|  |
| --- |
| *Create by :Riyan Syahrul Fadillah*SMK Plus Pelita Nusantara |



Racikan network engineer

**Daftar isi**

Kata pengantar..............................................................................................................3

Profile penulis................................................................................................................4

1.1 Network fundamental................................................................................6

1.2 jaringan dasar......................................................................................................7

1.3 network device.....................................................................................................8

1.4 UTP kabel..............................................................................................................10

1.5 the network as a platform...............................................................................11

1.6 ip address.............................................................................................................12

1.7 osi layer................................................................................................................17

1.8 configurasi dasar................................................................................................20

1.9 telnet dan ssh.....................................................................................................21

2.1 switching

2.2 vlan........................................................................................................................23

2.3 SVI........................................................................................................................25

2.4 trunk vlan.............................................................................................................28

2.5 trunk allowed.......................................................................................................30

2.6 trunk MLS............................................................................................................31

2.7 spanning tree protocol......................................................................................36

2.8 spanning tree port-past....................................................................................37

2.9 VTP.........................................................................................................................37

2.10 intervlan..............................................................................................................40

2.11 DHCP.....................................................................................................................42

2.12 switchport security...........................................................................................48

2.13 DTP........................................................................................................................49

2.14 etherchannel.......................................................................................................50

3.1 routing

3.2 static route...........................................................................................................53

3.3 dynamic routing....................................................................................................56

3.4 RIPv1.......................................................................................................................58

3.5 RIPv2.......................................................................................................................62

3.6 EIGRP......................................................................................................................63

3.7 OSPF........................................................................................................................67

3.8 eBGP.........................................................................................................................72

3.9 access-list(ACL)....................................................................................................76

3.10 NAT........................................................................................................................86’

3.11 tunnel GRE.............................................................................................................93

3.12 PPP(point-to-point)..............................................................................................97

3.13 high avaibility.......................................................................................................98

3.14 DHCP relay............................................................................................................103

3.15 NTP.........................................................................................................................108

**Kata pengantar.**

Alhamdulillah,saya panjatkan puji syukur kepada Allah S.W.T yang telah memberikan rahmat dan hidayahnya dan juga ridha nya,sehingga saya dapat menyelesaikan buku ini sampai selesai.dan juga saya berterima kasih kepada **orangtua** saya yang sudah memberikan ridhanya untuk belajar dan juga yang sudah mendidik saya,dan juga saya berterima kasih sebanyak-banyak nya untuk **mr.reynaldi** **mulyatama** yang sudah mengajari saya ilmu yang sangat banyak dan bermanfaat dan juga sekaligus mendidik saya,dan untuk teman-teman terima kasih yang sudah membantu saya menyelesaikan buku ini.

**Profile penulis**

Nama :Riyan Syahrul Fadillah

Pendidikan :SMK Pelita Nusantara

Email :ryansyahrul16@gmail.com

Instagram :ryan\_syahrul27

**1.1NETWORK FUNDAMENTAL**

GLOBAL CONNECTION

* explain how network affect the waywe interact learn,work&play

A.NETWORK OF MANY SIZE

* LAN:local area network(rumah,gedung)
* WAN:wide area network(antar negara)
* MAN:metropolitan area network(antar kota)

B.CLIENT AND SERVER

* client request and display information
* server provider information to other device on the network

C.PEER TO PEER

Apa itu peer to peer?adalah menghubungkan data dari leptop ke laptop

D.end devices

Apa itu end devices?adalah suatu perangkat yang tidak terhubung dengan komponen network

CONTOH :

* Laptop
* Printer
* Monitor

**1.2DASAR JARINGAN**

A. Jaringan merupakan sekumpulan perangkat jaringan(network device)yang saling terhubung dengan perangkat edhost(end device)yang bertujuan agar seluruh perangkat dapat bertukar informasi satu sama lain.

* LAN: merupakan skala jaringan yang sederhana yang biasa di pakai di rumah&gedung
* terkonek end device
* administrasinya oleh satu organisasi
* memberi bandwith dengan kecepatan tinggi untuk internal devices
* WAN: terkoneksi dengan LAN di administrasikan oleh beberapa serivceprovider yang memberikan kecepatan antar LAN
* MAN: merupakan skala jaringan yang lebih besar dari pada LAN yang dapat dikatakan sebagai kumpulan LAN dalam satu wilayah atau satu area yang merupakan antar gedung.

INTERNET

Apa itu internet?berasal dari kata inter connection networking.adalah hubungan berbagai komputer dengan berbagai sistem yang mencangkup seluruh dunia

INTRANET

apa itu intranet?adalah sama dengan internet tetapi jangkauan nya terbatas

EXTRANET

apa itu extranet?adalah jaringan pribadi yang menggunakan protokol internet dan sistem telekomunikasi publik untuk membagi sebagian informasi bisnis/operasi secara aman kepada penyalur suplier.

AKSES TOPOLOGI INTERNET

* ISP
* broadband cable
* broadband digital sucriber line (DSL)
* wireless WANS
* mobile service
* bussiness DSL
* metro ethernet

**1.3NETWORK DEVICE**

Untuk jaringan terdapat beberapa device yang harus kita ketahui yang biasa kita gunakan untuk membuat suatu jaringan seperti :router,switch,hub,mls(multi layer switch)

**ROUTER**

Router adalah suatu alat device yang berguna untuk menghubungkan suatu jaringan yang berbeda,dengan mendistribusikan IP address.



**SWITCH**

Perangkat ini digunakan untuk menghubungkan antar network,yang mana ia akan mengirim paket data melalui mac address,SWITCH terbagi menjadi 2 bagian yaitu:manage,dan unmanage.

**MLS(multi layer switch)**

Perangkat ini juga sering digunakan dalam jaringan yang mana perangkat ini sama seperti switch tetapi perangkat ini juga dapat difungsikan sebagai router,yang mana perangkat ini bekerja di layer 2&3.



**1.4KABEL UTP**

Kabel LAN/UTP konektornya adalah RJ45.dan biasanya telepon rumah memakai dengan konektor adalah RJ11

**A. BERIKUT URUTAN KABEL**

Urutan kabel di bagi menjadi 2 :

* STRAIGHT
* CROSS

**B.STRAIGHT**

(P-0),(O),(P-H),(B),(P-B),(H),(P-C),(C)

Apa bila sudah di pasang silahkan di cek dengan alatnya dengan urutan:

(1-1),(2-2),(3-3),(4-4),(5-5),(6-6),(7-7),(8-8)

**C.CROSS**

(P-H),(H),(P-O),(B),(P-B),(O),(P-C),(C)

Dengan urutan kabel:

(1-3),(2-6),(3-1),(4-4),(5-5),(6-2),(7-7),(8-8)

**KET:**

(PO) :PUTIH COKLAT

(O) :ORANGE

(HP) :HIJAU PUTIH

(BP) :BIRU PUTIH

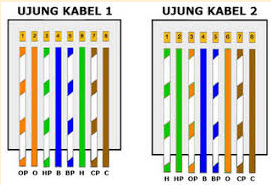
(H) :HIJAU

(CP) :COKLAT PUTIH

(C) :COKLAT

BERIKUT GAMBAR STRAIGHT&CROSS

**STRAIGHT CROSS**



**1.5 THE NETWORK AS A PLATFORM**

Setiap network memiliki peraturan tersendiri.

1. DASAR CARACHTERISTIK ARSITEKTUR JARINGAN

* toleransi kesalahan
* skabilitasi
* quality of service (qos)/kualitas layanan
* keamanan

B.NETWORK TRENDS

* BYOD (bring your own device)
* kolaborasi online
* vidcall (video communications)
* cloud computing

**C.NETWORK SECURITY**

* ancaman security (viruses,worms,and trojan horses)
* spyware and adware
* zero-day attack,also called zero hour attacks
* hacker attacks
* data interception and tueft
* indentity tueft
* **D.SOLUSI KEAMANAN**
* anti firus&anti spyware
* firewall filtering
* redicated firewall system
* acces control list (ACL)
* intrusion prevention system (IPS)
* virtual private networksc (VPNS)

**1.6 IP ADDRESS**

IP(internet protokol).adalah sebuah alamat komputer yang digunakan untuk berkomunikasi antar perangkat.contoh adalah smartphone,laptop,komputer,Dll.fungsi dari IP adalah sebagai pengalamat,komunikasi&indentitas.

IP dibagi menjadi dua : IPV4 dan IPV6. IPV4 adalah singkatan dari internet protocol versi 4. kalau IPV6 adalah internet protocol versi 6.

IP dibagi dua jenis yaitu IP publik,IP private. Apa itu IP publik?adalah suatu IP yang bisa didapat kan dari ISP(internet service provider).kalau IP private adalah suatu IP yang dapat kita buat sendiri,tetapi kita tidak bisa akses internet.

1. **SUBNETTING**

Nah sekarang kita masuk kedalam pembahasan subnetting.subnetting adalah teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan bit Host ID pada subnet mask untuk dijadikan Network ID baru. Subnetting merupakan teknik memecah network menjadi beberapa subnetwork yang lebih kecil. Subnetting hanya dapat dilakukan pada IP addres kelas A, IP Address kelas B dan IP Address kelas C. Dengan subnetting akan menciptakan beberapa network tambahan, tetapi mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.dibawah ini adalah pembagian dari kelas IP

Nah sekarang kita masuk kedalam penghitungan subnetting,bagaimana sih cara menghitung IP,berikut pembahasan nya.

Sebelum kita mulai apa itu network ID dan host ID.network ID adalah indentitas dari suatu IP address untuk menunjukan jaringan suatu IP.dan juga apa itu host ID?adalah ID yang digunakan oleh client.

Prefiks adalah untuk menentukan nilai IP yang dapat terkoneksi atau terhubung atau yang dapat di gunakan

* **kelas A** =/8 - /15
* **kelas B** =/16 - /23
* **kelas C** =/24 - /32

**KET** : apa yang dimaksud tanda (/)itu adalah tanda slas

**IP RANGE (jangkauan IP)**

* **kelas A** =1 - 126
* **kelas B** =128 - 191
* **kelas C** =192 - 223

Dalam IPV4 dia mempunyai 4 octet.apa itu octet?adalah tanda titik yang ada didalam IP contoh :192.168.10.1 seperti contoh disamping kita bisa lihat setiap setelah angka terdapat octet. 1 octet nilainnya adalah 8 BIT,jadi kalau empat adalah 32 BIT.

Dan juga dalam subnetting kita harus menentukan mana itu network ID dan host ID.setiap kelas berbeda network ID dan host ID nya.bagaimana cara menentukannya,seperti contoh dibawah ini.

* **kelas A**: network ID : 128.1.1.1 angka pertama seperti 128 itu

Adalah network ID dari kelas A,dan bernilai 8 BIT

: host ID :128.1.1.1 angka 1 dalam contoh tersebut adalah

Host ID,dan bernilai 24 BIT

* **kelas B** : network ID : 128.1.1.1 angka 1 setelah 128 dalam kelas Adalah network ID dari kelas B,dan bernilai 16 BIT

: host ID : 128.1.1.1 dua buah angka 1 dari belakang dalam

Dalam kelas B,itu adalah host nya.

* **kelas C**

|  |  |  |
| --- | --- | --- |
| total IP |  | Subnet mask |
| 256 | /24 | 255.255.255.0 |
| 128 | /25 | 255.255.255.128 |
| 64 | /26 | 255.255.255.192 |
| 32 | /27 | 255.255.255.224 |
| 16 | /28 | 255.255.255.240 |
| 8 | /29 | 255.255.255.248 |
| 4 | /30 | 255.255.255.252 |
| 2 | /31 | 255.255.255.254 |

bagaimana cara menghitung subnetmask?adalah total IP terbesar di bagi total IP tersebut contoh: kita pakai /24 maka cara menghitungnya adalah 256:256=0 (total ip terbesar adalah 256,dan total ip kita adalah 256.maka subnetmask nya adalah 255.255.255.0 seperti contoh di atas.

OKE...sekarang kita masuk kedalam rumus dan penghitungan IP.pertama kita mulai dari kelas C dulu lalu seterusnnya.

**CONTOH** :

**192.168.10.33/30** (/30 kelas C)

- Total IP : 4

- Subnet mask :255.255.255.252

- Network ID: host ID:total IP=lalu hasilnya dikali total IP.contoh:

33:4=8,2\*4=32 (192.168.10..32)

- Broadcast : network ID+total IP - 1 =32+4-1=35 (192.168.10.35)

- host ID :(network ID +1)-(broadcast-1)

(192.168.10.33)-(192.168.10.34)

**KET :**

- cara mencari network ID adalah total IP kita di bagi dengan host ID.lalu kalau sudah kita jumlahkan kita ganti host ID dari soal seperti 192.168.10.33 menjadi (192.168.10.32)seperti contoh di atas.

- bagaimana cara mencari broadcast?adalah hasil dari penjumlahan network ID ditambah total IP lalu dikurang 1.kalau sudah kita jumlahkan,seperti cara network ID,kita ganti dari (192.168.10.30)menjadi(192.168.10.35)

- cara mencari host ID.maksud soal di atas adalah kita masukan hasil network ID dan broadcast namu yang network ID harus di tambah 1,dan broadcast harus dikurang 1.

**KELAS B**

CONTOH:128.191.255.17/20

Total IP: 20+8=/28=16\*256=4086

Subnetmask: 255.255.240.0

Network ID :255:16=15,9=15\*16=240 (128.191.240.0)

Broadcast : 240+16-1=255 (128.191.255.255)

Host ID :(128.191.240.1)-(128.191.255.254)

**KET :**

- total IP:slash dari kelas B harus di tambah 8 terlebih dahulu untuk menjadi kelas C.lalu setelah menjadi kelas C kita kali dengan IP terbesar (256)

- subnetmask :total IP dari prefiksnya yang di ambil subnetnya.lalu apa bila soalnya adalah kelas B maka octet terakhirnya selalu 0

- network ID: host ID soal dibagi total IP yang sudah di rubah kedalam kelas C dan octet di belakang 0.

- broadcast : penghitungan sama tetapi octet ke-4 sama dengan octet ke-3 (nilainya)

**KELAS A**

CONTOH :100.100.100.100/11

- Total IP :11+8+8=/27=32\*256\*256=2123392

- Subnetmask: 255.225.0.0

- Network ID: 100:32\*32=96 (100.96.0.0)

- broadcast : 96+32-1=127 (100.127.255.255)

- host ID:(100.96.0.1)-(100.127.255.254)

**KET :**

* penghitungan total IP sama tetapi harus di tambah 8 sebanyak 2 kali untuk menjadi kelas C
* hasil host ID =hostmin octet terakhir yang di tambah,dan hostmax octet terakhir yang di kurang.

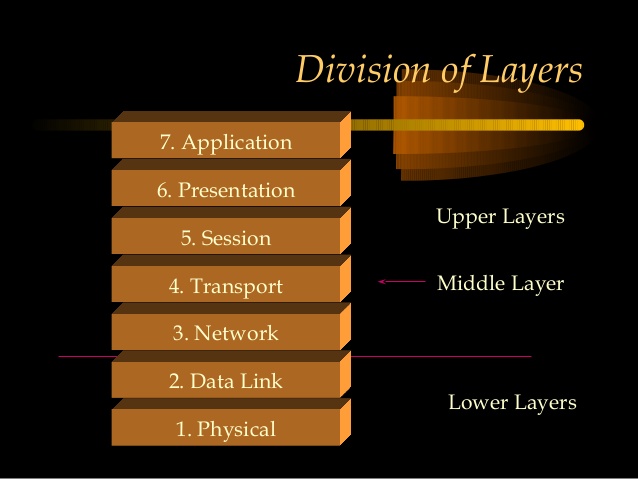
**CLASSFUL**

Apa itu classful?classful adalah pengalamatan jaringan dalam hal subnetmask (atau bisa juga dikatakan network)yang bernilai default,dalam arti tidak di subnet.classful ini adalah netmask,yang bernilai 1 dalam kelipatan 8.

**CLASSLESS**

Apa itu classless?adalah pengalamatan jaringan dalam hal subnetmask yang bernilai selain default,dalam arti telah di subnet,itu adalah kebalika dari classful.

**1.7 OSI LAYER**



OSI layer: kepanjangan dari OSI adalah operating system interconnection.yaitu sebuah model konsep atau sebuah logika.yang mendefinisikan tentang komunikasi jaringan komputer.

Model terbagi menjadi 7 lapisan,yaitu application,presentation

,session transport,network,data link,phsyical.yang dimana masing masing lapisan tersebut mewakili sebuah kumpulan konsep layanan.OSI model ini dapat mendeskripsi tentang komunikasi paket data.computer menggunakan lapisan protocol,yang berbeda dengan efektif.OSI leyer ini terbagi menjadi 2 porsi yaitu **upper layer** dan **lower layer.**

Open system interconnection atau OSI.OSI diciptakan oleh in ternational organizatio for standarization (ISO).dahulu sebelum OSI perangkat komunikasi tidak dapat saling berkomunikasi pada vendor yang berbeda.

**LAYER 7(APLICATION)**

Pada lapisan ini menjelaskan dimana aplikasi pengguna berkomunikasi.

Web browser adalah sebagai aplikasi pengguna,berkomunikasi dengan web browser sebagai layanan jaringan.selain itu pada lapisan ini menyediakan jasa untuk aplikasi pengguna dan bertanggung jawab atas pertukaran informasi antar program komputer,seperti emall.,server printer,protocol yang berada didalam lapisan ini adalah http,ftp,dns,dll

**LAYER 6(PRESENTATION)**

Pada lapisan ini untuk menerjemahkan data yang akan transmisikan oleh aplikasi yang ada di format yang dapat di transmisikan.maksudnya seperti mengkonvert sedangkan transmisi pada jaringan mempunyai yang sama pada kendaraan.transmisi pada kendaraan bergigi berfungsi meneruskan tenaga dari mesin keban dan nilainnya di ubah sesuai gigi.

**LAYER 5(SESSION)**

Pada lapisan ini bertanggung jawab sebagai membuat koneksi,memelihara,menjaga,menghancurkan koneksi.selain itu dilapisan ini juga.terjadinya resolusi nama.protocol yang berjalan pada lapisan ini adalah NETBIOS.

**LAYER 4(TRANSPORT)**

Pada lapisan ini bertugas memecah data kedalam paket data serta memberi nomor urut.ke paket-paket tersebut hingga dapat disusun kembali pada sisi tujuan setelah diterima.selain itu pada lapisan ini juga membuat sebuah tanda bahwa paket diterima dengan sukses.dan mentransmisikan ulang terhadap paket yang hilang di tengan jalan.

Maksud dari memecah data kedalam paket data serta memberi nomor urut?sama ibaratnya kita ingin mengirimkan monitor.

**LAYER 3(NETWORK)**

Pada lapisan ini mendefinisikan alamat-alamt IP,membuat header pada paket dan kemudian melakukan routing melalui internetwork dengan menggunakan router dan switch layer 3.dilapisan ini paket yang sudah dikemas.dilapisan transport diberi alamat dan header,protocol yang berjalan pada lapisan ini adalah.

* IP
* ICMP
* RIP
* EIGRP
* OSPF
* ISIS,Dll

**LAYER 2(DATA LINK)**

Di lapisan ini berfungsi untuk menentukan BIT-BIT dikelompokan menjadi format disebut sebagai ‘’frame’’disini juga bertanggung jawab,koneksi jaringan flow control.protocol yang berjalan pada lapisan ini adalah=PPP,PPTD,VLAN,TOKEN RING.

**LAYER 1**

Disini berkeuntungan dengan data mentah dalam bentuk sinyal listrik.

**APA ITU CISCO IOS ?**

Cisco IOS merupakan singkatan dari internetworking operating system.adalah system operasi yang digunakan oleh router&switch cisco nah untuk switch dulu system operasinya bernama CAT OS(cataliyst OS)IOS ini memiliki sifat proprietary.IOS adalah sebuah paket software dari kumpulan-kumpulan seperti: routing,switching,internetworking telekomunication,security dan masih banyak beberapa yang lainnya yang dijadikan sebagai feature di router dan switch.

Berikut beberapa command mode pada IOS :

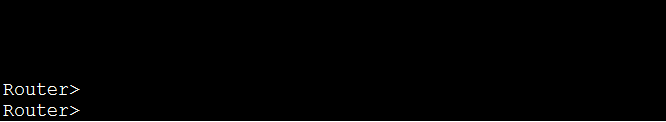
* User exec mode
* Privileged exec mode
* Global configuration mode
* ROM monitor mode
* Setup mode
* Dan lebih dari 100 commands mode dan sub mode yang ada di IOS.

Inti dari fungsi cisco IOS adalah memungkinkan komunikasi data antar jaringan.

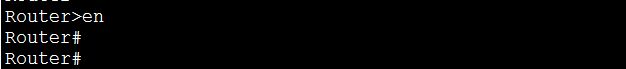
**1.8CONFIGURASI DASAR**

nah sekarang kita masuk dalam configurasi dasar.disini kita akan belajar bagaimana cara mengconfig/menseting router maupun switch.

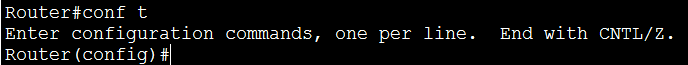
* **User mode & privilege mode**



Ketika tanda ‘’>’’ ini adalah posisi user mode



Ketika tanda ‘’#’’ kita dalam posisi privilege mode dengan cara kita ketik (enable/en).



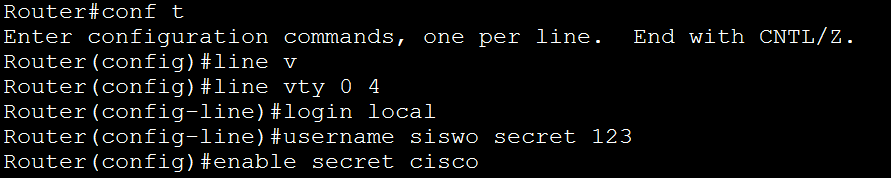
Ketika muncul ‘router(config)#’ini pada posisi global config mode.dari global config mode,jika ingin kembali ke privilege mode,kita tinggal menekan ‘’ctrl+z’’atau end.

* **Perintah show**

Perintah ‘’show run’’ ini digunakan untuk melakukan vertifikasi.atau untuk melihat yang sudah kita configurasikan.ini kita lakukan di mode privilege mode.

**1.9TELNET DAN SSH**

Selain menggunakan kabel console,untuk mengakses router bisa juga memakai telnet.kita bisa meremote router kita menggunakan protocol telnet/SSH.metode ini menggunakan ip address.untuk menggunakan telnet,yang akan kita configurasi adalah line vty.

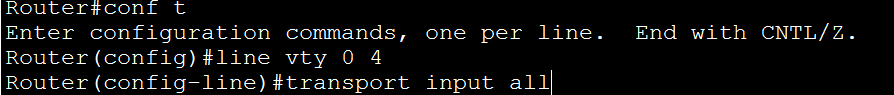


Yang dimaksud 0 4 adalah perangkat hanya bisa diremote oleh 4 oraang secara bersamaan.’’login local’’ berarti saat seseorang akan melakukan remote,maka dia harus menggunakan username dan password yang ada di router.untuk penggunaan secara bersamaan bisa berapa saja,tergantung administratornya.

Kalau hanya mengkonfigurasi seperti di atas,maka hanya protocol telnet saja yang dapat digunakan.agar SSH bisa dipakai,tambahkan command berikut.

ssh

Namun dengan command tersebut,justru telnet tidak bisa lewat,agar keduanya bisa lewat kita gunakan command berikut.

****

Untuk meremote syaratnya router/switch harus memiliki ip address yang reachable dari host.

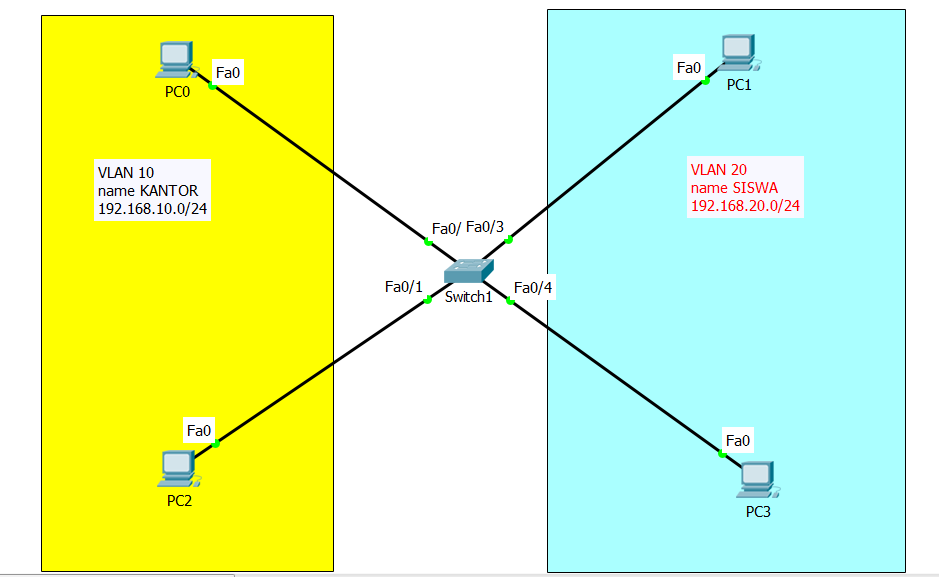
**2.1Switching**

* Enable SSH dan TELNET
* VLAN (virtual lan)
* TRUNK
* STP(spaning tree protocol)
* VTP(vlan trunking protocol)
* DTP(dynamic trunking protocol)
* interVLAN
* DHCP
* Switchport security
* Etherchannel

**2.2VLAN (virtual lan)**

Vlan yang mana dia akan difungsikan untuk membagi lingkup jaringanyang mana ia akan membaginya pada switch beberapa network.VLAN juga bisa digunakan dalam hal trobleshooting apa bila terjadi kesalahan jaringan karna networknya sudah di bagi oleh VLAN.

Untuk VLAN hanya bisa digunakan oleh switch manage,yang mana switch tersebut dapat kita konfigurasikan.

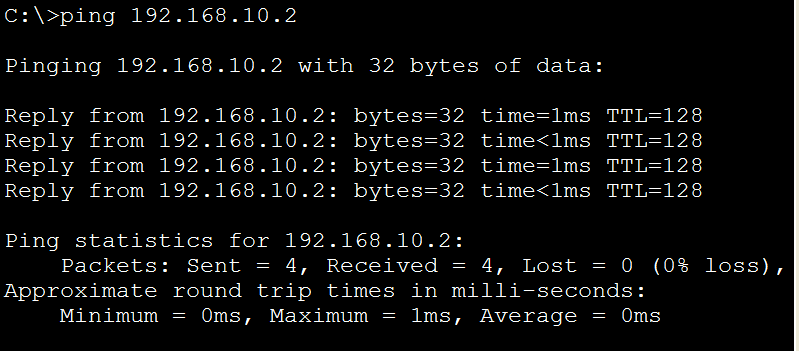


seperti topologi di atas yang mana terdapat dua VLAN yaitu VLAN10&VLAN20.danj juga setiap VLAN terdapat dua pc.dan setiap VLAN terdapat ip address,berikut cara konfigurasi VLAN.

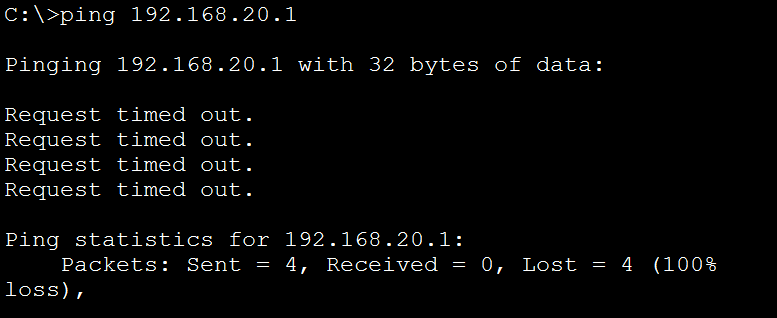
**CREAT VLAN**

Yah seperti contoh diatas,pertama kita harus membuat vlan nya dan lalu kita harus mentaging vlan di interface seperti contoh diatas.

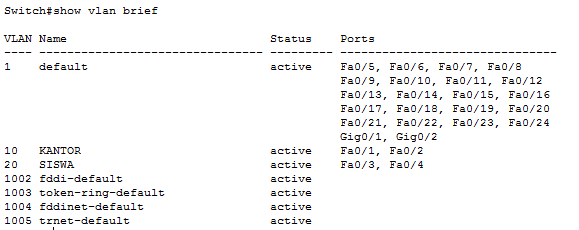
Untuk mengecek vlan mari kita ping pc satu vlan terlebih dahulu.



tapi kita masih belum bisa ping ke vlan sebelah atau vlan 20.seperti contoh.



Setelah kita membuat vlan dan mentaing vlan di masing masing interface kita bisa gunakan ‘’show vlan brief’’.

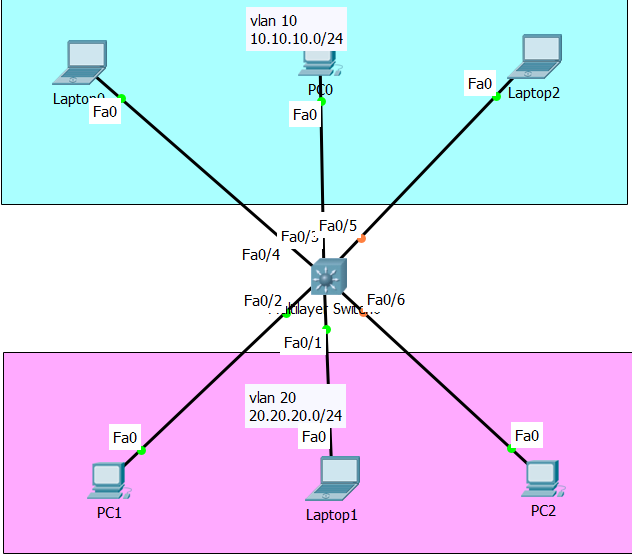


Yah bisa kita lihat,disitu terdapat vlan 10&20 yang sudah kita buat dan yang sudah kita taging vlannya.

**2.3SVI(switch virtual interface)**

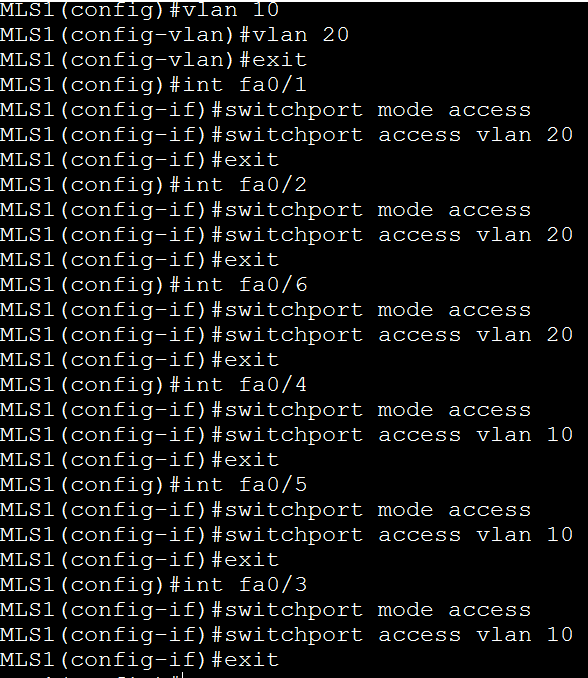
SVI(switch virtual interface)merupakan mekanisme sejenis interVLAN routing tetapi kita dapat mengkonfigurasi IP addrees pada vlan untuk menjadi gateway pada client,agar vlan tersebut saling terhubung.

Untuk pembahasan kali ini kita memakai MLS(multi layer switch)yang mana perangkat ini bekerja di dual layer.dan yang bisa mengkonfiguras SVI ini hanya MLS.



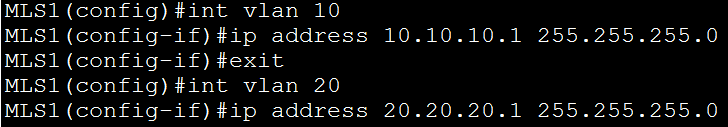
Langkah pertama yang harus kita lakukan adalah membuat vlan terlebih dahulu dengan mengikuti topology diatas.

**Konfigurasi VLAN :**



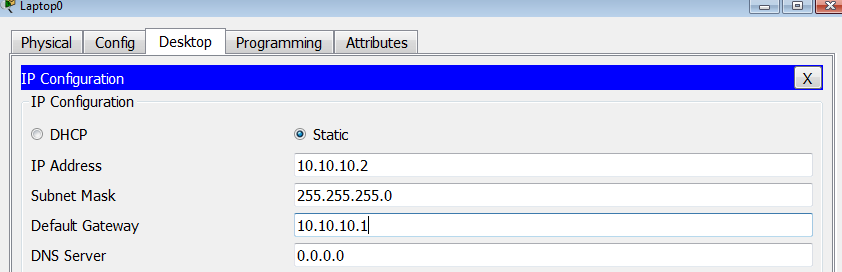
Kita sudah melakukan membuat vlan dan masukan vlan ke interface masing-masing,tetapi client hanya bisa ping ke 1 vlan atau masih satu network.agar client dapat terhubung dengan vlan yang berbeda atau berbeda network,kita akan mengkonfigurasi SVI dengan menambahkan IP address.

**IP address pada VLAN :**

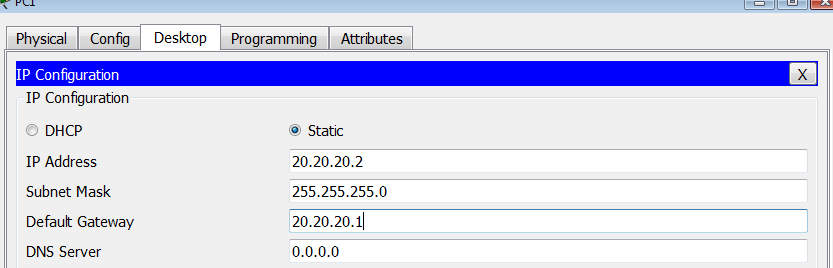


Setelah kalian sudah masukan IP addree ke VLAN,kalian coba memberikan IP address dan gateway di masing-masing pc dengan vlan yang sesuai.

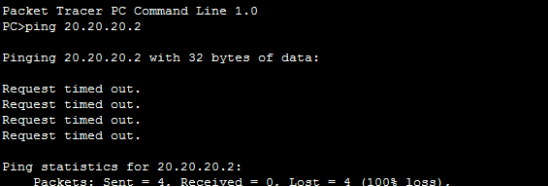
**Client VLAN 10**



**Client VLAN 20**



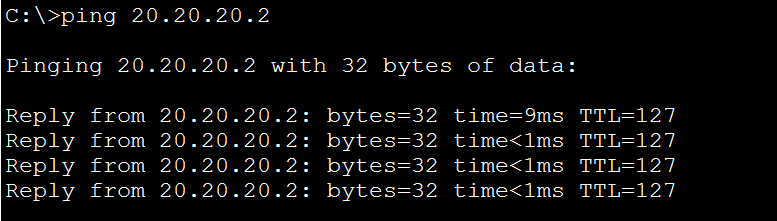
Sekarang kita sudah memasukan IP kepada client di vlan 10 dan vlan 20,sekarang kita test ping dari vlan 10 ke vlan 20 :



Kita bisa lihat hasilnya adalah RTO kenapa tidak bisa ping,karna kita belum mengaktifkan fungsi routing di MLS,maka dari itu kita dapat konfigurasikan *IP ROUTING.*

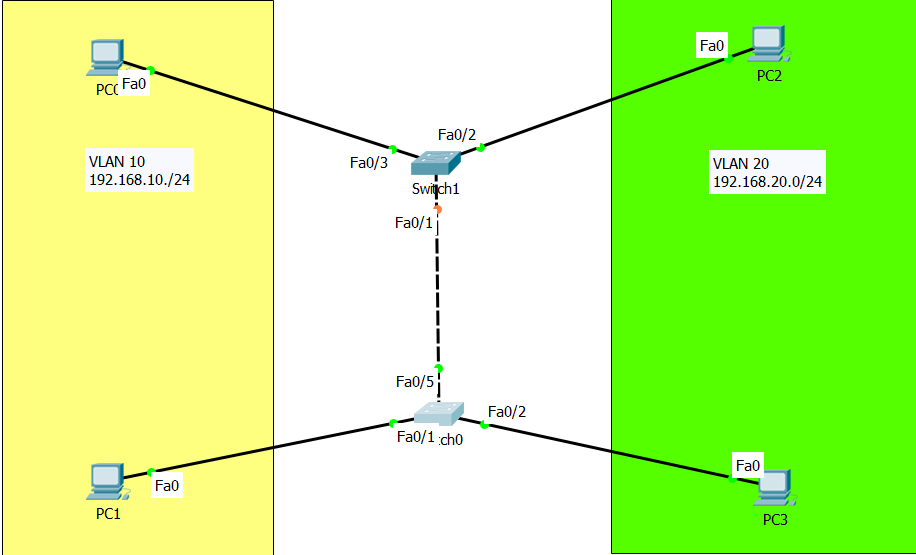


Kita bsudah melakukan *ip routing,*sekarang mari kita lihat apakah vlan 10 dapat ping ke vlan 20.



**2.4TRUNKING VLAN.**

Trunk berfungsi untuk menjembatani vlan.sehingga pada link tersebut bisa dilewati banyak vlan,atau bisa disebut untuk menjembatani/melewati traffic beberapa vlan dari switch ke switch atau ke router lain,beriku langkah langkah konfigurasi.



1.buat vlan di SW1,SW2





2.taging vlan ke interface masing masing.

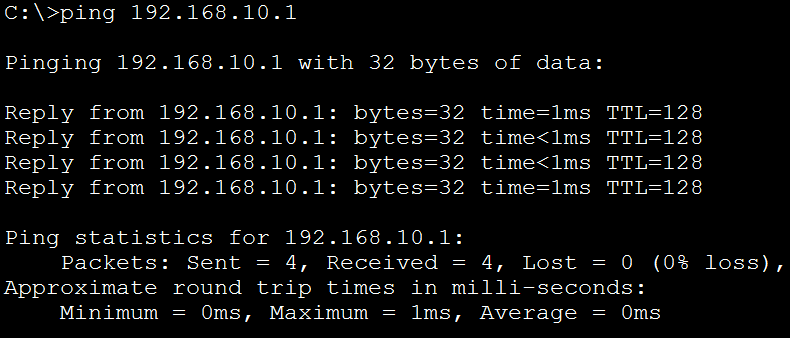




3.konfigurasi trunk di port sw1,sw2

Untuk melihat konfigurasi trunk ‘’show interface trunk brief’’.

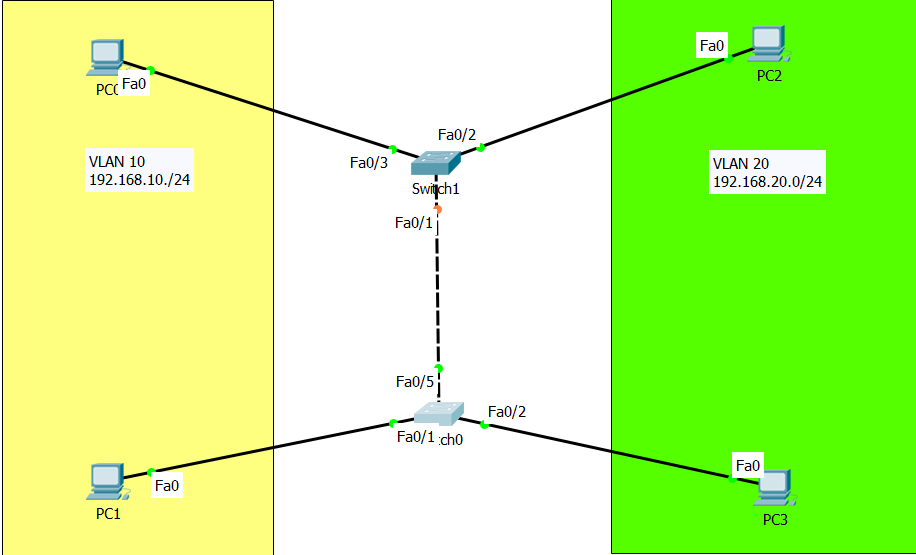
Untuk membuktikan kalau trunk sudah diaktifkan,tes ping dari PC0 ke PC1 sama vlan tetapi beda sitch.



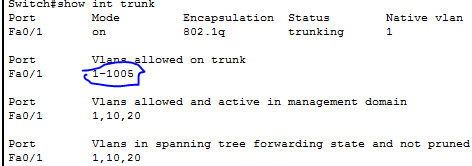
**2.5TRUNL ALLOWED**

Disaat kita mengkonfigurasi trunk pada interface antar switch,maka trunk tersebut akan membolehkan semua vlan untuk melewati trunk tersebut,sekarang di pembahasan kita,kita akan membolehkan vlan tertentu saja yang akan boleh melewati trunk tersebut,tentu saja kita membutuhkan konfigurasi trunk allowed.

Kita akan menggunakan topologi di lab sebelumnya,dan kita akan melihat dulu vlan mana yang diizinkan oleh trunk untuk melewati trunk.



**Kita akan melihat vlan yang diizinkan trunk :**



Lalu,kita akan mengkonfigurasikan allowed trunk dengan tujuan agar vlan yang diizinkan oleh trunk hanya vlan 10 dan 20 saja

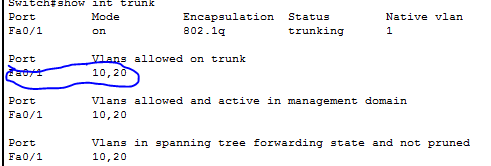
**KONFIGURASI TRUNK ALLOWED :**



Dan juga jangan lupa konfigurasi trunk allowed di switch satunya lagi.

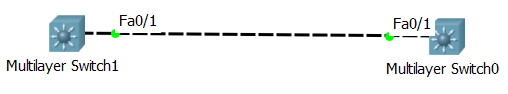


Setelah kita izinkan,kita dapat melihat vlan mana yang diizinkan untuk trunk.

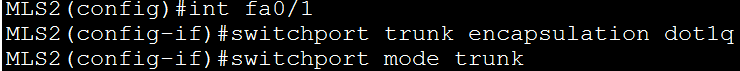
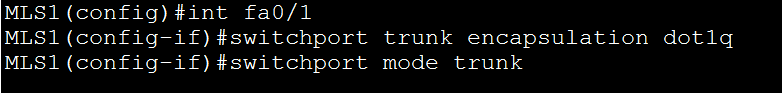


**2.6TRUNK MLS(multi layer switch)**

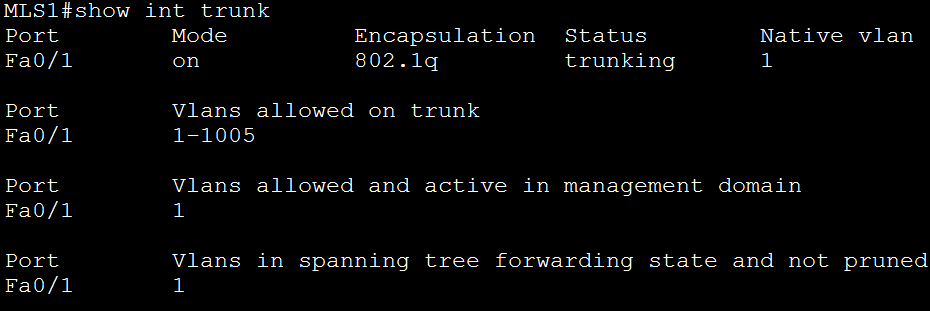
Pembahasan tadi kita melakukan trunk di switch dan router sekarang kita akan melakukan trunk di multi layer switch(MLS)disini hanya mempunyai sedikit perbedaan ketika di konfigurasikan trunk yang mana dia tidak langsung konfigurasi trunk seperti pada switch atau router tetapi di MLS kita harus mengkonfigurasikan encapsulation pada trunk kemudian baru kita konfigurasi trunk.



Ya,langsung saja kita konfigurasi trunk MLS,seperti pembahasan tadi kita harus encapsulation trunk terlebih dahulu lalu kita bisa konfigurasi trunk.



Setelah itu kita bisa lihat apakah trunk nya sudah terbuat untuk MLS :



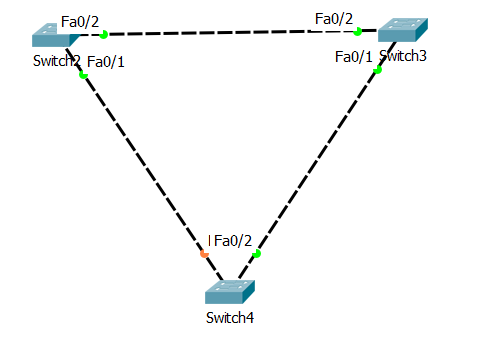
Bisa kita lihat interface 0/1 sudah trunking,tandanya MLS bisa terhubung.

**2.7SPANNING-TREE PROTOCOL(STP)**

Spanning tree protocol(stp) adalah protocol yang berfungsi mencegah mencegah loop pada switch ketika switch menggunakan lebih dari 1 link dengan maksud redudancy.STP secara defaultnya diset aktif pada cisco catalyst.STP merupakan open standar.

Dengan STP ini,salah satu port atau lebih (tergantung topologi)yang akan menjado blocking sehinggal hanya satu link yang digunakan agar tidak terjadi loop.

Berikut topologinya :



Dalam tersebut kita akan lebih menghitung terjadinya ‘’port interface mana yang akan menjadi blocking?.

* **Desigated port**

1. untuk menjadi root bridge yang pertama dilihat adalah nilai prioritynya,yang terpilih adalah yang terkecil.nilai defaultnya adalah 32768.dan dirubah nilain priority haruslah kelipatan 4096.
2. Jika nilai prioritynya sama, maka yang dilihat selanjutnya adalah mac address terkecil.

* **Root port**

Setiap port interface yang berhadapan langsung dengan root bridge,makai ia adalah root port.namun hal ini dilihat dari nilai costnya,semakin kecil nilai costnya maka interface tersebut yang semakin terpilih.

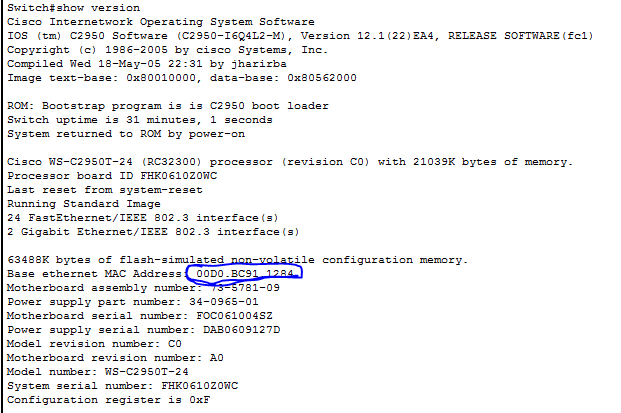
|  |  |
| --- | --- |
| Link speed | cost |
| 10 gbps | 2 |
| 1 gbps | 4 |
| 100 mbps | 19 |
| 10 mbps | 100 |

* **Designated port**

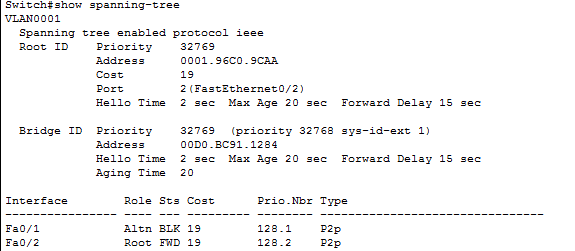
Setiap port interfacenya root bridge adalah designated port,untuk selain root bridge,maka dilihat dari nilai cost,jika sama maka MAC address.

Untuk perintah/command :

* **Untuk melihat MAC address**



* **contoh melihat status STP**



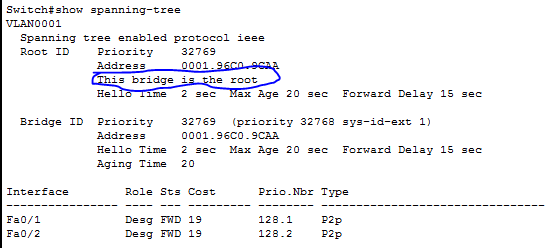
* **Contoh perintah untuk merubah nilai priority**



**Atau**



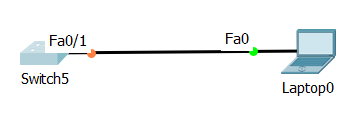
* **perintah untuk melihat status root bridge**



**2.8STP PORT-FAST**

Spanning tree port fast merupakan salah satu fitur STP,yang mana di saat kita menancapkan kabel pada switch kita akan loading atau harus melewati beberapa sesi terlebih dahulu,sampai akhirnya menjadi forwading,dengan spanning tree port fast ini kita akan di percepat dalam melewati beberapa proses tersebut.

Yang mana nanti switch akan melewati step-step yang ada sampai forwading,apa bila kita ingin langsung ke forwading tanpa melewati step-step yang ada maka,dibutuhkan spanning tree port-fast.port fast ini cocok digunakan untuk port yang mengarah ke end host,tetapi tidak direkomendasikan untuk port yang mengarah ke switch karena akan menonaktifkan fungsi STP dalam mencegah looping.



Bagaimana cara mengkonfigurasinya?simpel saja kita masuk ke interface 0/1 yang ingin di spanning tree port-fast.



Hanya dengan itu maka pada saat host mencolokan kembali ke port yang sudah dikonfigurasikan di switch ia akan langsung ke forwading atau kalau di cisco paket tracer lampunya akan langsung hijau,tidak orange lagi.

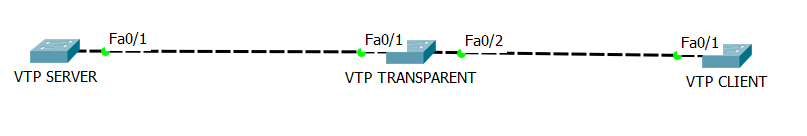
**2.9VTP(VLAN TRUNKING PROTOCOL)**

VTP atau yang disebut vlan trunking protocol adalah sebuah protocol cisco propietary yang hanya dapat digunakan oleh perangkat cisco saja switch saja.untuk menyebarkan definisi(informasi) vlan kepada seluruh perangkat switch di dalam jaringan(LAN).definisi yang disebarkan berguna untuk’’auto congfiguration’’,sehingga memudahkan NE.ada juga yang menyebutkannya bahwa VTP ini untuk meng-advertise kan informasi konfigurasi database VLAN.

VTP dibagi menjadi 3 metode yang kita konfigurasikan :

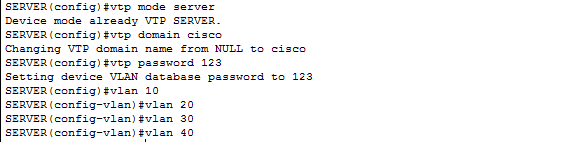
1. **VTP mode server :** di mode ini switch yang akan kita konfigurasikan akan menjadi induk/master bagi para switch yang lainnya,yang mana apa bila switch yang menjadi VTP mode server ini dapat menambahkan vlan atau pun menghapus vlan maka switch akan mengikuti switch yang ada dalam mode server ini.
2. **VTP mode client :** VTP mode ini yang akan menginduk kepada VTP mode server yang apa bila kita sudah satu domain dengan VTP server maka secara otomatis di switch yang sudah kita pasang dalam mode client akan menambahkan sendiri,dan apabila VTP server menghapus maka VTP client pun akan menghapus juga.
3. **VTP mode transparent :** VTP mode transparent ini ia dapat membuat vlan tetapi vlan yang dibuat hanya bersifat local/hanya untuk mode transparent saja,yang mana dia hanya meneruskan saja,tetapi ia tidak mendapatkan apa yang di update oleh VTP server.

**Dan berikut topologinya :**

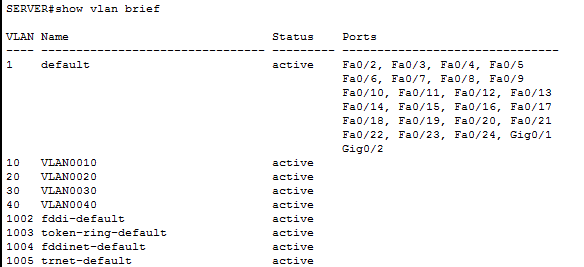
****

Kita akan mencoba seperti topologi diatas terdapat 3 switch yang masing masing switch sudah ada nama VTP yaitu server,transparent,client.hal pertama yang harus kita lakukan adalah trunk antar switch agar vtp client dapat update ke server.dan memasukan konfigurasi VTP.

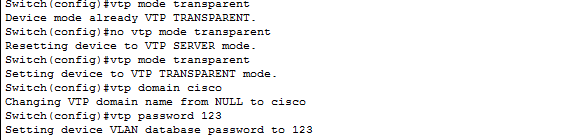
**VTP MODE SERVER**



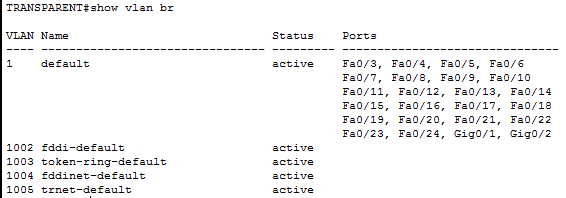
Lalu setelah itu cek vlan di mode server :



**VTP MODE TRANSPARENT**



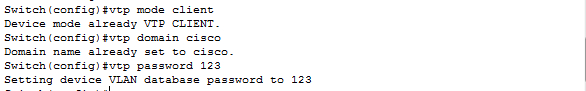
cek apakah vlannya bertambah di mode transparent ?



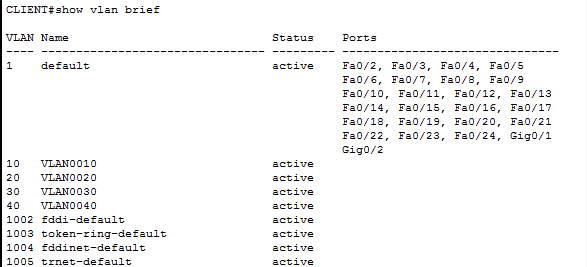
Dapat kita lihat,didalam mode transparent tidak terdapat vlan,ya dikarenakan mode transparent itu hanya bersifat untuk dirinya sendiri,dan juga hanya dilewati.

**VTP MODE CLIENT**

Sama seperti konfigurasi sebelumnya hanya tinggal di ganti mode saja.dan jangan lupa di trunk untuk menyambungkan.



Kalau sudah mari kita cek apakah vlan yang ada di mode server masuk ke mode client :

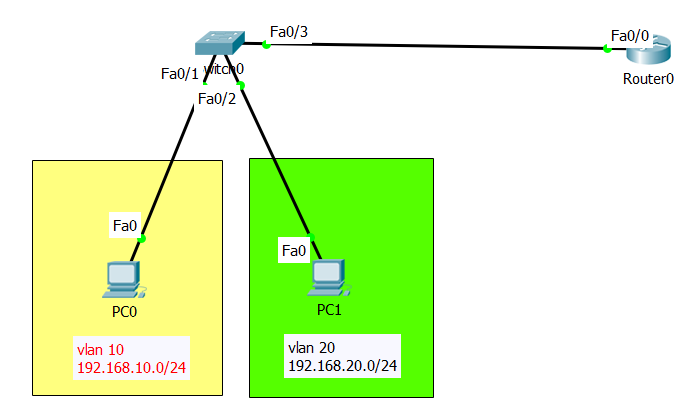


Ya bisa kita lihat di mode client,vlan yang kita masukan di mode server sudah terkirim di mode client.

Seperti itulah kerjanya VTP,VTP server membuat vlan dan melewati VTP transparent dan masuk ke VTP client,kenapa VTP client tidak dapat vlan yang sudah dikonfigurasi,karena VTP transparent hanya untuk dirinya sendiri atau local.

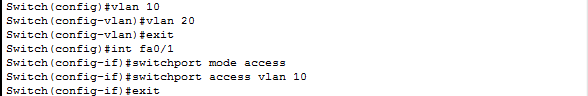
**2.10 INTER-VLAN**

Pada lab sebelumnya kita hanya belajar tentang VLAN yaitu hanya membuat VLAN tetapi tidak saling terhubung dengan vlan yang berbeda dkarenakan networknya berbeda.pada lab kali ini saya akan menjelaskan tentang interVLAN,agar vlan yang berbeda/berbeda network dapat saling terhubung,kita akan mengkonfigurasikan interVLAN dengan router sebagai penghubung antar VLAN,interVLAN digunakan di layer 3.



Berdasarkan topology diatas,terdapat 2 VLAN yaitu VLAN 10 dan VLAN 20.bydefault VLAN 10 tidak dapat terhubung/ping,sekarang kita masuk dalam konfigurasi interVLAN.

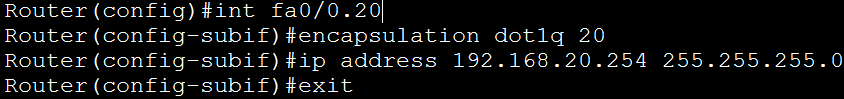
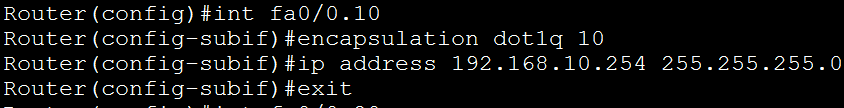
-langkah pertama kalian harus buat vlan dan masukan ke interface masing-masing/taging VLAN.



-setelah kalian sudah membuat VLAN dan masukan ke interface masing-masing,kalian harus menyambungkan VLAN ke router dengan menggunakan trunk.



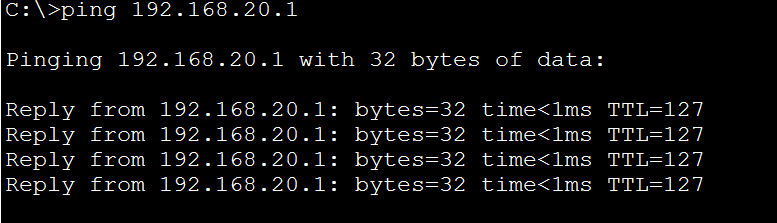
Ok,setelah kalian sudah trunk dari switch ke router,sekarang kita masuk kedalam konfigurasi yang kita sedang bahas,yaitu interVLAN.



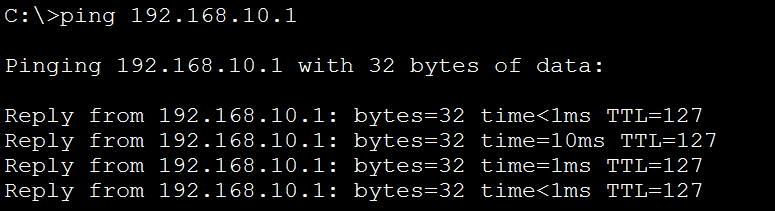
Sekarang kita sudah melakukan interVLAN,untuk pengetesan kita dapat mencoba pc vlan 10 ping ke pc vlan 20.jangan lupa kalian harus masukan dulu IP addres dan gateway di masing-masing pc kalian.

**Test ping :**

Vlan 10 menuju vlan 20



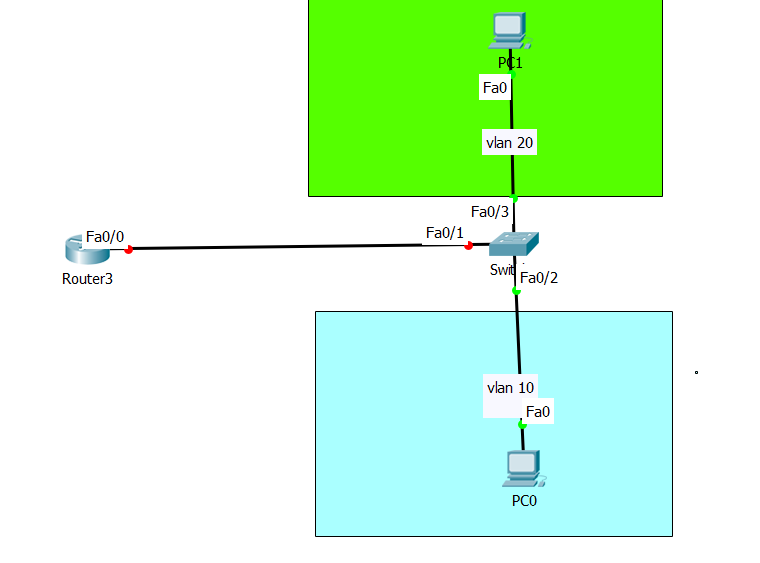
vlan 20 menuju vlan 10



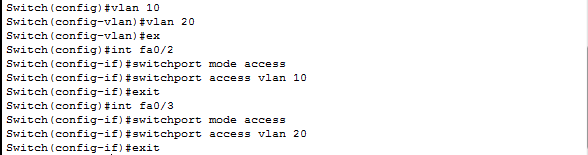
**2.11DHCP**

DHCP berguna untuk memberikan IP address kepada client secara otomatis,jadi client tidak perlu lagi untuk menambahkan IP address lagi secara manual.karena router nanti akan memberikan IP address secara manual ke client dengan cara DHCP.

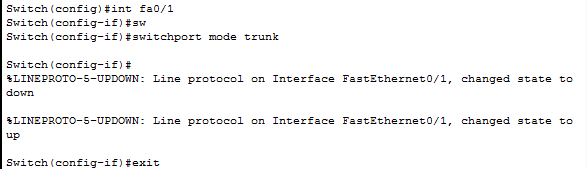
Di kesempatan ini kita akan menggunakan 1 router,1 switch,dan tentunya 2 buah pc,yang mana 2 client tersebut berbeda vlan.



Langkah pertama kita harus membuat vlan di switch terlebih dahulu.



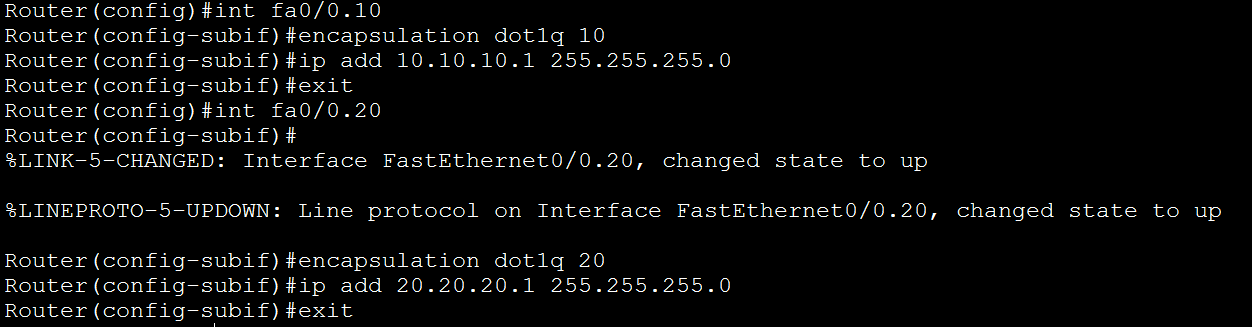
Setelah kita membuat vlan,kita harus menyambungkan vlan dari switch ke router dengan trunk.tentu yang kita konfigurasi yaitu di switch yang interface nya yang mengarah ke router.jangan lupa routernya di no shutdown terlebih dahulu.



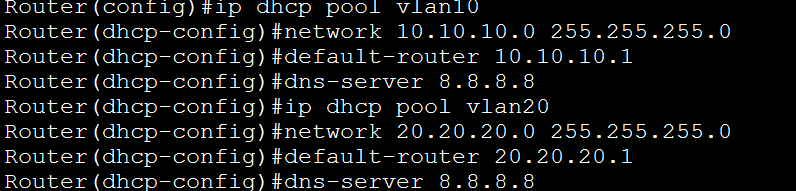
Setelah kita masukan trunk untuk menghubungkan vlan,lalu kita masuk ke router untuk konfigurasi inter-vlan agar pc mendapatkan IP gateway dari router.

**Router**

**Konfigurasi inter-vlan.**

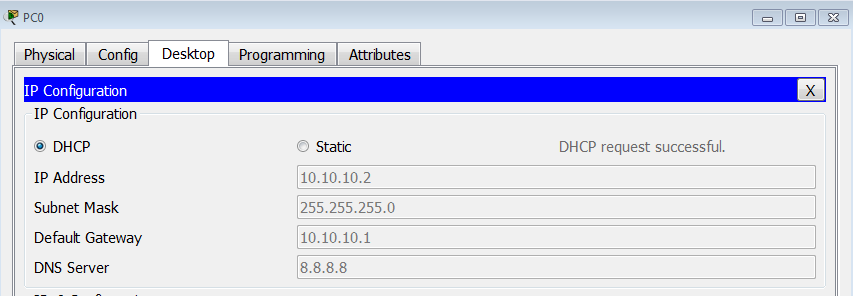
****

Setelah kita inter-vlan di router,sekarang kita bisa memasukan IP address ke client secara otomatis,dengan cara DHCP.

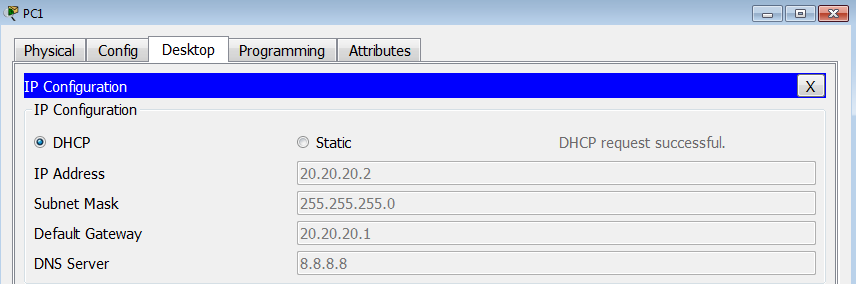


Setelah itu kita dapat mencoba/melihat apakah IP yang dari router terkirim ke pc dengan DHCP.

Client vlan 10 :



client vlan 20 :



Seperti yang sudah kita lihat pc vlan 10 sudah mendapatkan IP secara otomatis/DHCP dari router,begitu juga dengan pc vlan 20.

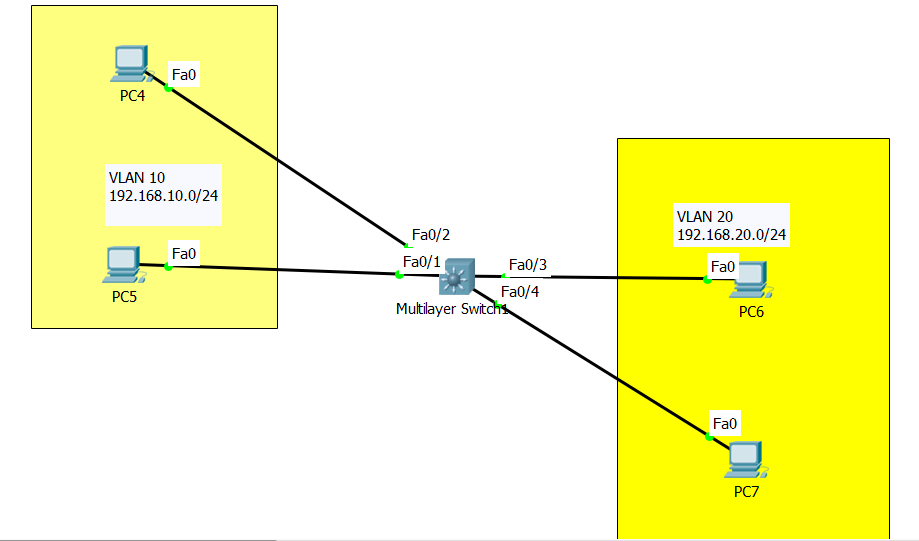
**DHCP excluded address :**

apa yang dimaksud pernyataan diatas,yaitu kita bisa memblok IP dari berapa sampai berapa yang tidak bisa di gunakan,contoh kita akan memblok IP 10.10.10.10.10,20.20.20.50 maka ip 10.10.10.10,20.20.20.50 tidak akan diberikan ke client,berikut contoh :



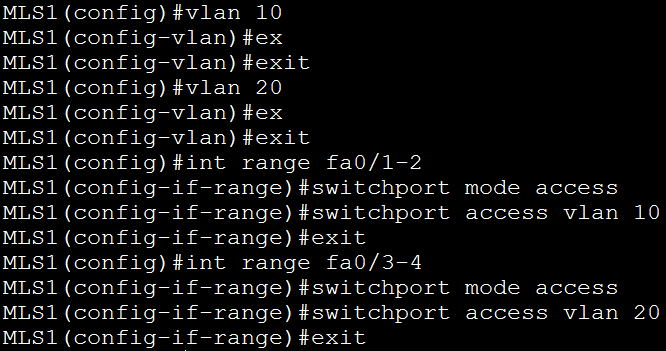
**DHCP MLS**

DHCP juga dapat digunakan di perangkat MLS karna MLS ini berjalan di multi layer 2 dan layer 3 yang ia switch yang dapat menjalankan fungsi routing juga,seperti topologi berikut :



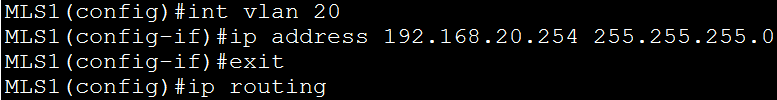
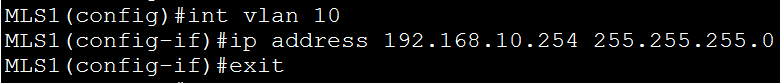
Disan kita sudah membuat topologi untuk DHCP MLS,disitu terdapat 1 MLS dan 2 VLAN yaitu vlan 10,vlan 20.nanti kita akan konfigurasi DHCP di MLS untuk memberikan IP address ke pada client yang ada pada VLAN,nanti setiap client akan mendapatkan IP address secara otomatis/dynamic.

**KONFIGURASI VLAN :**

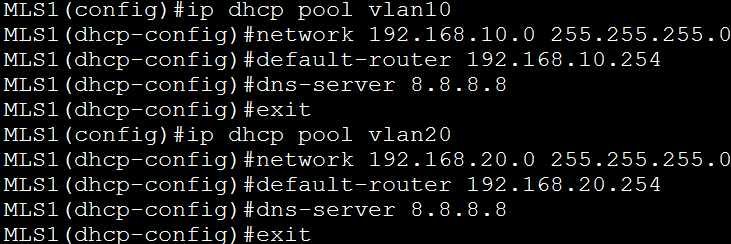


Setelah kita sudah membuat vlan dan memasukan vlan kedalam interface masing-masing,kita akan melanjutkan konfigurasi SVI,dengan maksud agar client yang berbeda vlan dapat saling terhubung dengan vlan yang lain(terhubung dengan network yang berbeda)

**KONFIGURASI SVI :**

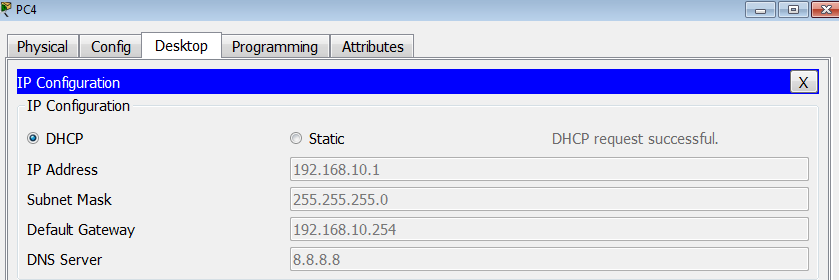


Setelah kita sudaah memasukan konfigurasi SVI,sekarang kita masukan konfigurasi DHCP :

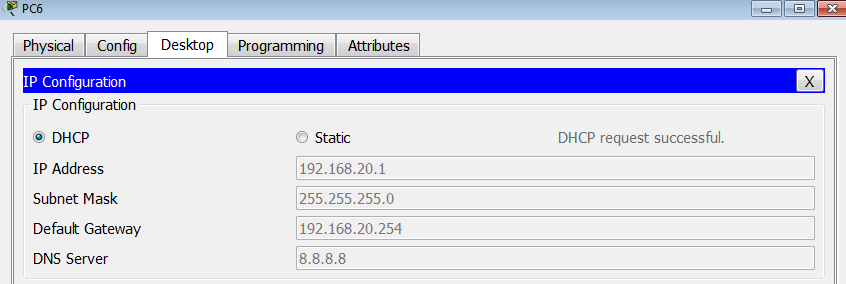


Tadi kita sudah membuat DHCP kepadal MLS untuk membagikan IP secara otomatis kepad client yang vlannya berbeda,sekarang kita lihat apakah IP yang dikirim MLS masuk kedalam client.

Client vlan 10 :



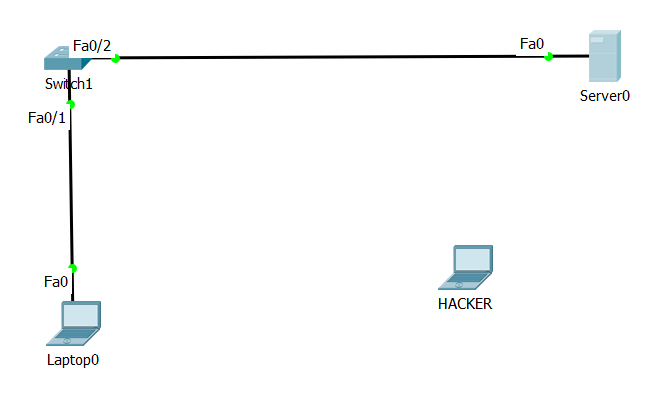
Client vlan 20 :



**2.12SWITCHPORT SECURITY**

Port security adalah suatu cara yang untuk mengamankan port interface,karna apabila kita tidak mengamankan port interface kita,maka apa bila ada seseorang ingin mengambil data yang ada di perangkat semua data akan hilang dari perangkata,maka karna itu diadakan port security untuk mengamankan port interface dan juga dapat mencegah MAC flooding

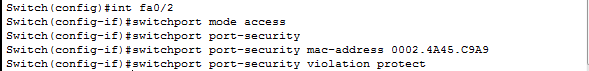
Pada port security,terdapat 3 mode,yaitu :



Seperti topology diatas,disitu terdapat laptop HACKER yang mana laptop itu akan mencoba mengambil data dari server,tetapi perangkat tersebut sudah di port security.

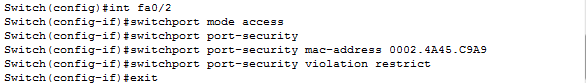
* **PROTECT**

data yang dikirimkan melalui interface tersebut tidak akan di forward(tidak dikirim)perintah :



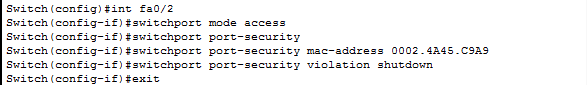
* **RESTRICT**

Pada restrict ini sepert protect,sama saja seperti violation protect,data tersebut akan diabaikan,dan dibiarkan.hanya saja ia mengirim notifikasi dengan SNMP,SNMP itu adalah protocol yang mana akan muncul apa bila ada penjahat ingin mengambil data ke server maka ia akan ditolak dan dikirimkan notifikasi.



* **SHUTDOWN**

Pada shutdown ketika ada yang mencolok ke perangkat kita maka interface yang dicolok akan mati,metode ini paling sering digunakan.



**2.13DYNAMIC TRUNKING PROTOCOL**

Dynamic trunking protocol(DTP)adalah sebuah protocol dari trunk,dan DTP ini adalah (cisco proprietary)atau yang hanya bisa digunakan sesama perangkat cisco,DTP ini digunakan untuk negosiasi trunk.yang dimaksud negosiasi ini adalah,yang dimana salah satu dari interface akan menjadi access atau trunk.

Dynamic trunking protocol ini terbagi menjadi 2 mode yaitu,dynamic desitable dan dynamic auto.

* **Dynamic desirable**

Dynamic desirable ini dia bersifat mengajak atau nembak duluan kepada port interface lawannya untuk menjadi trunk,interface yang modenya desirable menginginkan untuk menjadi trunk namun tidak menolak menjadi access juga.



* **Dynamic auto**

Kalau tadi dynamic desirable dia bersifat mengajak atau nembak duluan,sekarang dynamic auto dia bersifat menunggu yang dimaksud adalah,dia menunggu di tembak atau diajak untuk menjadi trunk.



**ETHERCHANNEL**

Dalam etherchannel ini,disini kita akan menggabungkan 8 interface menjadi 1 interface,loh..bagaimana caranya?dengan teknologi etherchannel kita bisa membundle link tersebut sehingga seolah-olah menjadi 1 link,dengan demikian link tersebut akan digunakan sebagai kirim data.dan keuntungan dari etherchannel ini adalah,bandwith nya bertambah cepat,semisal 1 interface nilainya 100mbps apa bila ada 8 interface maka bandwith nya 800 mbps.

Ada 3 tipe dalam etherchannel ini,yakni

* L2 etherchannel LACP(open standard)
* L2 etherchannel PAGP(cisco proprietary)
* ON



* **PAGP(port aggregatiom protocol)**

PAGP ini merupakan protocl cisco proprietary,keunggulan dari PAGP ini adalah dari kecepatannya yang dihasilkan dibanding yang lainnya.protocol PAGP ini terbagi menjadi dua mode yaitu desirable dan auto.



* **LACP(link aggregation control protocol)**

LACP ini merupakan open standar,yang mana ia bisa di pakai dengan berbeda vendor,LACP ini terbagi menjadi 2 mode :active,passive.

1. **active :**yang artinya dia mengajak untuk dijadikan etherchannel LACP
2. **Passive :**yang artinya dia akan menunggu sampai diajak menjadi etherchannel.



* **ON**

Mode ini bukan protocol sepertin LACP dan PAGP.ON ini tidak melakukan negosiasi tetapi hanya mekanisme.ON ini bisa dikatakan sebagai static link aggreation atau static etherchannel.

***3.1routing***

* **STATIC ROUTE**
* **DYNAMIC ROUTE**
* **OSPF**
* **EIGRP**
* **eBG**
* **EXTENDED-STANDARD ACCESS-LIST**
* **NAT(network address translation)**
* **GRE TUNNEL**
* **HIGH AVAIBILITY**
* **PPP(point-to-point-protocol)**
* **NTP**

**3.2STATIC ROUTE**

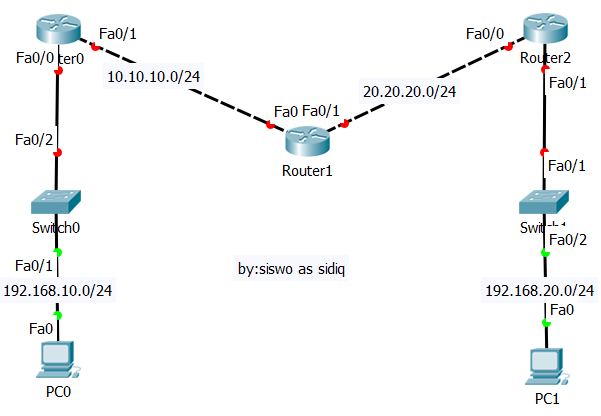
Static router adalah sebuah mekanisme dalam protocl routing yang mana kita akan menyambungkan satu network agar saling terhubung,dengan network lainnya secara static/manual.

Static router di konfigurasi secara manual agar untuk menentukan jalur,semakin banyak router yang kita pasang,semakin banyak kita mengkonfigurasi static route,keunggulan static router adalah ia memiliki administrative distance (AD)yang mana ia akan dipilih oleh routing protocol lain-lain.

Dan juga static route mempunya beberapa kekurangan yaitu :

1. administrator jaringan harus mengetahui semua informasi dari masing-masing router yang digunakan.
2. Hanya dapat digunakan untuk berskala yang kecil
3. Administrasinya cukup rumit dibanding routing dynamis,terlebih jika banyak router yang harus dikonfigurasi secara manual
4. Rentan terhadap kesalahan saant entri data routing statis yang dilakukan secara manual.

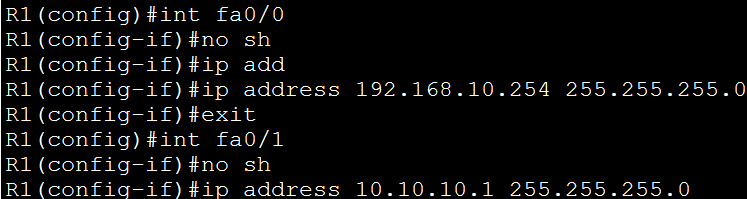
Untuk topoligi static route kita akan menggunakan 3 router dan 2 host:



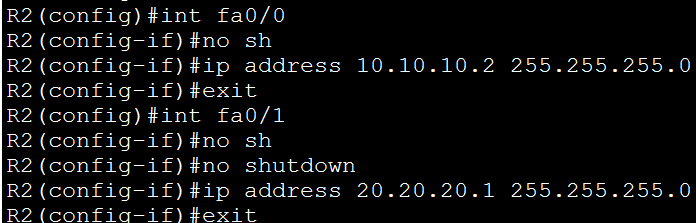
Disini kita akan konfigurasi static route agar kedua pc bisa saling terhubung/ping.

Pertama kita konfigurasi ip masing-masing interface sesuai topologi :

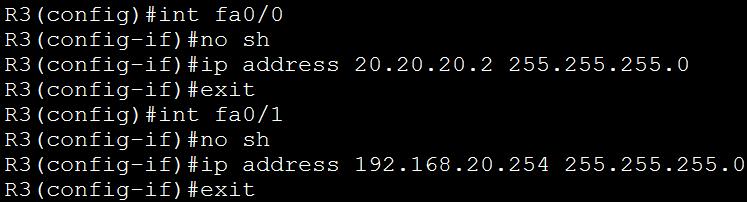
**R1**



**R2**



**R3**



Tadi kita sudah membuat IP di masing masing router,jika ingin melihat ip yang sudah kita pasang,kalian konfigurasi’’*show ip route’’*.

Sekarang kita masuk kedalam konfigurasi static route,kita akan static 3 router.

**R1**



**R2**



**R3**



dalam static route ini,kita harus saling mengenalkan satu sama lain,kecual yang directly connected:

1. R1 belum mengenali R3
2. R3 belum mengenali R1
3. R2 belum mengenali IP kedua client tersebut
4. .R1 belum mengenali IP client 192.168.20.0/24
5. R3 belum mengenali IP client 192.168.10.0/24

KET:rumus dari static ini,yaitu kita mau kemana dan kita harus lewat mana.

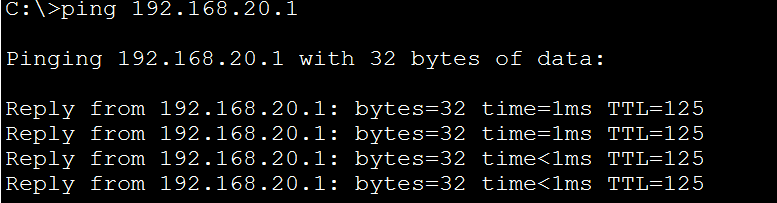
**R1 KEPADA CLIENT 192.168.20.0/24**



**R3 KEPADA CLIENT 192.168.10.0/24**

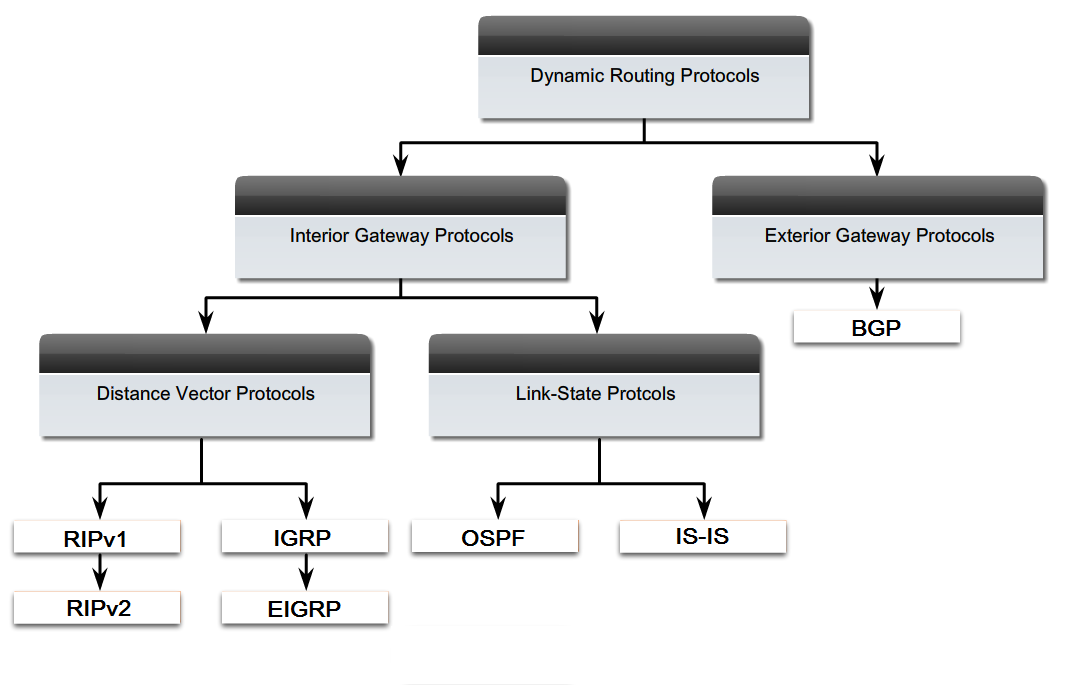


Jika kalian sudah melakukan konfigurasi static seperti diatas,mari kita coba apakah CLIENT 192.168.10.0/24 bisa ping ke CLIENT 192.168.20.0/24.



Sekarang kedua CLIENT tersebut dapat terhubung dengan konfigurasi static route.

**3.3DYNAMIC ROUTING**

****

Dynamic routing adalah sebuah teknologi dalam jaringan yang membuat data routing menjadi optimal.karena dynamic routing ini tidak seperti static rout,dynamic routing ini memiliki fitur yang mana router akan memilih jalur terbaiknya sesuai yang diinginkannya.

Dan juga dynamic routing lebih mudah dikonfigurasi dari pada static route,dynamic ini dia berjalan diatas protocol,sedangkan static dia adalah mekanisme.dynamic routing ini juga memiliki kekurangan yaitu,dynamic ini mengkonsumsi processor dan RAM lebih besar dari pada static.dan juga dynamic routing ini tingkat keamanannya lebih rendah dari pada static.

Router memilih jalur terbaiknnya dari routing table,yaitu dari administrative distance.administrative distance adalah nilai yang digunakan oleh router untuk memilih jalur terbaiknya.

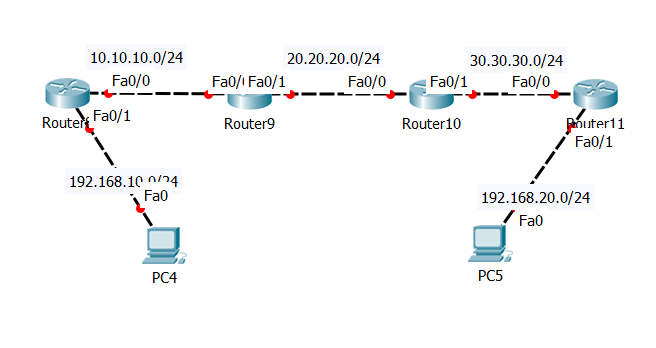
Berikut tablenya :

|  |  |
| --- | --- |
| **Routing technique** | **preference** |
| Connected interface | 0 |
| Static route | 1 |
| EIGRP sumary route | 5 |
| EBGP | 20 |
| Internal EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| RIP | 120 |
| EGP | 140 |
| ODR | 160 |
| External EIGRP | 170 |
| Internal BGP | 200 |
| unknown | 255 |
| ISIS | 115 |

Semakin kecil nilainya ,maka semakin terpilih protocol tersebut oleh router.

**3.4RIPv1**

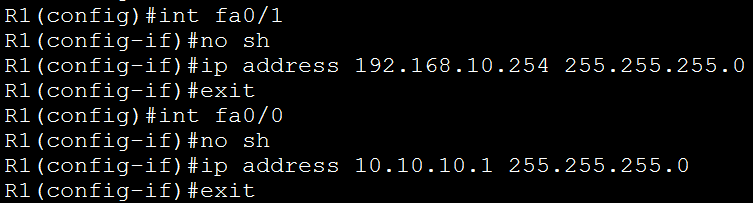
RIP singkatan dari routing information protocol,yaitu sebuah protocol routing yang digunakan untuk menyambungkan antar router dengan melewati jalur terbaiknnya,RIP ini mencari jalur terbaiknya berdasarkan hop count(jumlah loncatan).jumlah hop count pada RIP ini adalah 15 loncatan.jika loncatannya melebihi 15 maka RIP tidak akan mensupportnya.



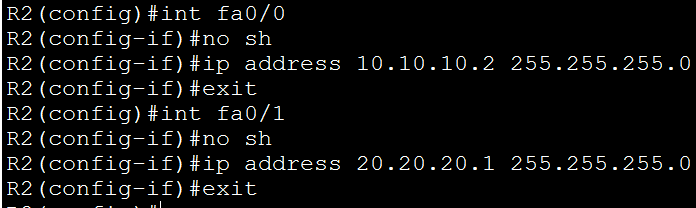
Seperti topologi diatas,terdapat 4 router dan 2 client.

Pertama kita akan memasukan IP address kepada setiap interface yang ada pada router.

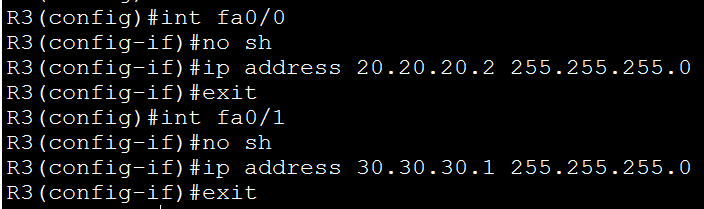
**R1**



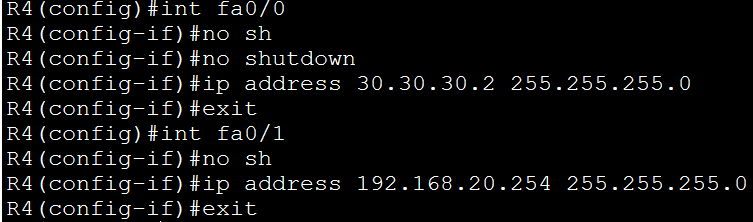
**R2**



**R3**

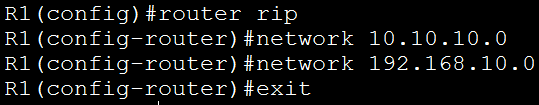


**R4**

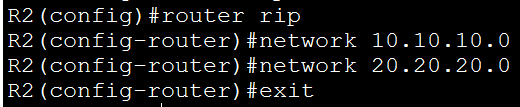


Sekarang kita langsung masuk saja kedalam konfigurasi RIPV1 :

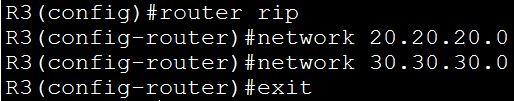
**R1**



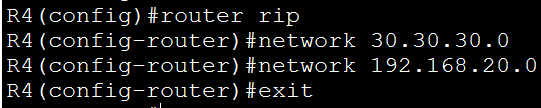
**R2**



**R3**

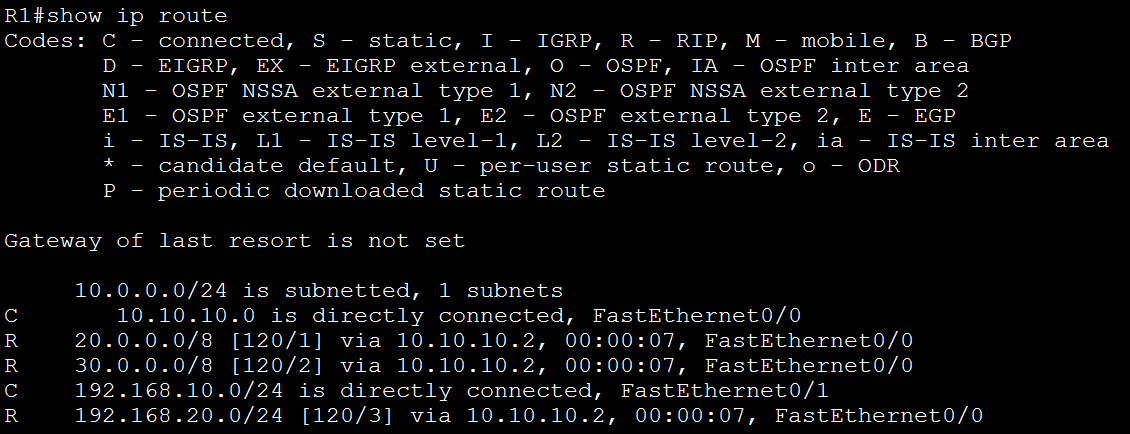


**R4**

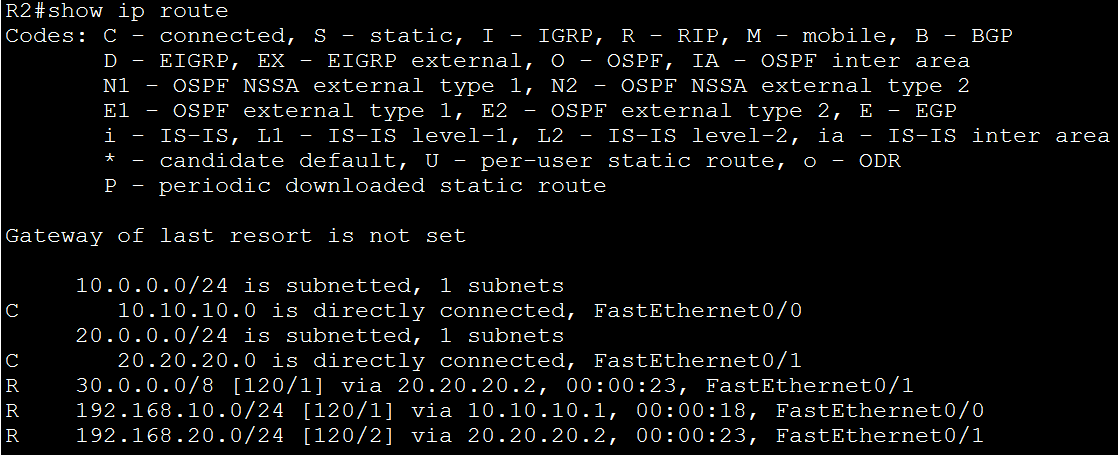


Untuk vertifikasi dengan command *‘’show ip route’’.*

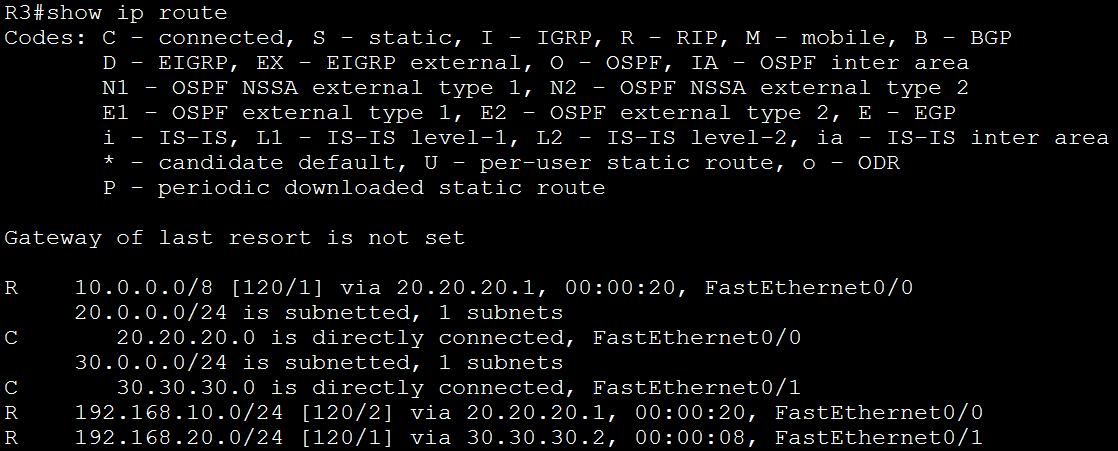
**R1**



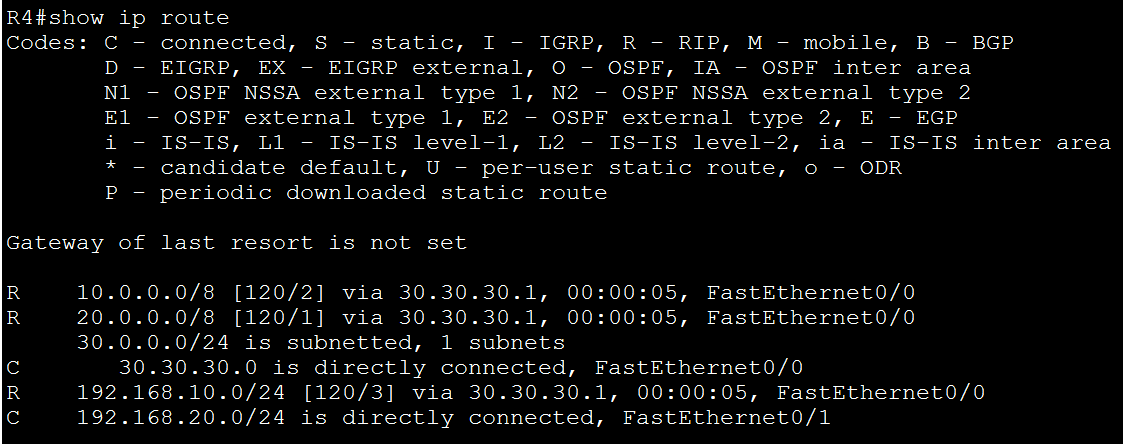
**R2**



**R3**



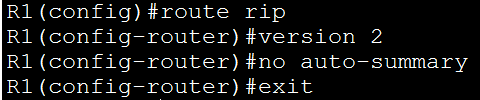
**R4**

**3.5RIPv2**

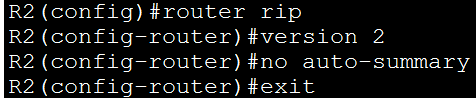
RIPv2 ini adalah perkembangan dari RIPv1. RIPv2 ini dikembangkan pada tahun 1993.fungsinya sama untuk menghubungkan router.

kita akan menggunakan topologi seperti RIPv1,konfigurasinya sama saja,hanya kita ganti menjadi version 2.

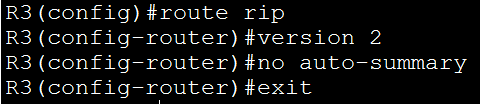
**R1**



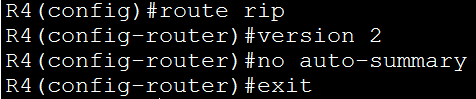
**R2**



**R3**



**R4**



**3.6DYNAMIC EIGRP**

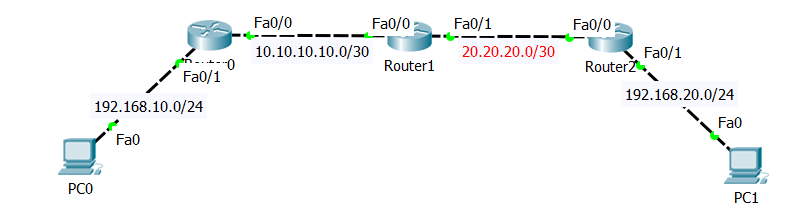
Pada lab sebelumny kita membahas tentang routing dengan static/manual.maka pada lab ini kita akan membahas tentang routing secara otomatis dengan menggunakan routing protocol EIGRP(enchanced interior gateway protocol).

EIGRP merupakan salah satu routing protocol dynamic route,dan EIGRP ini dia adalah cisco proprietary,dengan kata lain EIGRP ini hanya bisa digunakan untuk perangkat cisco.

EIGRP memiliki administrative distance sebanyak 90 seperti table diatas,update dalam EIGRP menggunakan multicast :224.0.0.10,jumlah hop count(loncatan)pada EIGRP adalah 255(default 100),memiliki kovergensi yang cepat.

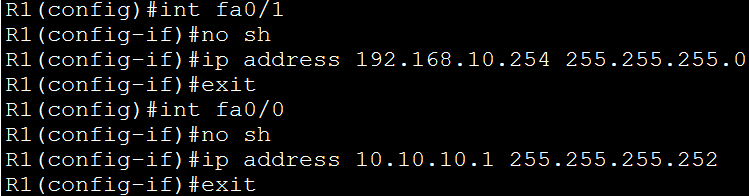
Keuntungan dari EIGRP adalah terdapat backup route jika best route down(successor=primary,feasible successor=backup)dan ia mendukung VLSM.routing EIGRP menggunakan autonomous system number (ASN)untuk mengidentifikasi route-router yang sharing informasi route.

Untuk topologi EIGRP sekarang,kita akan menggunakan 3 router dan 2 client.

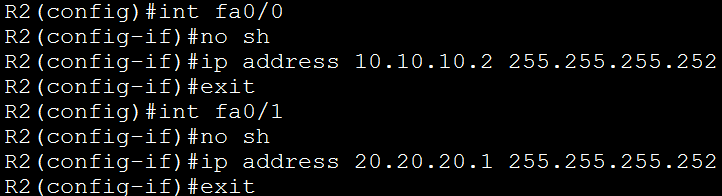


langkah pertama kita masukan IP address di masing masing router terlebih dahulu sebelum kita konfigurasi routing.

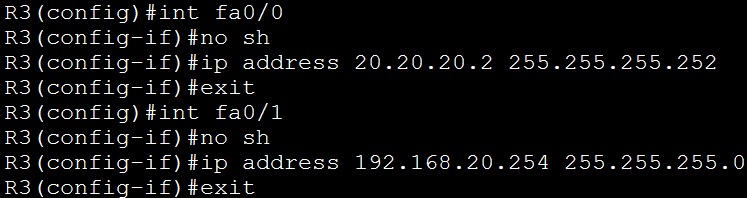
**R1**



**R2**

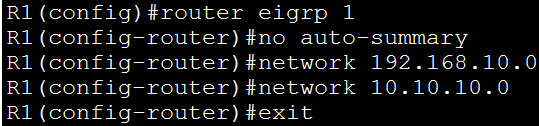


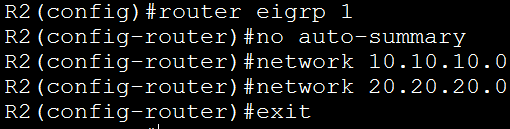
**R3**

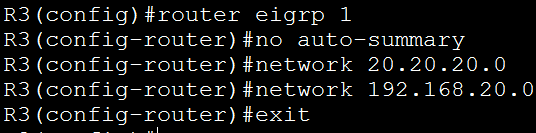


Setelah kita konfigurasi IP address pada setiap interface,maka sekarang kita dapat konfigurasi EIGRP.

Konfigurasi EIGRP :

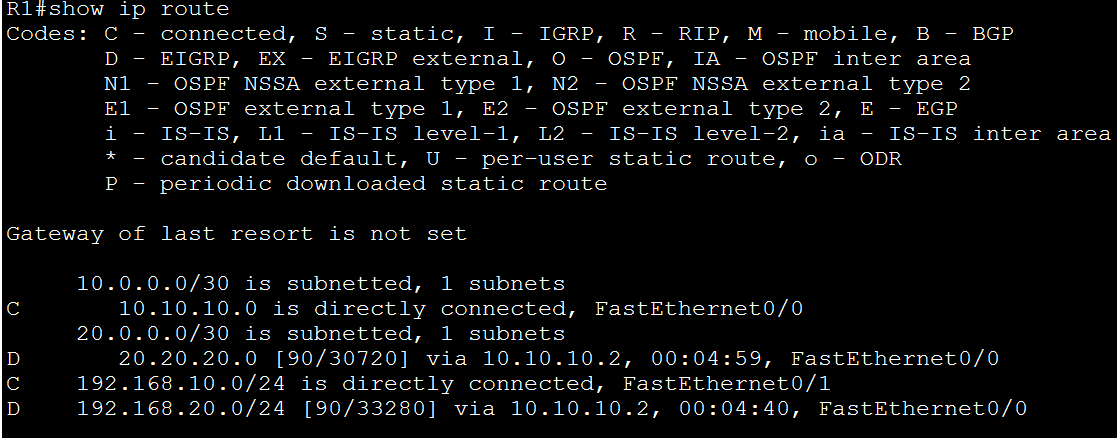




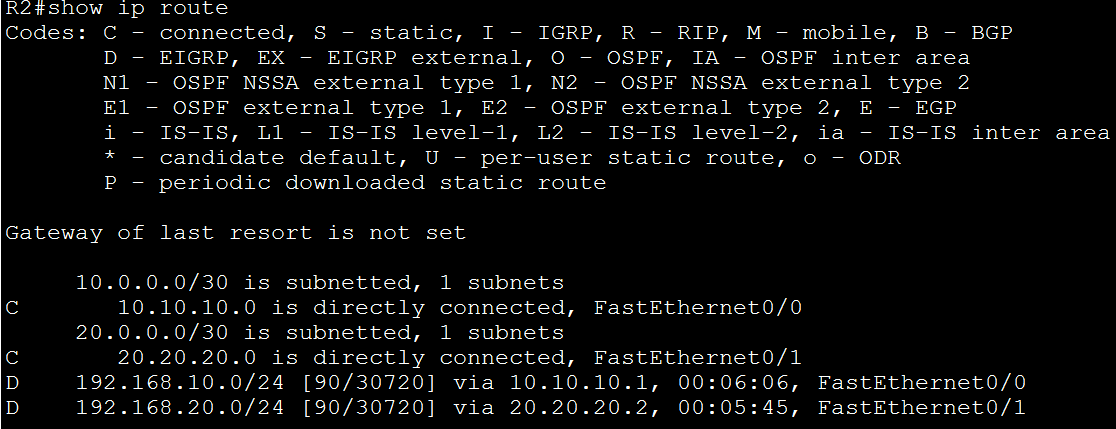


Setelah kita routing EIGRP kita bisa melihat di table routing dari masing masing router,pastikan masing msing router memiliki table routing yang lengkap pada semua network,yang memiliki status’’D’’ maka itu adalah EIGRP.

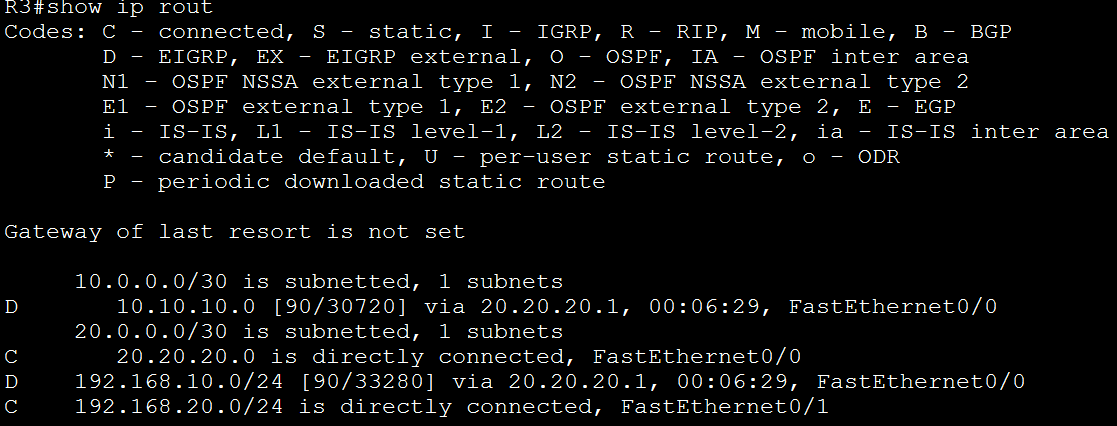
**R1**



**R2**

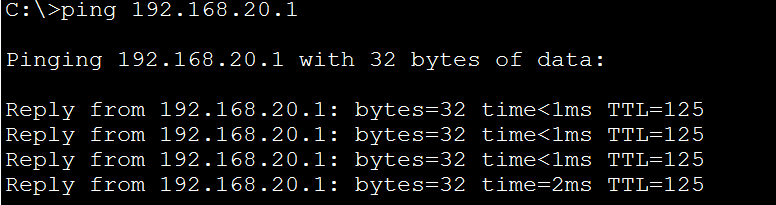


**R3**

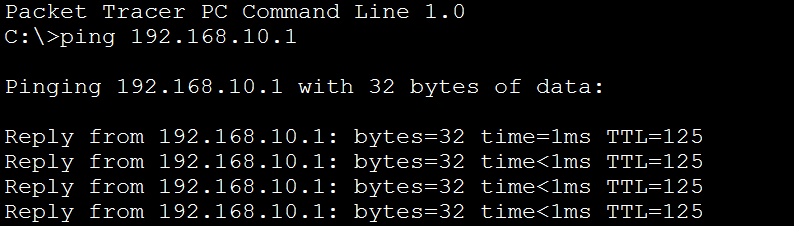


Sekarang kita bisa lihat masing-masing router sudah memilik routing table,kalau sudah sekarang kita bisa mencoba untuk test ping di PC1 ke PC2.

**PC1 menuju PC2**



**PC2 menuju PC1**



Sekarang PC1 dan PC2 sudah saling terhubung,dan konfigurasi EIGRP telah berhasil.

**3.7DYNAMIC OSPF**

Ok,pada lab kali ini kita akan membahas tentang routing protocol lain dalam dynamic routing yaitu OSPF(open shortest path first),OSPF ini termasuk kedalam link state seperti table yang pernah kita jelaskan.OSPF ini yang mana ia akan mengirim sebuah paket data melalui badwith yang besar .

Untuk penghitungan cost pada OSPF dapat di rumuskan dengan

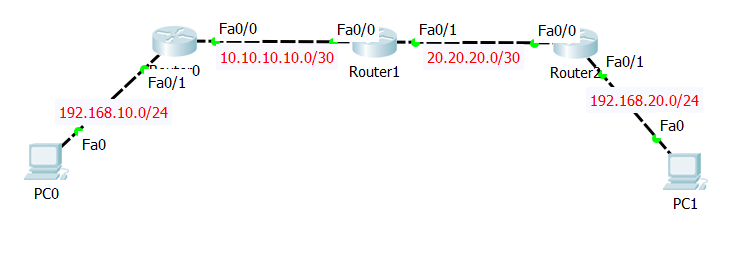
**REFERENCE BANDWITH**

BANDWITH

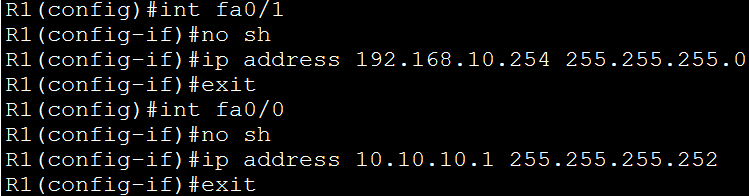
Reference bandwith adalah ketetapan bandwith yaitu 100mb,yang kemudian akan dibagi-bagi sesuai dengan bandwith pada kabel yang dipakai pada router :

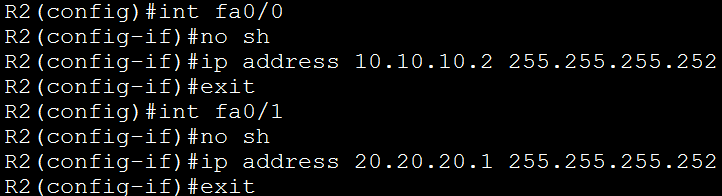
1. gigabyte ethernet :1000mb
2. .fast ethernet :100mb
3. Ethernet :10mb

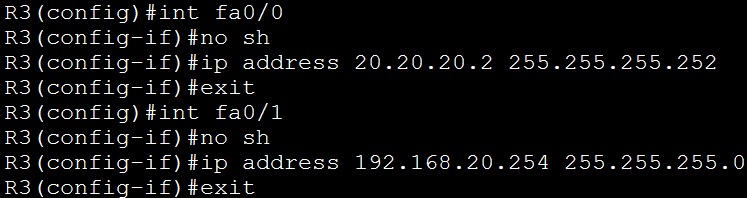
Sekarang kita masuk kedalam topologinym,untuk topologi sekarang kita akan menggunakan 3 router dan 2 client,dan kita akan mengkonfigurasikan dengan routing OSPF.



Seperti lab routing biasanya,pertama kita masukan IP address terlebih dahulu di masing-masing interface.

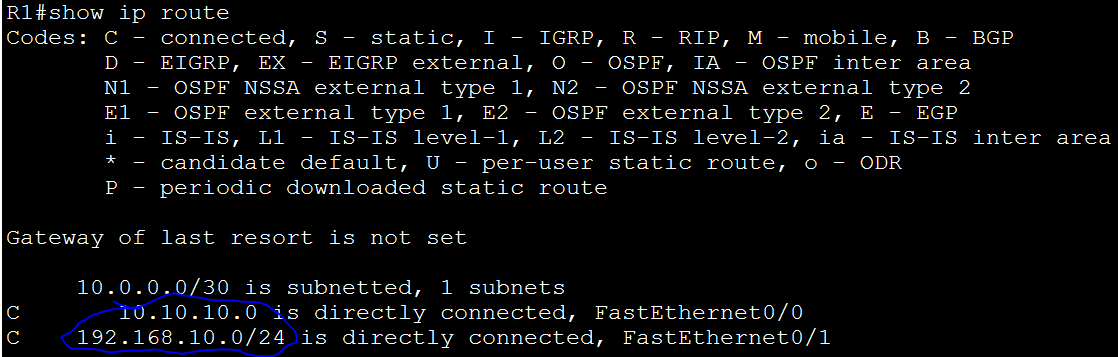




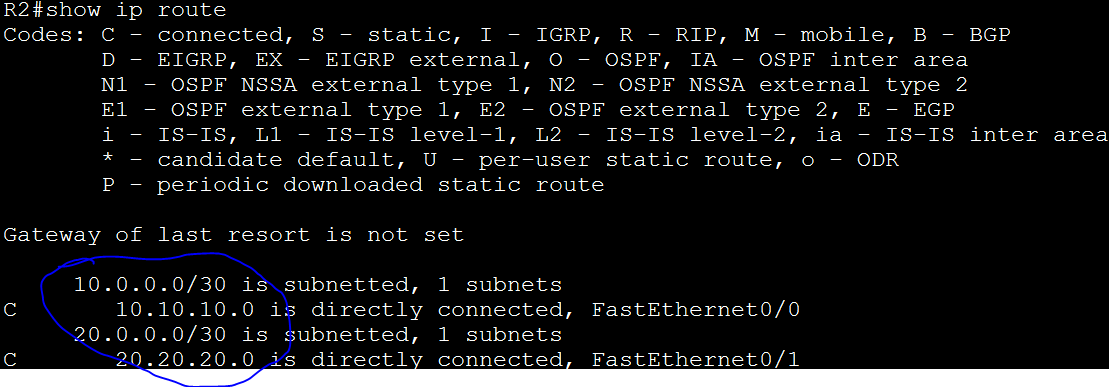


Tadi kita sudah masukan IP address di masing-masing interface.jika ingin membuktikan apakah IP sudah masuk,mari kita lihat table routingnya.

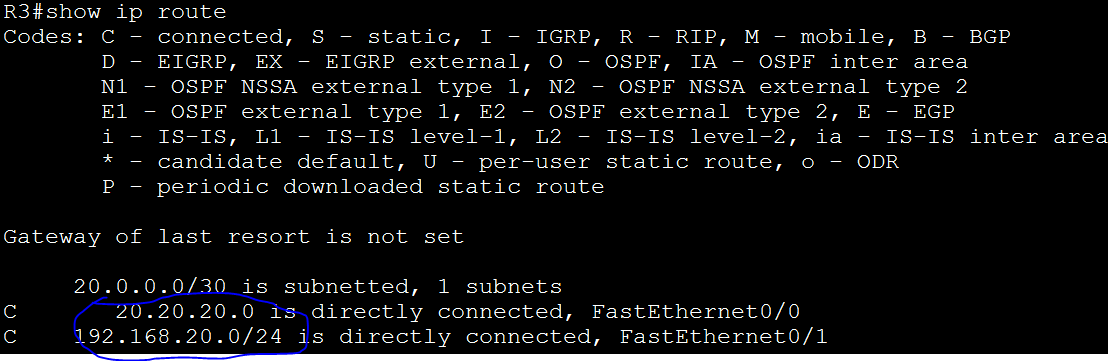
**R1**



**R2**



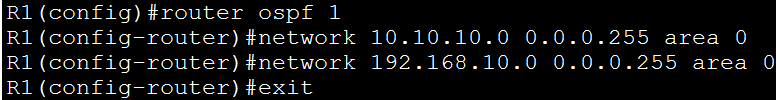
**R3**



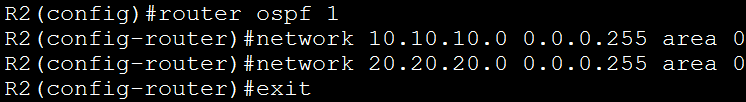
Pada routing OSPF ini kita akan memasukan network yang terhubung pada router tersebut atau yang terdapat pada table routing sebelum dirouting,kemudian kita msukan wildcart mask nya.

Dan untuk lab OSPF kali ini kita akan menggunakan 1 area yaitu area backbone atau area0.

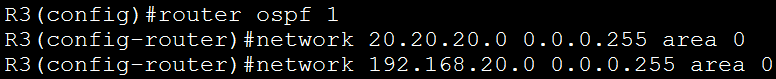
**R1**



**R2**

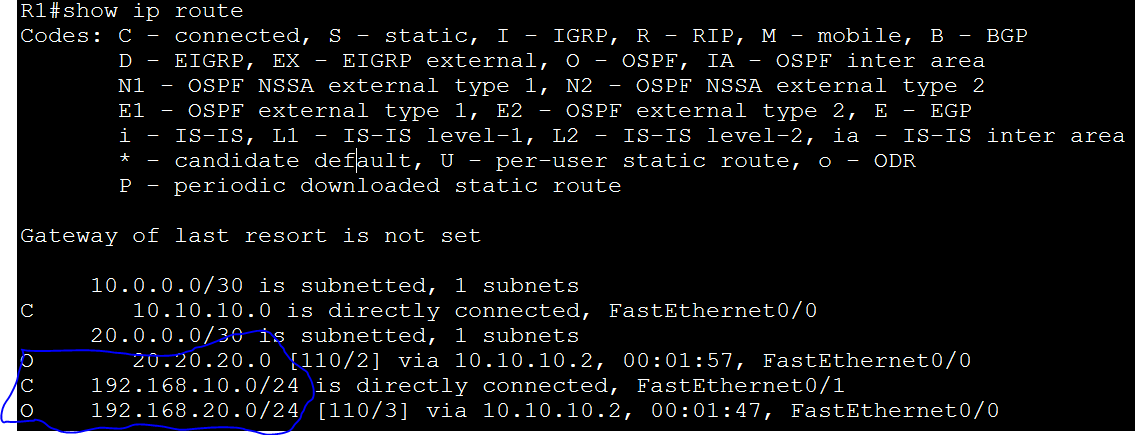


**R3**

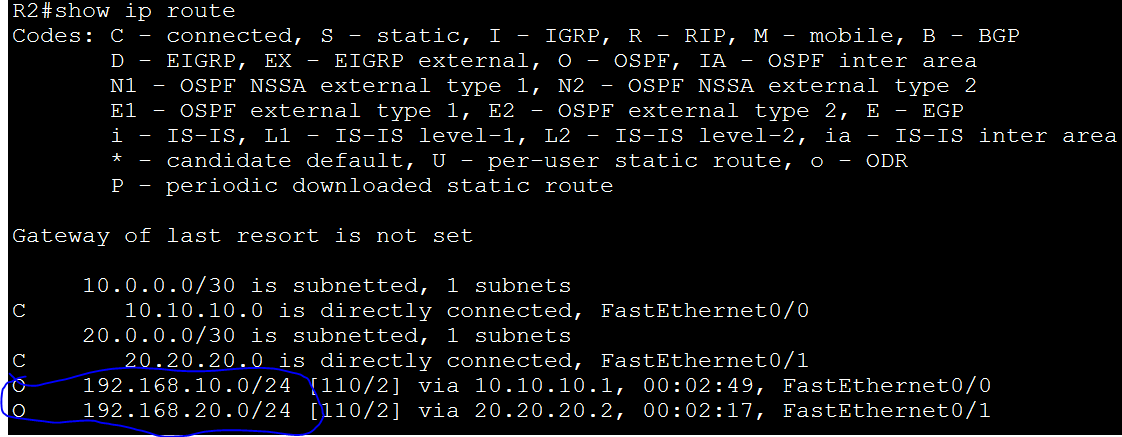


Kita sudah selesai mengkonfiurasi OSPF,maka sekarang kita akan melihat di table routing pada setiap router apakah sudah terdaftar network yang lain,jika sudah terdaftar statusnya adalah’’O’’.

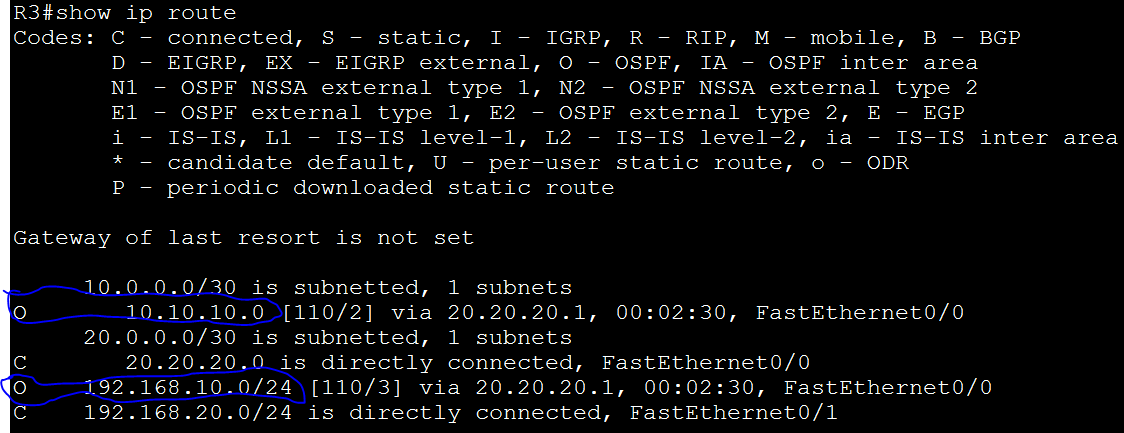
**R1**



**R2**

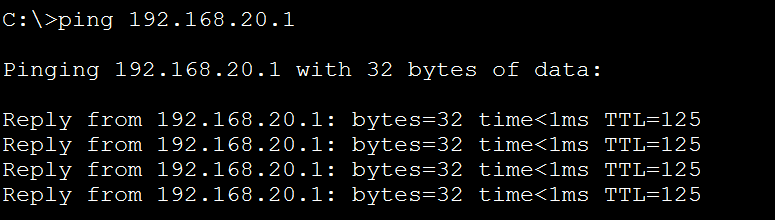


**R3**

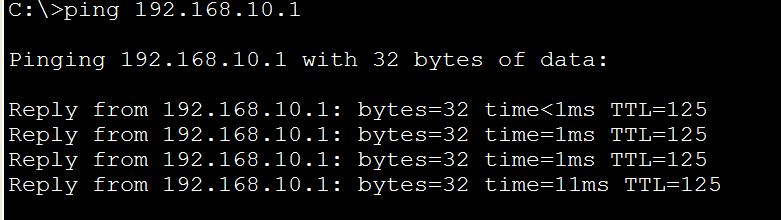


Kita bisa lihat,network yang lain sudah terdaftar dengan status’’O’’di masing-masing router,sekarang kita akan mencoba ping dari client PC1 ke PC2 dan sebaliknya.

**PC1 menuju PC2**

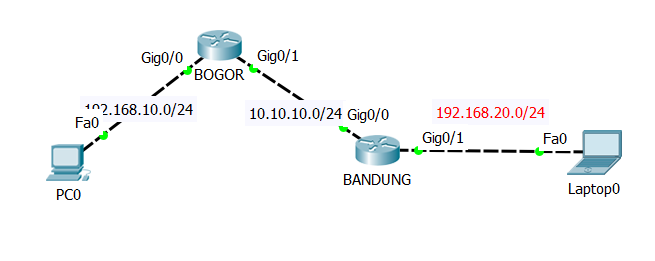


**PC2 menuju PC1**



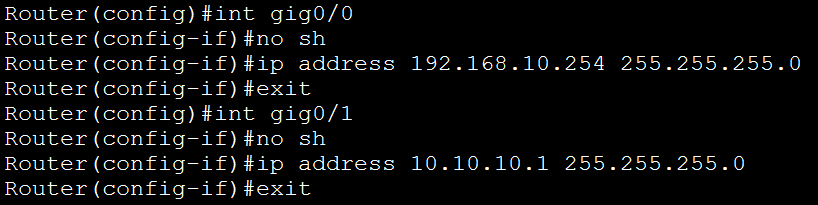
**3.8DYNAMIC eBGP**

Sebelumnya kita membahas tentang EIGRP yang menghubungkan router dengan AS yang sama,sekarang kita akan mempelajari sekaligus mengkonfigurasi salah satu dari protocol dynamic routing yaitu eGBP.eBGP ini adalah?dia menghubungkan AS yang berbeda metode ini biasanya dipakai di sebuah perusahaan

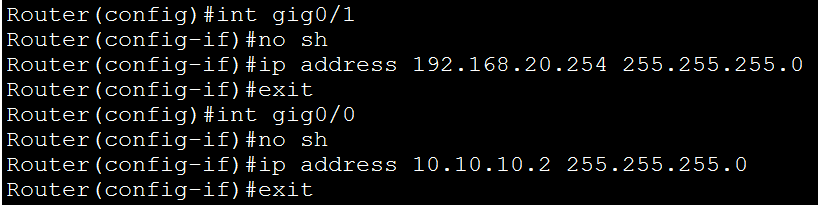
.

Langsung saja kita mulai,pertama kita masukan IP address pada interface yang ada di setiap router.

BOGOR :

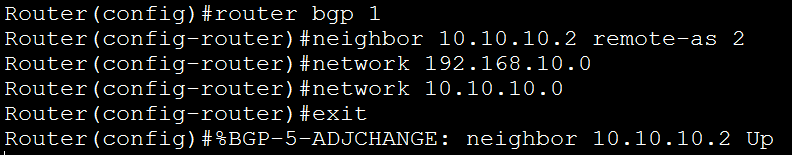


BANDUNG :

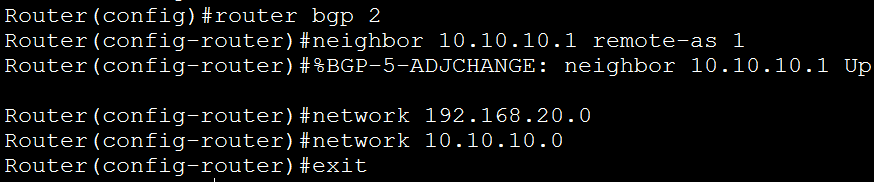


Dan sekarang kita akan mengkonfigurasikan eBGP,router bogor mempunyai AS 1 dan router bandung mempunyai AS 2.

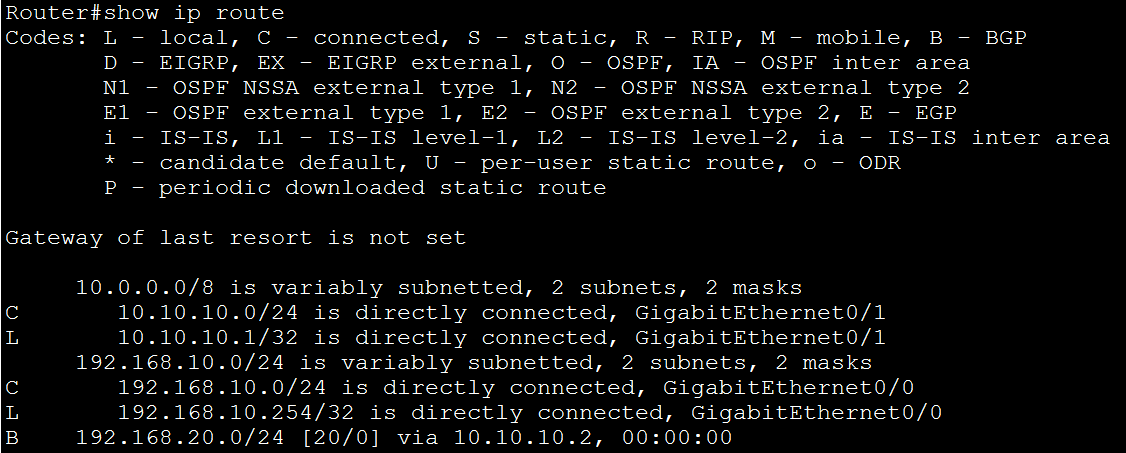
BOGOR :



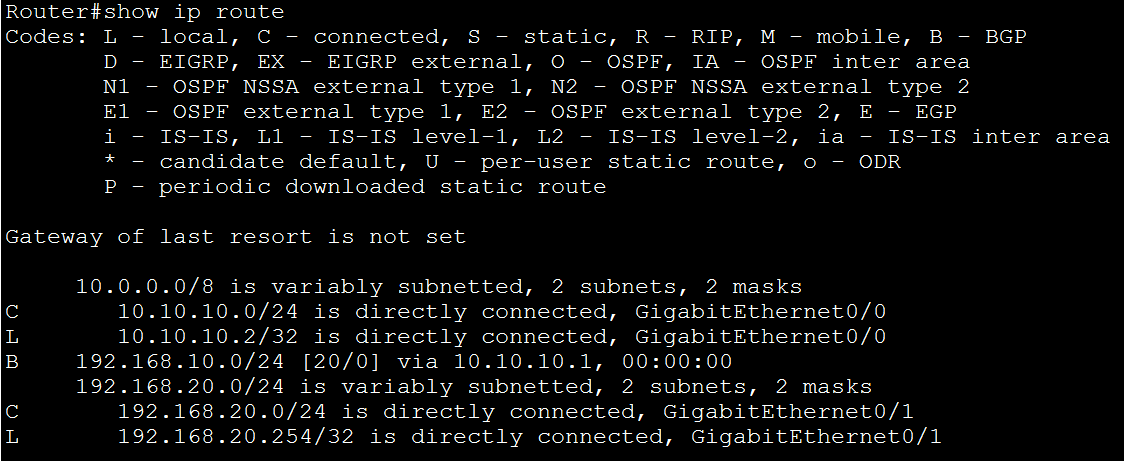
BANDUNG :



Kita sudah mengkonfigurasi eBGP,sekarang kita pastikan di routing table dengan command’’*show ip route’’*dengan status*’’B’’.*

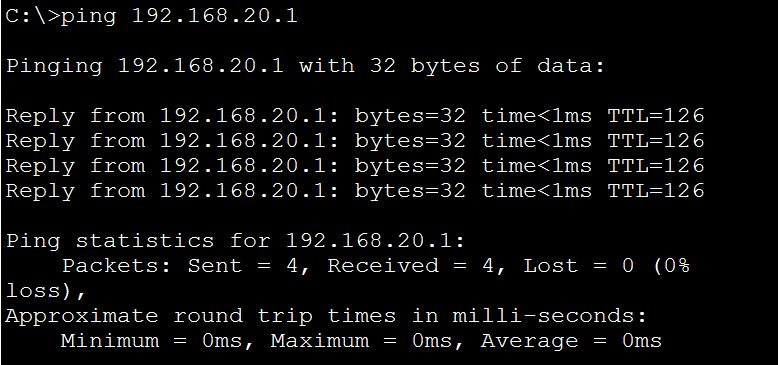
BOGOR :

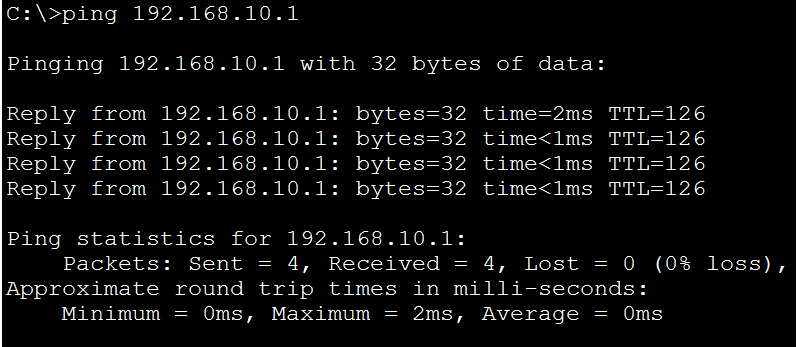
BANDUNG :



Sekarang kita test PING dari client bogor menuju client bandung dan sebaliknya.

BOGOR menuju BANDUNG :

BANDUNG menuju BOGOR :



Selesai sudah penjelasan kita mengenai eBGP,sekarang client BOGOR dan client BANDUNG dapat berkomunikasi.

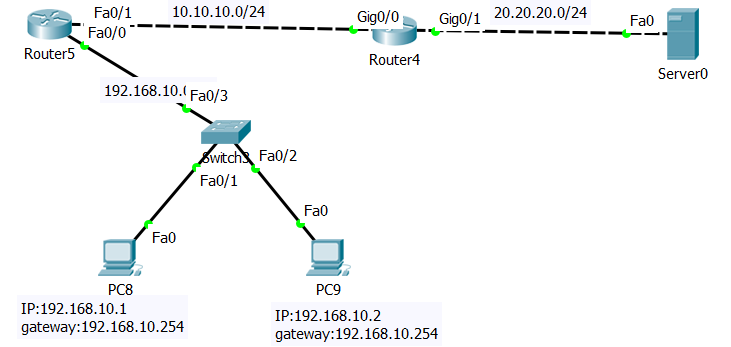
**ACCESS-LIST(ACL)**

Sekarang kita masuk kedalam pembahasan access-list,yang mana fungsi access-list ini berfungsi untuk filtering sebuah packet yang melewati router,jadi router akan memilih paket-paket mana saja yang boleh melewatinya dan tidak boleh melewatinya.

Access-list terbagi menjadi 2 jenis yaitu :

* **Standard access-list :**pada standard access-list ini kita hanya bisa memblock sebuah network,subnet dan host untuk action dalam menfilter nya hanya terdapat deny(dilarang)dan permit(dibolehkan),dan juga standard access-list ini akan dikonfigurasikan pada router yang terdekat dengan destination
* **Extended access-list :**extended access-list hampir sama dengan standard access-list,hanya saja yang membedakan pada ACL extended ini memiliki fitur yang lebih banyak,untuk konfigurasi ACL extended ini kalian tidak perlu mengkonfigurasi router yang terdekat dengan destination.pada extended ACL ini dia dapat menfilter source ataupun destination dan port ataupun protocol-protocol.

**STANDARD ACCESS-LIST**



Kita dapat melihat tpologi diatas,disitu terdapat 1switch,2router,1server,dan 2 client.

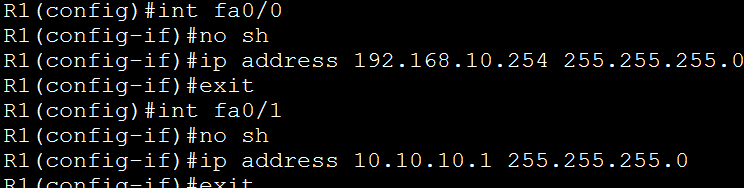
Tujuan pada lab kali ini kita akan memblov=ck network 192.168.10.0 agar tidak dapat terhubung dengan network server yaitu 20.20.20.0,tetapi network 10.10.10.0 masih bisa terhubung ke server,maka kita akan menggunakan ACL standard.

Sebelum kita masuk kedalam konfigurasi ACL standard,kita harus memasukan IP addres di setiap interfacenya,dan kita harus trunk dari switch ke router.

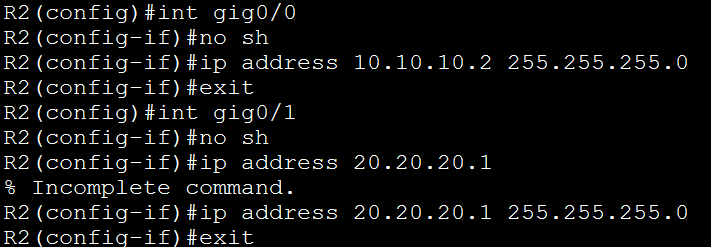
**SW1**



**R1**

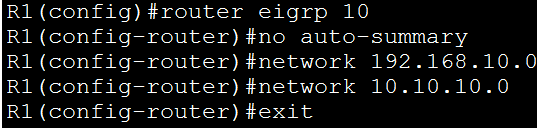


**R2**

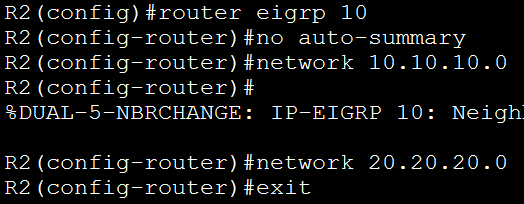


Tadi kita sudah menambahkan IP address kedala interface masing masing router,dan sekarang kita harus menggunakan routing protocol untuk menyambungkan semua router yang ada,kita memakai routing protocol EIGRP agar lebih mudah.

**R1**



**R2**



Sekarang semua router sudah terhubung oleh routing protocol EIGRP,maka kita dapat langsung konfigurasi ACL standard,kita konfigurasi ACL standard pada router yang terdekat dengan destination.

Sebelum kalian mulai,pastikan client-client di switch sudah dapat ping ke server.

Di lab ini destination kita adalah network 20.20.20.0 maka kita akan mengkonfigurasikan di R2 dan memberinya interface yang mengarah ke server yaitu out,dan apabila source(client)dari network 192.168.10.0

**Konfigurasi ACL pada R2 :**

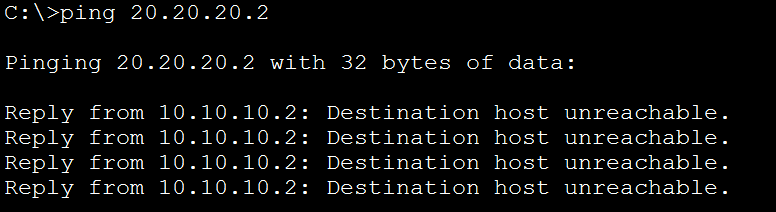


Kita sudah membuat ACL maka ACL tersebut harus kita masukan pada interface nya yang terdekat pada destination R2,di interface gig0/1 kita konfigurasikan out.



Kita sudah membuat ACL dan memasukan pada interfacenya yang terdekat dengan konfigurasi OUT,untuk membuktikan kalau ACL berhasil,masri kita ping dari client menuju ke server.

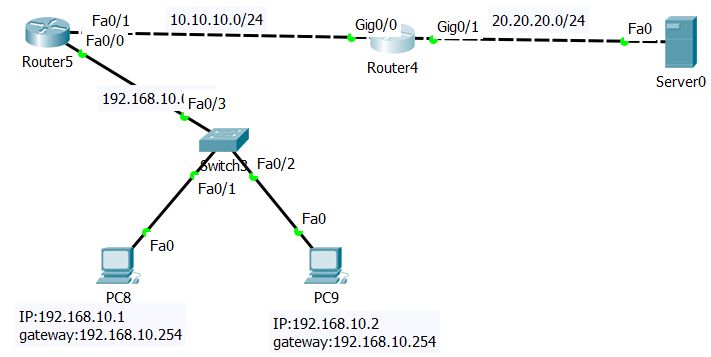
**Client menuju ke server :**



Hasilnya adalah unreachable,artinya ACL yang kita konfigurasikan untuk memblock network 192.168.10.0 sudah berhasil.

**EXTENDED ACCESS-LIST**

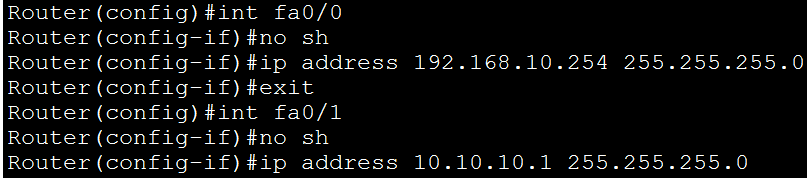
Pada lab sebelumnya kita sudah menjelaskan tentang ACL standard,sekarang kita akan membahas tentang ACL extended,yang mana perbedaannya yaitu dia memiliki fitur yang lebih mendalam dari pada ACL standard,di standard ACL kita hanya dapat menfilter yang berasal dari source saja,maka pada extended ini kita akan menfilter seperti destination.



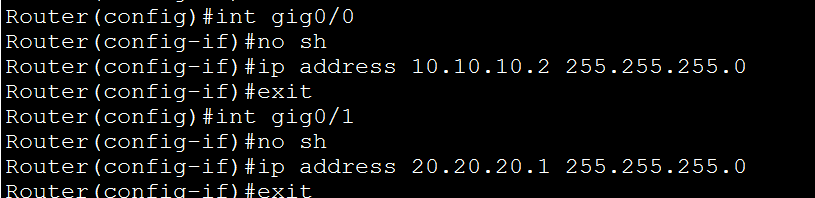
Kita akan menggunakan topologi yang terdapat di ACL standard,kali ini kita akan menfilter satu client dengan IP 192.168.10.1 agar tidak dapat melukukan PING ke server,dan untuk client IP 192.168.10.2 kita akan menfilter agar tidak dapat mengakses http.

Sebelum kita masuk kedalam konfigurasi ACL extended,kita harus konfogirasi ip address di setiap interface masing-masing,sesuai dengan topologi.

**R1**

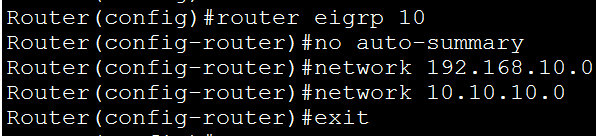


**R2**

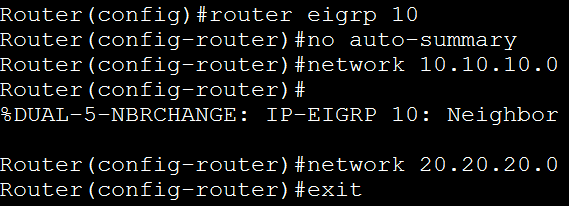


Setelah kita sudah mamberikan IP address kepada setiap interface,sekarang kita masukan konfigurasi EIGRP untuk menyambungkan router yang lainnya.

**R1**



**R2**



Kita sudah memasukan konfigurasi EIGRP,sekarang kita masuk kedalam konfigurasi ACL extended.kita akan memulai untuk client dengan IP 192.168.10.1 agar tidak dapat PING ke server dan client dengan IP 192.168.10.2 kita akan menfilter agar ia tidak dapat membuka http.

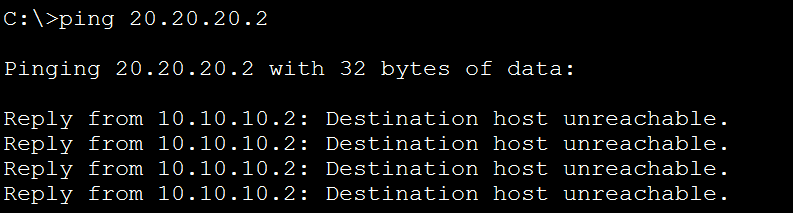


Seperti biasa,kalau kita sudah konfigurasi ACL kita harus tanamkan konfigurasi ACL ke dalam interface.

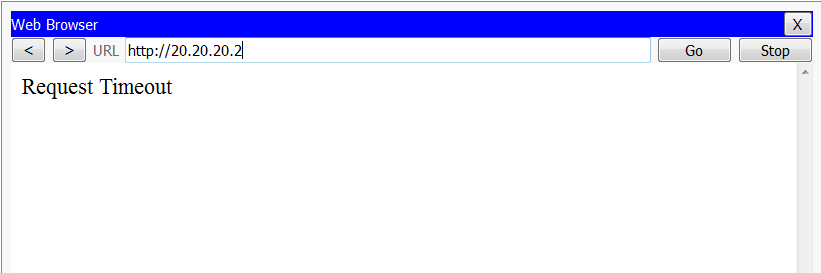


Sekarang kita akan mencoba untuk client dengan IP 192.168.10.1 untuk ping menuju ke server dan client dengan IP 192.168.10.2 pastikan dia tidak dapat mengakses http.

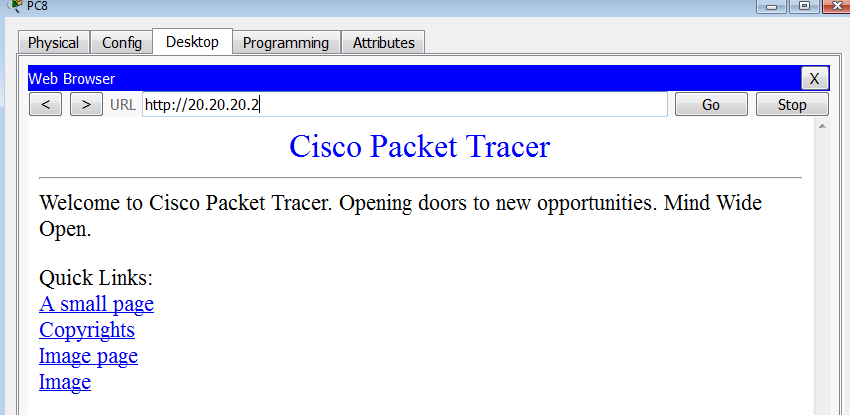
Client 192.168.10.1



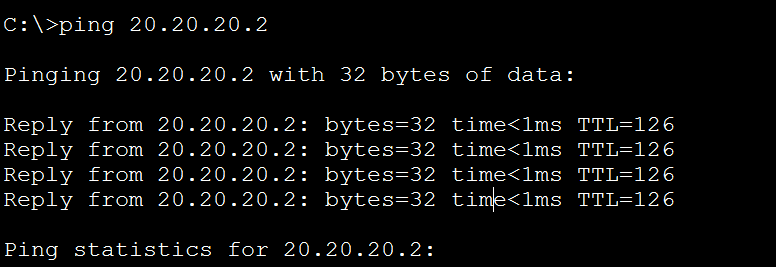
Client 192.168.10.2



client 192.168.10.1 tidak dapat mengakses internet,sekarang kita coba apakah dia dapat mengakses http :



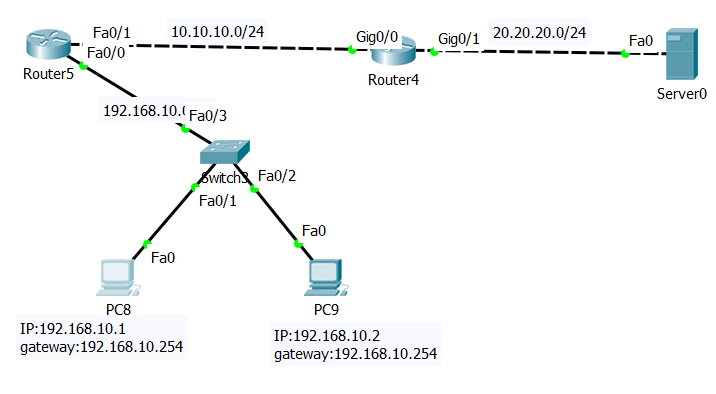
Tadi kita menfilter client 192.168.10.2 untuk tidak dapat mengakses internet,sekarang kita coba apakah client dengan IP 192.168.10.2 dapat PING menuju ke server. :



**NAMED ACCESS-LIST**

Di pembahasan ini kita akan mengkonfigurasikan ACL dengan menggunakan nama,yang mana pada lab kita kali ini kita dapat menentukan sequenece number atau dalam kata lain kita dapat mencutome urutan rule kita sendiri

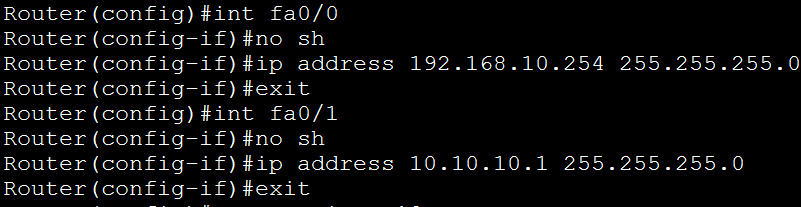
Kita akan menggunakan topologi seperti yang terdapat pada ACL sebelumnya.



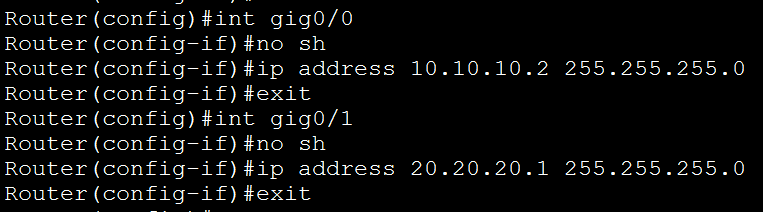
Kita akan konfigurasi ACL dengan menggunakan name,kita akan mendeny client1 dengan IP 192.168.10.1 deny ICMP dan client2 deny 192.168.10.2 deny http dan https.

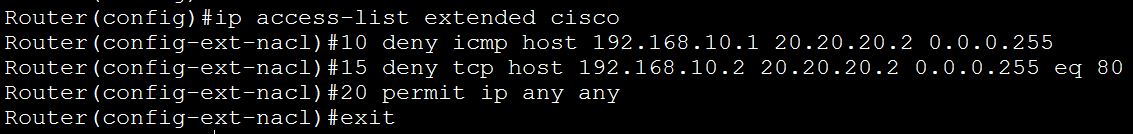
Sebelumnya kita dapat mengkonfigurasi kan pada interface di router.

R1



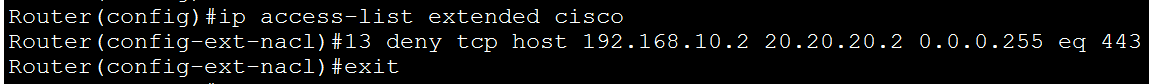
R2

 sekarang kita akan mendeny ICMP untuk client1 dan http untuk client2 kemudian permit any.



Ok,kita sudah konfigurasi ACL dengan konfigurasi ICMP(ping),http,dan permit any,tetapi kita belum konfigurasi deny untuk https

Sekarang kita akan menyisipkan rule diantara sequence 10 dan 15 untuk deny https.

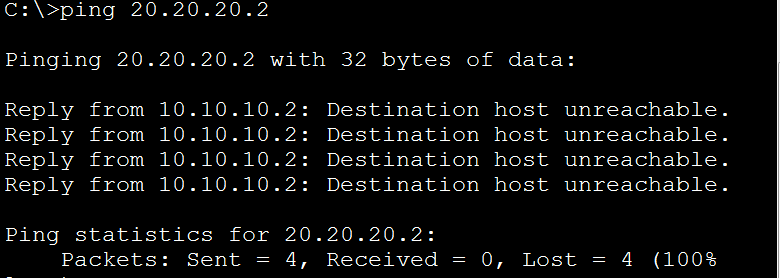


Dan jangan lupa,sesudah kita konfigurasi ACL kita harus tanamkan ACL di dalam interface dalam router.

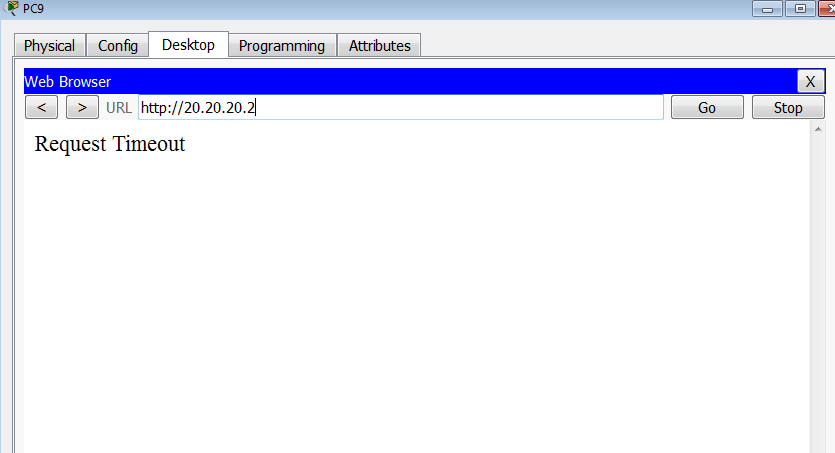


Untuk vertifikasi dapat di lakukan denga test ping dari client1 dan aksess http dan https pada client2.

Client1



client 2



**NAT(network address translation)**

NAT adalah sebuah metode yang membuat ip private menjadi ip publikKenapa Harus diubah Menjadi IP Publik? karena IP Private tidak bisa mengakses internet.

Dalam konfigurasi NAT interface,dibagi menjadi 2 kategori :

* **Inside :** traffic yang masuk ke interface yang berasal dari network
* **Outside :** traffic yang berasal dari interface yang menuju ke destination (internet)

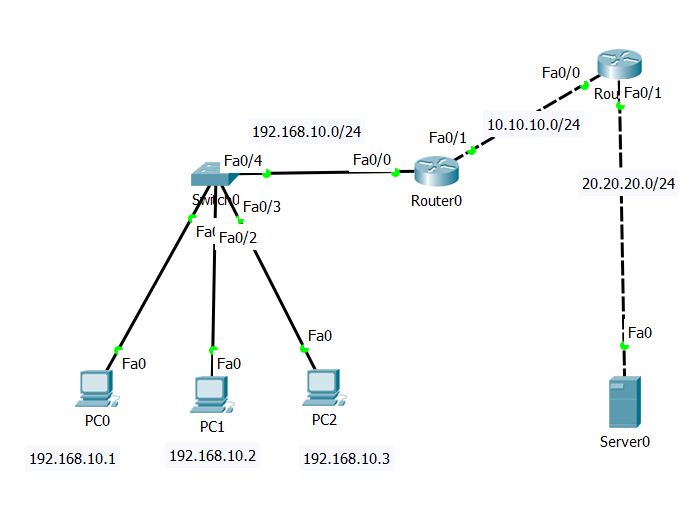
NAT dibagi menjadi beberapa tipe yaitu :

* **Static NAT :** sebuah metode NAT yang mengubah IP private ke IP publik secara manual,dalam static NAT ini IPnya harus sama jumlahnya,yang dimaksud adalah jika kita mempunyai 1IP publik maka yang dapat mengakses internet hanya 1IP private.
* **Dynamic NAT :** dynamic NAT ini samaj saja sepertin static NAT,hanya saja dynamic NAT ini bersifat otomatis,tetapi sayangnya dynamic NAT ini sifatnya sama saja sepertin static NAT,yaitu IP publik yang kita miliki harus sama dengan IP private yang kita miliki.
* **Overloading/PAT(port address translation) :** metode overloading/PAT ini paling sering digunakan,kenapa sering digunakan?dikarenakan metode ini sangat besar keuntungannya,dalam metode sebelumnya seperti static dan dynamic dia harus memiliki IP publik dan private yang sama jumlahnya,teknologi overloading ini kalian bisa menggunakan 1IP publik untuk banyak IP private(berapapun jumlah IP rivate tersebut)kalian mau buat IP rivate 100 atau lebih kalian bisa menggunakannya.

**STATIC NAT**

sebuah metode NAT yang mengubah IP private ke IP publik secara manual,dalam static NAT ini IPnya harus sama jumlahnya,yang dimaksud adalah jika kita mempunyai 1IP publik maka yang dapat mengakses internet hanya 1IP private.

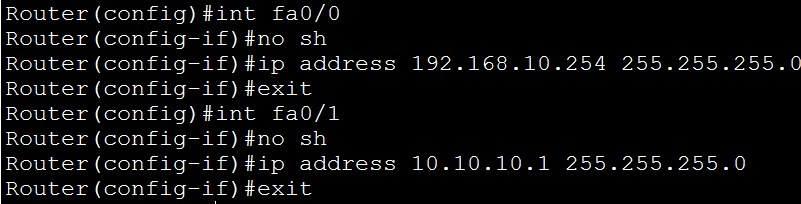
Langkah pertama yang harus dilakukan adalah kalian harus ACL terlebih dahulu untuk menandai IP rivate yang akan kita translasikan menjadi IP pubik.

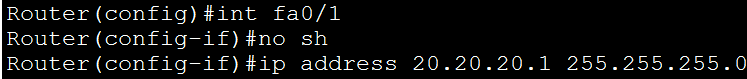
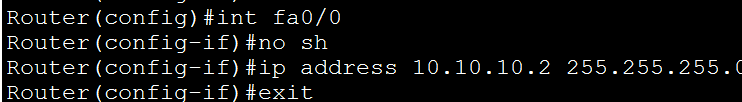


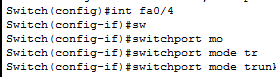
Kita akan menggunakan 2 router,1 switch,dan 3 client,yang mana kita akan mengizinkan clien denga IP 192.168.10.2 agar terhubung ke internet,dan kita akan membuat router dan server seolah-olah menjadi internet.

Pertama kita masukan terlebih dahulu IP address di setiap interface yang ada di router,dan kita trunk switch yang interfacenya menuju ke router.

**R1**



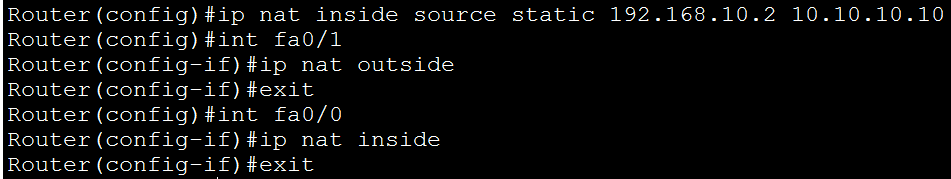
**R2**

**SW1**

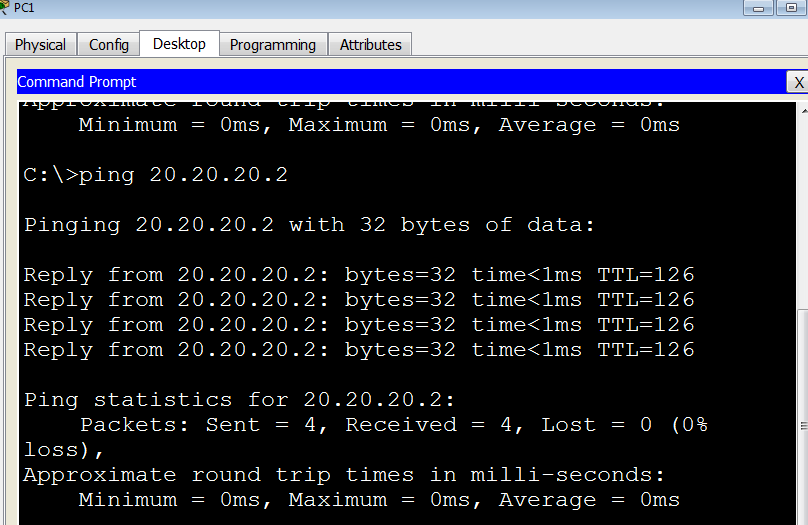
Lalu selanjutnya kita akan konfigurasi default router pada R1



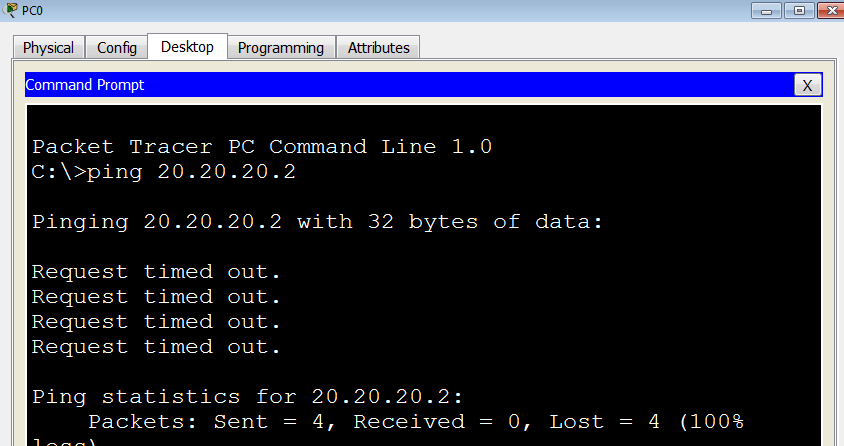
Sekarang kita masuk kedalam konfigurasi NAT :



Jika sudah kita NAT mari kita cek dengan menggunkan PING dari client yang kita izinkan untuk akses internet.



Kita bisa lihat,client yang kita izinkan sudah bisa mengakses internet,dan bagaimana dengan client yang lain,mari kita cek :

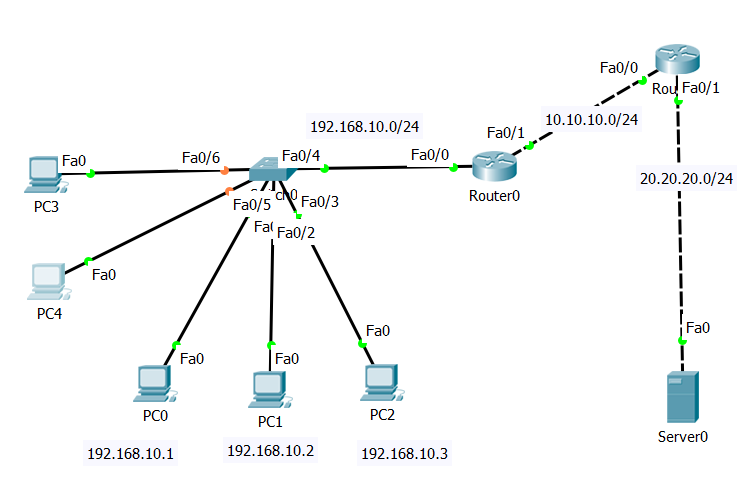


dan hasilnya adalah RTO,mengapa?dikarenakan client tersebut tidak diizinkan untuk mengakses internet.

**NAT OVERLOAD/PAT**

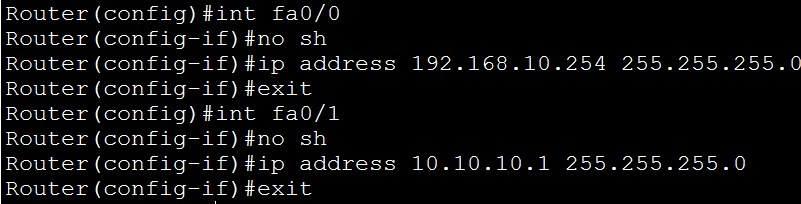
Di lab sebelumnya kita telah mengkonfigurasikan NAT static,apa bila kada beberapa PC maka kita haru NAT semua PC yang ada atau 1 by 1,kalau dengan memakai cara static apa bila ada banyak sekali PC itu tidak efisien,maka sekarang kita akan membahas konfigurasi oveload/PAT.

Kita akan menggunakan topologi seperti static,tetapi kita akan tambah PC nya.

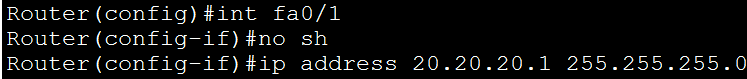
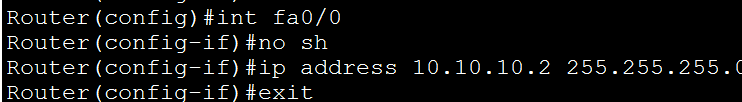


Kita masukan terlebih dahulu IP kepada interface masing-masing di router.

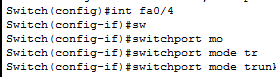
**R1**



**R2**



**SW1**



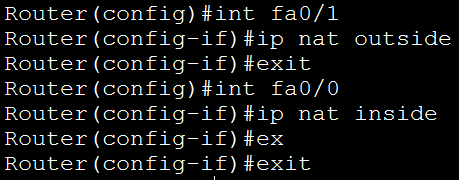
Setelah kita memasukan IP address dan membuat trunk,disini kita akan menggunakan ACL terlebih dahulu untuk source pada NAT nya dengan ACL permit any.



Lalu kita konfigurasikan NAT overload,dengan memasukan ACL yang telah kita buat pada source list.



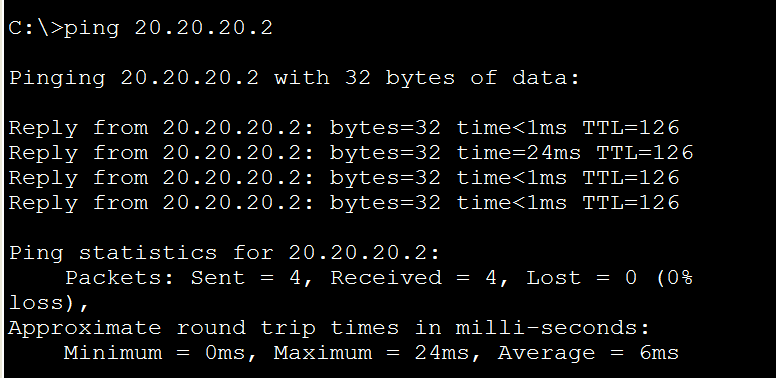
Lalu kita dapat konfigurasikan untuk NAT inside dan outside pada setiap interfacenya.



Kita telah konfigurasikan NAT,selanjutnya kita harus default route menuju internet dengan menggunakan IP route dengan gateway IP mengarah ke internet.



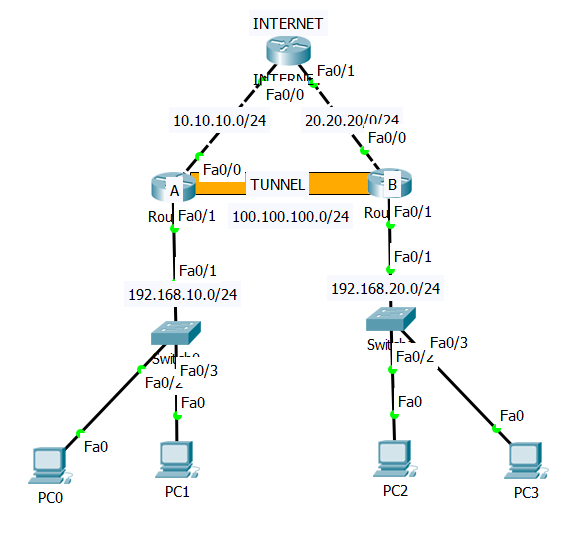
Setelah kita default route,mari kita PING di salah satu client apakah bisa atau tidak.



**TUNNEL GRE**

Tunnel merupakan salah satu cara pengiriman data melalui jalur tersendiri/private yang dapat kita buat dalam internet.agar suatu paket dapat terkirim walau jarak lingkupnya jauh,kalau kita memakai kabel itu tidak efisien dan memakan banyak uang.maka itulah terbentuk namanya teknologi tunnel yang mana tunnel itu dapat mengirim data tanpa menggunakan kabel,tunnel dapat diartikan seakan-akan ada terowongan yang menyambung antar kantor tersebut.

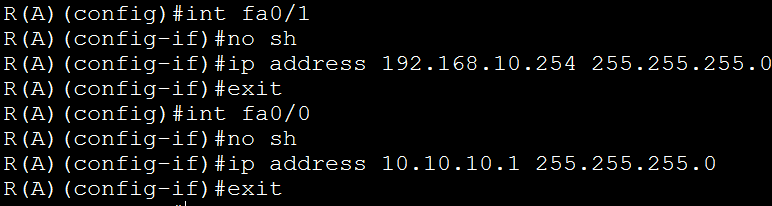
sekarang saya akan membuat topologi tunnel seperti berikut :

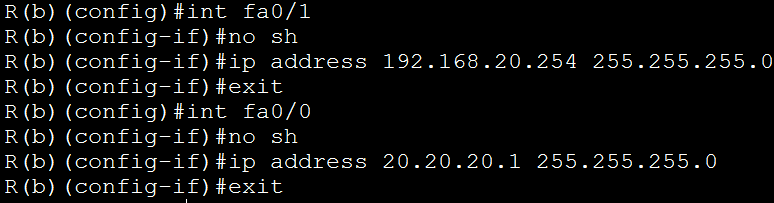


Didalam topologi diatas kita akan menghubungkan 2 router yaitu routerA dan routerB agar dapat terhubung melewati network 100.100.100.0 bukan melewati 10.10.10.0

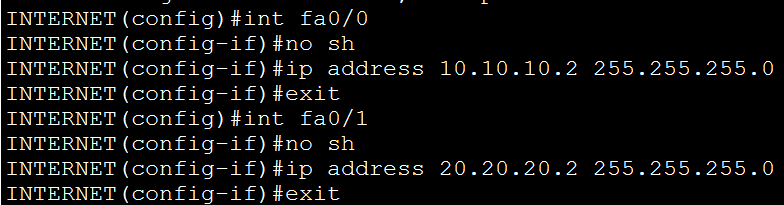
Sebelum kita mengkonfigurasi tunel,seperti biasa yang kita lakukan pada router,yaitu memberikan IP address pada setiap interface yang ada pada router.

**R(A)**

**R(B)**



**INTERNET**



Sekarang yang harus kalian lakukan adalah pastika kedua router bisa saling berkomunikasi dengan IP publiknya,setting default router di R(A) dan R(B).

**R(A)**

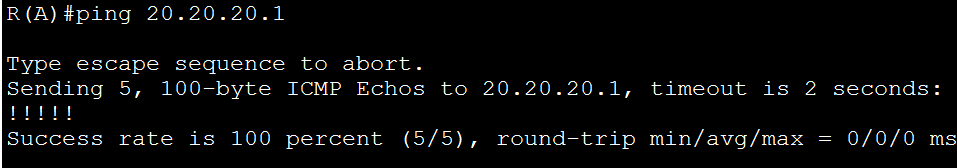


**R(B)**

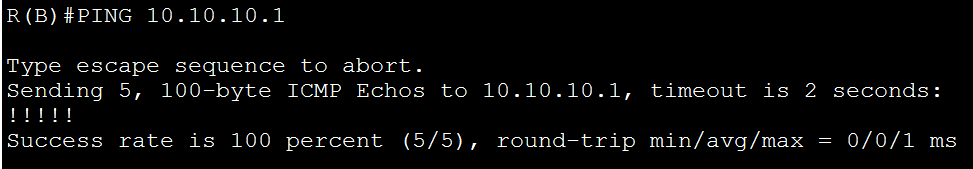


Sekarang kalian dapat pastikan kalau kedua router dapat berkomunikasi dengan IP publiknya.

**R(A)**

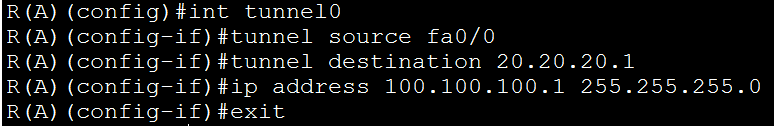


**R(B)**

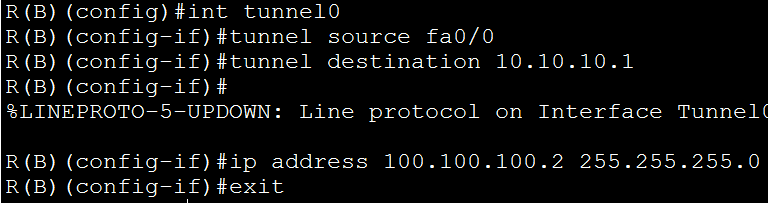


Sekarang kita akan masuk ke konfigurasi tunnel :

**R(A)**

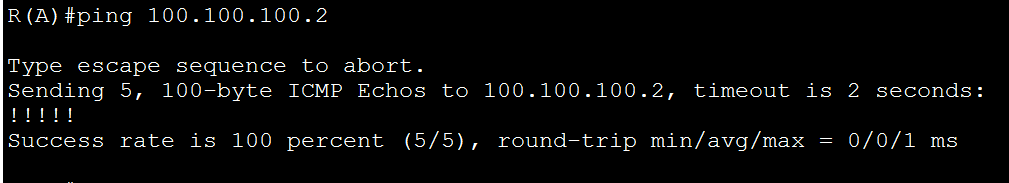


**R(B)**

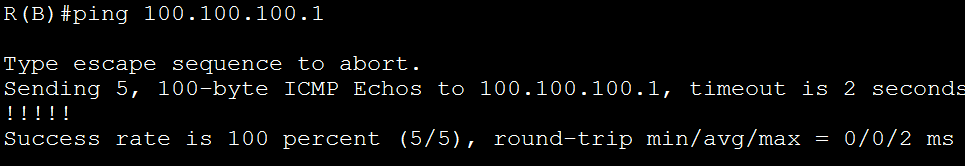


Jika sudah kalian tunnel,mari kita tes ping router-routernya dengan PING tunnel lawannya.

**R(A)**



**R(B)**



Sekarang kalian harus menyambungkan kedua HOST menggunakan routing protocol,kita akan menggunakan routing protocol static,tetapi jalur terdekatnya(nexthop)adalah ip address yang kita buat untuk tunnel.

**R(A)**



**R(B)**

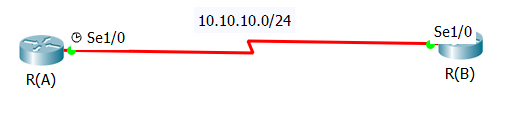


**PPP(point-to-point protocol)**

ppp adalah merupakan suatu WAN protocol selain HDLC (default cisco proprietary) dan frame relay,ppp sifatnya open standar sehingga bisa dipakai di banyak vendor.dan juga ppp merupakan protocol yang digunakan untuk mengoneksikan antar dua perangkat jaringan yang jauh/luar negri,kenapa ada PPP dikarenakan kalau kita menyambungkan dua perangkat yang jauh apa bila kita memakai kabel itu sangat tidak efisien dan membutuhkan biaya sangat besar.maka dari itu terbentuklah teknologi PPP

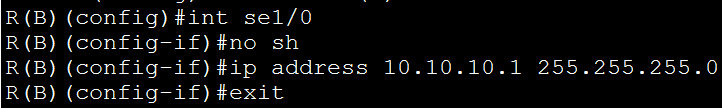
* PAP(tidak terenkripsi)
* CHAP(terenkripsi)

Berikut topologi untuk PPP :

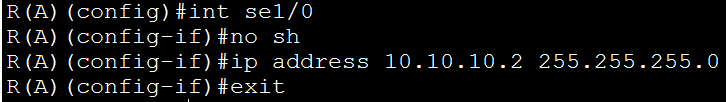


Pertaman kita masukan IP address di setiap interface yang ada pada router.

**R(A)**

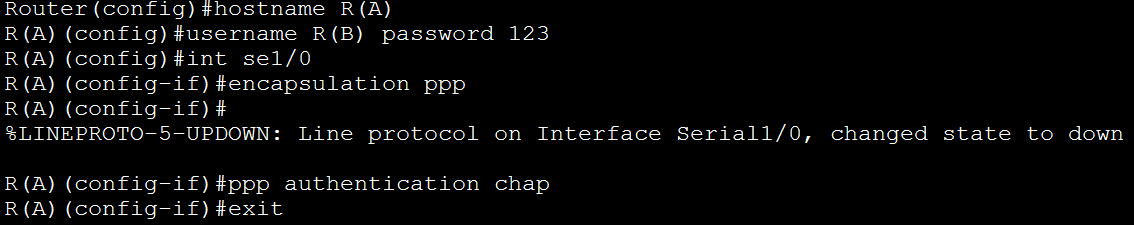


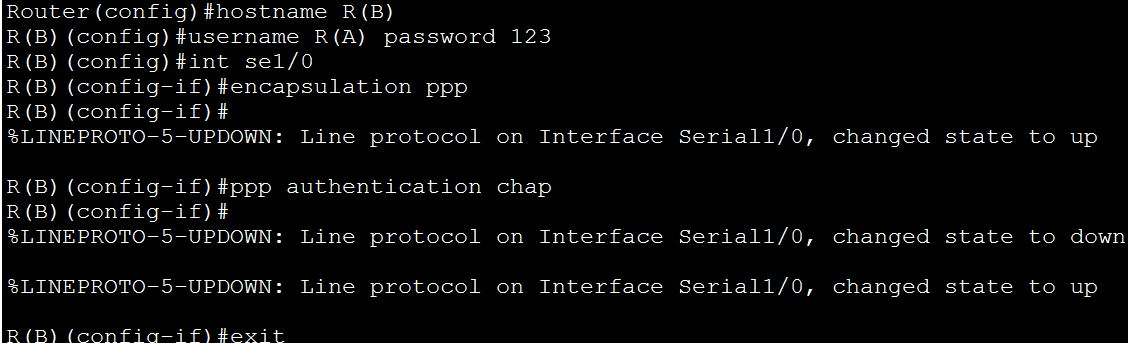
**R(B)**



Setelah kita masukan IP address,kita akan masuk kedalam konfigurasi PPP,didalam PPP kita bernegosiasi dengan perusahaan otomatis kita harus mengetahui satu sama lain.

**R(A)**

**R(B)**



Itulah contoh konfigurasi PPP,kunci dari konfigurasi PPP ini adalah?kita jika kita ingin bekerja sama kita harus bernegosiasi dengan cara mengenal satu sama lain.

**HIGH AVAIBILITY**

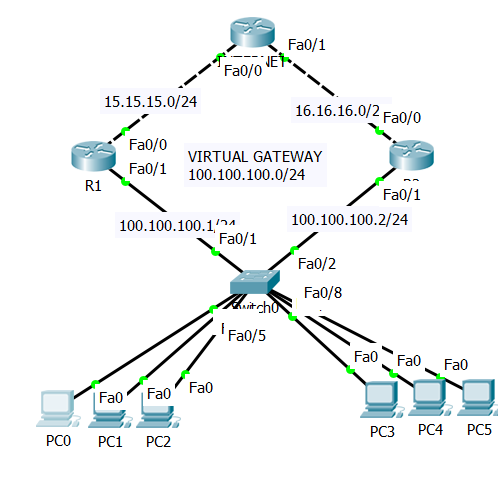
High avaibility ini adalah suatu metode apa bila dikantor kita ada salah satu router yang mati otomatis semua pc yang terhubung akan mati/tidak dapat internetan,high avaibility ini kita akan backup link ke internet,yang artinya kita akan mempunyai 2 buah gateway untuk ke internet.dengan high avaibility,ini kita dapat membuat seolah-olah terdapat IP gateway,sehingga walaupun salah satu gateway down,pc client akan tetap internetan.

High avaibility ini terbagi menjadi 3,yaitu :

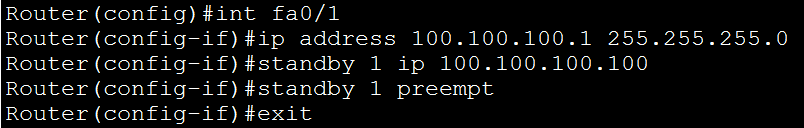
* HSRP(cisco proprietary)
* VRRP(open standard)
* GLBP(cisco proprietary)

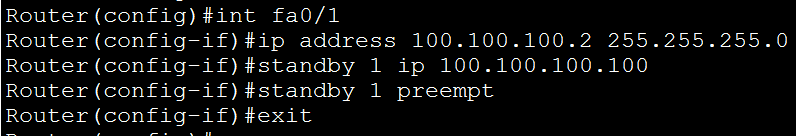
**HSRP**

HSRP ini termasuk dari cisco proprietary,HSRP berfungsi untuk jika ada salah satu gateway yang mati maka client yang terhubung dengan gateway tersebut akan berpindah jalur ke gateway sebelahnya.HSRP ini adalah file-over yaitu,dia menggunakan satu jalur untuk menjadi jalur utama gateway dan gateway sebelahnya akan menjadi back up.



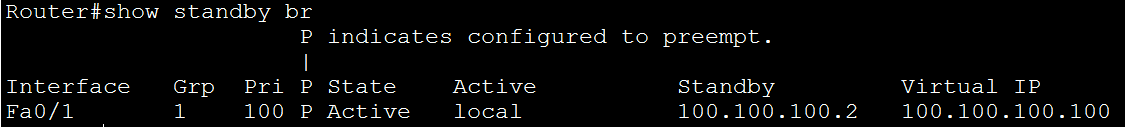
**R1**



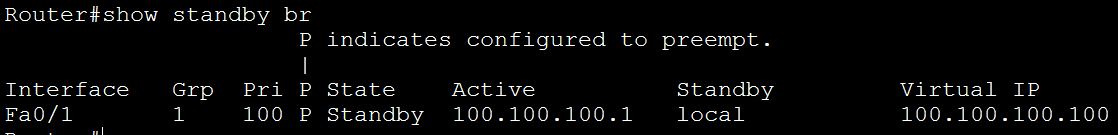
**R2**

Untuk verifikasi :

**R1**

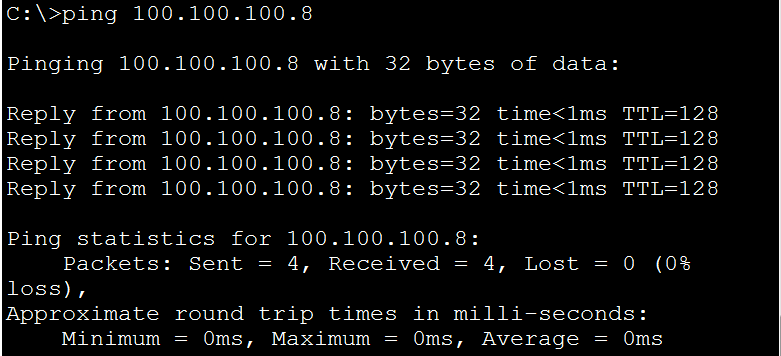


**R2**



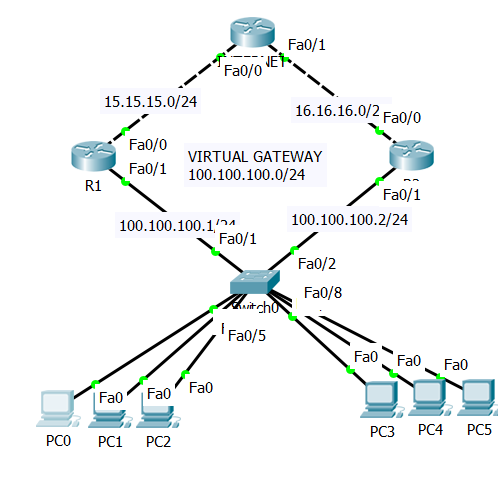
Dan sekarang kita akan test ping :

Pc 1 menuju pc 5:



**VRRP**

VRRP adalah termasuk open standar(bebas vendor)VRRP ini funsinya sama dengan HRRP.VRRP ini termasuk kedalam file-over



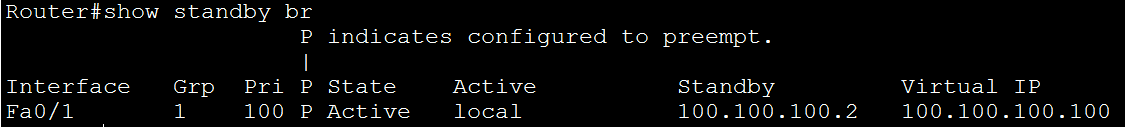
Dikarenakan VRRP ini tidak support kepada cisco packet tracer,saya disini hanya akan menampilkan konfigurasinya,sebenarnya sama saja konfigurasinya hanya saja,didalam konfigurasi VRRP dia menggunakan konfigurasi sebagai berikut :

R1(config)#int fa0/1

R1(config-if)#vrrp 1 ip 100.100.100.100

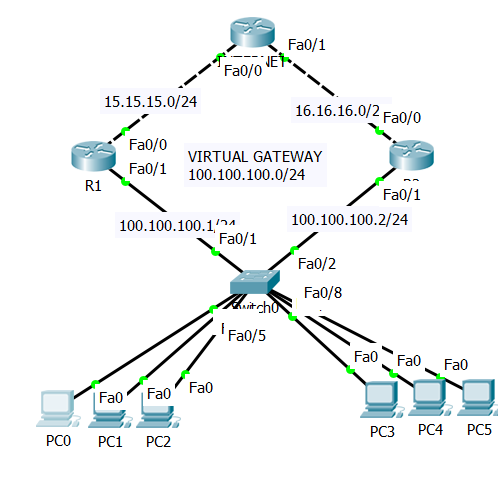
R1(config-if)#vrrp 1 preempt

Hanya itu saja perbedaannya,dan untuk verifikasi dengan command *‘’show stanby brief’’.*



**GLBP**

GLBP ini merupakan cisco proprietary,protocol ini berbeda dengan HRRP dan VRRP,perbedaan dari GLBP ini adalah kedua jalur gateway protocol ini adalah jalur utama dan juga jalur backup



dari GLBP ini hanya konfigurasinya yang sedikit berbeda,seperti contoh berikut ini :

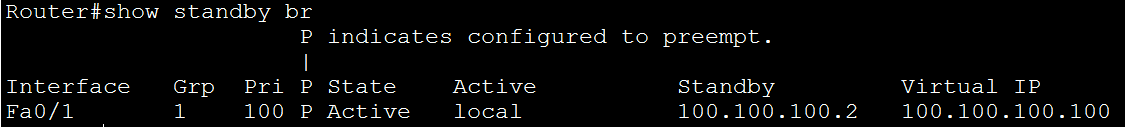
R1(config)#int fa0/1

R1(config-if)#ip address 100.100.100.1 255.255.255.0

R1(config-if)#glbp 1 ip 100.100.100.100

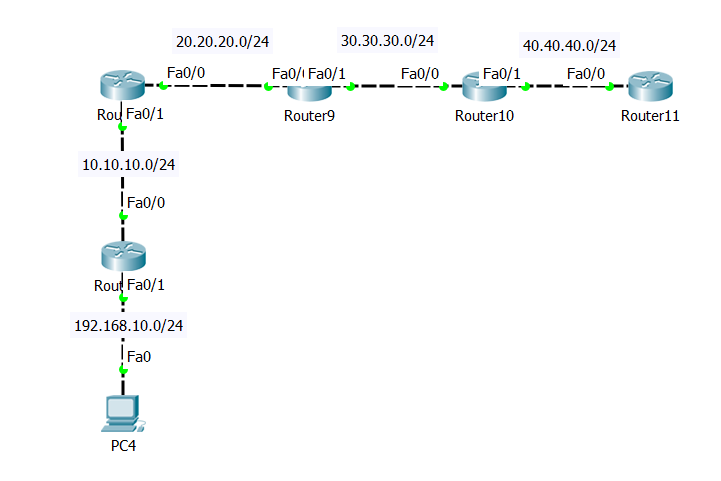
R1(config-if)#glbp 1 preempt

Untuk verifikasi sama saja seperti protocol yang lainnya *‘’show standby brief’’* :



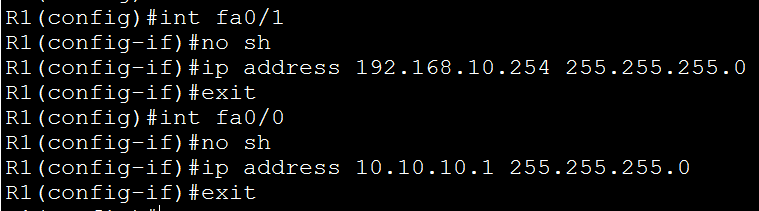
**3.14DHCP RELAY**

DHCP relay yaitu sebuah metode yang mana kita memberikan IP kepada client denga yang berbeda segment,langsung saja kita masuk menuju kekonfigurasi DHCP relay.

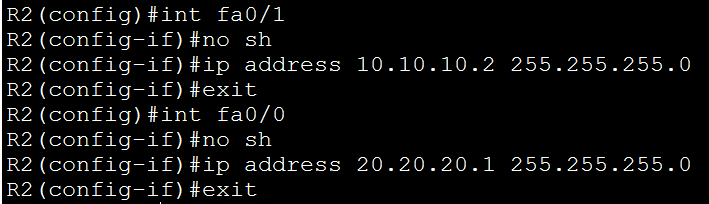


Masukan ip address disetiap interface yang ada pada router.

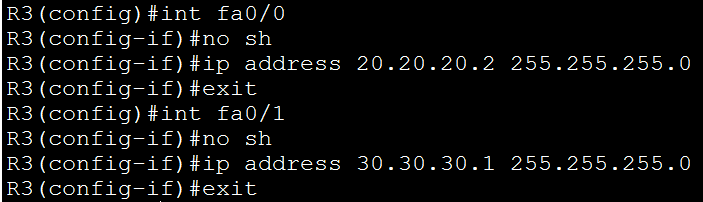
**R1**



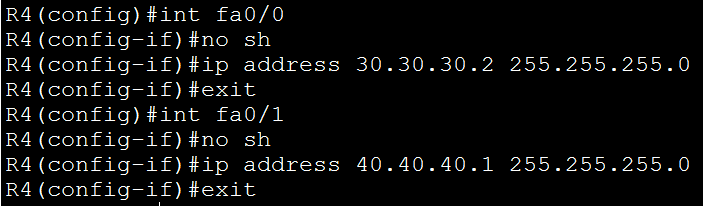
**R2**



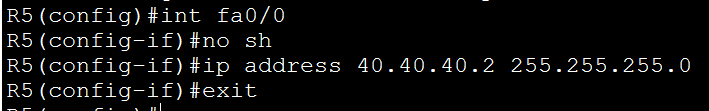
**R3**



**R4**

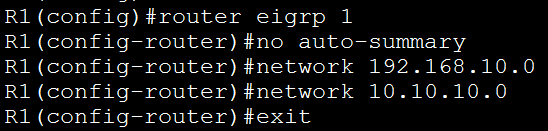


**R5**

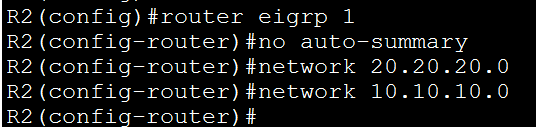


Jika sudah kalian masukan ip address,sekarang kalian harus mengubungkan semua router yang ada pada topologi menggunakan routing protocol,kita akan menggunakan routing protocol EIGRP.

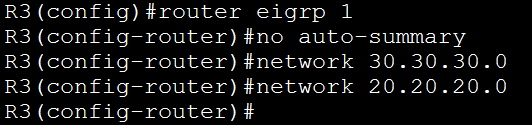
**R1**



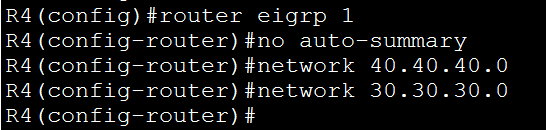
**R2**



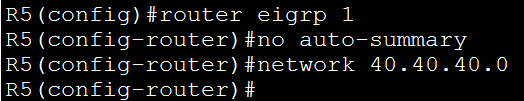
**R3**



**R4**

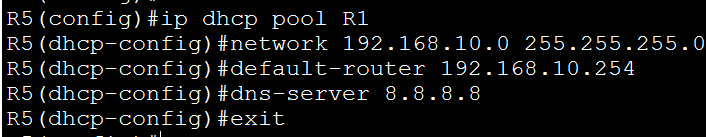


**R5**



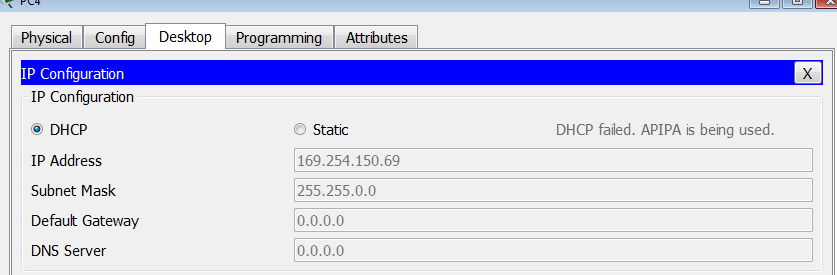
Tadi kita sudah memasukan routing protocol EIGRP,maka sekarang kita masuk kekonfigurasi DHCP relay,kita akan konfigurasi DHCP relay di router 5,karena dia juga berbeda segment.

**R5**

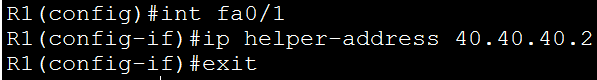


Sekarang mari kita coba,apakah client mendapatkan ip yang kita DHCP.

Client :

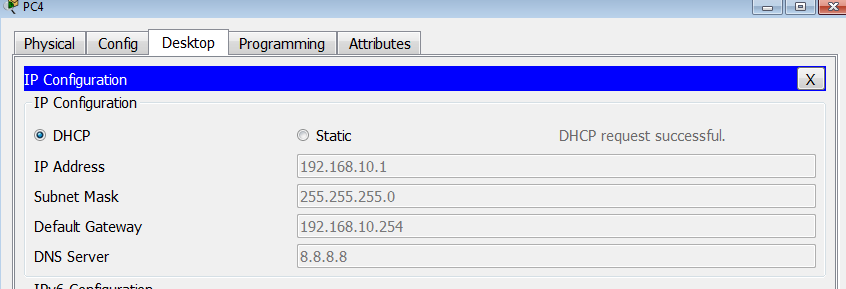


Bisa kalian lihat hasilnya adalah APIPA,mengapa?karena kita membutuhkan bantuan dari interface router terdekatnya,mari kita coba :



Kita hanya menulis commandI’’*ip helper-address(pengirim DHCP)’’pengirim DHCP dengan IP 40.40.40.2 atau di router terakhir seperti topologi diatas,sekarang mari kita coba apakah sudah bisa :*

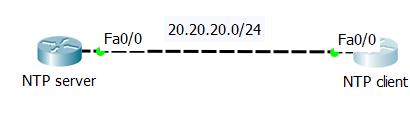
*Client :*



Dan hasilnya successfull,begitulah konfigurasi DHCP relay.

**3.15NTP**

NTP(network time protocol)adalah sebuah protocol yang digunakan untuk mensinkronasikan waktu antara 2 device.NTP server yaitu dia yang memberikan layanan singkronasi waktu.dan NTP client adalah perangkat yang melakukan peer ke NTP server.



Langsung saja kita masuk kedalam konfigurasi NTP.

* Konfigurasi NTPserver :

R1#clock set 09:00:00 18 marc 2018

R1#show clock

R1(config)#ntp master

R1(config)#int fa0/0

R1(config-if)#no sh

R1(config-if)#ip address 20.20.20.1 255.255.255.0

* Konfigurasi NTPclient :

R2(config)#int fa0/0

R2(config-if)#no sh

R2(config-if)#ip address 20.20.20.2 255.255.255.0

R2(config)#ntp server 20.20.20.1

* Untuk vertifikasi :

R1#show clock