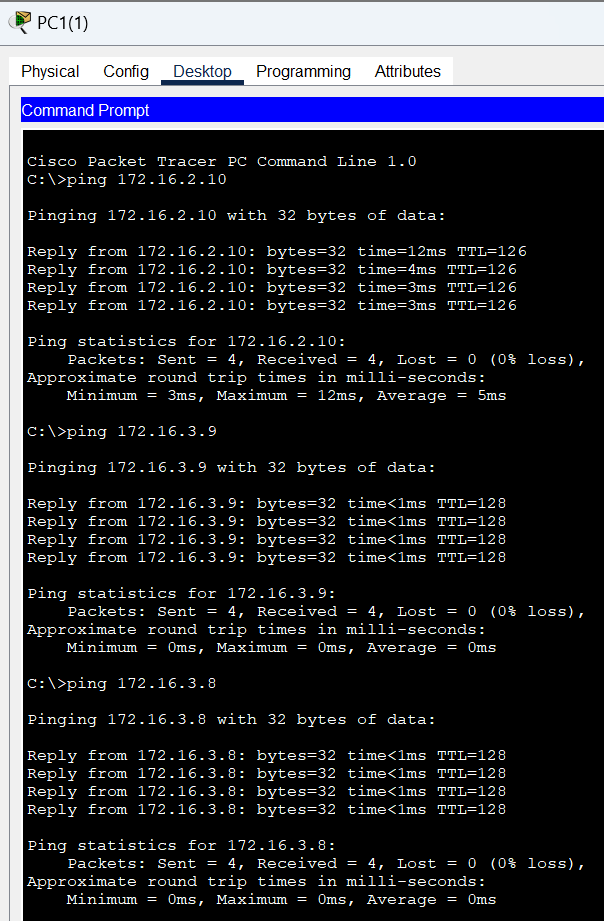


* Pengujian tes ping dari masing-masing PC

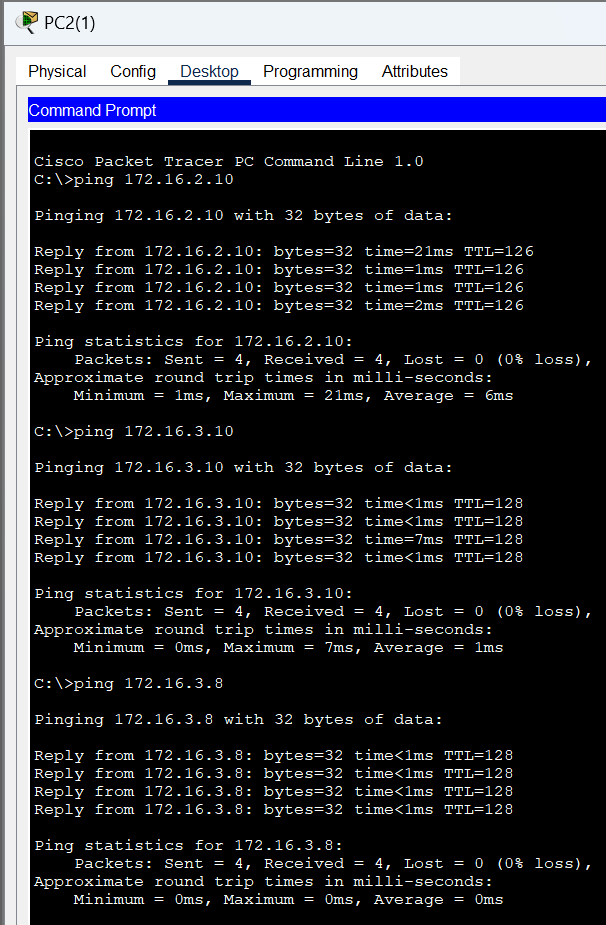
1. PC 0



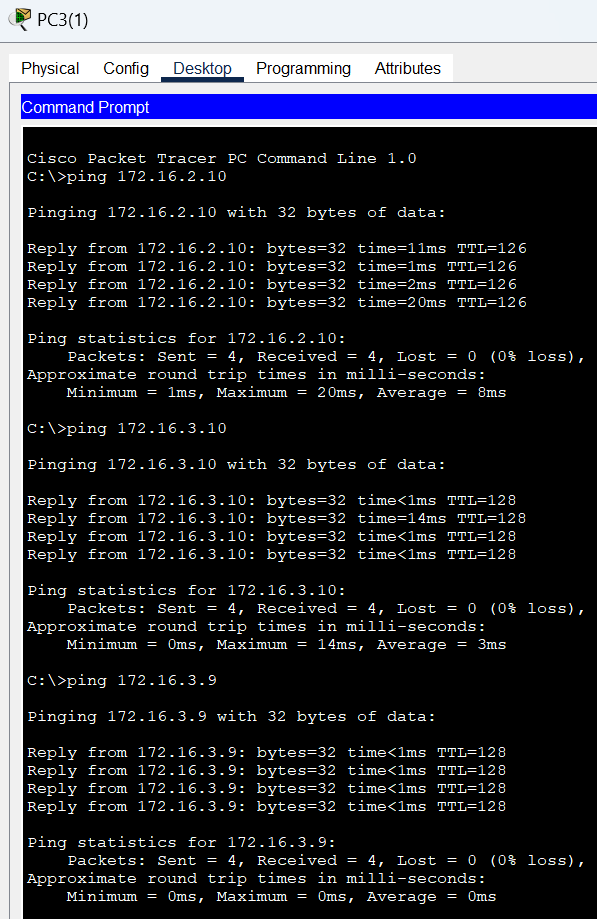
1. PC 1



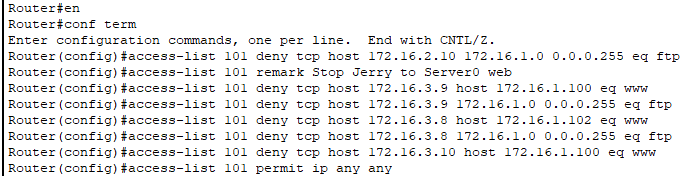
1. PC 2



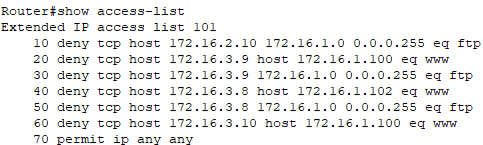
1. PC 3

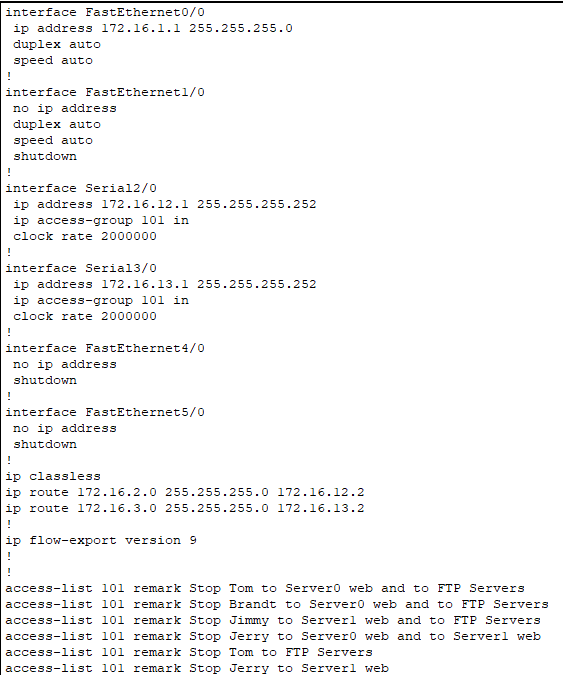
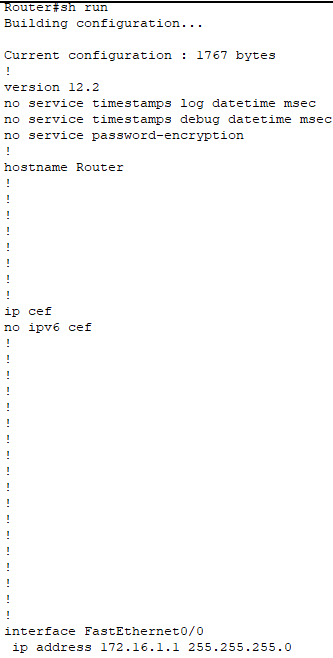


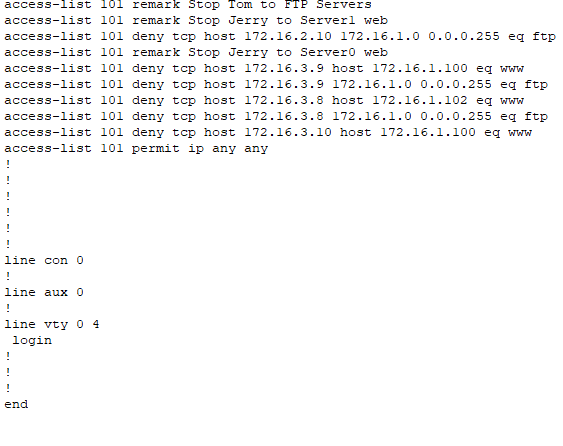
* Konfigurasi Extended ACL



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

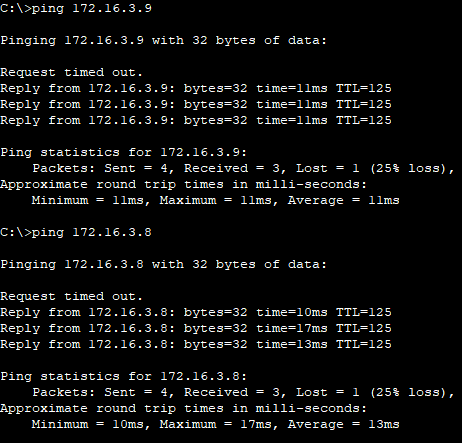
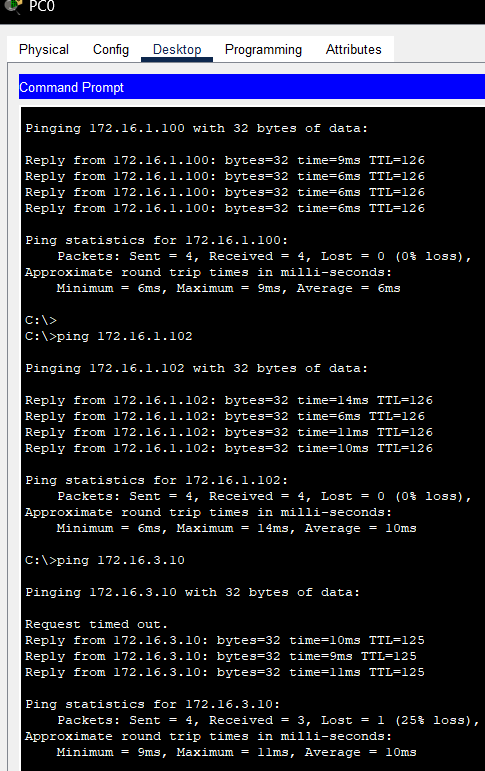




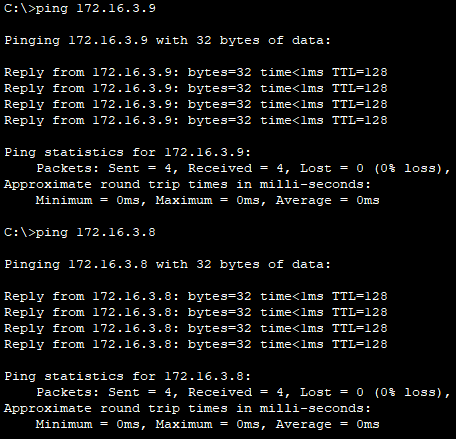
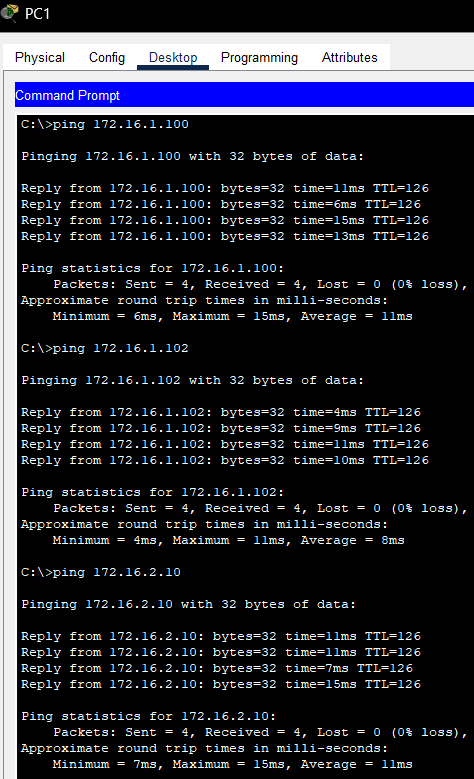


* Pengujian tes ping dari masing-masing PC

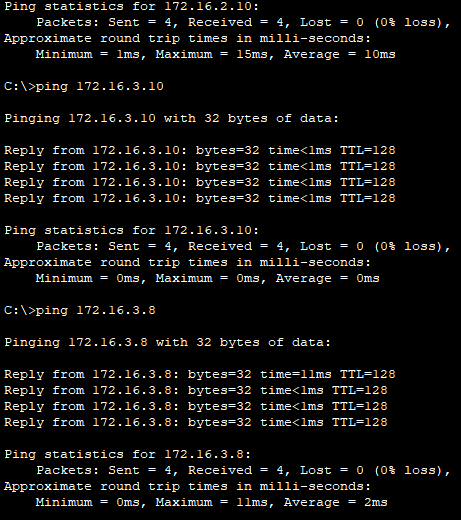
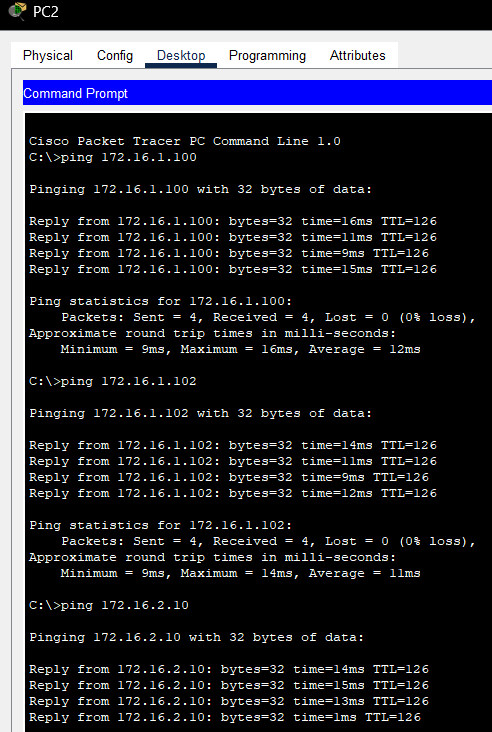
1. PC 0



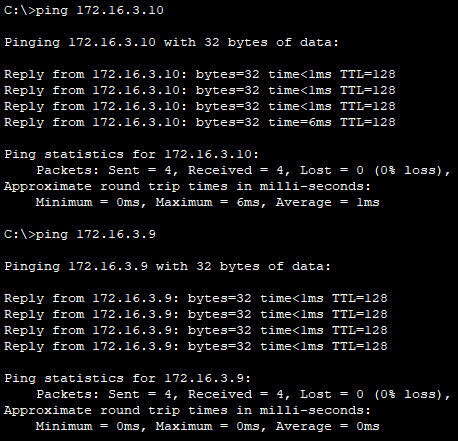
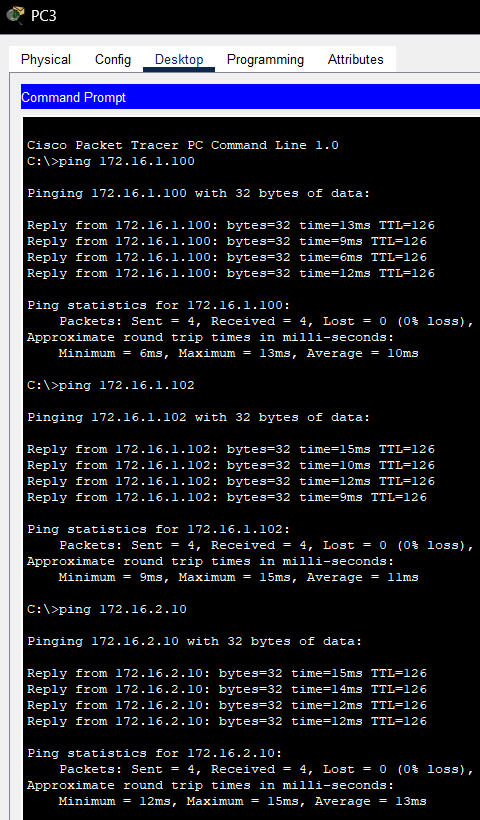
1. PC 1



1. PC 2



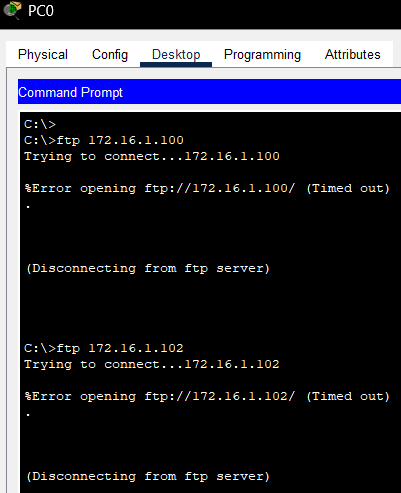
1. PC 3



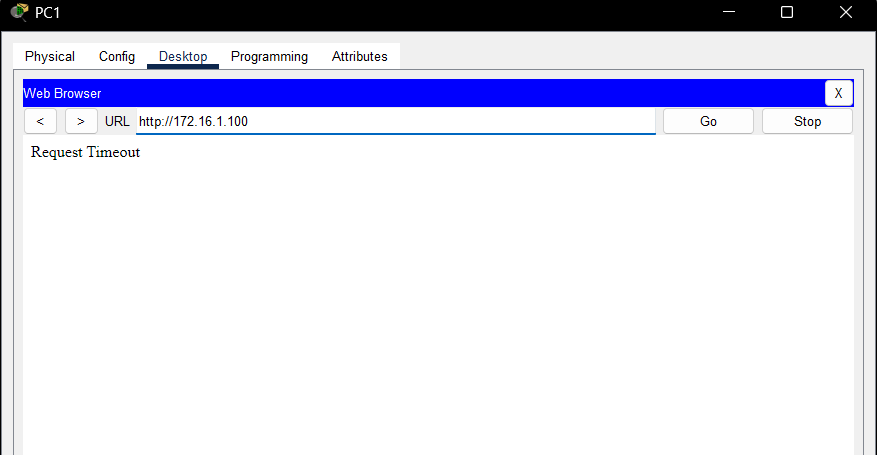
* Pengujian perintah FTP dan akses web di masing-masing PC ke Server

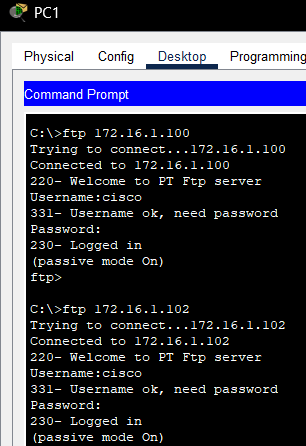
1. PC 0



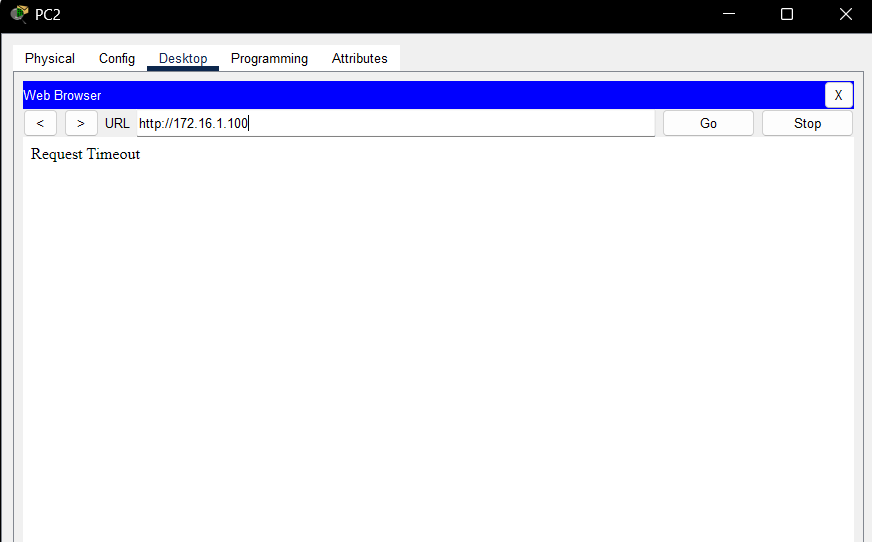


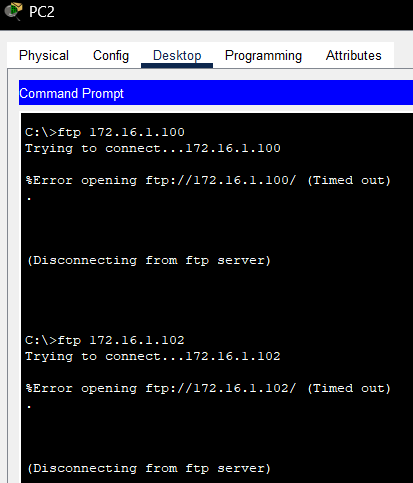
1. PC 1



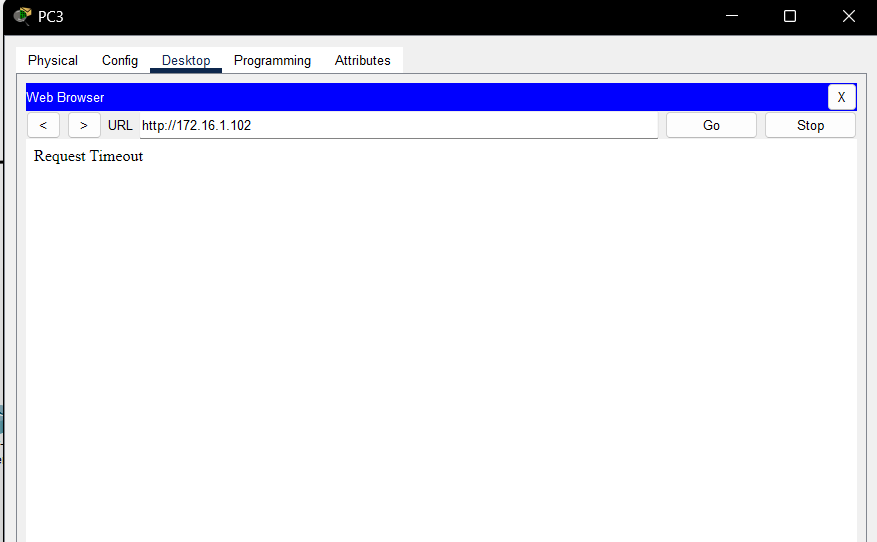


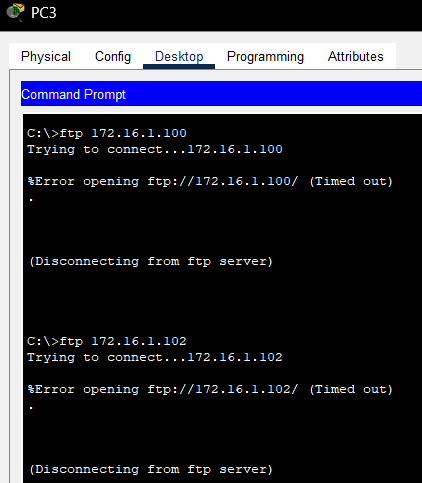
1. PC 2



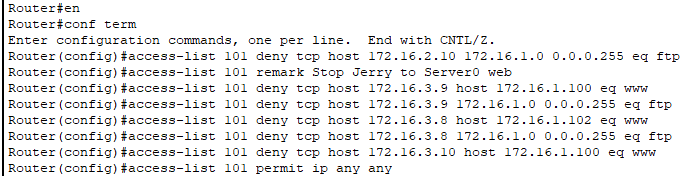


1. PC 3



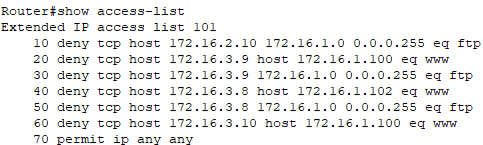


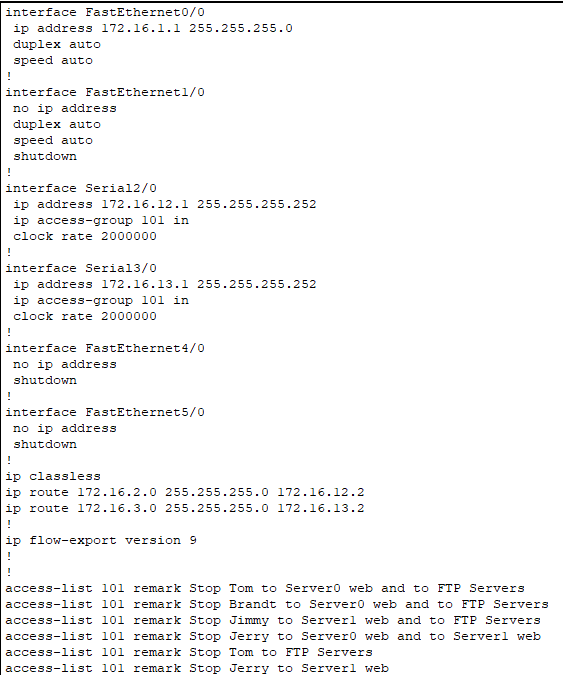
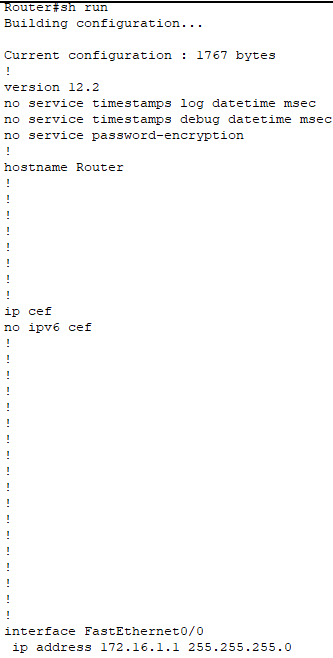
Dari perubahan konfigurasi Extended ACL dari percobaan menjadi seperti ini

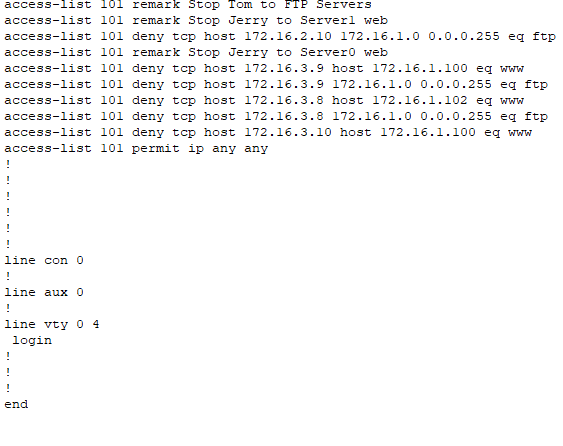


Hal ini berarti memblokir akses PC2 untuk mengakses port web server 0 dan port ftp kedua server, PC3 di blokir aksesnya untuk mengakses port web server1 dan port ftp kedua server, PC1 juga diblokir aksesnya untuk mengakses port web server 0 saja, dan PC0 diblokir aksesnya untuk mengakses port ftp kedua 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







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.

1. 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.