

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.

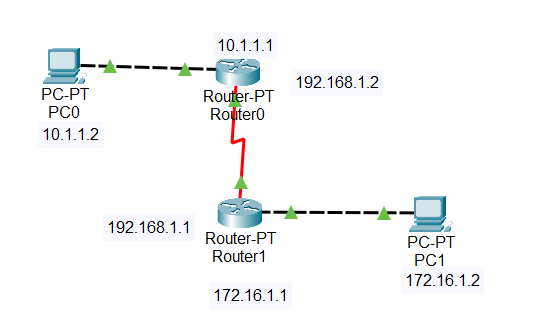
Keunggulan utama Standard ACL terletak pada kesederhanaannya, membuatnya mudah dikonfigurasi dan dikelola, terutama bagi administrator jaringan pemula. Namun, karena hanya dapat mengevaluasi alamat IP sumber, kemampuannya sangat terbatas untuk skenario pengamanan kompleks yang memerlukan kontrol berdasarkan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

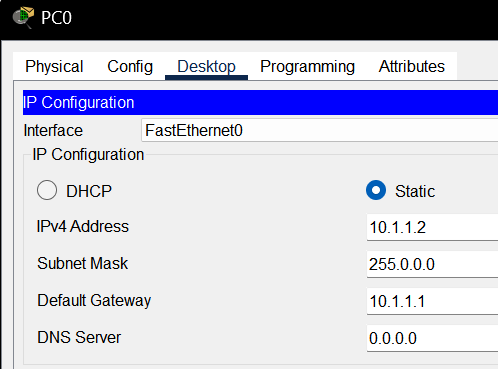
b. Network devices: Switch, Router

c. Connections: Copper Straight-Through, Serial DCE

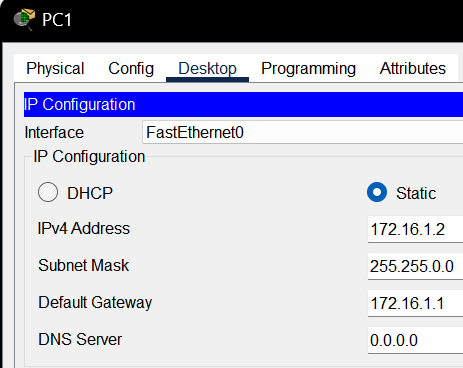


* 1. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device:

1. PC 0

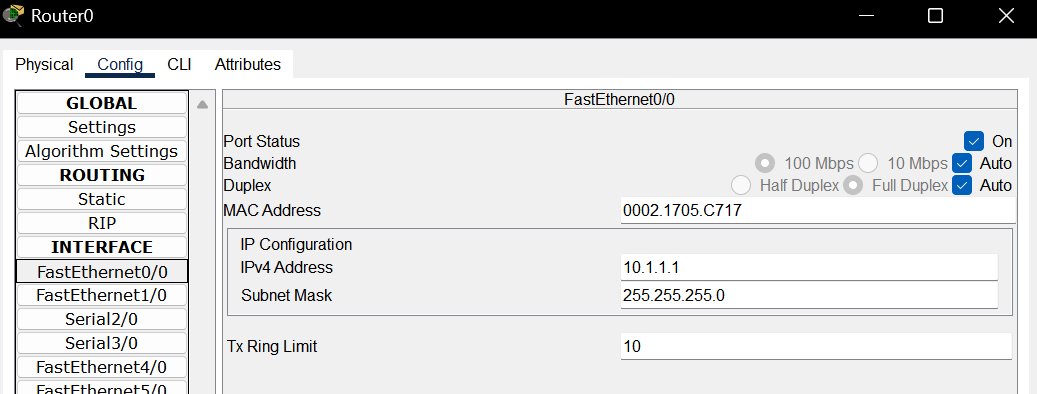


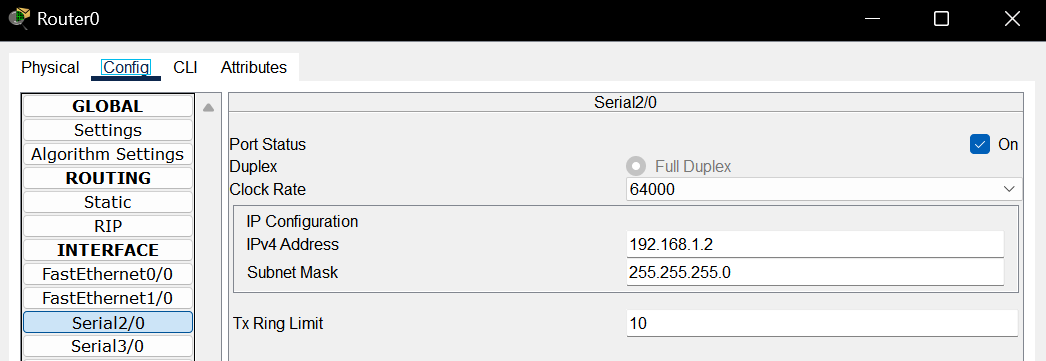
1. PC 1



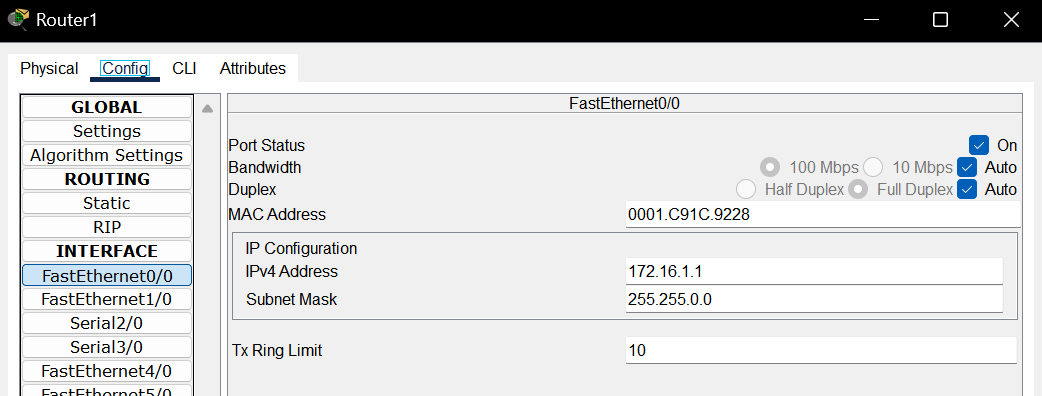
* 1. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

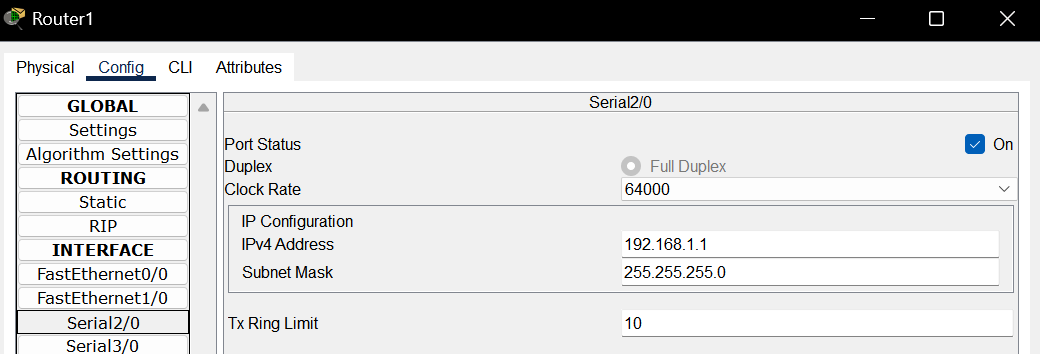
1. Konfigurasi Fast Ethernet 0/0 dan Serial 2/0 pada Router 0





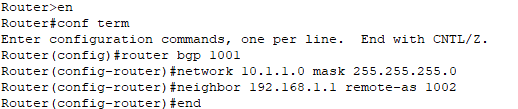
1. Konfigurasi Fast Ethernet 0/0 dan Serial 2/0 pada Router 1



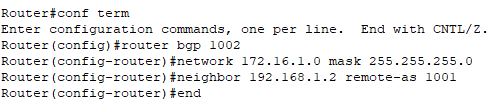


* 1. Lakukan konfigurasi routing dinamis menggunakan protokol BGP pada Router, seperti berikut:

1. Router 0

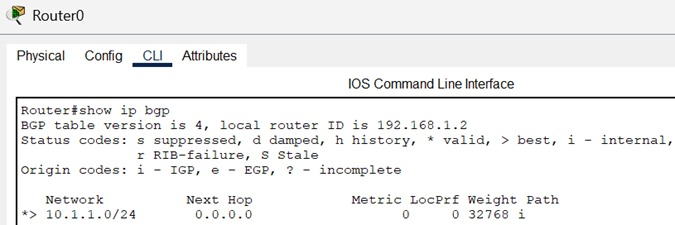


1. Router 1



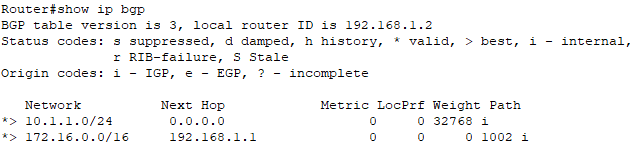
Lakukan analisa terhadap perintah-perintah di atas, selanjutnya jalankan perintah: #show ip

bgp, kemudian tampilkan hasilnya.



(saat router 1 belum dikonfigurasikan)

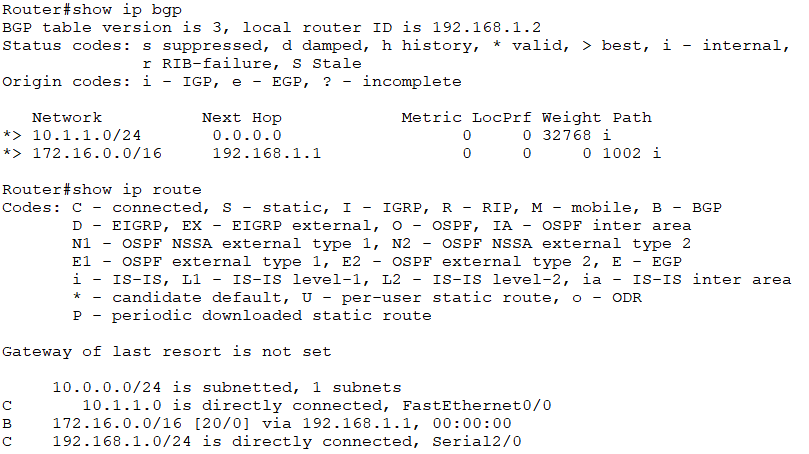
Lakukan konfigurasi routing dinamis menggunakan protokol BGP pada Router\_2 seperti padaprosedur no.4 dan sesuaikan IP address seperti pada topologi. Selanjutnya jalankan perintah: #show ip bgp , kemudian tampilkan hasilnya. Apakah ada perbedaan dengan hasil pada prosedur no.4.



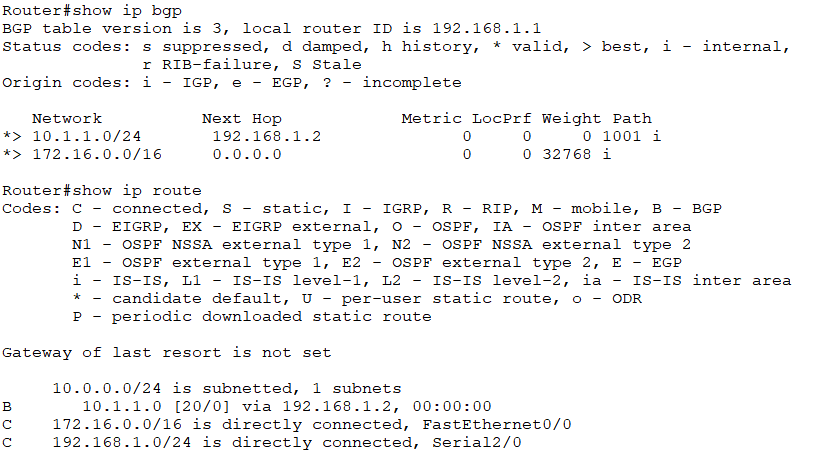
(setelah router 1 dikonfigurasikan BGP nya)

* 1. Jalankan perintah : #show ip bgp kembali pada Router\_1, bagaimana hasilnya? Kemudian jalankan perintah : #show ip route pada semua router. Tampilkan hasilnya dan lakukan analisa terhadap tabel routing.

1. Router 0

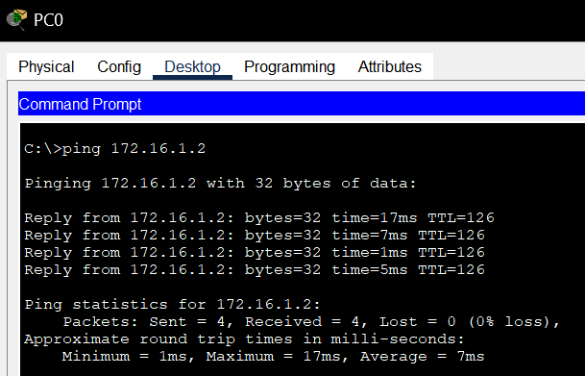


1. Router 1

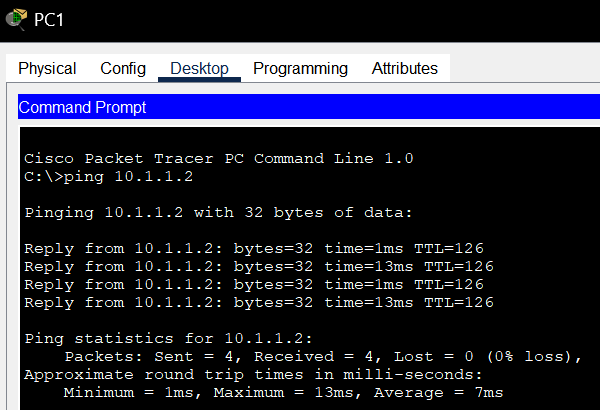


* 1. Lakukan tes ping ke semua PC, kemudian tampilkan hasil percobaan anda.

1. PC 0 ke PC lain

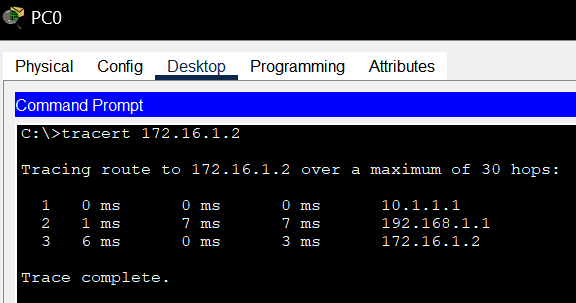


1. PC 1 ke PC lain

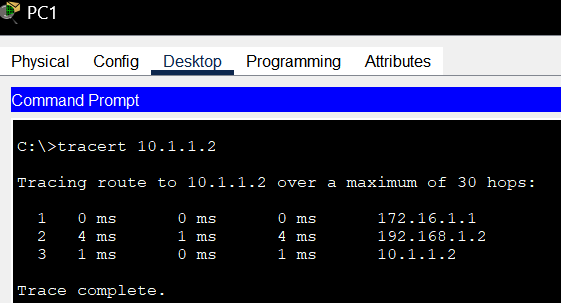


* 1. Gunakan perintah tracert untuk menganalisa pengiriman paket data dari pengirim hingga penerima pada semua PC

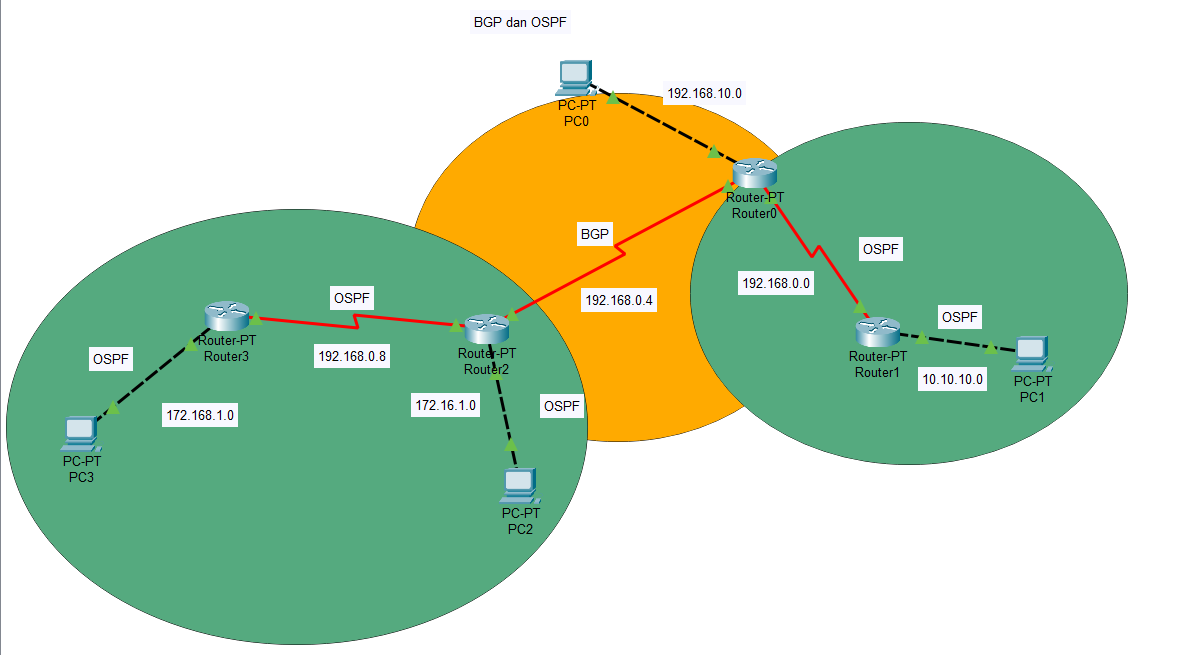
1. PC 0



1. PC 1

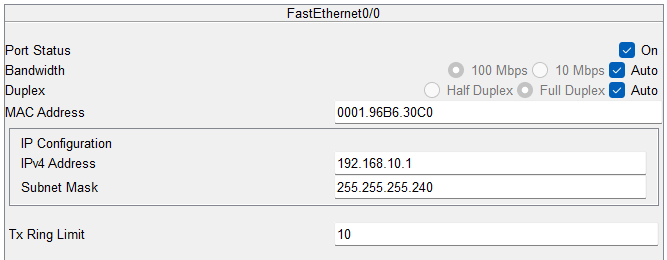


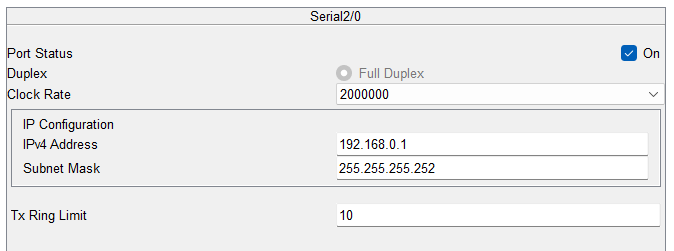
* 1. Rancanglah sebuah topologi jaringan dimana anda mengintegrasikan topologi jaringan pada gambar 1 dengan interior gateaway routing (IGP) routing, seperti redistribusi rute BGP ke OSPF atau sebaliknya.

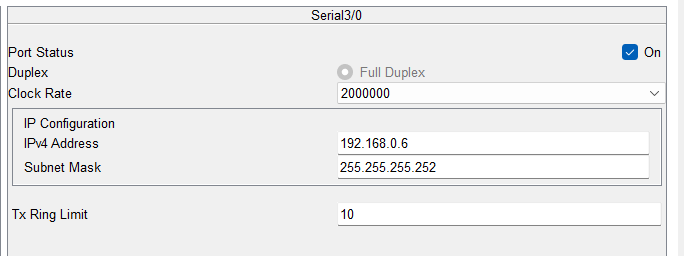


Konfigurasi IP router:

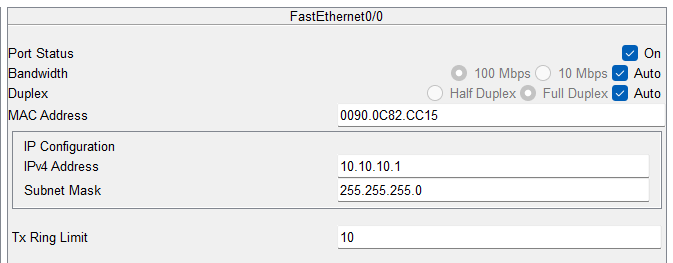
1. Router 0

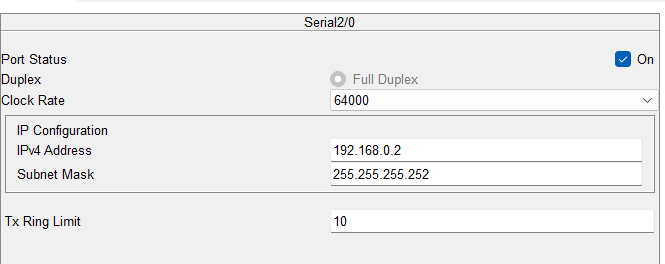




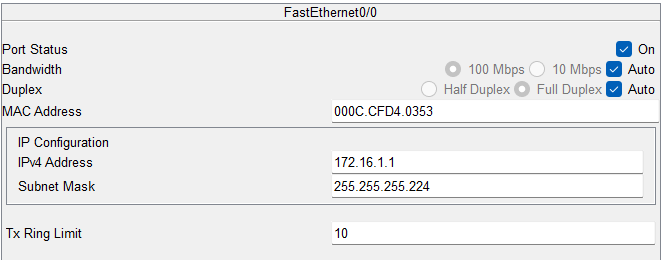


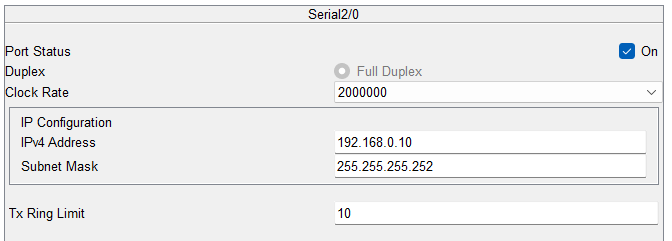
1. Router 1

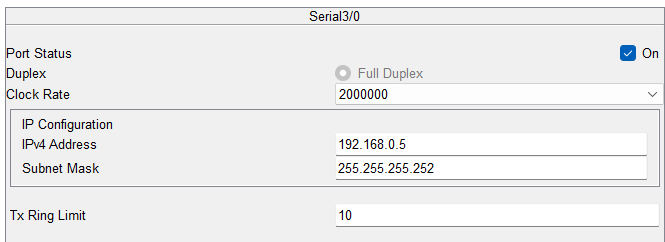




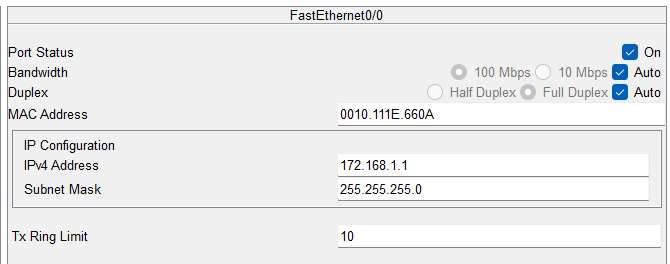
1. Router 2

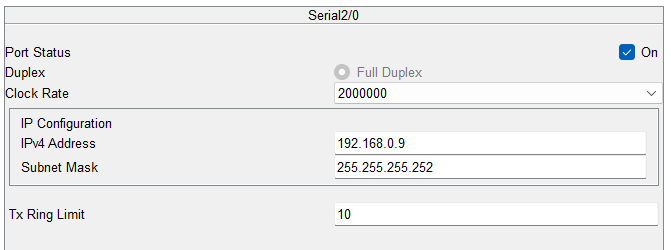






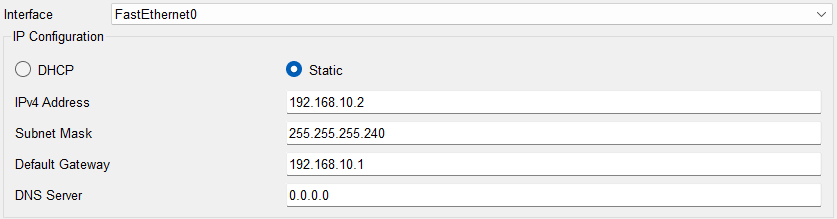
1. Router 3



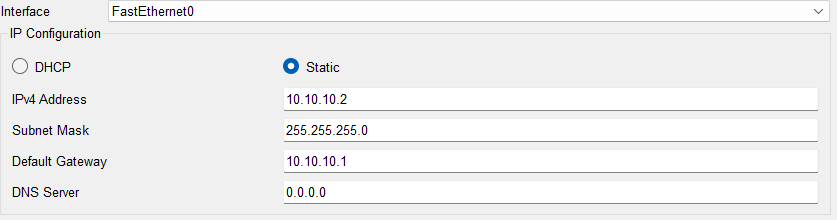


Konfigurasi IP PC:

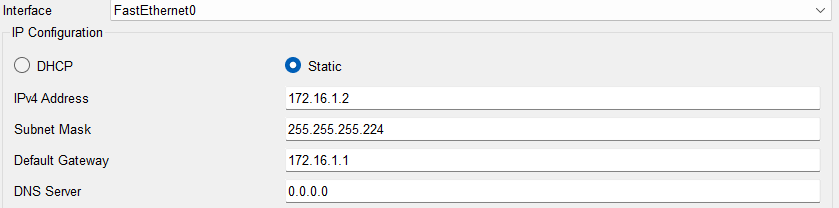
1. PC0



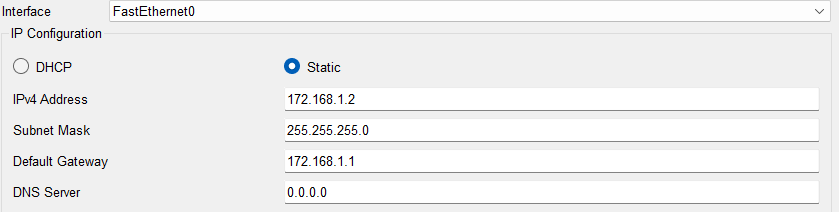
1. PC1



1. PC2



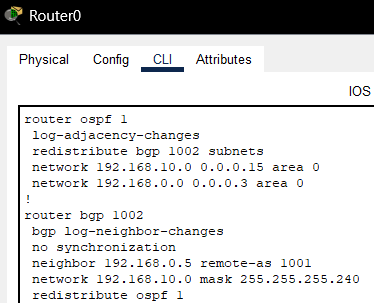
1. PC3



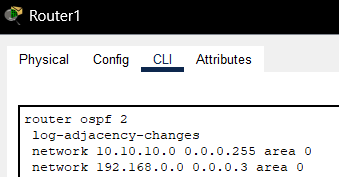
* 1. Setelah anda merancang topologi jaringan beserta IP address-nya, lakukan pengujian koneksi menggunakan tes ping dan tracert

Konfigurasi router yang telah diterapkan dapat dilihat melalui perintah `#show running-config`:

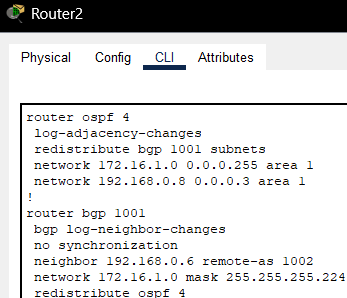
1. Router 0



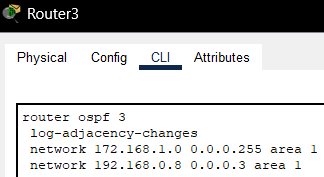
1. Router 1



1. Router 2

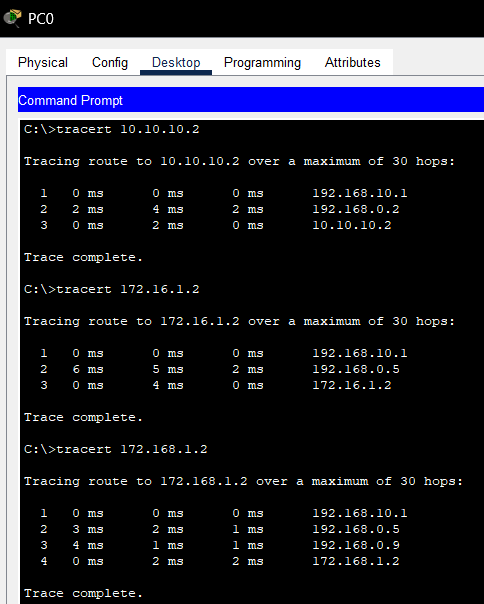
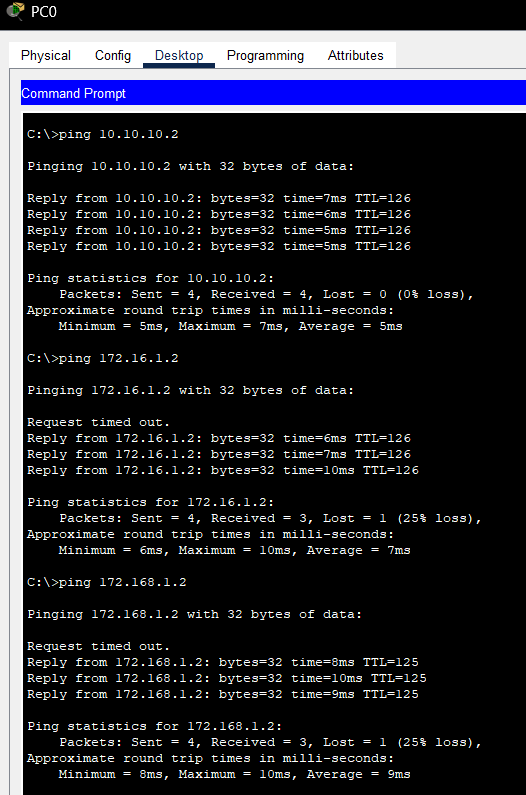


1. Router 3

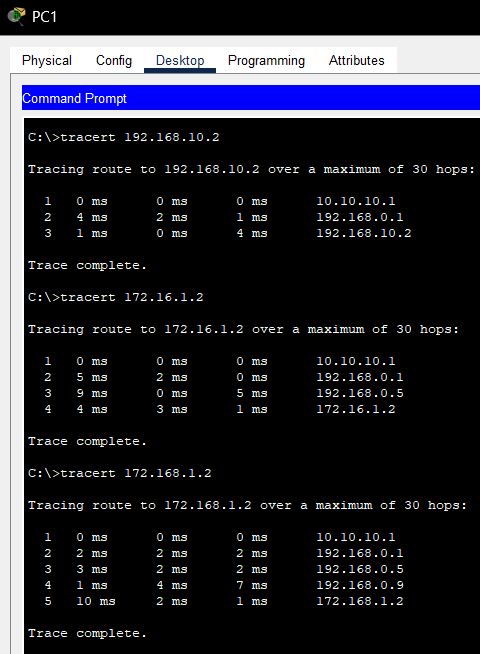
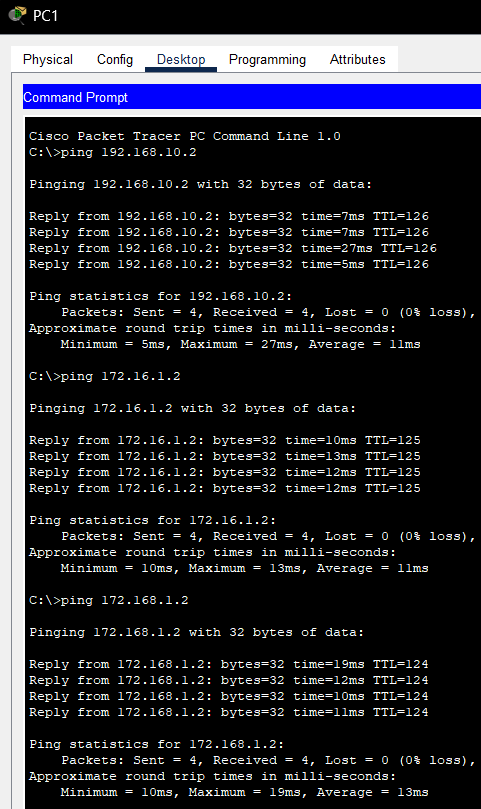


Hasil ping dan tracert dari masing-masing PC:

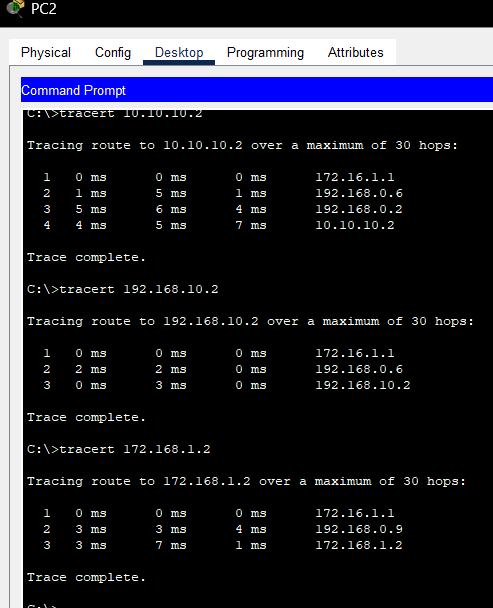
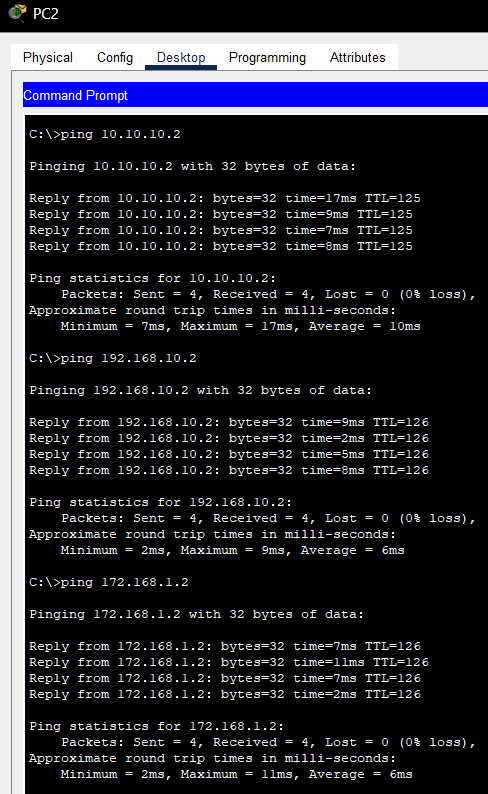
1. PC0



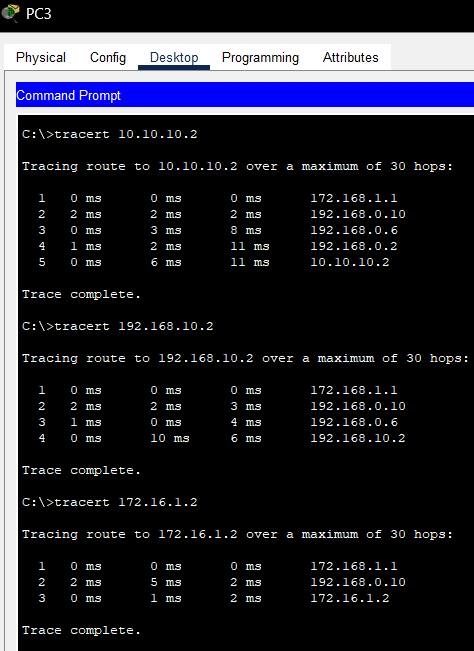
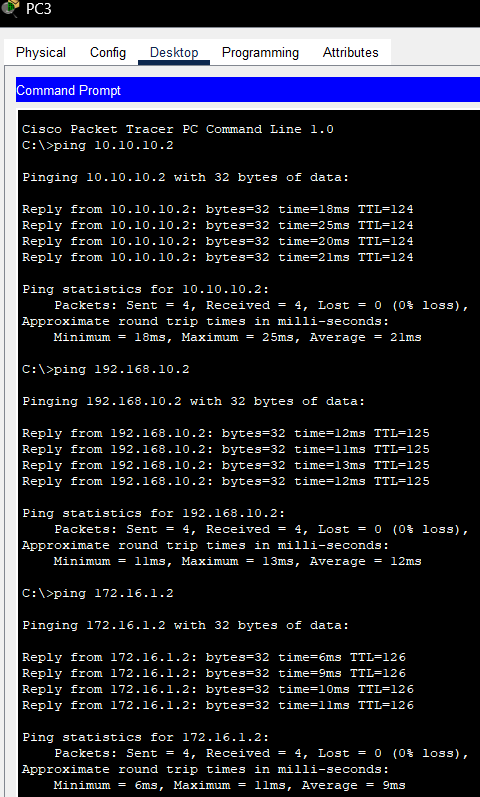
1. PC1



1. PC2



1. PC3

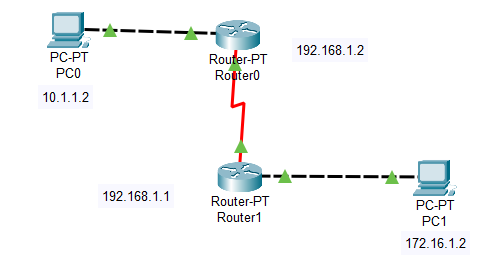


* 1. Lakukan analisa dari desain topologi jaringan yang anda buat.

1. Analisa

Pada Praktikum Keempat ini dilakukan perutean network secara dynamic menggunakan metode BGP atau Border Gateaway Protocol. Mtode dynamic routing ii digunakan untuk tipe Exterior Gateaway Protocol Dimana digunakan untuk komunikasi antar Autonomous Synchronous yang mana contohnya dari AS itu adalah sekolompok ISP yang mana nanti dengan BGP tersebut packet-packet dari satu ISP akan dikirim ke ISP yang lain untuk menuju perutean packet ISP tersebut. Jadi missal kita mengirim suatu pesan ke teman yang berbeda internet provider, maka saat packet-packet data itu berpindah dari satu ruote ISP ke ISP yang lain penghubung rute tersebut akan emnggunakan BGP, tetapi proses perpindahan packet dalam satu rute ISP itu biasanya menggunakan dynamic routing Interior Gateaway Protocol (IGP) seperti OSPF dan RIP. Maka dari itu dalam praktikum ini akan dicoba untuk mengkoneksikan satu router dan router yang lain menggunakan dynamic routing BGP.

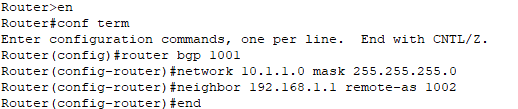
Dalam percobaan pertama akan dibuat topologi seperti ini:

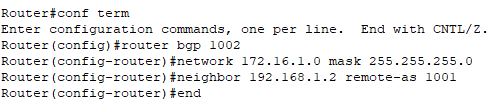


Dalam topologi diatas terdapat dua network lokal nya yaitu 10.1.1.0 yang ada di router 0 dan 172.16.0.0 yang ada di router 1. Lalu network yang digunakan untuk menghubungkann antar routernya adalah 192.168.1.0. ketiga network ini akan saling berhuungan dan menggunakan Exterior Gateaway Protocol untuk komunikasi antar routernya. Karena hal terseut dua router ini bisa diandaikan seperti router dari satu ISP ke router ISP lainnya, hal ini agar tiap ISP bisa mengkonfigurasikan sendiri apakah packet data dari network yang mereka sediakan bisa diteruskan ke ISP lainnya atau tidak.

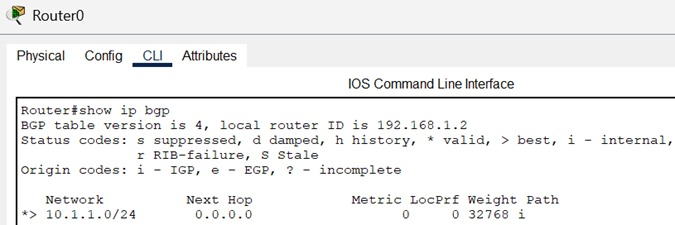
Lalu untuk pengiinisialisasian default gateaway nya tentunya seperti biasanya yang mana router akan emmiliki nilai terkecil IP host nya dari network ID yang disediakan. Jadi router 0 Ip nya adalah 10.1.1.1 lalu router 1 adalah 172.16.1.1. setelah selesai menginisialisasi semua Alamat IP dan default gateaway di semua koneksi end device dan router maka lanjut untuk mengkonfigurasi protocol BGP di setiap router nya.

Karena menggunakan BGP, maka konfigurasinya akan dilakukan di CLI routernya, jadi harus decoding sendiri. Berikut konfigurasi BGP dari router 0 dan router 1:

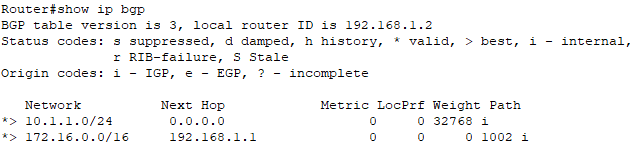




Sebelumnya jika hanya mengkonfigurasi BGP salah satu router saja, missal hanya mengkonfigurasi BGP di router 0 saja, mka data yang didapat jika menggunakan perintah #show ip bgp adalah

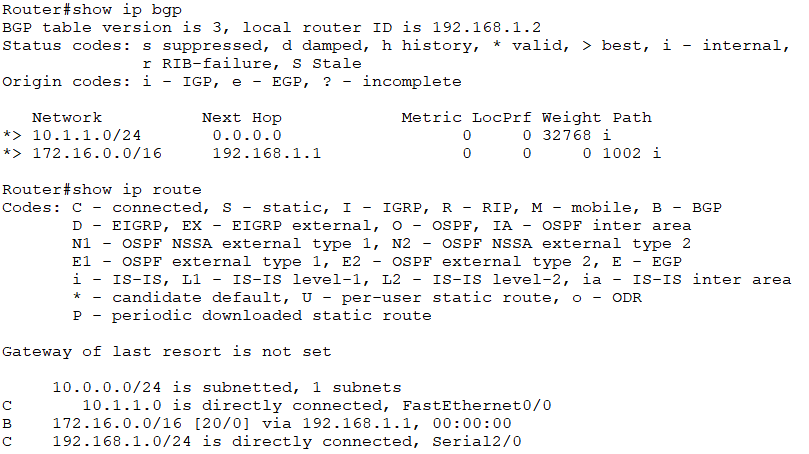


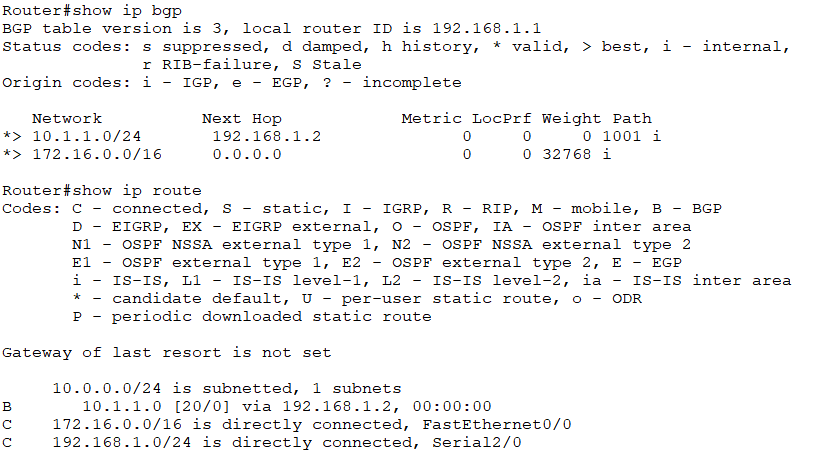
Sedangkan jika sudah selesai mengkonfigurasikan router satunya lagi yaitu router 1, maka hasilnya adalah



Setelah selesai keduanya dikonfigurasikan maka show ip bgp akan muncul prefix seperti itu, hal ini dikarenakan sebelumnya saat gambar awal sebelum router 1 dikonfigurasi maka protocol BGP masihb belum menemukan neighbor BGP atau peer yang aktif untuk saling terkoneksi, karena router 1 belum mengkonfigurasikan protocol BGPnya, jadi dua router tersebut akan saling terkoneksi jika benar-benar kedua nya bisa peering atau membentuk neighborship dengan menghubungkan Autonomous Snychonus mereka Dimana Router 0 adalah 1001 dan router 1 adalah 1002. Akhirnya saat keduanya suadh terkonfigurasi maka network 172.16.0.0 bisa berkoneksi dengan network 10.1.1.0 dengan hop atau perantara melewati IP router 1 yaitu 192.168.1.1 dengan AS nya adalah 1002.

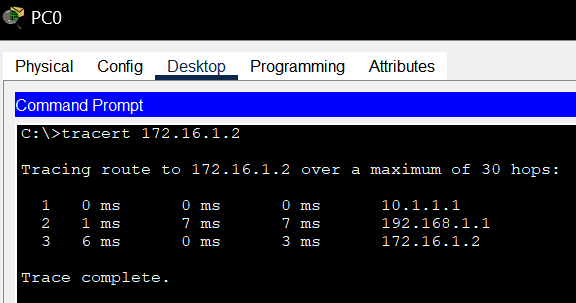
Lalu jika keduanya sudah di konfigurasikan dengan baik, jika menjalakan perintah #show Ip route, hasilnya adalah

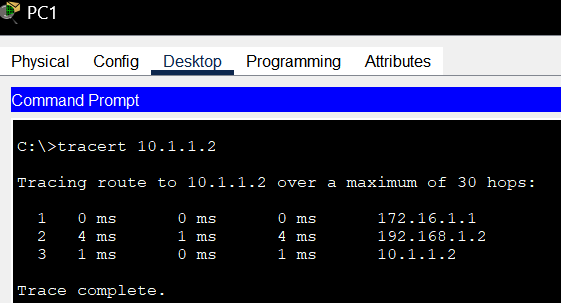




Dari table oertama router 0 hasilnya adalah C atau Connected di network 10.1.1.0 dan juga dengan network 192.168.1.0 yang digunakan untuk komunikasi antar routernya, lalu B atau BGP dengan network end device dari router 1 yaitu 172.16.0.0. hal ini juga berlaku ke Router 1 yang terkoneksi dengan network nya sendiri untuk dan device nya yaitu 172.16.0.0 dan network komunikasi routernya 192.168.1.0, lalu terkoneksi BGP Degnan network di router 1 yaitu 10.1.1.0 melalui IP router 192.168.1.2 atau router 0.

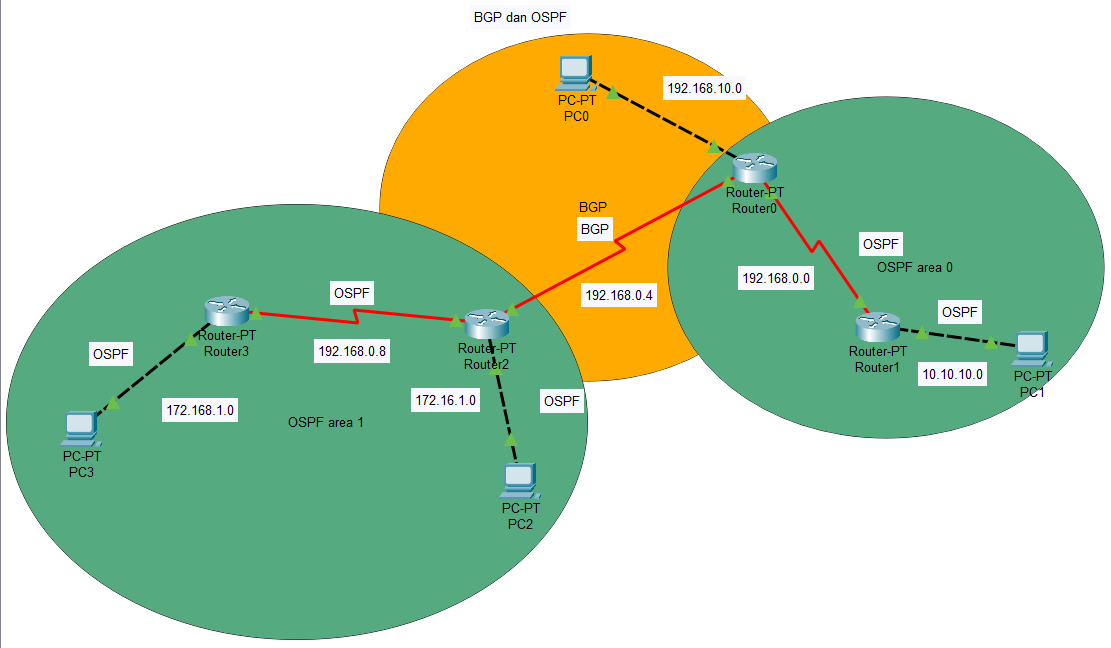
Lalu jika kedua router sudah terkoneksi, maka jika menggunakan tracert dari PC 0 ke PC 1 atau sebaliknya. maka akan tampil hal ini





Dari PC0 packet akan melewati diawalnya ayitu default gateaway router 0 nya dahulu lalu menuju default gateaway dari PC1 nya yaitu router 1, barulah dari gateawaynya masuk ke end device PC 1 nya. Hal itu juga sama seperti alur PC 1 ke PC 0 nya.

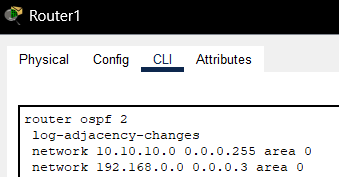
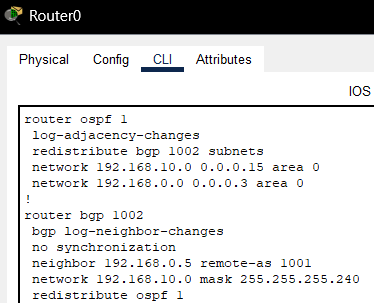
Lalu percobaan kedua akan membentuk topologi sebagai berikut:

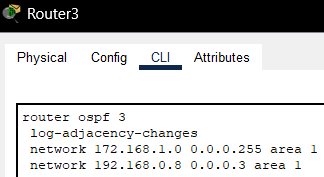
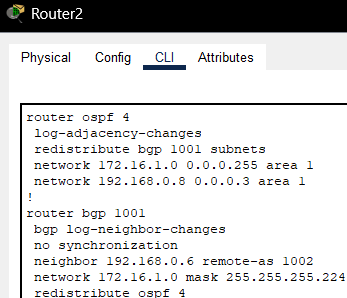


Pada percobaan yang terkahir ini adalah merancang topologi jaringan yang mana diintegrasikan dynamic routing IGP seperti OSPF atau RIP dengan BGP, tetapi disini digunakan routing OSPF saja sebagai IGP nya. Hal ini merupakan Gambaran simulasi Dimana IGP sebagai routing yang berada dalam satu Autonomous System yang mana bisa jadi koneksi IGP ini adalah koneksi antar router yang masih terpaut di satu Perusahaan atau di satu provider internet, lalu BGP sebagai egp akan menghubungkan jaringan satu Perusahaan atau satu provider ke provider atau ke Perusahaan lainnya.

Disitu terdapat dua area OSPF yaitu dikanan adalah termasuk area 0 yang mana termasuk di bagian network router 0 dan router 1, lalu OSPF dikiri adalah area 1 yang mana termasuk di bagian network router 2 dan router 3. Barulah router 2 sebagai perwakilan atau ujung dari OSPF area 1 dan router 0 sebagai perwakilan dari OSPF area 0 ingin area keseluruhannya bisa berkomunikasi yang mana kedua router tersebut di routing menggunakan metode egp Border Gateaway Protocol.

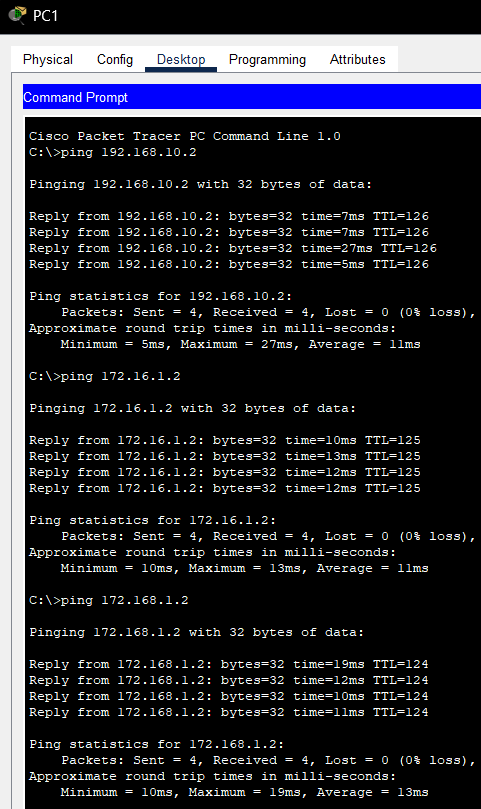
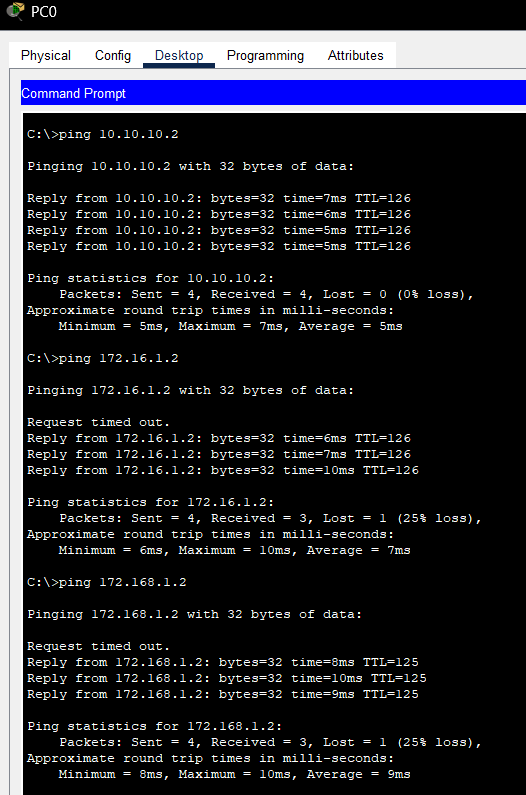
Pertama-tama seluruh router akan dikonfigurasikan OSPF dan BGP nya sesuai dengan pembagian areanya, bisa dilihat datanya seperti ini nantinya setelah dikonfigurasi semua

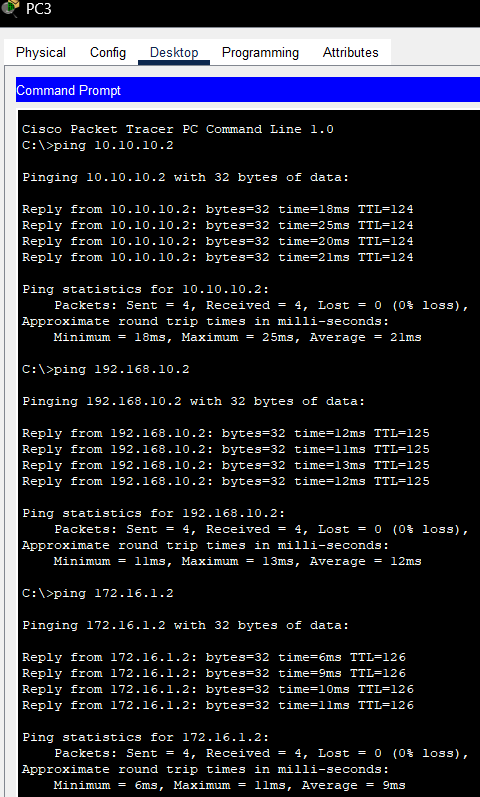
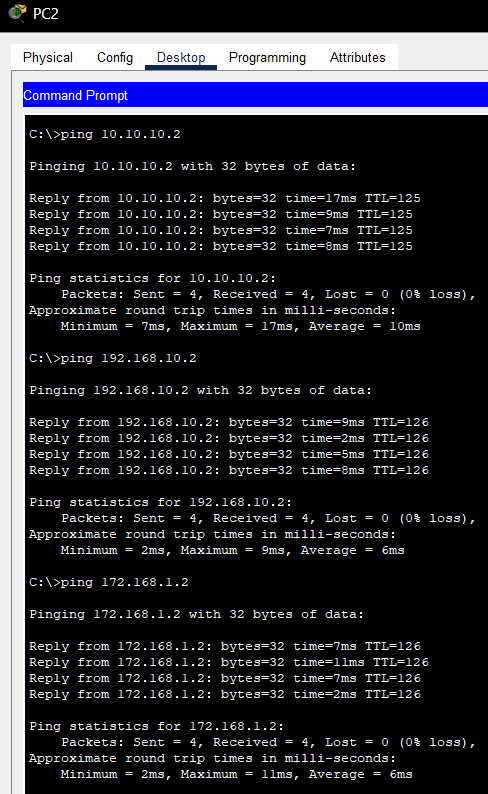




Nah setelah keempat router ini dikonfigurasikan routeran OSPF dan BGP nya, unutk menghubungkan antar router 2 dengan router 0 adalah dengan memasukkan perintah redistribute. Untuk router 0 menggunakan perintah redistribute bgp 1002 subnets untuk konfigurasi OSPF dan redistribute ospf 1 untuk konfigurasi BGP nya, lalu untuk router 2 menggunakan perintah redistribute bgp 1001 untuk konfigurasi OSPF nya dan redistribute ospf 4 untuk konfigurasi bgp di masing-masing router tersebut. Perintah ini akan memungkinkan rute yang dipelajari atau yang diketahui melalui BGP akan diterjemahkan dan ditujukan ke dalam domain OSPF, begitu pula OSPF ke BGPnya.

Setelah terkoneksi perintah redistribute nyam aka bisa dicoba untuk saling ping dari satu PC ke PC yang lainnya:





Bisa dilihat bahwasannya semua PC sudah terdaftar dan sudah terkonkesi walaupun memiliki kelompok network OSPF yang berbeda yang mana nanti dihubungkan dengan BGP routing.

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. Jelaskan apa yang anda ketahui tentang Border Gateaway Protocol (BGP)

Jawab:

Border Gateway Protocol (BGP) merupakan protokol routing yang penting dalam infrastruktur internet, yang berfungsi untuk pertukaran informasi jalur dan keterjangkauan antar Autonomous System (AS). Dalam konteks jaringan global, internet tersusun atas berbagai AS yang dikelola oleh entitas yang berbeda. BGP berperan sebagai mekanisme komunikasi utama yang memungkinkan router-router di setiap AS untuk mengiklankan jaringan mereka dan mempelajari jalur terbaik menuju jaringan di AS lain. Dengan demikian, BGP memfasilitasi pengiriman data yang efisien dan handal melintasi batas batas administratif jaringan yang beragam.

2. Jelaskan apa yang dimaksud peers pada mekanisme routing BGP

Jawab:

Dalam mekanisme routing BGP, istilah peers merujuk pada router-router BGP yang telah membentuk sesi komunikasi TCP untuk saling bertukar informasi routing. Pembentukan peering terjadi melalui konfigurasi manual di mana setiap router BGP secara eksplisit mendefinisikan alamat IP dan nomor AS dari tetangganya. Setelah sesi TCP terbentuk, router-router ini akan mengirimkan pesan-pesan BGP, seperti Open, Update, Keepalive, Notification, dan Route-Refresh, untuk membangun dan mempertahankan hubungan peering serta menyebarkan informasi tentang jaringan yang dapat dijangkau. Pada praktikum ini, Router 0 dan Router 1 (atau Router 0 dan Router 2 pada topologi kedua) yang dikonfigurasi dengan perintah neighbor dapat dianggap sebagai peers.

1. Jelaskan tabel routing dari 2 topologi yang anda buat pada praktikum kali ini.

Jawab:

BGP itu singkatan dari Border Gateway Protocol, yaitu protokol routing yang digunakan untuk bertukar informasi rute antar router, terutama ketika jaringan yang terhubung itu besar atau beda organisasi. Secara konsepnya BGP ini punya dua jenis hubungan utama: iBGP (internal BGP) dan eBGP (external BGP).

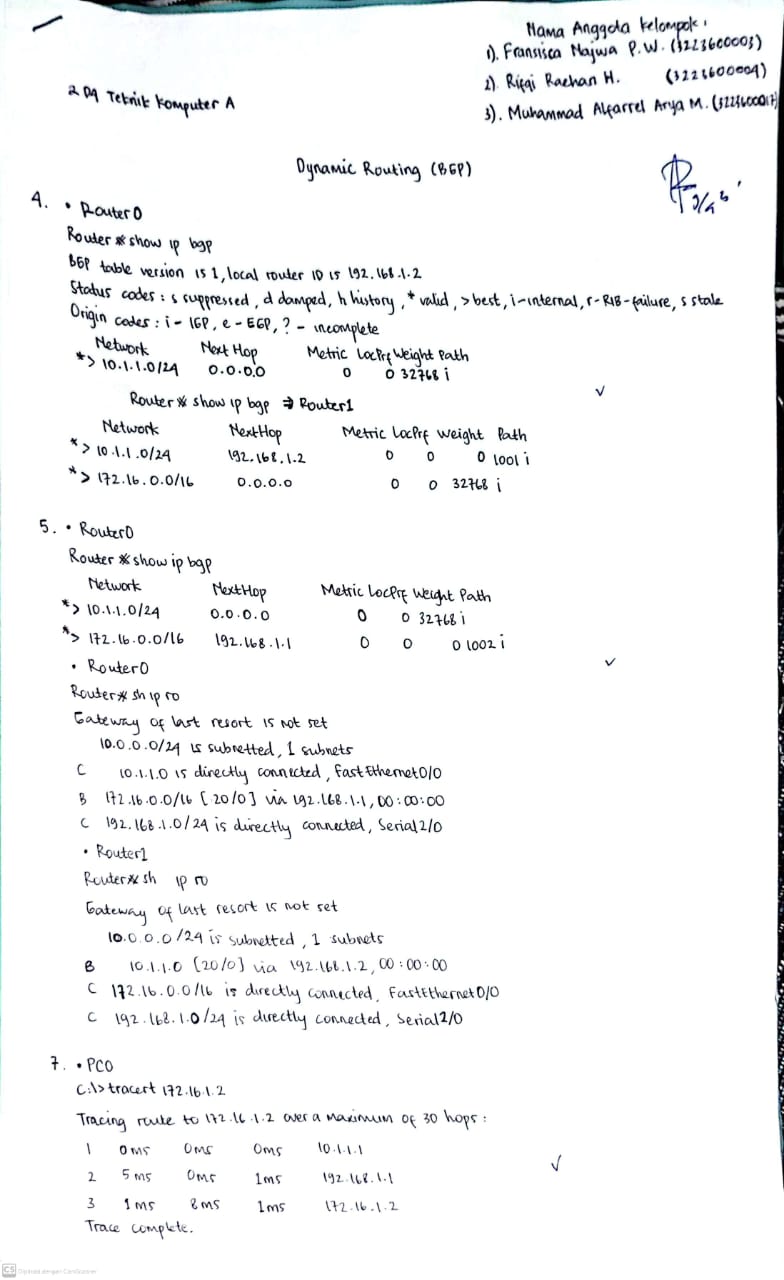
iBGP digunakan antar router yang masih dalam satu Autonomous System (AS). Jadi, meskipun router-router itu beda lokasi atau subnet, tapi kalau mereka masih pakai AS number yang sama, maka hubungan BGP-nya disebut iBGP. Biasanya ini terjadi di dalam satu perusahaan besar, ISP, atau organisasi yang punya banyak router. iBGP itu punya aturan penting, salah satunya yaitu rute yang didapat dari satu iBGP peer tidak boleh diteruskan ke iBGP peer lainnya, karena takut terjadi loop. Makanya, di iBGP biasanya harus ada full-mesh connection, atau pakai route reflector agar lebih efisien.

Sementara eBGP digunakan antar router yang berbeda AS atau beda organisasi atau beda penyedia jaringan. Contohnya seperti ISP A yang terhubung ke ISP B, atau perusahaan yang terkoneksi ke internet lewat dua provider berbeda. Dalam eBGP, informasi rute yang diterima bisa diteruskan ke router eBGP lainnya tanpa aturan seketat iBGP.

1. Jelaskan proses establishment untuk peering session pada protokol BGP

Jawab:

Proses pembentukan peering session pada protokol BGP melibatkan serangkaian langkah yang dimulai dengan inisiasi koneksi TCP antara dua router BGP pada port 179. Router yang memulai koneksi (biasanya yang dikonfigurasi dengan alamat IP tetangga yang lebih rendah) akan mengirimkan pesan Open yang berisi informasi tentang nomor AS lokal, BGP identifier (biasanya Router ID), dan parameter negosiasi lainnya seperti hold time. Router tetangga yang menerima pesan Open akan memeriksa parameter-parameter tersebut dan, jika dapat diterima, akan membalas dengan pesan Open miliknya. Setelah kedua router saling bertukar pesan Open yang valid, sesi BGP akan memasuki status Established, dan kedua peers mulai bertukar pesan Update yang berisi informasi tentang rute-rute yang dapat dijangkau. Pesan Keepalive kemudian dikirim secara periodik untuk memastikan bahwa sesi peering tetap aktif. Jika terjadi kesalahan, pesan Notification akan dikirim untuk mengakhiri sesi.

1. Lampiran Laporan Sementara

