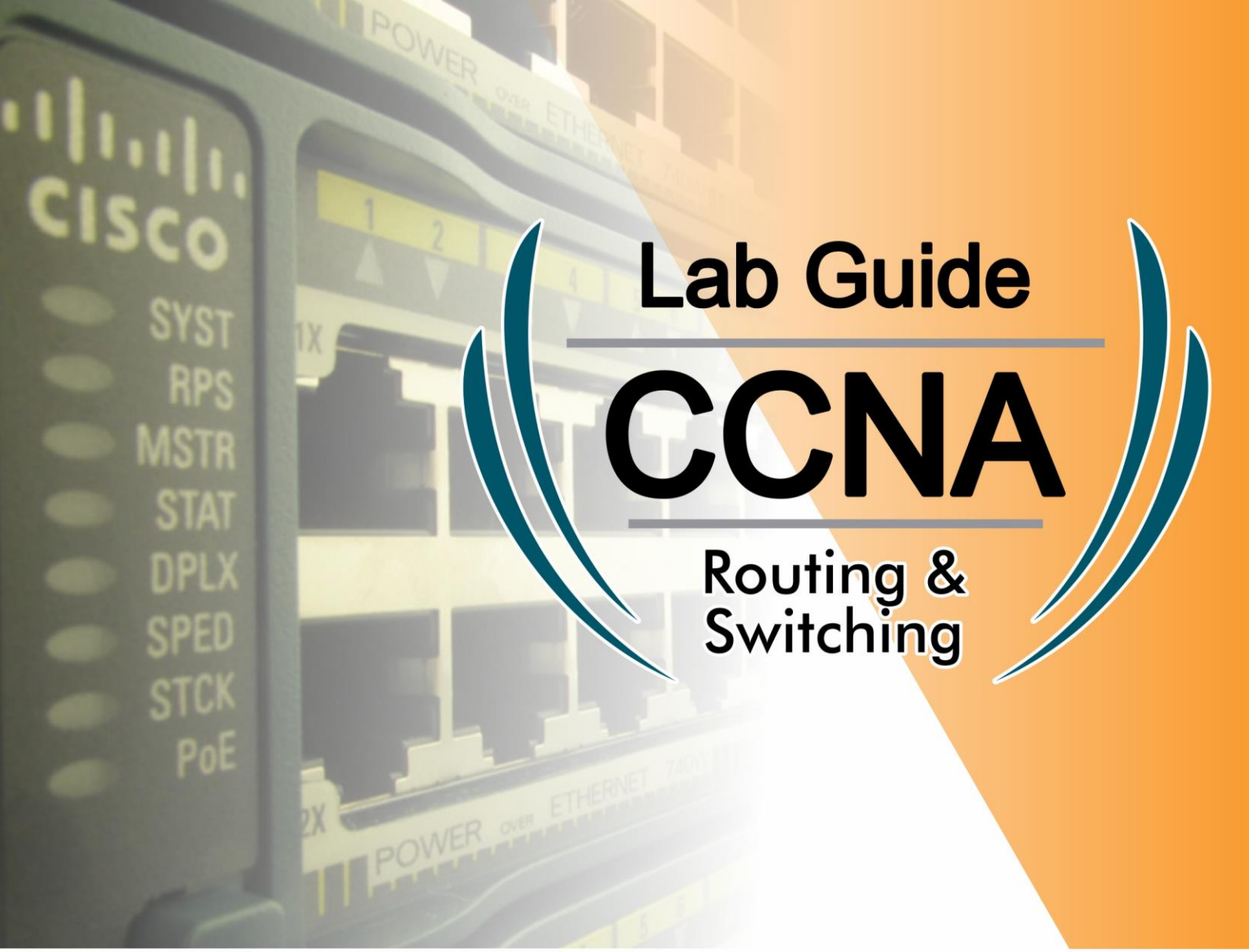



# Lab Guide

# CCNA

## Routing & Switching

Muhammad Zaky Nur Fuadi

Pondok Timur Indah
Jl. Intan Blok I no 95

+62 8131 4281 605

visit my blog https://www.aytindeso.wordpress.com

# KATA PENGANTAR

بسم الله الرحمن الرحيم

**Assalamu'alaikum Warokhmatullohi Wabarokaatuh..**

Segala puji bagi Allah SWT yang telah memberikan karunia serta ribuan nikmatnya untuk kita semua, sehingga sampai saat ini kita semua masih bisa beraktivitas sebagai mana mestinya dan tentunya sesuai dengan petunjuk Allah SWT.

Penulis mengucapkan rasa syukur yang sedalam-dalamnya karna telah menyelesaikan modul "Lab Guide materi CCNA" ini. Rasa terima kasih juga penulis sampaikan kepada teman-teman yang sudah bersedia sharing materi yang di susun dalam buku ini.

Special thanks to IDN atas ilmu yang sudah diberikan kepada penulis, sehingga penulis lebih terbuka lagi dalam wawasan/ilmu networking yang sebenarnya. Dan semoga dengan adanya buku/modul ini bisa membantu belajar teman-teman yang membutuhkannya.

Penulis berharap semoga kelak buku/modul ini bisa bermanfaat bagi semua kalangan, baik pelajar, mahasiswa ataupun umum. Sehingga mereka yang belajar menggunakan buku ini bisa mengajarkan kembali kepada temannya.

Demikian kata pengantar singkat ini, semoga Allah ridhoi semua langkah dan niat baik kita dalam menyampaikan ilmu.

Bekasi, April 2017
Penulis,

**Muhammad Zaky Nur Fuadi**

*Remember me in your pray*

# NETWORK FUNDAMENTAL

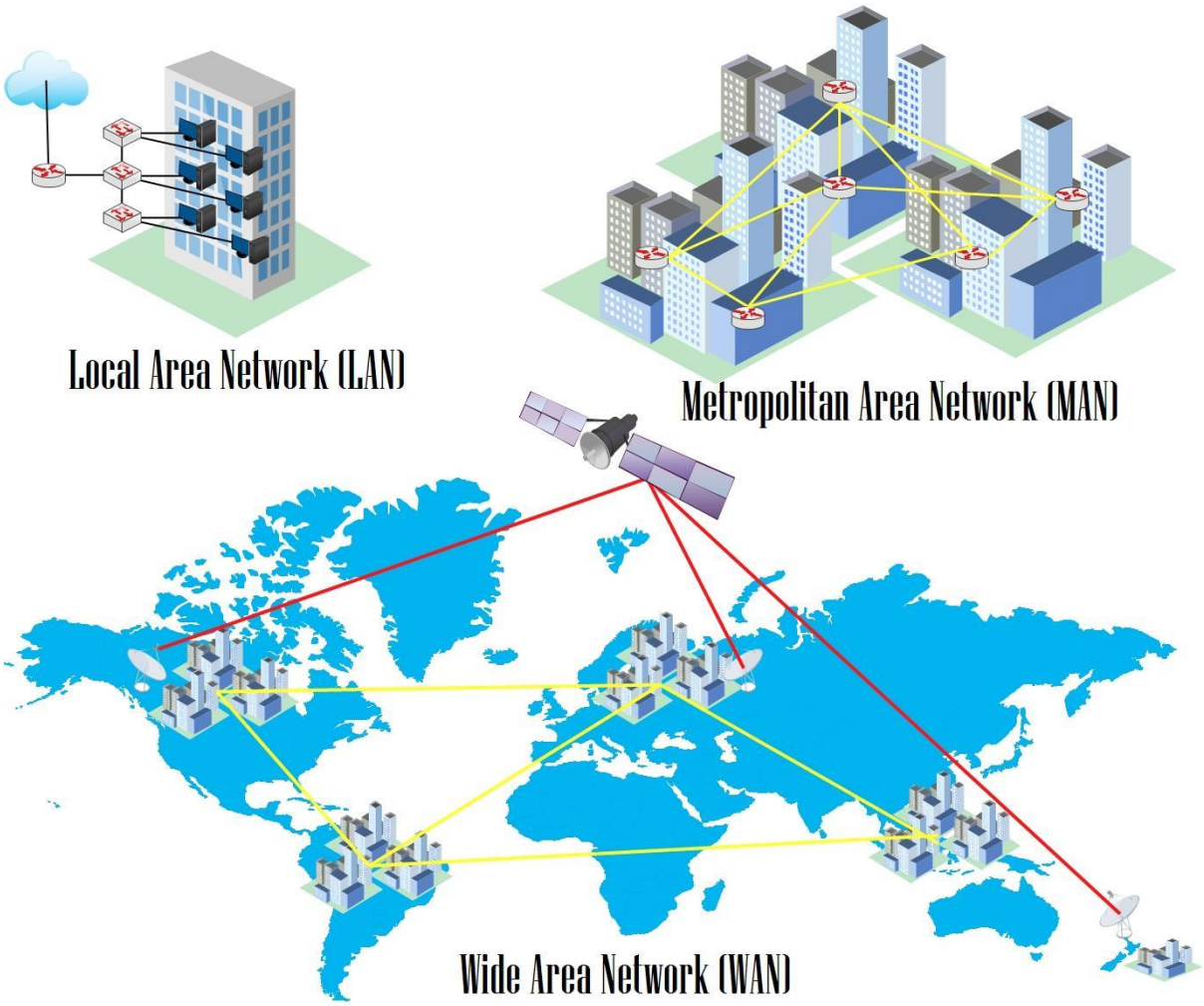
**Pengertian Jaringan Komputer**

Jaringan atau network adalah kumpulan perangkat jaringan (network devices) dan perangkat endhost (end devices) yang terhubung satu sama lain dan dapat melakukan sharing informasi serta resources.

Komponen pembentuk jaringan:

1. Network devices: hub, bridge, switch dan router.
2. End devices: PC, laptop, mobile, dll.
3. Interconnection: NIC, konektor, media (cooper, fiber optic, wireless, dll).

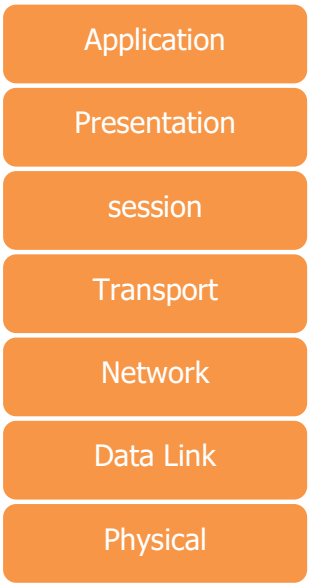
**Jaringan berdasarkan Area**



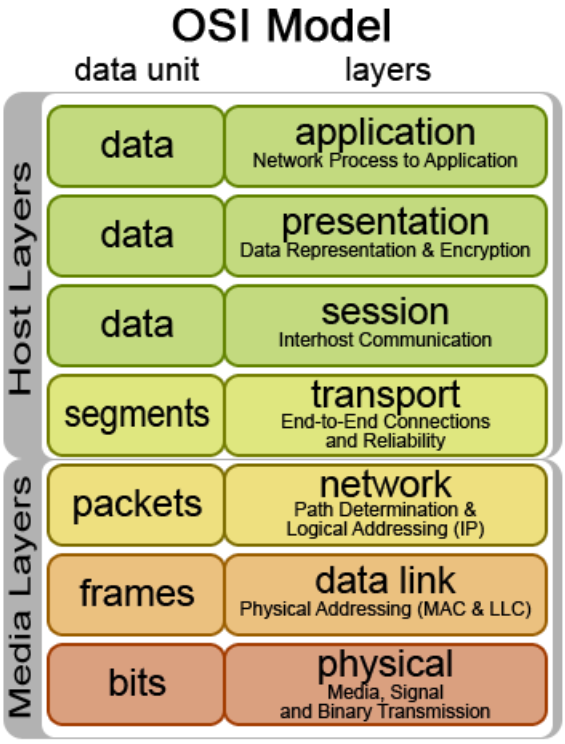
- Local Area Network (LAN) merupakan jaringan sederhana dalam satu gedung, kantor, rumah atau sekolah. Bisaanya menggunakan kabel UTP.
- Metropolitan Area Network (MAN) adalah gabungan dari banyak LAN dalam suatu wilayah.
- Wide Area Network (WAN) adalah jaringan yang menghubungkan banyak MAN antar pulau, negara atau benua. Medianya dapat berupa fiber optic dan satelit.

**Osi Layer**

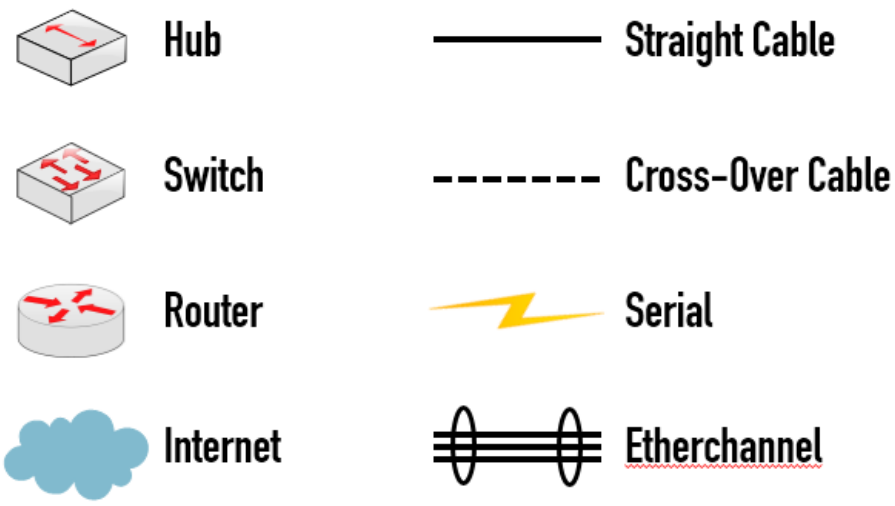
Adalah standar dalam perangkat jaringan yang membuat berbagai perangkat kompatibel satu sama lain. Ada 7 layer dalam OSI layer, dari bawah layer 1 physical sampai atas layer 7 application.




Seorang network engineer wajib memahami layer 1 sampai 4 untuk memahami fungsi dan cara kerja perangkat jaringan.




**Perangkat Jaringan dan Simbol**




*Remember me in your pray*

**Internat Service Provider**

1. ISP

   ISP (Internet Service Provider) adalah perusahaan atau badan usaha yang menjual koneksi internet atau sejenisnya kepada pelanggan. ISP awalnya sangat identik dengan jaringan telepon, karena dulu ISP menjual koneksi atau access internet melalui jaringan telepon. Seperti salah satunya adalah telkomnet instant dari Telkom.

   Sekarang, dengan perkembangan teknologi ISP itu berkembang tidak hanya dengan menggunakan jaringan telepon tapi juga menggunakan teknologi seperti fiber optic dan wireless. Di Bali, denpasar pada khususnya ISP dengan teknologi wireless paling banyaktumbuh.

   *Sumber : http://en.wikipedia.org/wiki/ISP*

   Karena teknologi ini "paling murah". Tidak perlu membangun jaringan kabel, mudah dipindahkan, tidak ada biaya ijin dan lain-lain.

   Lalu gimana sebenarnya kerja internet dengan adanya ISP ini? ISP terkoneksi satu sama lain dalam Internet Exchange, interkoneksi. Sebagian besar ISP memerlukan upstream. ISP yang tidak memiliki upstream disebut Tier1, tier1 hanya memiliki pelanggan dan interkoneksi.

2. Prosedur berlangganan

   Pelanggan yang berlangganan dengan sebuah ISP harus mengikuti aturan-aturan berlangganan yang ditetapkan oleh ISP tersebut. Biasanya masing-masing ISP memiliki kebijakan-kebijakan tersendiri namun pada umumnya ISP-ISP tersebut melarang pelanggan untuk menggunakan koneksi internet untuk keperluan-keperluan yang negative dan melanggar hukum.

   Kita mungkin sudah kenal dengan Telkomnet instant, produk layanan internet ini adalah salah satu produk internet yang sudah cukup lama hadir di masyarakat. Pemakai sangat gampang dalam melakukan koneksi ke internet, cukup sediakan sebuah modem yang terhubung ke PC dan line telepon, pelanggan langsung bisa melakukan koneksi dengan mudah, cukup dial nomer tertentu masukkan username dan password, beres?.

   Tipe layanan dari ISP biasanya dapat kita kategorikan menjadi 2 bagian yaitu :

1. Dial on demand Internet

   Dial on demand ini adalah layanan internet dimana pelanggan tidak terkoneksi secara terus menerus ke internet. Pelanggan akan dibebani biaya berdasarkan lamanya mereka terkoneksi ke internet.

   Contoh layanan internet dial on demand adalah : Telkomnet instant dari Telkom, layanan-layanan dial up dari ISP yang lain, juga beberapa layanan dari ISP wireless local.

2. Dedicated Internet

   Pelanggan yang menggunakan dedicated internet akan terhubung terus dengan internet 24/7. Sistem pembayaran dari layanan ini juga biasanya dilakukan per bulan dimana pelanggan akan membayar sesuai dengan paket yang ditawarkan, baik selama sebulan tersebut pengguna memang benar menggunakan internet 24 jam penuh atau tidak.

   Sistem dedicated ini biasanya mahal, dan biasanya untuk menekan biaya langganan, ISP memberikan beberapa metode untuk menekan harga misalnya dengan membatasi jumlah data yang boleh didownload dan diupload oleh pelanggan selama 1 bulan. Jumlah batasan data ini biasanya disebut dengan quota.

   Contoh layanan internet dedicated internet adalah layanan-layanan dari Channel 11, ERA AKSES, Speedy dari Telkom dan layanan-layanan dari ISP wireless local.

3. Isi dari ISP

   Apa sih isi dari ISP itu?

   ISP itu isinya adalah orang dan peralatan-peralatan yang diperlukan untuk memberikan service koneksi internet kepada pelanggan-pelanggannya Peralatan-peralatan tersebut biasanya berupa server, router, peralatan-peralatan untuk koneksi ke pelanggan-pelanggannya dan peralatan-peralatan interkoneksi mereka ke upstream. Biasanya ISP bekerja sama dengan operator jaringan dalam menjalankan usahanya. Jadi ada juga ISP yang tidak memiliki peralatan jaringan. Mereka hanya punya SDM untuk penjualan, customer support dan billing atau penagihan. Sisanya, mulai bandwidth, system jaringan, diserahkan kepada operator jaringan. Misalnya saya adalah sebuah

ISP bekerja sama dengan pemilik jaringan telepon untuk membuat system koneksi internet dial up. Saya juga membeli bandwidth dari pemilik jaringan telepon tersebut dan saya terima beres semuanya. Setelah itu saya tinggal menjual produk internet dial up tersebut, menyediakan system customer support dan menangani pembayaran.

4. FAQ tentang Pemilihan ISP

   Pertanyaan-pertanyaan yang sering saya jumpai :

   1. Mengapa ISP tidak bisa membersihkan virus?

      Yang bisa membersihkan virus adalah sebuah program antivirus. Antivirus hanya bisa mengidentifikasikan atau menebak sebuah file/data/program itu adalah virus, jika file/data/program itu sudah utuh.

      Sedangkan file/data/program yang diterima dan dilewatkan oleh ISP itu adalah dalam bentuk pecahan.

   2. ISP yang bagus :

      Kriteria apa sih yang bisa dipakai acuan oleh calon pengguna internet ?

      a. Pelanggannya banyak

         Sebuah ISP dengan ratusan pelanggan, mestinya secara kualitas lebih baik dibanding ISP yang masih memiliki puluhan pelanggan. Sebab ngga mungkin donk ratusan orang salah pilih. Dan kesempatan calon pelanggan untuk bertanya kepada pengguna ISP tersebut juga semakin gampang. Malah bisa jadi teman anda sudah menggunakannya. Kan lebih enak kalau kata ISP tersebut bagus atau tidak keluar dari teman yang bisa kita percaya.

         Jadi pertanyaan calon pengguna internet kepada bagian marketing atau sales dari sebuah ISP adalah : Berapa jumlah pelanggan Anda?

      b. Service.

         ISP dan jaringan computer yang saling berkaitan pada dasarnya dibangun pada sebuah system yang tidak reliable. Masalah pada koneksi internet itu sangat lumrah terjadi. Bencana alam, kesalahan manusia, umur peralatan, kesalahan manusia saat mengoperasikan peralatan, listrik dsb bisa menyebabkan koneksi internet pelanggan

mati. Jadi pastikan saat anda mengalami masalah dengan internet anda mempunyai tempat untuk berkonsultasi. Setidaknya anda tahu nanti masalah terjadi dimana dan kira-kira kita harus bagaimana sekarang untuk bisa mendapatkan koneksi internet lagi. Ini penting bagi anda-anda yang awam dengan internet dan orang-orang yang menggunakan internet 24 jam sehari.

Kemudian jaminan-jaminan apa yang akan anda dapatkan jika menggunakan layanan sebuah ISP?

Sebab harga insvestasi awal untuk melakukan koneksi ke internet masih cukup mahal ya. Apakah ada jaminan terhadap investasi anda tersebut, kemudian jaminannya dalam bentuk apa? Apakah ada kontrak khusus dengan anda, dan bagaimana sistemnya?

c. Mempunyai system redundancy.

   System redundancy itu apa sih?

   Bahasa awamnya adalah system koneksi cadangan. Dimana koneksi ini akan berfungsi jika koneksi utama mereka mati. Sangat penting, seperti kondisi saat kabel FO dunia di Taiwan putus, kalau ISPnya tidak memiliki koneksi cadangan yang bagus, maka dipastikan selama 3 minggu koneksi anda tidak akan bisa digunakan.

d. Harga

   Iya, harga sebenarnya adalah factor utama. Tapi sebenarnya pemilihan koneksi internet bagusnya dilihat dari perbandiangan antara harga dengan bandwidth dan kebutuhan anda. Sebab sekarang harga bandwidth internet di Denpasar sudah cukup standar dimana umumnya internet paling murah itu rata-rata dimulai dari 300ribu rupiah, walaupun ada saya dengar bisa 100-200ribu rupiah tapi saya belum pernah ketemu langsung dengan orang yang menggunakannnya. Harga sebanding dengan bandwidth atau kecepatan internet. Semakin murah, semakin kecil kecepatannya. Kita tidak perlu berargumen banyak dalam hal ini sebab, fakta secara teknis memang begitu. Kalau dari sisi marketing, beda cerita lah

**IP Address**

IP address dipakai untuk pengalamatan dalam jaringan.

- IP Network sebagai identitas network/jaringan. Jika ada IP 192.168.1.0/24 berarti mewakili suatu kelompok IP (network) dari 192.168.1.1 – 192.168.1.254
- IP broadcast merupakan IP terakhir dalam network yang dipakai untuk membroadcast packet broadcast. Misal 192.168.1.255/24.
- Host adalah ip yang disediakan untuk host. Misal: 192.168.1.111/24.

Ada beberapa jenis IP:

- IP public digunakan untuk mengakses internet.
- IP private digunakan untuk jaringan local.

**Ethernet Cable**

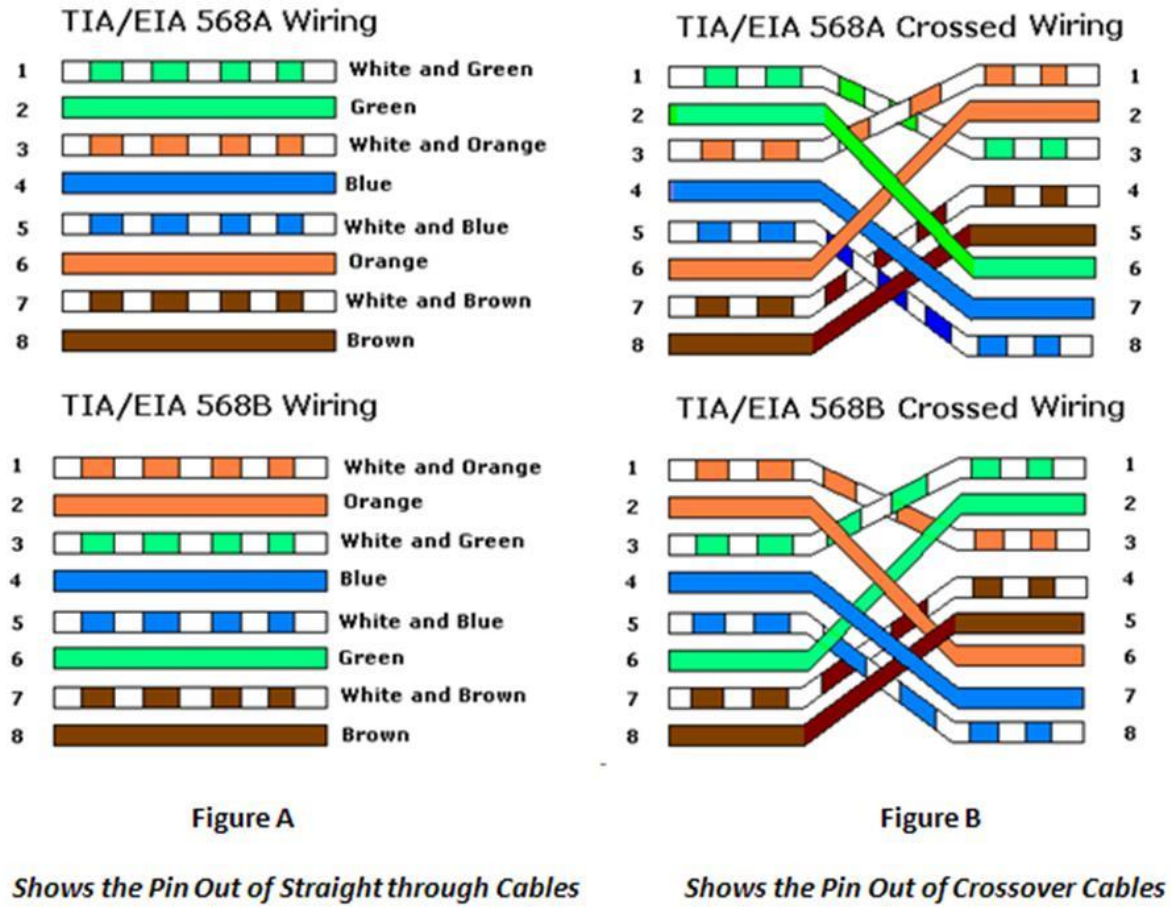



**Figure A**

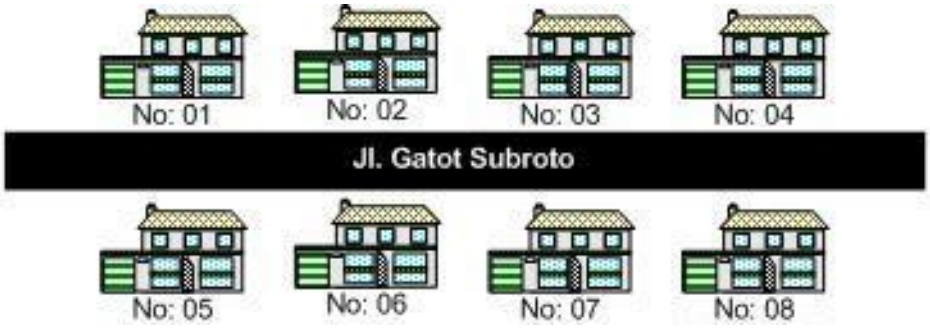
***Shows the Pin Out of Straight through Cables***

**Figure B**

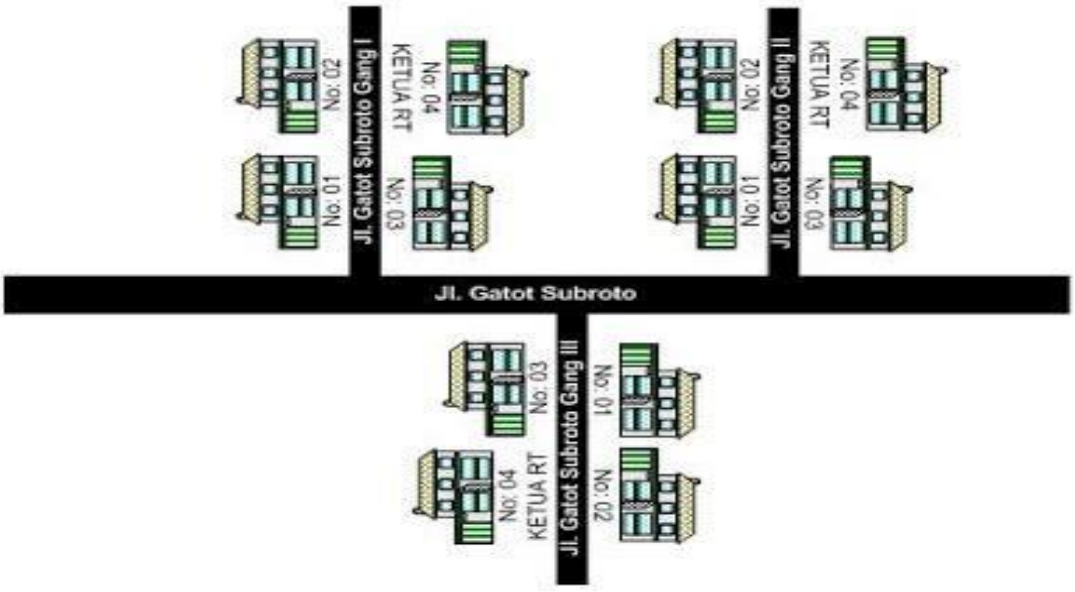
***Shows the Pin Out of Crossover Cables***

Subneting adalah membagi suatu netwok menjadi subnetwork yang lebih kecil. Inilah yang disebut subnet. Salah satu aspek dalam suatu design jaringan yang baik adalah pengoptimalan alamat ip. Subneting meminimalisir alamat ip yang tidak terpakai atau terbuang.

Subneting juga mempermudah dalam pengelolaan dan kinerja jaringan. Jika subneting dianalogikan dalam kehidupan nyata, maka akan seperti gambar dibawah. Dengan pengaturan subneting, maka akan terbentuk seperti ganggang kecil ke komplek masing-masing sehingga mudah dalam membedakan jaringan dan pengiriman data ke tujuan.




**Tanpa Subnet**




**Dengan Subnet**

Subneting ini adalah hal yang wajib dikuasai oleh seorang network engineer. Untuk memahami subneting ini, terlebih dahulu mengerti tentang bilangan decimal dan biner (nol atau satu). Dalam subneting, ada beberapa hal yang paling sering dicari.

**Subnetmask**

Misal ada ip 192.168.2.172/26 maka subnetmask atau netmask nya adalah /26 = 11111111.11111111.11111111.11000000. Prefix /26 mengindikasikan biner 1 (NetID) berjumlah 26 dan sisanya yaitu Host ID berjumlah 6.

Dari 11111111.11111111.11111111.11000000 ini ketika didesimalkan maka didapat subnet mask dari adalah 255.255.255.192

**Total IP**

Total IP ini dihitung dari Host ID. Dari contoh soal, didapat Host ID ada 6bit. Karena IPv4 32bit jadi 32-26 sisa 6. Sehingga maksimal IP didapat 2^6=64.

*Rumus menghitung maksimal IP: 2^Host ID*

**Jumlah Subnet**

Jumlah subnet dihitung dari Net ID. Karena Net ID subnet /26 adalah 26 maka Subnet ID nya 2.

*Loh kok bisa?*

Karena Net ID 26 dikurangi 24 karena kelas C jadi 2. Intinya klo kelas C dikurangi 24, kelas B dikurangi 16, kelas A dikurangi 8. Didapat banyak subnetnya adalah 2^2=4 subnet.

*Rumus menghitung banyak subnet dengan rumus: 2^subnet ID*

**Mencari IP Network dan Broadcast**

Karena soalnya IP 192.168.2.172, maka gak mungkin termasuk subnet/network pertama karena 72>64. Jadi IP tersebut masuk ke subnet ke berapa ya? Kita hitung aja kelipatan 64. IP Network pasti paling awal dan broadcast paling akhir.

*Gampangnya ip network setelahnya dikurang 1 itulah broadcast.*

| IP Network | IP Broadcast |
|---|---|
| 192.168.2.0 | 192.168.2.63 |
| 192.168.2.64 | 192.168.2.127 |
| 192.168.2.128 | 192.168.2.191 |
| 192.168.2.192 | 192.168.2.255 |

Jadi IP 192.168.2.172 masuk dalam subnet ke 3 dengan ip network 192.168.2.128 dan broadcastnya 192.168.2.191.

**IP Client**

Dan ini adalah yang paling gampang, yaitu menghitung maksimal ip yang dapat dipakai host. Rumusnya adalah total ip dikurangi 2 karena dipakai untuk network id dan broadcast. Jadi IP Client tiap subnet adalah 64-2=62.

Untuk menghafal subnet lebih cepat, kita dapat memanfaatkan tabel subnet dibawah ini.

| | | | | Subnets | | | Hosts | | |
|---|---|---|---|---|---|---|---|---|---|
| | | / | Netmask | Block Size | Class A | Class B | Class C | Class A | Class B | Class C |
| Class A Network | | 8 | 255.0.0.0 | 256 | 1 | | | 16777214 | | |
| | | 9 | 255.**128**.0.0 | 128 | 2 | | | 8388606 | | |
| | | 10 | 255.**192**.0.0 | 64 | 4 | | | 4194302 | | |
| | | 11 | 255.**224**.0.0 | 32 | 8 | | | 2097150 | | |
| | | 12 | 255.**240**.0.0 | 16 | 16 | | | 1048574 | | |
| | | 13 | 255.**248**.0.0 | 8 | 32 | | | 524286 | | |
| | | 14 | 255.**252**.0.0 | 4 | 64 | | | 262142 | | |
| | | 15 | 255.**254**.0.0 | 2 | 128 | | | 131070 | | |
| | Class B Network | 16 | 255.255.0.0 | 256 | 256 | 1 | | 65534 | 65534 | |
| | | 17 | 255.255.**128**.0 | 128 | 512 | 2 | | 32766 | 32766 | |
| | | 18 | 255.255.**192**.0 | 64 | 1024 | 4 | | 16382 | 16382 | |
| | | 19 | 255.255.**224**.0 | 32 | 2048 | 8 | | 8190 | 8190 | |
| | | 20 | 255.255.**240**.0 | 16 | 4096 | 16 | | 4094 | 4094 | |
| | | 21 | 255.255.**248**.0 | 8 | 8192 | 32 | | 2046 | 2046 | |
| | | 22 | 255.255.**252**.0 | 4 | 16384 | 64 | | 1022 | 1022 | |
| | | 23 | 255.255.**254**.0 | 2 | 32768 | 128 | | 510 | 510 | |
| Class C Network | | 24 | 255.255.255.0 | 256 | 65536 | 256 | 1 | 254 | 254 | 254 |
| | | 25 | 255.255.255.**128** | 128 | 131072 | 512 | 2 | 126 | 126 | 126 |
| | | 26 | 255.255.255.**192** | 64 | 262144 | 1024 | 4 | 62 | 62 | 62 |
| | | 27 | 255.255.255.**224** | 32 | 524288 | 2048 | 8 | 30 | 30 | 30 |
| | | 28 | 255.255.255.**240** | 16 | 1048576 | 4096 | 16 | 14 | 14 | 14 |
| | | 29 | 255.255.255.**248** | 8 | 2097152 | 8192 | 32 | 6 | 6 | 6 |
| | | 30 | 255.255.255.**252** | 4 | 4194304 | 16384 | 64 | 2 | 2 | 2 |

**Contoh Soal Subnetting**

Dalam pembahasan ini, kita akan belajar untuk mengerjakan berbagai variasi soal subneting. Soal subnetingnya sebagai berikut guys ☺ Carilah total ip, netmask, ip network, broadcast dan host untuk masing-masing ip dibawah:

a) 192.168.10.10/25
b) 10.10.10.10/13

Ok langsung aja kita bahas soal di atas.

a) 192.168.10.10/25 merupakan kelas C

| | | | |
|---|---|---|---|
| a. | Total IP | 128 | Didapat dari 2^7 = 128, 7 merupakan Host ID dari subnet /25 |
| b. | Netmask | 255.255.255.128 | Didapat dari 256 – Total IP = 256 – 128 = 128 menjadi |
| c. | IP Network | 192.168.10.0 | Jumlah subnet adalah 2^1, 1 adalah Subnet ID. IP 192.168.2.10 masuk dalam subnet ke-1 karena berada dalam range 0-127 sehingga IP Networknya 192.168.10.0 |
| d. | Broadcast | 192.168.10.127 | IP Network setelahnya dikurangi 1 => 192.168.10.128 – 1 = 192.168.10.127 |
| | Host | 192.168.10.1 – 192.168.10.126 | Jumlah ip yg dapat dipakai adalah 126 didapat dari 128 – 2 karena dipakai untuk IP Network dan broadcast. |

b) 10.10.10.10/13

| | | | |
|---|---|---|---|
| a. | Total IP | 524288 | Subnet 13 merupakan subnet kelas A sehiggga untuk memudahkan diubah dulu menjadi subnet kelas C dengan ditambah 8 dua kali menjadi 29. Total host subnet 29 adalah 8. Lalu 8 x 256 x 256 menjadi 524288. Dikali 256 dua kali karena sebelumnya ditambah 8 dua kali untuk menjadi subnet kelas C. |

*Remember me in your pray*

| | | | |
|---|---|---|---|
| b. | Netmask | 255.248.0.0 | Seperti bisaa 248 didapat dari 256 – total ip. Karena kelas A ditambah 8 dua kali jadi kelas C maka subnet dimajukan 2 kali dari 255.255.255.248 menjadi 255.248.0.0 |
| c. | IP Network | 10.8.0.0 | Setelah disamakan menjadi kelas C (13+8+8=29), maka didapat jumlah subnet /29 adalah 2^5, 5 adalah Subnet ID. Total IP dari subnet /29 adalah 8, maka IP 10.10.10.10 masuk dalam IP Networknya 10.8.0.0. |
| d. | Broadcast | 10.15.255.255 | IP Network setelahnya dikurangi 1 => 10.16.0.0 – 1 = 10.15.255.255 |
| e. | Host | 10.8.0.1 – 10.15.255.254 | umlah ip yg dapat dipakai adalah 524286 didapat dari 524288 – 2 karena dipakai untuk IP Network dan broadcast |

# BASIC CONFIGURATION

Dalam CLI cisco terdapat beberapa mode atau hak ases pada router ataupun switch, yang terbagi menjadi 3 :

- *User mode* yang di tandai dengan "**>**" : pada mode ini kita tidak dapat melakukan konfigurasi apapun
- *Privilege mode* yang di tandai dengan "**#**" : pada mode ini kita hanya dapat melihat konfigurasi dengan tidak dapat menambah konfigurasi
- *Global configuration* yang di tandai dengan "**(config)#**" : pada mode ini kita baru dapat melakukan konfigurasi, entah itu menambah atau pun menghapus

Untuk masuk ke Privilange mode dari user mode ketikan "*enable*" di mode user (>) dan setelah masuk ke privilange mode untuk masuk ke global config bisa ketikan "configure terminal"

```
Router>enable     ← masuk ke mode privilege
Router#configure terminal     ← masuk ke mode global configure
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ← mode global configure
```

Setelah masuk ke dalam mode Global config di situ lah kita dapat mulai mengkonfigurasi router atau pun switch. Dan untuk kembali ke user mode yang sebelum nya bisa dengan megetikan "exit" (kembali ke mode sebelumnya) atau pun "ctrl + Z" (untuk kembali ke mode privilege.

**Cara mengganti nama pada router atau pun switch**

Mengganti hostname dalam router merupakan salah satu perintah dasar, yang biasa di gunakan agar kita tidak salah mengkonfigurasikan switch ataupun router, dengan cara masuk terlebih dahulu ke Global config.

```
Router(config)#hostname ZAKY (ini hanya penamaan, jadi bias diberi nama apa saja)
ZAKY(config)#
```

**Cara menyimpan konfigurasi pada router atau switch**

Setelah kita telah banyak melakukan konfigurasi pada router atau pun switch maka jangan lupa untuk menyimpan konfigurasi tersebut di penyimpan di router atau yang biasa di sebut dengan *Nvram*

```
ZAKY#write
Building configuration...
[OK]
ZAKY#
```

Atau bias juga menggunakan do write (ini dilakukan ketika berada di luar mode privilege).

```
ZAKY(config)#do write
Building configuration...
[OK]
ZAKY(config)#
```

**Konfigurasi Password pada router/switch**

Pemberian password pada router atau pun switch sangatlah penting untuk yang bertujuan untuk keamanaan jaringan, agar para tangan – tangan jahil tidak bias mengambil data – data kita

```
ZAKY(config)#enable password 123
ZAKY(config)#enable secret 1234
```

Enable password adalah mode password saja dan tidak ter-encripsi. Artinya dalam hal ini ketika memberkan password di perangkat tidak aman, karna ketika kita show running-config password kita akan terlihan dengan jelas, berbeda dengan enable secret, metode ini meng-encrisikan password kita menjadi md5.

```
ZAKY#show running-config
Building configuration...

Current configuration : 618 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ZAKY
!
!
!
enable secret 5 $1$mERr$4dpRATIgxQacPVK0CfNV4/
enable password 123
```

Sekarang lakukan pengujian, apakah password yang sudah kita buat tadi berhasil atau tidak.

```
ZAKY>enable
Password:  (ini jika kita input password tidak ditampilkan)
ZAKY#
```

**Melihat infomasi interface router atau pun switch**

Untuk melihat informasi interface kita seperti apa saja kah yang sudah ada di innterface kita dan juga salah satu cara dalam melakukan troubleshooting

```
ZAKY#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet0/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
```

**Melihat konfigurasi tang sedang berjalan (show running-config)**

Fungsi dari melihat konfigurasi yang sedang berjalan di router atau pun di switch yang biasa di gunakan untuk troubleshooting

```
Building configuration...

Current configuration : 618 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ZAKY
!
!
!
enable secret 5 $1$mERr$4dpRATIgxQacPVK0CfNV4/
enable password 123
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
```

```
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

# MOTD (Messenger Of the Day)

Dalam lab ini, kita akan konfigurasikan banner untuk menandai atau memberikan label di perangkat cisco.

Hal ini dilakukan ketika kita sudah banyak menggunakan perangkat. Agar kita tidak kebingungan dalam memanajeman perangkan, alangkah baiknya kita konfigurasikan banner motd z.

```
ZAKY(config)#banner motd z
Enter TEXT message. End with the character 'z'.
---------------------------------------------
CISCO PACKET TRACER
---------------------------------------------
z
ZAKY(config)#
```

Untuk pengujiannya silahkan exit sampai mode user.

```
---------------------------------------------
CISCO PACKET TRACER
---------------------------------------------


ZAKY>
```

Jika brhasil, maka tampilannya akan seperti gambar di atas.

**Mereset Konfigurasi**

Untuk membersihkan seluruh konfigurasi, kita bias lakukan dengan cara **write erase** pada mode privilege atau gunakan **do** di luar mode privilege.

```
ZAKY#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]  (ENTER)
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
ZAKY#RELOAD  Lanjutkan dengan command reload untuk melakukan restart device
```

# Chapter 1
## SWITCHING

Virtual LAN (VLAN)

Trunking

InterVlan Routing

SVI (Switch Virtual Intreface) L3

VTP (VLAN Trunking Protocol)

DHCP (Router & Switch)

Port Security

Telnet & SSH

Spanning Tree Protocol

Root Bridge STP

Spanning Tree Port Fast

Etherchannel

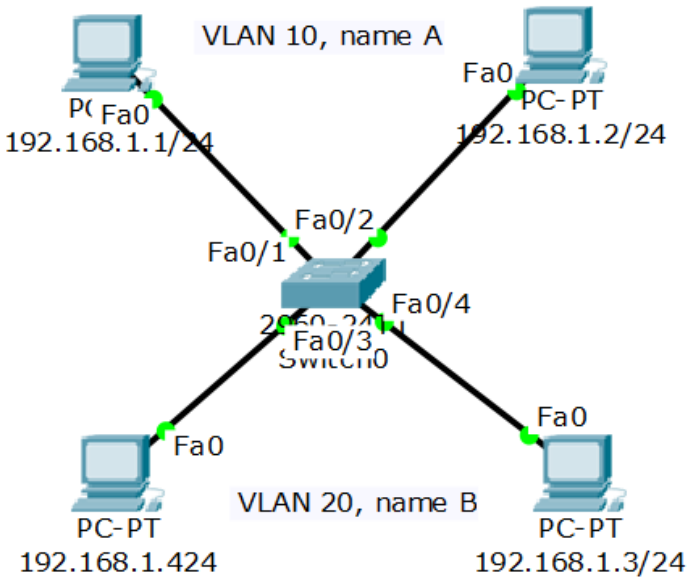
Virtual Link VLAN

*Remember me in your pray*

# VIRTUAL LAN (VLAN)

VLAN adalah kelompok device dalam sebuah LAN yang dikonfigurasi (menggunakan software manajemen) sehingga mereka dapat saling berkomunikasi asalkan dihubungkan dengan jaringan yang sama walaupun secara fisikal mereka berada pada segmen LAN yang berbeda

VLAN juga bisa juga diartikan mengelompokkan jaringan sesuai dengan kelompokknya dan berkomunikasi hanya dengan kelompoknya saja.




Dari topologi di atas semua PC terhubung melalui network 192.168.1.0/24 dan dibedakan dengan hostnya saja. Dan jika kita coba tes ping, maka semua pc ini bisa saling berkomunikasi. Karena tidak ada konfigurasi VLAN di dalamnya.

C:\>ping 192.168.1.1 (dicoba dari PC3)

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

*Remember me in your pray*

Sekarang kita akan konfigurasikan VLAN untuk memisahkan antara PC/jaringan di bagian atas dan bawah.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name A
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name B
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface range fa0/3-4
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#
```

Untuk memastikan, kita lakukan show vlan brief

```
Switch#show vlan brief
VLAN Name                              Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   A                                 active    Fa0/1, Fa0/2
20   B                                 active    Fa0/3, Fa0/4
1002 fddi-default                      active
```

Bisa kita lihat bawah masing-masing dari port (fa) sudah mengarah ke vlannya masing-masing sesuai dengan topologi.

Untuk pengujiannya, silahkan lakukan PING ke sesame vlan (hasilnya reply) dank e beda vlan (hasilnya RTO)

Saya gunakan PC1 (Vlan 10) untuk uji coba

C:\>ping 192.168.1.4 **(ke beda VLAN)**

Pinging 192.168.1.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.4:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.1 **(ke sesame VLAN)**

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 3ms, Average = 0ms

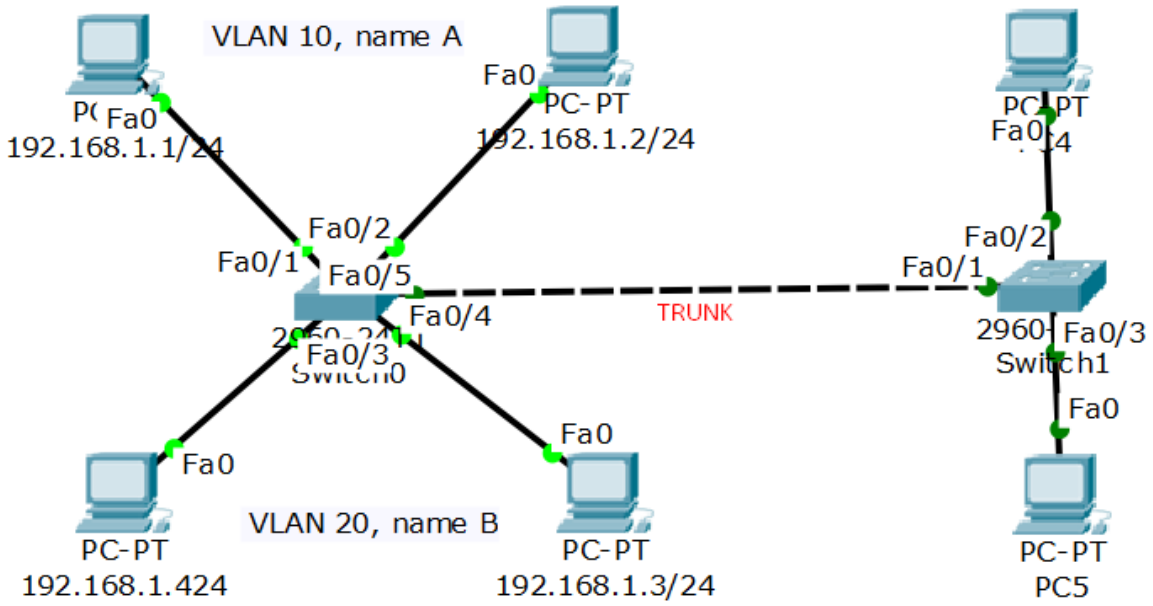
Jika hasilnya seperti di atas, maka kita sudah benar dalam mengkonfigurasi vlan.

# TRUNKING

Pada lab kali ini kita akan mengkonfigurasikan trunk yang dapat di fungsikan untuk melewati trafic dari suatu switch ke switch atau router lain. Dan pada lab kali ini kita akan mengkonfigurasikan agar vlan yang sama dapat saling terhubung walaupun berbeda switch.

Ada 2 trunking protocol yang biasa digunakan:

- **ISL** = cisco proprietary, bekerja pada ethernet, token ring dan FDDI, menambahi tag sebesar 30byte pada frame dan semua traffic VLAN ditag.
- **IEEE** 802.11Q (dot1q) = open standard, hanya bekerja pada ethernet, menambahi tag sebesar 4byte pada frame.




Pada topologi ini kita bisa lihat bahwa ada penambahan switc dan PC. Dan terlihat pada fa0/1 switch1 mengarah ke fa0/5 switch0. Jika PC yang baru ditambahkan tadi ingin melakukan komunikasi ke sesame vlannya, maka kita harus konfigurasikan trunk pada jalur fa0/1 di switch1, dan untuk fa0/5 di switch0sudah tidak perlu lagi di trunk, karena mreka sudah saling terhubung dengan 1 kabel.

Jika kita lakukan ping ke sesame vlan pun tidak akan bisa/RTO, hal ini disebabkan karena traffic yang dikirim dari sw1 ke sw0 tidak ada penghubungnya.

Langsung saja kita konfigurasikan trunk pada switch1

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name A    (buatkan vlan)
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name B
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#sw acc vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#sw acc vlan 20
Switch(config-if)#int fa0/1
Switch(config-if)#sw mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up
```

Sekarang lakukan ping ke sesame vlan dan beda vlan

pengujian dari Vlan 10 PC4

```
C:\>ping 192.168.1.3  (ke sesame VLAN)

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.1.5   (ke beda VLAN)

Pinging 192.168.1.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# TRUNK ALLOWED

Secara default, saat kita mengkonfigurasikan trunk pada interface antar switch maka trunk tersebut memboleh kan semua vlan (1 – 1005) untuk melewati trunk tersebut. Lalu bagaimana jika kita ingin vlan-vlan tertentu saja yang dapat berkomunikasi melalui trunk tersebut?. Jawabannya adalah trunk allowed.

Sebelum kita memulai konfigurasi kita dapat melanjutkan pada topologi di lab sebelumnya, kemudian kita dapat melihat terlebih dahulu vlan yang di izinkan oleh trunk untuk melewati trunk tersebut

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
```

Kemudian kita akan mengkonfigurasi kan *allowed trunk* dengan tujuan agar vlan yang di izin kan oleh trunk hanya vlan 10 dan 20 saja

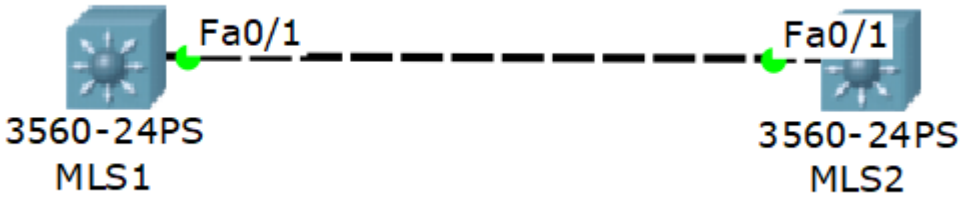
```
Switch(config)#int fa0/1
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#
```

Lalu lakukan pengecekan trunk kembali seperti langkah di atas.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       10,20

Port        Vlans allowed and active in management domain
Fa0/1       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20
```

# TRUNUK DI MULTILAYER SWITCH

Konfigurasi trunk pada Multilayer switch memilikisedikit perbedaan dalam melakukan trunknya. Tidak dapat langsung di konfigurasikan switchport mode trunk seperti di switch biasa (layer2), akan tetapi kita harus konfigurasikan encapsulation pada trunk, lalu switchport mode trunk.




Untuk memastikan, bahwa kita tidak bisa langsung memberikan trunk sebelum dikonfigurasikan encapsulation, sekarang kita coba tanpa menambahkan encapsulation.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname MLS1
MLS1(config)#int fa0/1
MLS1(config-if)#sw mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can
not be configured to "trunk" mode.
MLS1(config-if)#
```

Terlihat bahwa encapsulation  mode auto tidak dapat menjadi trunk, oleh karna itu kita harus menkonfigurasikan encapsulation terlebih dahulu, setelah itu kita barulah membuat interface trunk.

```
MLS1(config)#int fa0/1
MLS1(config-if)#switchport trunk encapsulation dot1q
MLS1(config-if)#switchport mode trunk
```

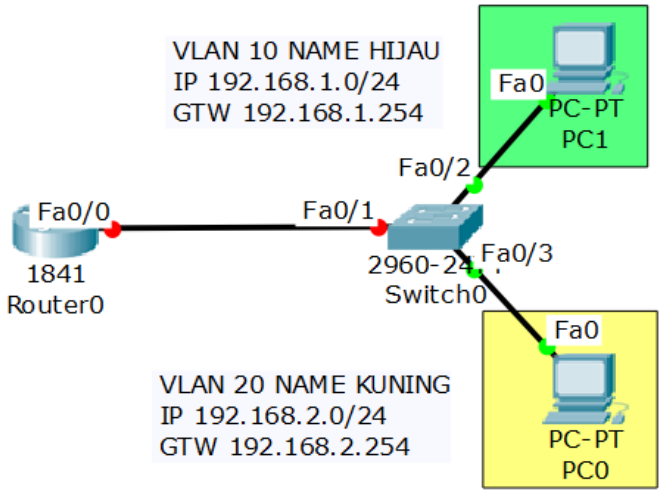
Selanjutnya lakukan pengecekan trunk pada MLS1

```
MLS1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

# INTERVLAN ROUTING

Jika pada sebelumnya konsep vlan itu tidak mengizinkan vlan yang berbeda untuk berkomunikasi, sekarang kita akan konfigurasikan berbeda vlan agar bisa saling komunikasi dengan menambahkan sub interface pada router. Dan router ini fungsinya sebagai media penghubung antar vlan melalui gateway.

Inter vlan di gunakan pada perangkat layer3 seperti router multilayer switch

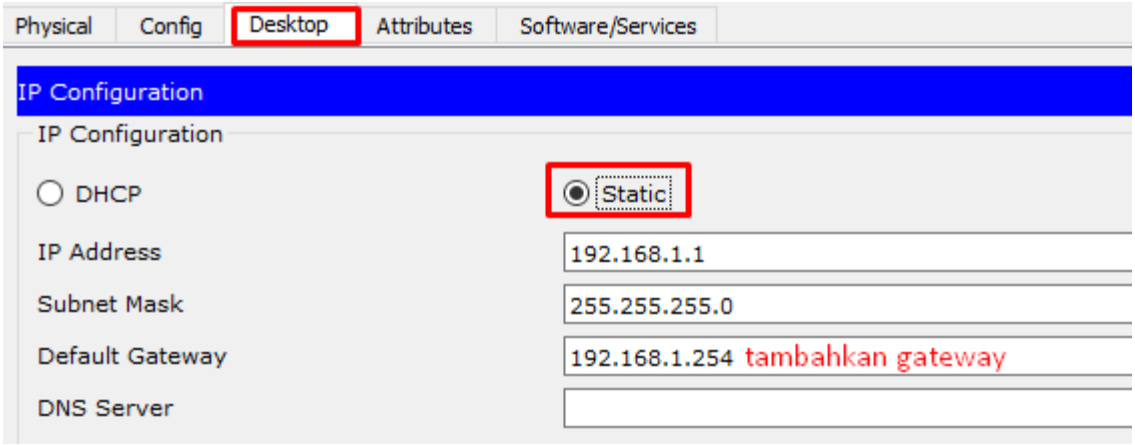



Dari topologi di atas secara logical tidak mungkin bisa kita mengkonfigurasikan 2 network yang berbeda pada interface router0 (fa0/0). Maka kita butuh sub interface untuk mengkonfigurasikan intervlan agar 2 network tersebut kita lewatkan melalui interface fa0/0 saja.

```
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name HIJAU  (buatkan vlan)
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name KUNING
Switch(config-vlan)#int fa0/2
Switch(config-if)#sw acc vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#sw acc vlan 20
Switch(config-if)#int fa0/1
Switch(config-if)#sw mode trunk  (trunk untuk kea rah router)
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0   (interface ini hanya diaktifkan saja)
Router(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
to up
Router(config)#int fa0/0.10   (sub interface untuk menambahkan ip di vlan 10)
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed
state to up
Router(config-subif)#encapsulation dot1Q 10  (tambahkan encaps agar bisa diisi ip)
Router(config-subif)#ip add 192.168.1.254 255.255.255.0

Router(config-subif)#int fa0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed
state to up
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.168.2.254 255.255.255.0
```

Isi ip address sesuai vlannya masing-masing dan tambahkan gateway.




*Remember me in your pray*

Setelah ip addres semua diisi berdasarkan vlannya, sekarang lakukan ping antar vlan. Dan hasilnya harus reply.

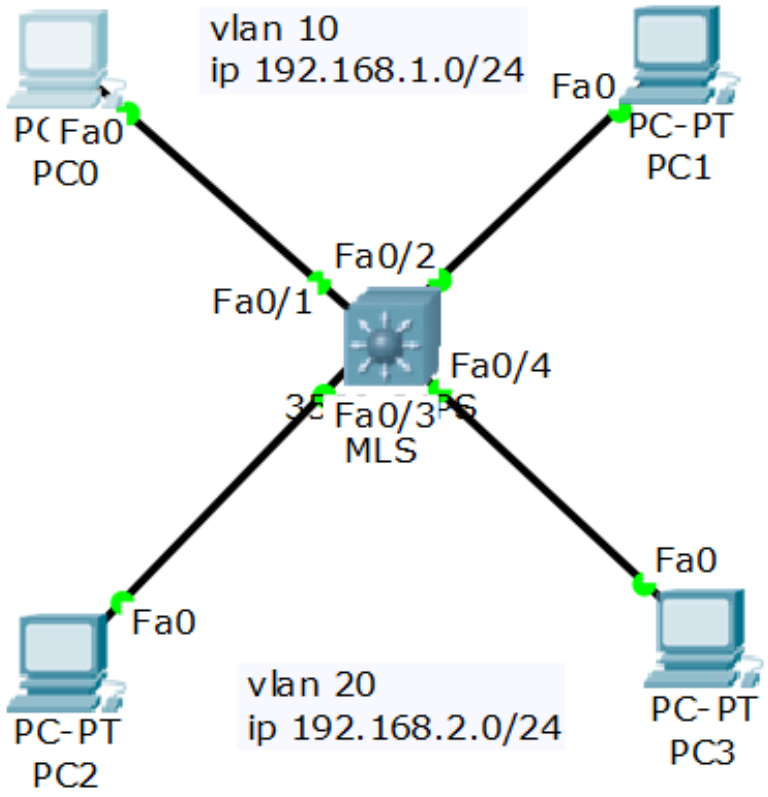
Saya menggunakan VLAN KUNING (PC0) untuk pengujiannya.

```
C:\>ping 192.168.1.1  (ping ke vlan hijau)

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=12ms TTL=128
Reply from 192.168.1.1: bytes=32 time=13ms TTL=128
Reply from 192.168.1.1: bytes=32 time=15ms TTL=128
Reply from 192.168.1.1: bytes=32 time=25ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 25ms, Average = 16ms
```

# SVI (SWITCH VIRTUAL INTERFACE)

SVI (Switch Virtual Interface) merupakan sebuah mekanisme untuk melakukan sejenis routing seperti intervlan routing yang mana pada SVI kita dapat mengkonfigurasi kan ip address pada vlan untuk menjadi gateway pada client yang berada pada vlan tersebut agar dapat saling terhubung dengan beda vlan

Untuk perangkat switch kita harus menggunakan switch yang mendukung fungsi router atau yang dapat bergerak di doubel layer, dan switch yang dapat mengkonfigurasi kan SVI tersebut hanyalah switch MLS (Multilayer Switch)




Sebelum kita mengkonfigurasi kan SVI pada MLS kita dapat memulai dengan mengkonfigurasi kan vlan terlebih dahulu sesuai dengan topologi

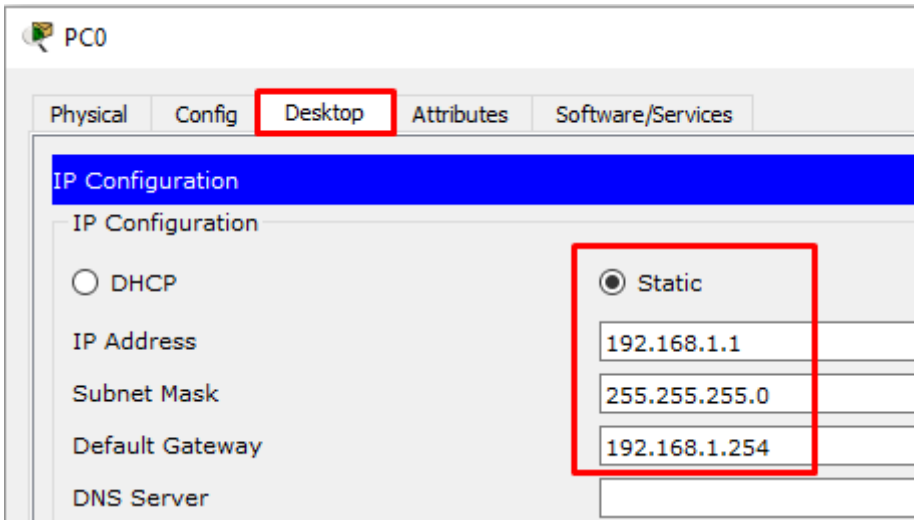
```
Switch>en
Switch#conf t
Switch(config)#host MLS
MLS(config)#vlan 10
MLS(config-vlan)#name ATAS
MLS(config-vlan)#vlan 20
MLS(config-vlan)#name BAWAH
MLS(config-vlan)#int range fa0/1-2
MLS(config-if-range)#sw acc vlan 10
MLS(config-if-range)#int range fa0/3-4
MLS(config-if-range)#sw acc vlan 20
```

Pada tahapan ini maka client kita hanya dapat melakukan ping pada client yang satu vlan atau masih satu network, agar kita client dapat saling terhubung dengan vlan yang berbeda kita dapat mengkonfigurasi kan SVI dengan menambah kan ip address pada vlan yang nanti nya akan di gunakan client untuk menuju vlan lain

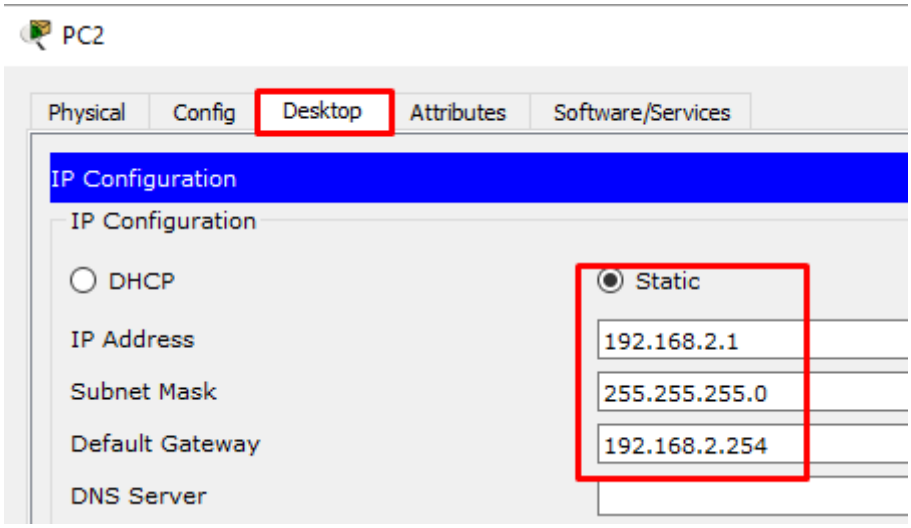
```
MLS(config)#int vlan 10
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
MLS(config-if)#ip add 192.168.1.254 255.255.255.0
MLS(config-if)#int vlan 20
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
MLS(config-if)#ip add 192.168.2.254 255.255.255.0
```

Setelah itu berikan ip address pada masing–masing client dengan gateway ip vlan yang tadi kita konfiguasi kan sesuai dengan vlan.

Client di VLAN 10




Client di VLAN 20




Setelah kita konfigurasi kan ip pada setiap client beserta dengan gateway nya dengan ip pada vlan, kita dapat mencoba dengan melakukan tes ping dengan ping antar client yang berbeda vlan, apakah bisa ..??

```
C:\>ping 192.168.2.1  (ip vlan 20)
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

*Remember me in your pray*

Terlihat disana bahwa berbeda vlan masih tetap tidak mau berkomunikasi. Hal ini disebabkan karena tidak adanya fitur routing untuk mengantarkan paket yang dikirim oleh vlan 10.

Yang kita perlukan hanyalah *ip routing* untuk menghubungkan antara vlan 10 dan 20 pada lab SVI ini.

```
MLS(config)#ip routing
```

Cukup sepele, tapi jika tidak di konfigurasi akan berdampak RTO.

Sekarang kita ulangi ping beda vlan.

```
C:\>ping 192.168.2.1  (ip vlan 20)

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Maksud dari konfigurasi *ip routing* yaitu untuk mengaktifkan fungsi routing agar client yang berbeda network dapat saling terhubung dengan ip routing

# VTP (VLAN TRUNKING PROTOCOL)

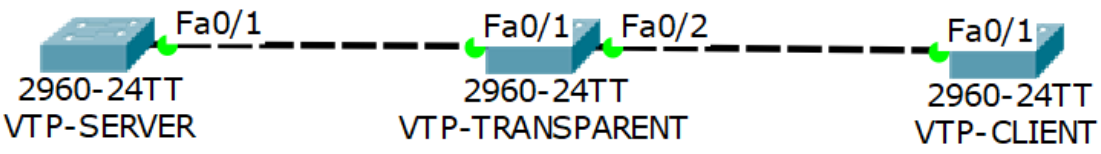
Vlan trunking protocol atau yang akrab di sebut dengan VTP ini adalah sebuah suatu cara agar kita dapat memanagement VLAN secara terpusat, yang di mana kita dapat lebih mudah menambakan atau pun mengurangi vlan dalam satu switch saja dan switch–switch yang lain nya akan mengikuti nya perubahan yang baru saja kita buat tadi.

Dalam VTP terbagi mejadi 3 mode untuk kita konfigurasikan :

1. **VTP mode server** : yaitu di mode ini switch yang akan kita konfigurasikan akan menjadi induk bagi para switch yang lain nya, yang mana apabilaswitch yang yang menjadi VTP mode server menambahkan vlan ataupun menghapus nya maka switch yang lain nya akan ikut mengupdate apa yang telah kita edit di switch yang di pasang mode server
2. **VTP mode client** : vtp mode yang akan menginduk kepada vtp server yang apa bila kita sudah satu domain dengan vtp server maka secara otomatis di switch kita yang sudah di pasang vtp mode client akan menambahkan sendiri, dan apa bila VTP server menghapus vlan maka client pun akan ikut terhapus juga
3. **VTP mode transparent** : vtp mode transparent ini ia dapat membuat vlan tetapi vlan yang di buat nya hanya lah bersifat local, yang mana iya hanya meneruskan saja, tetapi ia tidak mendapatkan update dari vtp server

| | VTP Server | VTP Client | VTP Transparent |
|---|---|---|---|
| Create/Modify/Delete VLAN | Yes | No | Only local |
| Syncronizes itself | Yes | Yes | No |
| Forwards advertisements | Yes | Yes | Yes |

Berikut topologinya:




Kita akan mencoba dengan 3 switch yang memiliki mode server, transparent, client. Hal yang harus kalian seting adalah membuat trunk terlebih dahulu antar switch agar vtp

client mendapat kan update dari server, setelah itu kita akan membuat domain untuk server dan password nya, yang kemudian di sesuaikan dengan vtp transparent dan client nya.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host VTP-SERVER
VTP-SERVER(config)#vtp mode server
Device mode already VTP SERVER.
VTP-SERVER(config)#vtp domain zaky
Changing VTP domain name from NULL to zaky
VTP-SERVER(config)#vtp password zaky
Setting device VLAN database password to zaky

VTP-SERVER(config)#int fa0/1
VTP-SERVER(config-if)#sw mode trunk

BUATKAN VLAN
VTP-SERVER(config)#vlan 10
VTP-SERVER(config-vlan)#vlan 20
VTP-SERVER(config-vlan)#vlan 30
```

Lakukan pengecekan vlan

```
VTP-SERVER#sh vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     active
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host VTP-TRANSP
VTP-TRANSP(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
VTP-TRANSP(config)#vtp domain zaky
Domain name already set to zaky.
VTP-TRANSP(config)#vtp password zaky
Setting device VLAN database password to zaky
VTP-TRANSP(config)#int fa0/2
VTP-TRANSP(config-if)#sw mode trunk
```

Lakukan pengecekan apakah mode transparent mengupdate informasi dari mode server

```
VTP-TRANSP#sh vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Jawaban nya tentu tidak karna memang vtp mode transparent hanya bersifat local dan ia hanya meneruskan saja dari vtp server dan tidak mengupdate konfigurasi dari vtp server.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host VTP-CLINT
VTP-CLINT(config)#vtp mode client
Setting device to VTP CLIENT mode.
VTP-CLINT(config)#vtp domain zaky
Domain name already set to zaky.
VTP-CLINT(config)#vtp password zaky
Setting device VLAN database password to zaky
VTP-CLINT(config)#
```

Lakukan pengecekan, apakah vtp client sudah mengupdate informasi dari vtp-server atau belum.

```
VTP-CLINT#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Gig0/2
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      active
```

Terlihat disana ada vlan 10, 20, 30 seperti yang di buat oleh vtp-server. Dan jika sudah seperti di atas, berarti vtp yang kita konfigurasi sudah benar.

Dan pada switch VTP transparent ia tidak akan mengupdate tetapi di hanya memiliki jaringan lokalnya saja, ia hanya bisa menambahkan vlan untuk dirinya sendiri dan tidak mengupdate ke vtp yang lain.

Sebagai contoh saya akan tambahkan vlan 100 di vtp-transparent

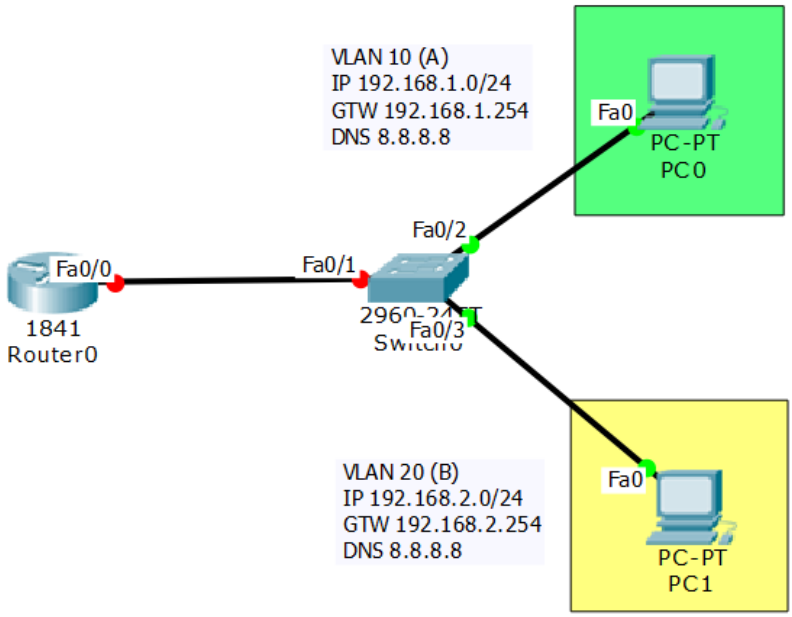
```
VTP-TRANSP(config)#vlan 100
VTP-TRANSP(config-vlan)#name ASAL
```

Jika kita show vlan brief di mode client, maka vlan 100 tidak akan di update oleh vtp-client

```
VTP-CLINT#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     active
```

# DHCP SERVER

Seperti yang telah kita ketahui DHCP berguna untuk memberikan ip secara otomatis, pada lab kali ini kita akan memberikan IP secara otomatis ke client agar client tidak perlu susah lagi memberi IP secara static/manual maka dengan DHCP router akan memberi IP secara otomatis ke setiap client menurut vlan dengan IP yang berbeda per vlan nya.




Dari topologi di atas, hal pertama yang harus kita lakukan adalah konfigurasi vlan pada switch dan mengarahkan port seseuai dengan vlannya

```
Switch>en
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name A
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name B
Switch(config-vlan)#int fa0/2
Switch(config-if)#sw acc vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#sw acc vlan 20
Switch(config-if)#int fa0/1
Switch(config-if)#sw mode trunk
```

Setelah itu buatkan sub interface untuk memberikan ip vlannya.

```
Router(config)#int fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 192.168.1.254 255.255.255.0
Router(config-subif)#int fa0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 192.168.2.254 255.255.255.0
```

Jika sudah di buat seperti di atas, pastikan sub interface sudah ada ip nya dengan cara show ip interface brief

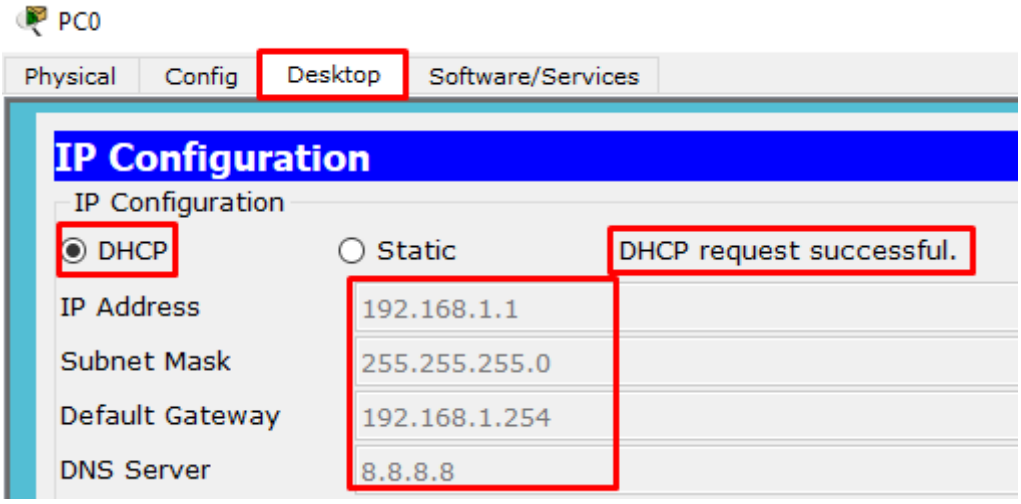
```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.10     192.168.1.254   YES manual up                    up
FastEthernet0/0.20     192.168.2.254   YES manual up                    up
```

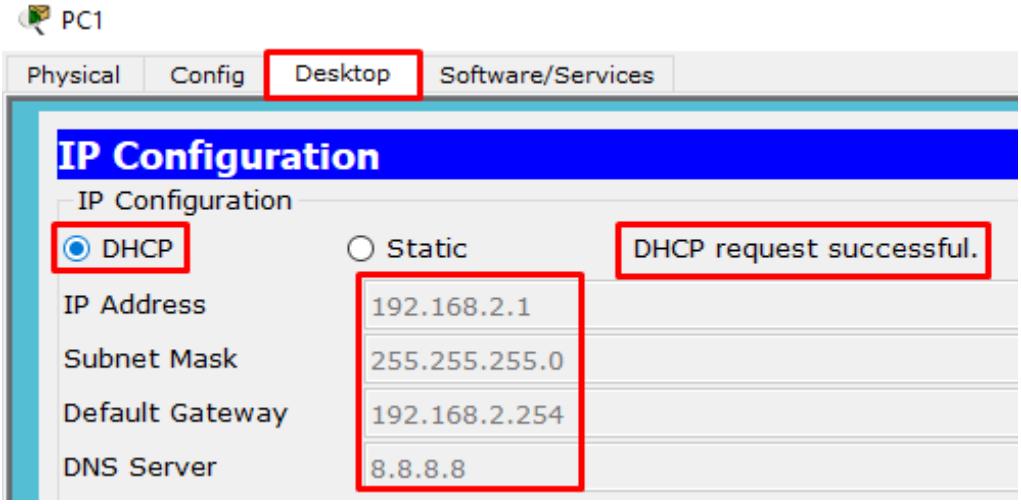
Setelah itu konfigurasikan DHCP pada router. Yang di butuhkan untuk konfigurasi dhcp adalah Ip address (sudah di sub interface), pool, network, netmask, default router/gateway, Dns (optional).

```
Router(config)#ip dhcp pool vlan10  (nama pool bebas)
Router(dhcp-config)#network 192.168.1.0 255.255.255.0  (network sub interface)
Router(dhcp-config)#default-router 192.168.1.254
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ex
Router(config)#ip dhcp pool vlan20
Router(dhcp-config)#net 192.168.2.0 255.255.255.0
Router(dhcp-config)#def 192.168.2.254
Router(dhcp-config)#dns 8.8.8.8
```

Sekarang saatnya kita uji coba apakah dhcp yang sudah kita buat tadi berhasil/tidak.

Arahkan ip client ke dhcp.




Coba lakukan ping ke beda vlan

PC>ping 192.168.1.1 **(dari vlan 20 ke 10)**

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

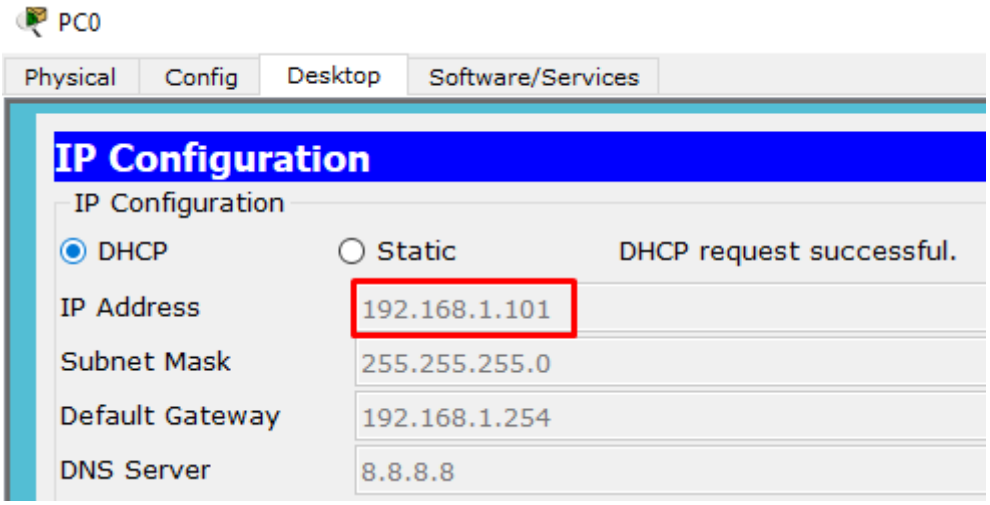
Jika dhcp sudah berhasil dan smua pc vlan bisa saling berkomunikasi dengan baik, sekarang kita perhatikan bahwa ip pada client diawali dengan host (1).

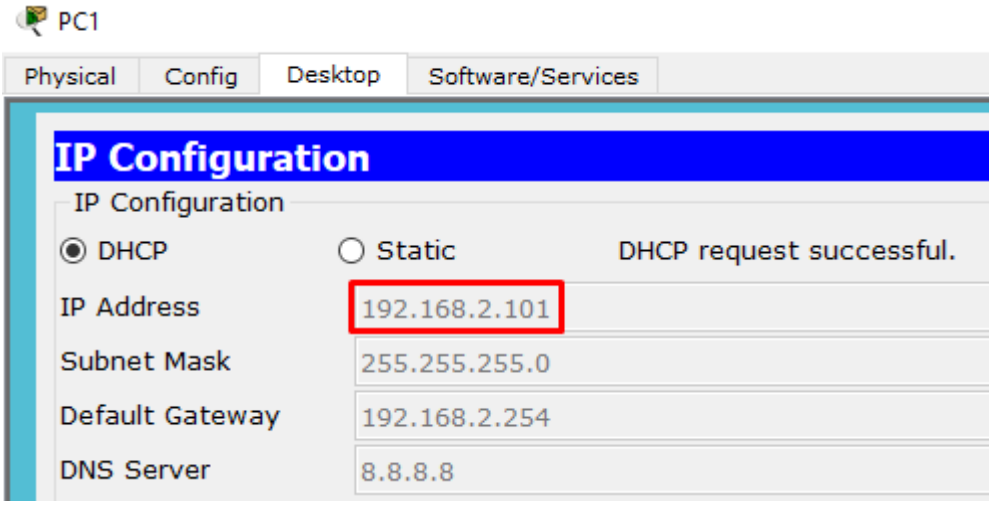
Ada kalanya kita bisa menyesuaikan ip mana saja yang boleh gunakan. Missal, ip yang berada pada PC0 (vlan 10) kita akan konfigurasikan tidak berawal dari 192.168.1.1, melainkan dimulai dari 192.168.1.101 begitu pula pada vlan 20.

Konfigurasinya adalah

```
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.100
Router(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.100
```

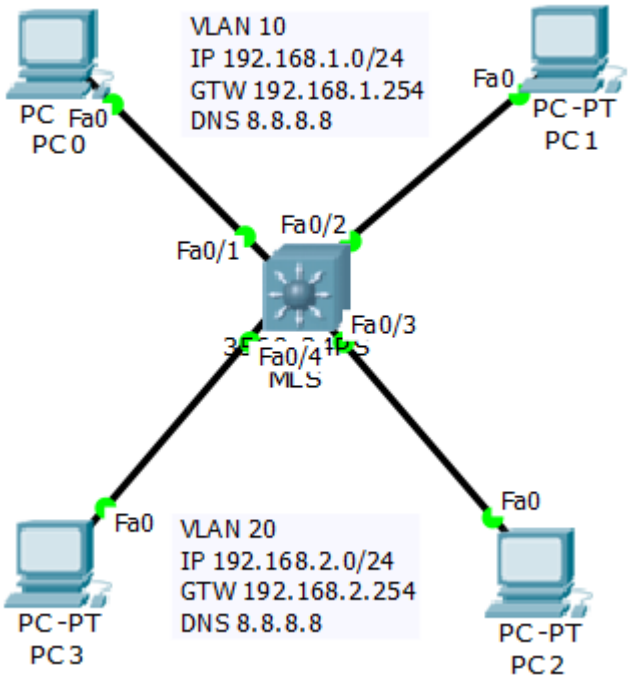
Sekarang kita ujicoba, silahkan pindahkan dari dhcp ke static lalu dhcp kan lagi.



# DHCP DI MULTILAYER SWITCH

Selain konfigurasi dhcp di router, dhcp juga bisa di konfigurasi pada multilayer switch karna switch ini support pada Layer 3 dan bisa menjalankan fungsi routing.




Pertama kita konfigurasikan vlan dan mengarahkan port sesuai dengan vlannya.

```
Switch#conf t
Switch(config)#host MLS
MLS(config)#vlan 10
MLS(config-vlan)#vlan 20
MLS(config-vlan)#int range fa0/1-2
MLS(config-if-range)#sw acc vlan 10
MLS(config-if-range)#int range fa0/3-4
MLS(config-if-range)#sw acc vlan 20
```

Cara di atas menggunakan ranges, jika port berurutan dan berada dalam vlan yang sama alangkah baiknya gunakan ranges agar lebih cepat dalam mengkonfigurasi.

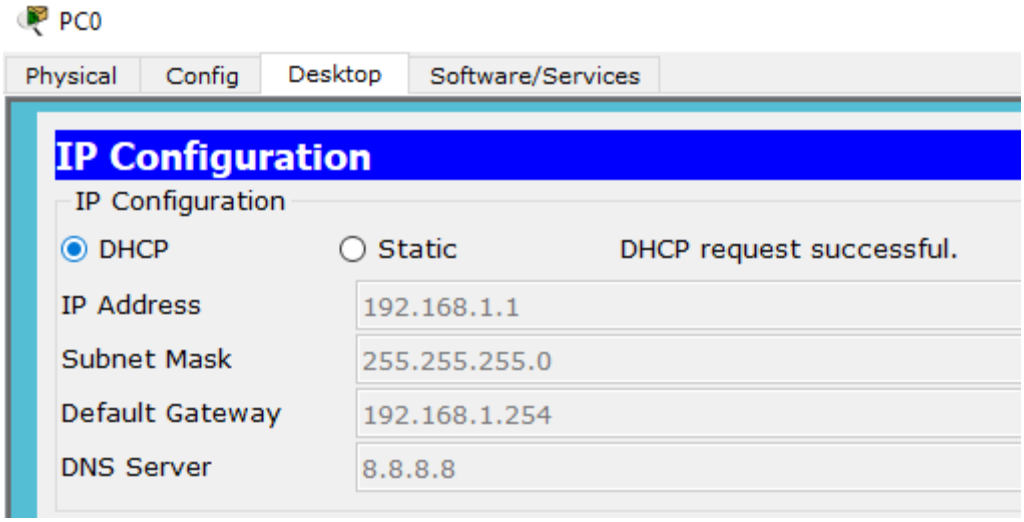
Konfigurasikan SVI

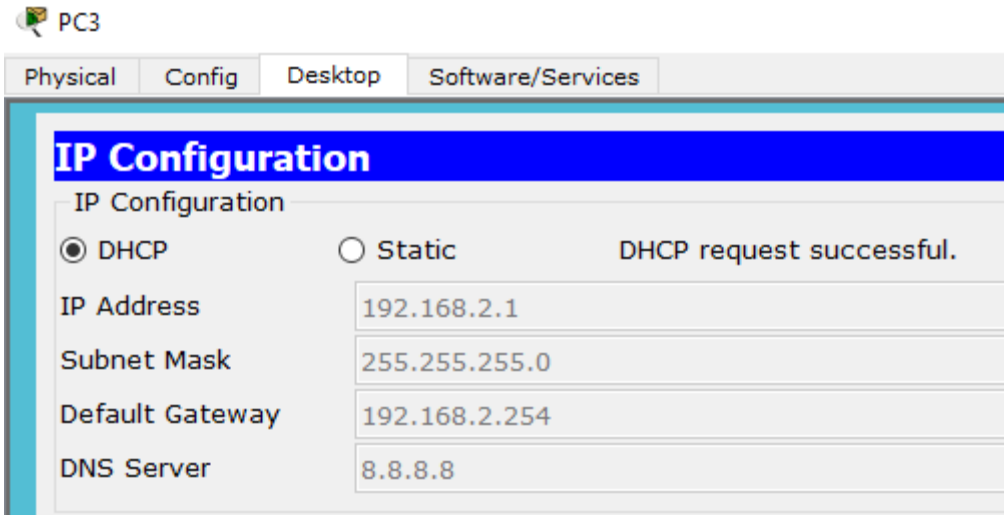
```
MLS(config)#int vlan 10
MLS(config-if)#ip add 192.168.1.254 255.255.255.0
MLS(config-if)#int vlan 20
MLS(config-if)#ip add 192.168.2.254 255.255.255.0
MLS(config)#ip routing  (jangan lupa di routing)
```

Konfigurasikan DHCP pada MLS

```
MLS(config)#ip dhcp pool vlan10
MLS(dhcp-config)#net 192.168.1.0 255.255.255.0
MLS(dhcp-config)#def 192.168.1.254
MLS(dhcp-config)#dns 8.8.8.8
MLS(dhcp-config)#ip dhcp pool vlan20
MLS(dhcp-config)#net 192.168.2.0 255.255.255.0
MLS(dhcp-config)#def 192.168.2.254
MLS(dhcp-config)#dns 8.8.8.8
```

Sekarang kita ujicoba dhcp yang sudah di konfigurasikan.






Setelah semuanya sudah mendapatkan dhcp, silahkan lakukan ping ke sesame dank e beda vlan. Dan pastikan hasilnya reply.

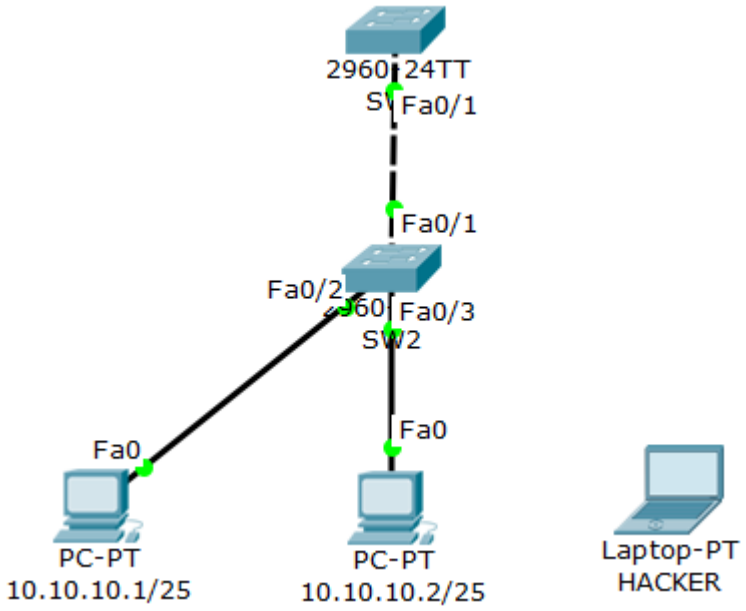
PC>ping 192.168.2.1 **(ke sesame vlan)**
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Reply from 192.168.2.1: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.1 **(ke beda vlan)**
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

# PORT SECURITY

Port security merupakan sebuah fitur yang memungkinkan kita untuk mengamankan switch dari gangguan orang-orang yang tidak bertanggung jawab. Dengan mengaktifkan port security, nantinya interface pada switch bisa otomatis mati ketika ada orang yang tidak bertanggung jawab menghubungkan komputernya dengan switch.

Untuk praktik konfigurasi port security ini, kita akan menggunakan topologi seperti berikut




Berikut konfigurasi yang perlu kita lakukan di SW1 untuk mengaktifkan port Security

```
Switch#conf t
Switch(config)#host SW1
SW1(config)#int fa0/1
SW1(config-if)#switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
```

Perhatikan bahwa saat kita mencoba mengaktifkan port security, ada sebuah pesan error yang menunjukkan bahwa kita tidak bisa mengaktifkan port security pada dynamic port, sehingga kita harus merubah dulu mode port tersebut menjadi static

```
SW1(config)#int fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#switchport port-security maximum 2
SW1(config-if)#switchport port-security violation shutdown
```

Perintah-perintah diatas digunakan untuk mengaktifkan port security pada interface fa0/1 SW1. Adapun penjelasan dari masing-masing perintah tersebut adalah sebagai berikut

- ***Switchport Port-Security*** Digunakan untuk mengaktifkan port security
- ***Switchport Port-Security Mac-Address Sticky*** Digunakan untuk mengkonfigurasikan metode dalam mendapatkan MAC Address. Ada dua metode yang dapat kita gunakana, yaitu static dan sticky. Sticky artinya switch akan mencatat MAC Address secara otomatis, MAC Address dari komputer pertama yang terhubung yang akan dicatat.
- ***Switchport Port-Security Maximum 2*** Digunakan untuk menentukan jumlah maximum device yang bisa connect
- ***Switchport Port-Security Violation Shutdown*** Digunakan untuk menentukan policy yang akan diterapkan saat ada device asing terhubung ke switch

Setelah mengaktifkan port security, kita coba lihat daftar mac address yang terhubung ke switch

```
SW1#show mac address-table
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
```

Perhatikan bahwa SW1 belum memiliki daftar mac address komputer yang terhubung dengan dirinya. Hal ini dikarenakan belum ada trafic sama sekali pada jaringan tersebut. Kita coba ping dari PC1 ke PC2 agar ada trafic yang beredar.

Setelah melakukan ping, kita coba lihat lagi tabel mac address di SW1

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0007.ec5a.6a01    STATIC      Fa0/1
   1    0060.709b.ac56    STATIC      Fa0/1
```

Perhatikan bahwa saat ini ada dua mac address yang terdaftar di SW1. Kita coba lihat status port security.

```
SW1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)       (Count)       (Count)
---------------------------------------------------------------------
       Fa0/1       2          2              0         Shutdown
---------------------------------------------------------------------
```

Perintah seperti diatas akan menunjukkan kepada kita status port security secara simpel. Untuk melihat status port security secara detail, gunakan perintah berikut

```
SW1#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0007.EC5A.6A01:1
Security Violation Count   : 0
```

Untuk melihat daftar mac address port security, kita bisa menggunakan perintah berikut

```
SW1#show port-security address
                          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address   Type                  Ports          Remaining Age
                                                           (mins)
----    -----------   ----                  -----          -------------
1       0060.709B.AC56      SecureSticky          FastEthernet0/1              -
1       0007.EC5A.6A01      DynamicConfigured     FastEthernet0/1              -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
```

Untuk pengujian, kita coba hubungkan PC hacker ke switch, kemudian kita coba ping dari PC penjahat ke IP manapun, tujaunnya adalah agar ada trafic dari PC penjahat Sesaat setelah melakukan ping, maka akan ada peringatan yang menunjukkan bahwa interface pada SW1 berubah menjadi shutdown

Untuk memastikan, kita langsung cek port-security fa0/1

```
SW1#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 0004.9A4C.34CB:1
Security Violation Count   : 1
```

Perhatikan bahwa saat ini status dari interface fa0/1 adalah shutdown. Untuk mengaktifkannya kembali, kita harus shutdown kemudian no shutdown secara manual

```
SW1(config)#int fa0/1
SW1(config-if)#sh
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
SW1(config-if)#
SW1(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up
```

Pada contoh diatas, kita menggunakan violation shutdown, selain shutdown, ada dua violation lagi yang dapat kita gunakan pada port security. Berikut beberapa violation pada port security beserta penjelasannya

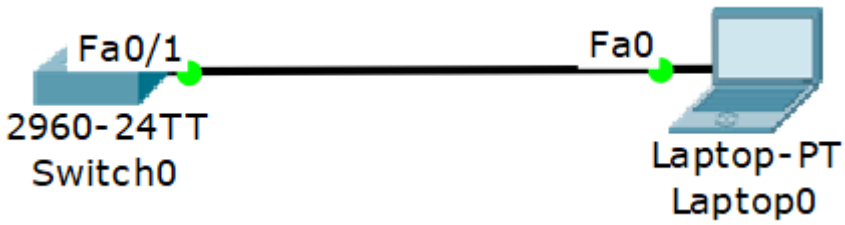
- **Shutdown** Interface akan shutdown saat ada PC asing yang konek
- **Protect** Data yang dikirimkan melalui interface tersebut tidak akan diforward (tidak dikirimkan)
- **Restrict** Sama halnya dengan protect, namun akan mengirimkan notifikasi SNMP

# TELNET DAN SSH

**Telnet** (Telecommunication network) adalah sebuah protokol jaringan yang digunakan untuk mengakses sebuah perangkat baik Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal.

SSH adalah aplikasi pengganti remote login seperti telnet, rsh, dan rlogin, yang jauh lebih aman. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Sama seperti telnet, SSH Client menyediakan User dengan Shell untuk remote ke mesin. Tidak seperti telnet, SSH menyediakan koneksi enkripsi antara klien dengan server. Dalam prakteknya, penggunaan menggunakan telnet dan ssh seperti perbedaan dengan mengakses website biasa dengan website yang lebih aman (HTTPS).

Jadi intinya, Telnet dan SSH merupakan sebuah protocol yang dapat di gunakan untuk melakukan remote access pada sebuah perangkat yang pada lab kali ini kita akan melakukan konfigurasikan pada switch agar switch dapat di remote melalui Telnet atau pun SSH




Dalam pengaktifan telnet kita harus mengkonfigurasikan IP pada switch terlebih dahulu, tetapi dengan catatan karna switch memang sebenar nya tidak dapat di beri IP maka kita dapat memberi IP pada vlan di switch yaitu vlan 1/vlan default.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#no shut
```

Selanjutnya isi ip addres Laptop0 sesuai ip yang sudah di konfigurasi tadi, dengan membedakan hostnya dan lakukan ping ke gateway (192.168.1.1)

```
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

Pastikan komunikasinya berjalan dengan baik.

Selanjutnya konfigurasikan telnet.

```
Switch(config)#line vty 0 4
Switch(config-line)#login local
Switch(config-line)#username zaky password 123
Switch(config)#enable secret 1234
```

Penjelasan :

**Line vty 0 4** → Line vty itu ialah virtual interface untuk meremote perangkat via network. Line vty 0 4, artinya dalam satu waktu bersamaan, maksimal bisa ada 5 koneksi yg mengremote perangkat tersebut (0 - 4 ada 5 bilangan: 0 1 2 3 4). Maksimal nya ialah 16 koneksi pada saat bersamaan (line vty 0 15)

**Login Local** → Loginnya menggunakan network yang berada pada localnya saja

**Username dan password** → digunakan pada saat login telnet, sedangkan enable scret digunakan untuk mengakses perangkan ketika kita ketikkan *enable*.

Jika semua sudah di konfigurasikan, sekarang kita ujicoba akses switch tersebut melalui telnet pada command prompt di Laptop0.

C:\>**telnet 192.168.1.1**
Trying 192.168.1.1 ...Open
User Access Verification
Username: zaky
Password:
Switch>enable
Password:

**Ini saya coba show running-config untuk melihat isi konfigurasi switch**
Switch#show running-config
Building configuration...

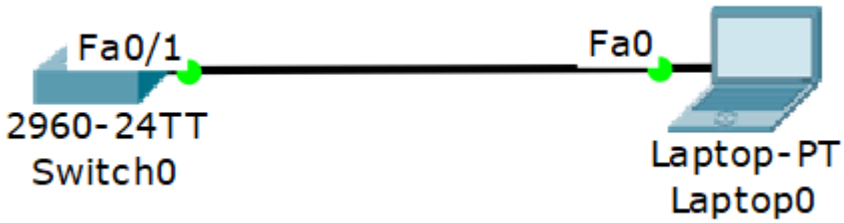
Current configuration : 1156 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$4dpRATIgxQacPVK0CfNV4/
!
!
!
!
username zaky privilege 1 password 0 123

Jika sudah masuk seperti di atas, berarti konfigurasi telnet kita sudah berjalan dengan baik.

***Lalu bagaimana dengan SSH di switch..??***

Pada dasar nya sebenar nya dilapangan telnet sudah jarang di pakai, hal ini di karna kan telnet tidak melakukan enskripsi terhadap packet yang di lewatkan, sehinggga packet kurang aman dan sangat mudah di ketahui oleh para orang yang kurang bertanggung jawab, maka dengan itu kita dapat melakukan remote access melalui SSH

Dan untuk topologi pada SSH kita sama menggunakan topologi pada telnet, tetapi kita hanya merubah service telnet menjadi SSH saja.




Konfigurasi username dan password masih sama, sekarang kita hanya menambahkan ip domain-name kedalam switch

```
Switch(config)#ip domain-name aytindeso.com
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
```

Terlihat disana ada warning bahwa kita harus mengganti hostname terlebih dahulu

```
Switch(config)#host SW1
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.aytindeso.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: ENTER
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
SW1(config)#line vty 0 4
*Mar 1 0:6:18.175:  RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:6:18.176:  %SSH-5-ENABLED: SSH 1.5 has been enabled
SW1(config-line)#transport input ssh
SW1(config-line)#login local
```

Jika sudah seperti di atas, sekarang kita uji coba login menggunakan ssh

```
Switch(config)#host SW1
SW1(config)#ip ssh version 2
*Mar 1 0:2:49.59:  RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:2:49.59:  %SSH-5-ENABLED: SSH 1.5 has been enabled
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
SW1(config)#line vty 0 5
SW1(config-line)#transport input ssh
SW1(config-line)#password zaky
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#
```

Jika sudah, silahkan login menggunakan ssh melalui laptop

```
C:\>ssh -l ssh 192.168.1.1
Open
Password:
SW1>en
Password:
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#
```

# SPANNING TREE PROTOCOL

Spanning Tree Protocol (STP) merupakan protocol yang berfungsi mencegah loop pada switch ketika switch menggunakan lebih dari 1 link dengan maksud redundancy. STP secara defaultnya diset aktif pada Cisco Catalyst. STP merupakan open standard (IEEE 802.1D).

Ada beberapa jenis STP:

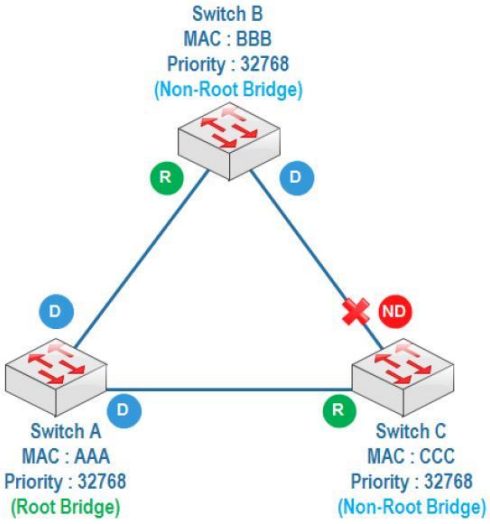
- Open Standard : STP (802.1D), Rapid STP (802.1W), Multiple Spanning Tree MST (802.1S)
- Cisco Proprietary : PVST (Per Vlan Spanning Tree), PVST+, Rapid PVST.


Ketika SwitchA mengirim packet data dengan destination yang tidak terdapat pada MAC address tabelnya, maka SwitchA akan membroadcast ke semua port sampai ke SwitchB. Jika pada tabel MAC address SwitchB juga tidak terdapat destination tadi maka Switch1 akan kembali membroadcast ke SwitchA dan akan seperti itu sehingga network down.

Ada beberapa cara mengatasi hal tersebut:

- Hanya menggunakan 1 link (no redundancy)
- Shutdown salah satu interface, melakukan shutdown manual pada salah satu interface atau secara otomatis menggunakan STP.

STP akan membuat blocking atau shutdown pada sala hsatu port untuk mencegah terjadinya loop. Ketika link utama down maka port yang sebelumnya blocking akan menjadi forward. Port blocking ditunjukkan dengan warna merah.




**Cara kerja STP :**

1. Ketika STP aktif, masing-masing switch akan mengirimkan frame khusus satu sama lain yang disebut *Bridge Protocol Data Unit (BPDU*).
2. Menentukan Root Bridge

   Switch dengan bridge id terendah akan menjadi root bridge. Bridge id = priority + MAC address. Dalam satu LAN hanya ada satu switch sebagai root bridge, switch lain menjadi non-root bridge. Default priority adalah 32768 dan bisa diubah.
3. Menentukan Root Port

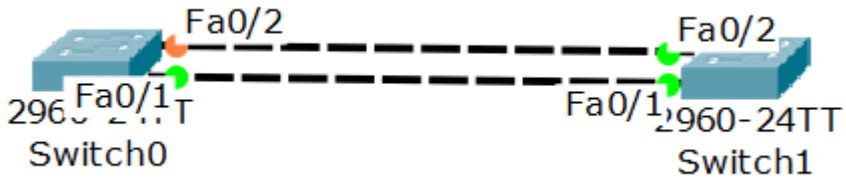
   Yang menjadi root port adalah path yang paling dekat dengan root bridge. Untuk setiap non-root bridge hanya punya 1 root port.
4. Menentukan designated port dan non-designated port

   Designated port adalah port yang forward dan non designated port adalah port yang blocking. Untuk root bridge semua portnya adalah designated port. Switch dengan priority terendah, salah satu portnya akan menjadi nondesignated port atau port blocking. Jika priority sama maka akan dilihat MAC address terendah.

STP akan membuat blocking atau shutdown pada salahsatu port untuk mencegah terjadinya loop. Ketika link utama down maka port yang sebelumnya blocking akan menjadi forward. Port blocking ditunjukkan dengan warna merah. STP menggunakan link cost calculation untuk menentukan root port pada nonroot switch.

# ROOT BRIDGE STP

Kali ini kita akan menetukan switch yang akan menjadi sebuah root bridge, dengan mengecilkan prioirty nya atau yang priority nya paling kecil dari yang lainnya.




```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0060.47DD.328E
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0060.7019.6078
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
```

Secara otomatis, Switch0 menjadi root bridge di karna mac–address nya yang paling kecil salah satu cara agar menjadi root bridge dengan cara di lihat dari IP – loopback atau dilihat dari priority semua portnya yang fordward (berwarna hijau), agar Switch1 yang menjadi root bridge, ubah priority pada Switch1

Terlihat disana bahwa root id prioritynya adalah 32769 dan jalur yang ke blok adalah fa0/2 di switch0.

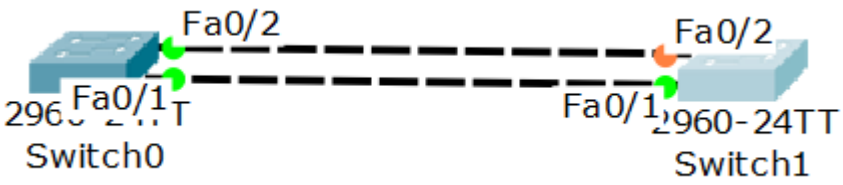
Ubah priority pada vlan nya dalam spanning – tree :

```
Switch(config)#spanning-tree vlan 1 priority 12288
```

Besar prioritry dapat di pilih dari 1 – 61440 , tetapi kita harus memasukan angka – angka nya yang lebih spesifik yang sudah ada pilihan nya yaitu :

**0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440**

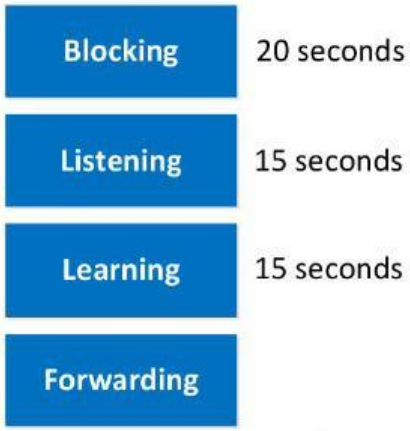
Dan priority default dari spanning – tree adalah 32768 dan 1 nya itu di tambah dari vlan nya (default vlan)




Maka switch yang menjadi root bridge yaitu yang priority nya lebih kecil

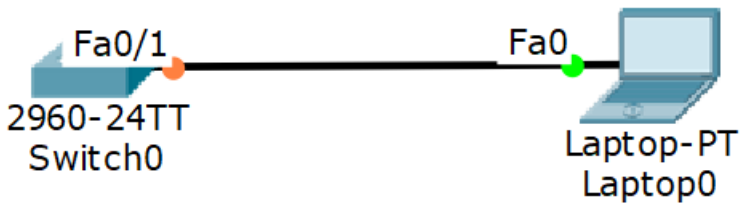
# SPANNING TREE PORT FAST

Spanning tree port fast merupakan salah satu fitur STP,yang mana di saat kita menancapkan kabel pada switch maka kita akan melewati beberapa sesi, sampai yang akhir nya menjadi forwading, dengan Spanning tree port fast ini kita akan di percepat dalam melewati beberapa proses tersebut




Switch akan melewati step blocking sekitar 20 detik kemudian melewati step listening sampai 15 detik lalu learning sampai 15 detik dan kemudian sampai lah pada step forwading, dan apabila kita menginginkan agar dapat langsung melewati dari step blocking langsung ke step forward tanpa harus melewati listening dan learning terlebih dahulu maka di butuhkan spanning tree port fast.

Port fast ini cocok di gunakan untuk port yang mengarah ke end host, tetapi tidak direkomendsikan untuk port yang mengarah ke switch karena akan menonaktifkan fungsi STP dalam mencegah looping.

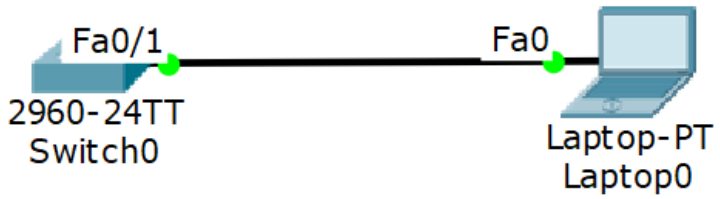



Langsung saja kita konfigurasikan di interface fa0/1 yang ingin di konfigurasikan STP port-fast

```
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree portfast
```

*Remember me in your pray*

Hanya dengan itu maka pada saat host mencolokan kembali ke port yang sudah dikonfigurasikan ia akan langsung ke step forward atau kalau di di cisco packet tracer lampu nya akan langsung hijau tidak oren terlebih dahulu seperti pada gambar di berikut.



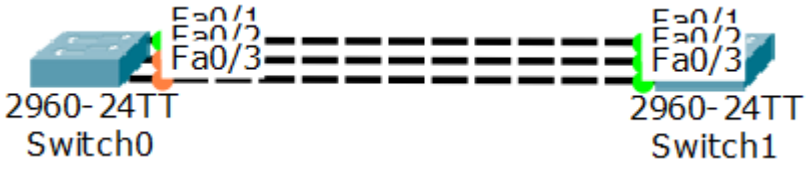
# ETHERCHANNEL

Kalau pada lab sebelum nya kita membahas tentang spanning tree protocol (STP) yaitu membuat beberapa interface kita block dan menyisakan satu interface agar tidak membuat looping, dan pada lab kali ini kita akan mengambung kan beberapa interface/link dan menggambungkan menjadi satu interface/link yang mana kita harus menoaktifkan STP yang mana tidak ada yang nama nya blocking port.


Dalam etherchanel terdapat 3 protocol :

1. **LACP** (Link Aggregation Control Protocol) – open standard IEEE 802.1AD. Yang mana ia telah open std, pada perangkat yang lain yang terbagi menjai beberapa mode :
   - **Active** : yang artinya ia mengajak untuk di jadikan etherchannel LACP
   - **Passive** : yang artinya ia akan menuggu di ajak menjadi ethercahnnel
2. **PAGP** (Port Agregation Protocol)
   PAGP merupakan cisco proprietary yang hanya masih di miliki oleh cisco, dan pada PAGP terdapat beberapa mode :
   - **Desirable** : yang arti nya ia akan mengajak untuk menjadi etherchannel
   - **Auto** : yaitu sebalik nya ia akan menuggu untuk di jadikan etherchannel
3. **Static Etherchannel (L3)** :
   Static Etherchannel hanya bekerja pada layer 3 dngan menggunakan IP, dalam etherchannel layer3 hanya memiliki 1 mode, yaitu Mode **ON** : mode ini sama saja dengan mengajak.

Untuk etherchannel LACP dan PAGP kita akan mengunaka topologi yang sama, dengan dua switch.



**Etherchannel LACP**

Konfigurasikan trunk ke semua interface di semua switch

```
Switch#conf t
Switch(config)#host SW1
SW1(config)#int range fa0/1-3
SW1(config-if-range)#sw mode trunk
```

```
Switch#conf t
Switch(config)#host SW2
SW2(config)#int range fa0/1-3
SW2(config-if-range)#sw mode trunk
```

Konfiguarsikan LACP untuk yang satu nya mengajak dan yang satu nya menunggu atau bisa juga dengan ke dua nya sama – sama mengajak :

```
SW1(config-if-range)#channel-group 1 mode active
```

```
SW2(config-if-range)#channel-group 1 mode passive
```

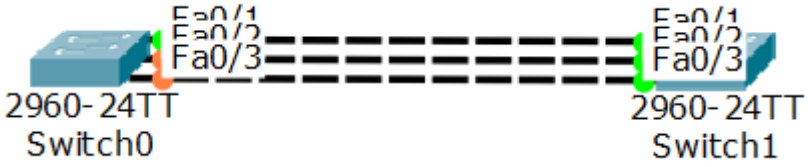
Untuk melihat statusnya bisa kita show etherchannelnya

```
SW1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          LACP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

```
SW2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          LACP    Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

**Etherchannel PAGP**

Masih menggunakan topologi lab sebelumnya.




```
Switch#conf t
Switch(config)#host SW1
SW1(config)#int range fa0/1-3
SW1(config-if-range)#sw mode trunk
```

```
Switch#conf t
Switch(config)#host SW2
SW2(config)#int range fa0/1-3
SW2(config-if-range)#sw mode trunk
```

```
SW1(config-if-range)#channel-group 1 mode desirable
```

```
SW2(config-if-range)#channel-group 1 mode auto
```

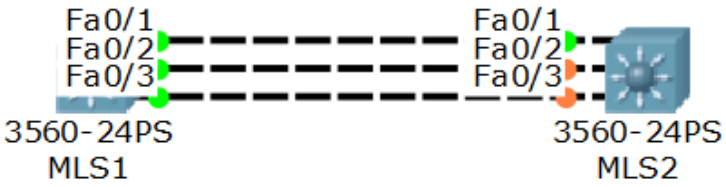
Sekarang kita show ethercannelnya, dan pastikan sudah menjadi pagp

```
SW1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          PAgP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

```
SW2#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          PAgP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

## Static Etherchannel (L3)

Dalam etherchannel layer 3 kita akan mengunakan multi layer switch atau MPLS yang mana pada layer 3 kita akan mengunakan IP, dan akan menonaktifkan fungsi switch. Pada lab kali ini kita akan menggunakan 2 perangkat MPLS




Dalam etherchannel layer 3 kita tidak perlu membuat interface trunk, jadi kita langsung saja membuat etherchannel dengan mode on.

```
Switch>en
Switch#conf t
Switch(config)#host MLS1
MLS1(config)#int range fa0/1-3
MLS1(config-if-range)#channel-group 1 mode on
```

```
Switch#conf t
Switch(config)#host MLS2
MLS2(config)#int range fa0/1-3
MLS2(config-if-range)#channel-group 1 mode on
```

Setelah kita buat interface channel-group tersebut maka kita harus masuk ke interface tersebut kemudian menonaktifkan fungsi switch agar bisa di beri IP.

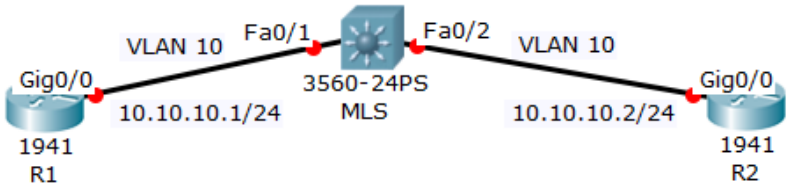
```
MLS1(config)#int port-channel 1
MLS1(config-if)#no sw
MLS1(config-if)#ip add 192.168.1.1 255.255.255.0
```

```
MLS2(config)#int port-channel 1
MLS2(config-if)#no sw
MLS2(config-if)#ip add 192.168.1.2 255.255.255.0
```

# VITRUAL LINK VLAN

Dalam vlan, ada juga virtual link. Yaitu metode menghubungkan perangkat router dengan router lainnya menggunakan vlan. Jadi simpelnya, jika ada router ingin berkomunikasi baik satu network maupun beda network bisa menggunakan metode ini. Jika sebelumnya vlan itu hanya untuk membedakan PC, sekarang kita akan hubungkan router dengan vlan sebagai pengantar paketnya.

Berikut topologinya :




Dari topologi di atas, silahkan masukkan ip address sesuai dengan interfacenya, kemudian pada MLS hanya mengarahkan vlan sesuai vlannya.

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/0
R2(config-if)#ip add 10.10.10.2 255.255.255.0
R2(config-if)#no sh
```

Jika sudah sampai langkah ini, R1 dan R2 belum bisa berkomunikasi, karena dia tidak bisa mengenali ip/network antara keduanya. Maka dari itu kita harus konfigurasikan MLS sebagai penjembatan komunikasi melalui vlan.

MLS

```
Switch>en
Switch#conf t
Switch(config)#host MLS
MLS(config)#vlan 10
MLS(config-vlan)#int range fa0/1-2
MLS(config-if-range)#sw access vlan 10
```

Jika sudah, silahkan lakukan ping antar router dan pastikan hasilnya bisa reply.

```
R1#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

# Chapter 2
## ROUTING

Static Route

Default Route

Dynamic Route (EIGRP)

Dynamic Route (OSPF Backbone Area/Area 0)

Dynamic Route (OSPF Multi Area)

ACL (Access List)

Standard ACL

Extended ACL

Named ACL

NAT (Network Address Translation)

Static NAT

Overload NAT (PAT)

High Availability (HSRP)

DHCP Relay

Redistribute

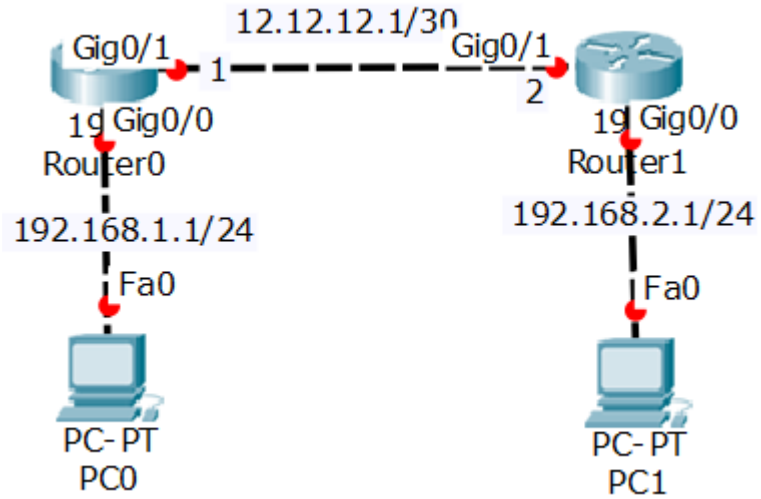
# STATIC ROUTE

Static router merupakan suatu mekanisme dalam routing yang mana kita akan mengkonfigurasi kan suatu network agar dapat saling terhubung dengan network lain nya dengan mengkonfigurasi secara static/manual.

Untuk static route sendiri di konfigurasikan secara manual untuk menentukan setiap jalurnya, jadi semakin banyak routing banyak konfigurasi yang kita lakukan. Salah satu keunggulan static route ia memiliki Administrative Distance (AD) 1 yang ia akan lebih di pilih dari pada routing protocol-protocol lainnya. Sedangkan kekurangan dari static route adalah :

- No CPU cycles are used to calculate and communicate routes.
- The path a static route uses to send data is known.
- Konfigurasi dan maintenance yang memakan waktu
- Tidak cocok untuk network skala besar.
- Untuk jaringan kecil yang tidak akan terjadi perubahan topologi secara significant
- hanya mempunyai 1 exit path (karena hanya mempunyai satu neighbor).
- Untuk unknown network menggunakan default route untuk topologi.

Berikut topologinya



Langkah pertama ialah kita konfigurasikan dulu ip address di setiap portnya.

```
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int gig0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.252
R1(config-if)#no sh
```

```
Router#conf t
Router(config)#host R2
R2(config)#int gig0/1
R2(config-if)#ip add 12.12.12.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#int gig0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no sh
```

Setelah ip address sudah di konfigurasikan di setiap portnya, sekarang kita konfigurasikan static route untuk menentukan jalur routing sesuai topologi.

```
R1(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
```

```
R2(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
```

Kosnep static route intinya adalah (network tujuan-netmask-nexthops) menambahkan jalur routing ke tujuan dengan cara manual, artinya seorang administrator harus membuat manual jalur routingnya. Dalam bahasa mudahnya static route itu "*mau kemana lewat mana*". Maka yang menjadi barometer adalah nexthops nya (jalur terdekat)

Sekarang kita coba lihat jalur yang sudah kita buat tadi

Lakukan pengecekan static route yang kita buat tadi.

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/30 is directly connected, GigabitEthernet0/1
L       12.12.12.1/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
S    192.168.2.0/24 [1/0] via 12.12.12.2
```

Tanda S disitu berarti menunjukan bahwa routing protocol nya menggunakan static

Jika sudah silahkan lakukan ping antar pc, dan pastikan pc bisa saling komunikasi.

```
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

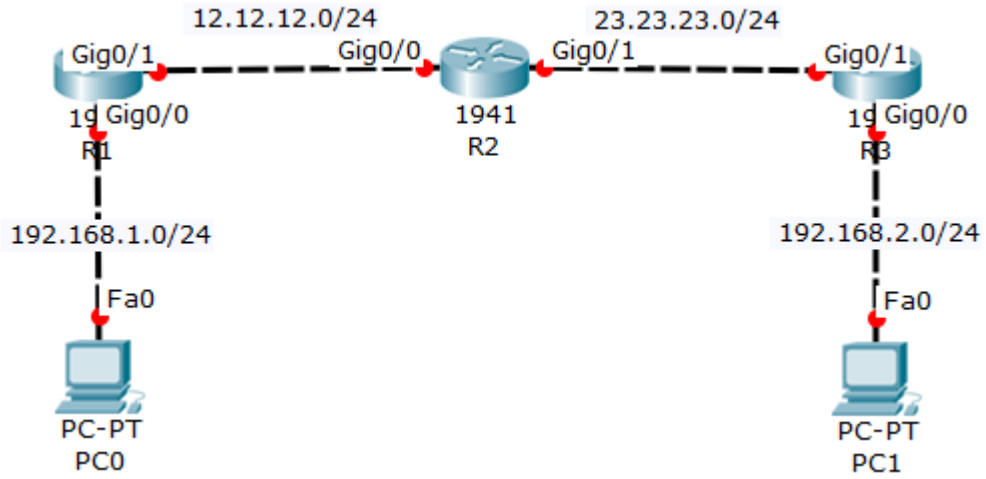
Maka hasil nya pun reply, dan setelah kita test ping antar PC, maka untuk mengetahui jalur pengeriman data nya maka kita dapat tracert untuk menuju destinationnya dengan tracerroot

```
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1   0 ms     0 ms     0 ms     192.168.1.1
  2   0 ms     0 ms     0 ms     12.12.12.2
  3   0 ms     0 ms     0 ms     192.168.2.2

Trace complete.
```

# DEFAULT ROUTE

Default routing sebenarnya masuk dalam static routing. Biasa digunakan untuk routing ke internet. Pada tabel routing, default routing selalu berada paling bawah dan selalu menjadi last preferred (pilihan terakhir).

ip route (spasi) 0.0.0.0 (spasi) 0.0.0.0 (spasi) ip/interface next- hop




Konsepnya masih sama dengan lab sebelumnya, hanya saja konfigurasi kali ini tidak menggunakan ip interface untuk menambahkan table routingnya, akan tetapi menggunkan default routing yaitu 0.0.0.0

Isi ip address di setiap interface

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh

R1(config-if)#int gig0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh

R2(config-if)#int gig0/1
R2(config-if)#ip add 23.23.23.1 255.255.255.0
R2(config-if)#no sh
```

R3

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int gig0/0
R3(config-if)#ip add 192.168.2.1 255.255.255.0
R3(config-if)#no sh

R3(config-if)#int gig0/1
R3(config-if)#ip add 23.23.23.2 255.255.255.0
R3(config-if)#no sh
```

Sekarang konfigurasikan default routingnya

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2

R2(config)#ip route 0.0.0.0 0.0.0.0 23.23.23.2
R2(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.1

R3(config)#ip route 0.0.0.0 0.0.0.0 23.23.23.1
```

Lakukan verifikasi

```
R1#sh ip route
S*   0.0.0.0/0 [1/0] via 12.12.12.2

R2#show ip route
S*   0.0.0.0/0 [1/0] via 23.23.23.2
              [1/0] via 12.12.12.1

R3#sh ip route
S*   0.0.0.0/0 [1/0] via 23.23.23.1
```

Default route ditandai dengan S*

Dan lakukan pengujian jg dari pc client bisa sling komunikasi.

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=14ms TTL=128
Reply from 192.168.2.2: bytes=32 time=4ms TTL=128
Reply from 192.168.2.2: bytes=32 time=4ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 5ms
```

Hasilnya pun akan sama persis dengan static route, hanya saja kali ini kita menggunakan default route sebagai table routingnya.

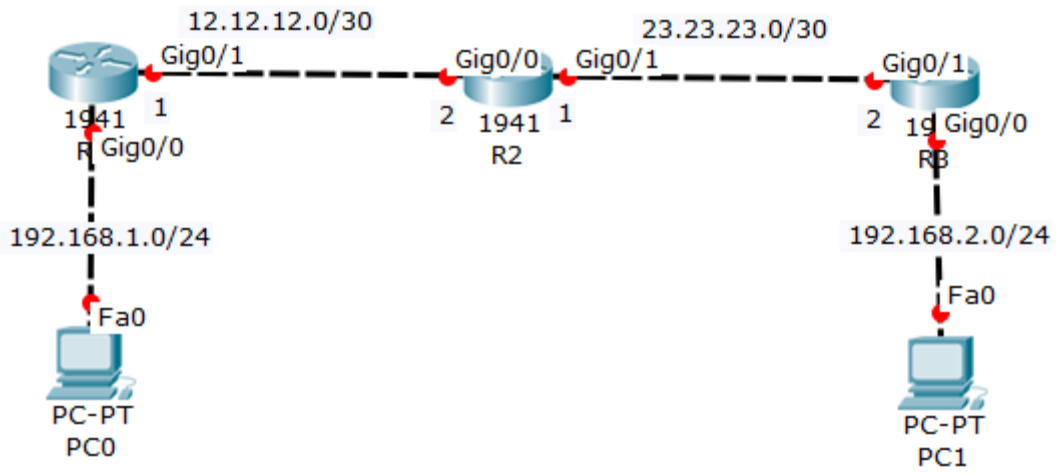
# DYNAMIC ROUTE (EIGRP)

Kalau pada lab sebelum nya kita telah membahas tentang routing dengan static/manual, maka pada lab kali ini kita akan membahas salah satu protocol routing dynamic yaitu EIGRP *(Enhanced Interior Gateway Protocol)* EIGRP merupakan salah satu protocol dalam dynamic route yang hanya dimiliki oleh cisco, yang dalam kata lain routing EIGRP ini merupakan salah satu dari cisco propitary yang mana ia hanya dapat di gunakan pada perankat cisco saja Routing EIGRP ini memiliki administrative distance sebanyak 90, update dalam routing EIGRP mengunakan multicast : 224.0.0.10, jumlah maksimal hop count nya 255 (default 100), memiliki konvergensi yang cepat, pengirirman hello packet di kirim setiap 5 second (dead interval 15 second), mendukung equal dan unequal cost load balancing.

Keuntungan routing EIGRP yaitu 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 router – router yang sharing informasi route, atau yang dapat di artikan hanya router yang memiliki ASN yang bisa shraring informasi route.

Untuk topolgi pada lab kali ini kita akan menggunakan 3 router dan 2 client yang mana kita akan menghubung kan beberapa network yang berbeda dengan menggunakan routing EIGRP



Sebelum kita konfigurasi routing pada router maka kita harus konfigurasikan terlebih dahulu ip address pada setiap router sesuai pada topologi

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int gig0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.252
R1(config-if)#no sh
```

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#int gig0/1
R2(config-if)#ip add 23.23.23.1 255.255.255.252
R2(config-if)#no sh
```

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int gig 0/0
R3(config-if)#ip add 192.168.2.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int gig0/1
R3(config-if)#ip add 23.23.23.2 255.255.255.252
R3(config-if)#no sh
```

Setelah mengkonfigurasi kan ip address pada setiap interface maka kita dapat memulai mengkonfigurasikan routing EIGRP

Karna default dari routing EIGRP classfull apabila kita ingin mengkonfigurasi kan dengan IP clasess maka kita harus mengkonfigurasikan *"no auto summary"*, dan kita harus sama saat memasukan AS number nya apabila berbeda maka router tidak akan bisa bertukar informasi routing nya

Konfigurasi routing EIGRP:

```
R1(config)#router eigrp 10
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.1.0
R1(config-router)#net 12.12.12.0
```

```
R2(config)#router eigrp 10
R2(config-router)#no auto-summary
R2(config-router)#net 12.12.12.0
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 12.12.12.1 (GigabitEthernet0/0) is up: new adjacency

R2(config-router)#net 23.23.23.0
```

Terlihat disana sudah ada adjency antara network 12.12.12.0 dari R1 dan R2

```
R3(config)#router eigrp 10
R3(config-router)#no auto-summary
R3(config-router)#net 23.23.23.0
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 23.23.23.1 (GigabitEthernet0/1) is up: new adjacency

R3(config-router)#net 192.168.2.0
```

Network 23.23.23.0 pun sudah adjency.

Setelah itu kita dapat meilihat tabel routing dari masing – masing router pastikan disetiap router memiliki tabel routing yang lengkap pada semua network, yang akan memiliki status "D" yang berarti EIGRP :

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/30 is directly connected, GigabitEthernet0/1
L       12.12.12.1/32 is directly connected, GigabitEthernet0/1
     23.0.0.0/30 is subnetted, 1 subnets
D       23.23.23.0/30 [90/3072] via 12.12.12.2, 00:03:28, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D    192.168.2.0/24 [90/5632] via 12.12.12.2, 00:01:46, GigabitEthernet0/1
```

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/30 is directly connected, GigabitEthernet0/0
L       12.12.12.2/32 is directly connected, GigabitEthernet0/0
     23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       23.23.23.0/30 is directly connected, GigabitEthernet0/1
L       23.23.23.1/32 is directly connected, GigabitEthernet0/1
D    192.168.1.0/24 [90/5376] via 12.12.12.1, 00:05:29, GigabitEthernet0/0
D    192.168.2.0/24 [90/5376] via 23.23.23.2, 00:03:41, GigabitEthernet0/1
```

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     12.0.0.0/30 is subnetted, 1 subnets
D       12.12.12.0/30 [90/3072] via 23.23.23.1, 00:05:28, GigabitEthernet0/1
     23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       23.23.23.0/30 is directly connected, GigabitEthernet0/1
L       23.23.23.2/32 is directly connected, GigabitEthernet0/1
D    192.168.1.0/24 [90/5632] via 23.23.23.1, 00:05:28, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
```

Setelah masing – masing router sudah memiliki tabel routing yang kengkap maka kita dapat coba test ping antar PC1 dengan PC2 apakah sudah dapat saling terhubung atau reply :

```
C:\>ping 192.168.2.2   dari PC0 ke PC1

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=125
Reply from 192.168.2.2: bytes=32 time=11ms TTL=125
Reply from 192.168.2.2: bytes=32 time=12ms TTL=125
Reply from 192.168.2.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 8ms
```

Apabila reply maka konfigurasi pada routing EIGRP sudah berhasil kita lakukan, dan antar router sudah dapat bertukar data/informasi.

# OSPF BACBONE AREA (0)

Pada lab kali ini kita akan membahas routing protocol lain nya dalam routing dynamic yaitu OSPF (Open Shortest Path First), routing protocol OSPF ini termasuk bagian dari *link state* yang mana ia akan mengirim sebuah data atau packet melalui jalur yang bandwith terbesar atau nilai cost yang kecil, untuk jumlah administratif distance berjumlah 110.

OSPF ini sekarang merupakan protocol yang sudah banyak di pakai perusahan dalam routing untuk jaringan yang berskala besar di karna kan mudah nya mengkonfigurasikan nya dan juga yang bersifat open vendor/yang dapat di konfigurasi kan di setiap vendor.

Untuk perhitungan cost pada OSPF dapat di rumuskan dengan

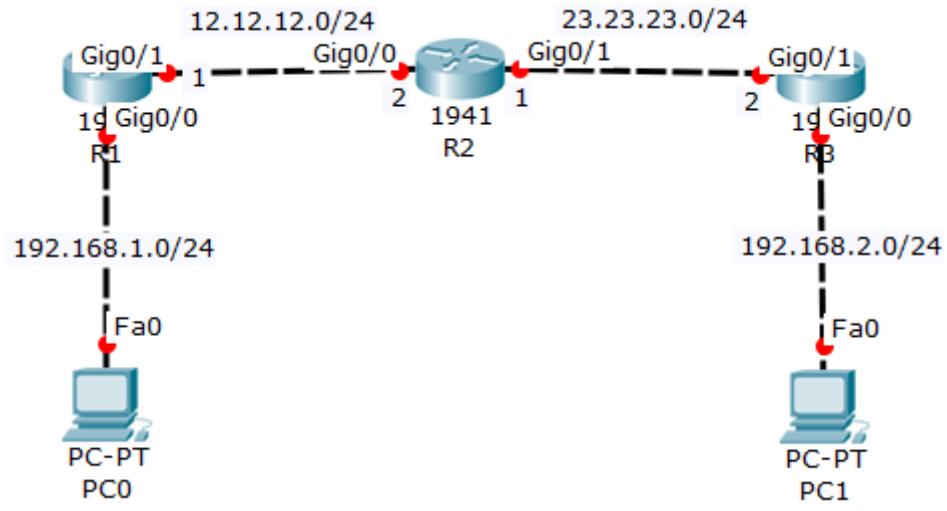
$$\frac{\text{Reference Bandwith}}{\text{Bandwith}}$$

Reference bandwith adalah ketetapan bandwith yaitu 100mb, yang kemudian dibagi bandwith yang sesuai dengan bandwith pada kabel yang di pakai pada router :

- Gigabyte Ethernet : 1000MB
- Fast Ethernet : 100MB
- Etherner : 10MB

Maka hasil dari pembagian tersebut merupakan cost dari suatu link OSPF tersebut

Kita akan gunakan topologi yang sama seperti lab sebelumnya, yang perlu kita lakukan adalah menghapus konfigurasi EIGRP terlebih dahulu.



Pada routing Dynamic OSPF kita akan memasukan network yang terhubung pada router tersebut atau yang terdapat pada tabel routing sebelum di routing, kemudian kita masukan wildcart masknya Cara mencari wildcart mask yaitu 255.255.255.255 di kurang subnet mask, karna pada lab kali ini kita mengunakan prefix 24 maka subnetmask nya yaitu 255.255.255.0 kemudian apabila dikurang dengan 255.255.255.255 maka hasil nya adalah 0.0.0.255 maka itu adalah wildcart mask yang akan kita gunakan.

Dan untuk lab OSPF pada kali ini kita hanya akan mengunakan 1 area yaitu area backbone atau *area0.*

Konfigurasi ip address

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int gig0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
```

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int gig0/1
R2(config-if)#ip add 23.23.23.1 255.255.255.0
R2(config-if)#no sh
```

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int gig0/0
R3(config-if)#ip add 192.168.2.1 255.255.255.0
R3(config-if)#no sh
R3(config)#int gig0/1
R3(config-if)#ip add 23.23.23.2 255.255.255.0
R3(config-if)#no sh
```

Konfigurasi OSPF

```
R1(config)#router ospf 1
R1(config-router)#net 192.168.1.0 0.0.0.255 area 0
R1(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#net 12.12.12.0 0.0.0.255 area 0
R2(config-router)#net 23.23.23.0 0.0.0.255 area 0
```

```
R3(config)#router ospf 1
R3(config-router)#net 192.168.2.0 0.0.0.255 area 0
R3(config-router)#net 23.23.23.0 0.0.0.255 area 0
```

Maka dengan ini maka konfigurasi routing OSPF sudah selsai maka coba kita lihat kembali tabel routing pada setiap router apakah sudah terdaftar network router yang lain, dan pastikan status nya yaitu "O" yang berarti OSPF.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, GigabitEthernet0/1
L       12.12.12.1/32 is directly connected, GigabitEthernet0/1
     23.0.0.0/24 is subnetted, 1 subnets
O       23.23.23.0/24 [110/2] via 12.12.12.2, 00:03:29, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/3] via 12.12.12.2, 00:01:19, GigabitEthernet0/1
```

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, GigabitEthernet0/0
L       12.12.12.2/32 is directly connected, GigabitEthernet0/0
     23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       23.23.23.0/24 is directly connected, GigabitEthernet0/1
L       23.23.23.1/32 is directly connected, GigabitEthernet0/1
O    192.168.1.0/24 [110/2] via 12.12.12.1, 00:06:20, GigabitEthernet0/0
O    192.168.2.0/24 [110/2] via 23.23.23.2, 00:03:37, GigabitEthernet0/1
```

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     12.0.0.0/24 is subnetted, 1 subnets
O       12.12.12.0/24 [110/2] via 23.23.23.1, 00:04:42, GigabitEthernet0/1
     23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       23.23.23.0/24 is directly connected, GigabitEthernet0/1
L       23.23.23.2/32 is directly connected, GigabitEthernet0/1
O    192.168.1.0/24 [110/3] via 23.23.23.1, 00:04:42, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
```

Selanjutnya silahkan isi ip pada masing-masing pc sesuai dengan ip nya.

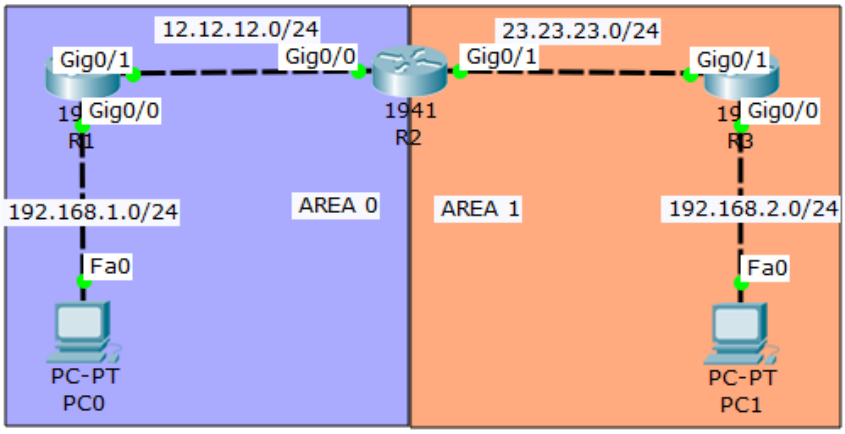
Lakukan verifikasi dengan cara ping antar pc dalam topologi

```
C:\>ping 192.168.2.2   Ping dari PC0 ke PC1

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=125
Reply from 192.168.2.2: bytes=32 time=11ms TTL=125
Reply from 192.168.2.2: bytes=32 time=11ms TTL=125
Reply from 192.168.2.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

# OSPF MULTI AREA

Melanjutkan materi dari lab sebelumnya, yaitu OSPF. Akan tetapi kali ini kita akan buat dua area, yaitu backbone (area 0) dan area 1.

Masih menggunakan topologi yang sama, dan hapus konfigurasi ospf disemua router




```
R1(config)#no router ospf 1

R2(config)#no router ospf 1

R3(config)#no router ospf 1
```

R1

```
R1(config)#router ospf 10
R1(config-router)#net 192.168.1.0 0.0.0.255 area 0
R1(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

R2

```
R2(config)#router ospf 11
R2(config-router)#net 23.23.23.0 0.0.0.255 area 1
R2(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

R3

```
R3(config)#router ospf 12
R3(config-router)#net 192.168.2.0 0.0.0.255 area 1
R3(config-router)#net 23.23.23.0 0.0.0.255 area 1
```

Untuk verifikasi, lakukan show ip route di setiap router

```
R1#sh ip route
Gateway of last resort is not set
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, GigabitEthernet0/1
L       12.12.12.1/32 is directly connected, GigabitEthernet0/1
     23.0.0.0/24 is subnetted, 1 subnets
O IA    23.23.23.0/24 [110/2] via 12.12.12.2, 00:02:03, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O IA 192.168.2.0/24 [110/3] via 12.12.12.2, 00:00:30, GigabitEthernet0/1
```

Tanda IA menunjukkan bahwa destination route berada pada area yang berbeda

Kalukan ping antar PC

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms
```

# ACCESS LIST (ACL)

Pada lab kali ini kita akan membahas tentang yang nama nya access – list, yang mana fungsi dari access – list bisa di katakan sebagai filtering sebuah packet yang melewati router, jadi router akan memfilter packet–packet mana saja yang di boleh kan atau di larang melewati router.

Dalam access – list sendiri terbagi menjadi 2 jenis yaitu :

- Standard Access – list : pada standard access – list ini ACL akan di konfigurasikan pada router yang terdekat dengan destination, pada ACL standard ini kita hanya dapat memblock sebuah network, subnet, dan host untuk action dalam memfilter nya hanya terdapat deny (dilarang) dan permit (dibolehkan)
- Extended Access – list : hampir sama dengan standard ACL, yang membedakan pada ACL extended ini memiliki fitur yang lebih

| Standard Access List | Extended Access List |
|---|---|
| ACL Number Range 1-99 | ACL number range 100-199 |
| Can block a network, host and subnet | Can allow or deny a network, host, subnet and ***service*** |
| All service are blocked | Select device can be blocked |
| Implemented closest to the destination | Implemented closest to the destination |
| Filtering based on source IP Address only | Filtering based on source ip address, destination ip, protocol and port number |

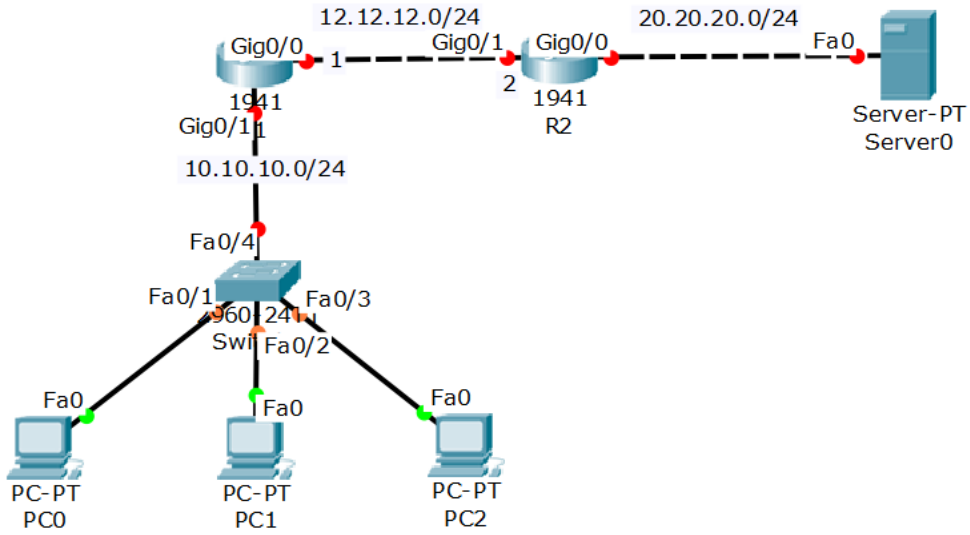
Untuk default dari ACL sendiri yaitu deny (dilarang/menolak) jadi di saat kita mengkonfigurasi kan ACL maka otomatis semua trafick yang lewat akan terblock atau deny, yang pada dasar nya kita hanya mengkonfigurasi kan hanya beberapa host saja yang di block, tetapi semua nya akan ikut terblock, itu di karna kan default dari ACL deny, maka dari itu kita harus mengkonfigurasi kan permit any (bolehkan semua) pada rule terkahir.

# STANDARD ACL

Standard ACL :

- Standard ACL hanya dapat melakukan filtering berdasarkan IP host atau IP network source nya saja.
- Standard ACL mengunnakan ACL number 1 – 99
- Konfigurasi sedekat mungkin dengan destination
- Direction in dan out nya ditentukan berdasarkan arah packet nya dari source menuju destination

Berikut topologi untuk standard acl




Tujuan pada lab ini kita akan men-deny (memblock) network 10.10.10.0 agar tidak dapat terhubung dengan network server yaitu 20.20.20.0 tetapi network 10.10.10.0 masih dapat terhubung ke network 12.12.12.0 maka kita akan memfilter nya dengan menggunakan ACL standard.

Sebelum kita mengkonfigurasi kan ACL maka kita dapat mengkonfigurasikan IP address pada router sesuai topologi dan konfigurasi trunk pada switch yang mengarah ke router.

SW1

```
Switch>en
Switch#conf t
Switch(config)#host SW1
SW1(config)#int fa0/4
SW1(config-if)#sw mode trunk
```

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/1
R1(config-if)#no sh
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#int gig0/0
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/1
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int gig0/0
R2(config-if)#ip add 20.20.20.1 255.255.255.0
R2(config-if)#no sh
```

Karna antar router kita memiliki network yang berbeda, oleh karena itu kita harus mengkonfigurasi kan juga routing pada setiap router, agar lebih mudah kita dapat membuat routing dynamic EIGRP

R1

```
R1(config)#router eigrp 10
R1(config-router)#no auto-summary
R1(config-router)#net 12.12.12.0
R1(config-router)#net 10.10.10.0
```

R2

```
R2(config)#router eigrp 10
R2(config-router)#no auto-summary
R2(config-router)#net 12.12.12.0
R2(config-router)#net 20.20.20.0
```

Setelah setiap perangkat sudah di konfigurasikan IP masing – masing dan sudah di routing maka kita dapat langsung mengkonfigurasikan ACL pada router terdekat dengan destination.

Sebelum nya pastikan bahwa semua client di switch sudah dapat PING ke server, karna pada lab kali ini destination kita adalah network 20.20.20.0 maka kita dapat

mengkonfigurasikan nya di R2 dan memberi nya di interafce yang mengarah ke server yaitu out apabila source nya dari network 10.10.10.0

Konfigurasikan ACL pada R2 :

```
R2(config)#access-list 1 deny 10.10.10.0 0.0.0.255
R2(config)#access-list 1 permit any
```

Setelah kita membuat ACL maka ACL tersebut harus kita masukan atau tanamkan pada interface yang terdekat pada destination di R2, yaitu interface gig0/0. Jika kita analisa apabila source address yang berasal dari network 10.10.10.0 maka interface nya kita konfigurasikan out

```
R2(config)#int gig0/0
R2(config-if)#ip access-group 1 out
```

untuk verivikasi kita dapat melakukan ping dari PC menuju server

PC0 ke server

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1 ke server

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

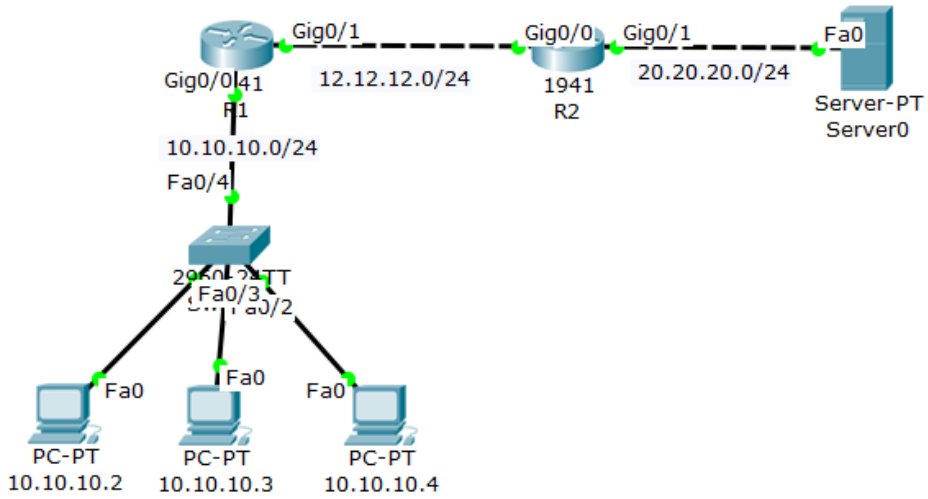
PC2 ke server

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Maka client dari network 10.10.10.0 akan ter-deny ketika menuju network 20.20.20.0 yang mengarah kan server

**Standard Access List (Contoh-2)**

Pada lab kali ACL standard contoh-2 kita akan memblock source yang berasal dari salah satu host / satu client saja, kalau pada lab ACL standard sebelum nya kita memblock seluruh host dengan memblock network nya, maka pada lab kali ini kita hanya memblock salah satu saja yang tidak dapat terhubung sedangkan yang lain nya masih dapat terhubung.




Tujuan pada lab kali ini yaitu agar host yang memiliki ip 10.10.10.2 tidak dapat mengakses network 20.20.20.0 tetapi host yang lain nya atau yang berIP 10.10.10.3 dan 10.10.10.4 masih dapat mengakses network 20.20.20.0

Lalu bagaimana kah cara nya ..??, maka kalau pada lab sebelum nya kita mendeny sebuah network maka pada lab kali ini kita akan mendeny hostnya kemudian kita masukan IP dari host yang ingin kita deny tadi.

Kita akan lanjutkan topologi sebelumnya. Kita hanya perlu menghapus konfigurasi routing eigrp pada lab sebelumnya, dan menghapus acl yang sudah di konfigurasi tadi, dan pastikan sudah tidak ada lagi routing kecuali hanya network yang terhubung lasngsung saja (direcly connected)

```
R1(config)#no router eigrp 10


R2(config)#no router eigrp 10
R2(config)#no access-list 1 deny 10.10.10.0 0.0.0.255
R2(config)#no access-list 1 permit any

R2(config-if)#no ip access-group 1 out  ← menghapus out dari interface gig0/1
```

Selanjutnya kita konfigurasikan topologi di atas yang akan mendeny pada host 10.10.10.2 dan allow untuk 10.10.10.3 dan 10.10.10.4

Konfigurasikan ospf dngan AD 10

```
R1(config)#router ospf 10
R1(config-router)#net 10.10.10.0 0.0.0.255 area 0
R1(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 10
R2(config-router)#net 20.20.20.0 0.0.0.255 area 0
R2(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

Setelah sudah maka pastikan setiap client dapat ping ke server, maka setelah itu kita dapat langsung mengkonfigurasi kan ACL pada router yang paling terdekat pada destination yaitu R2

IP host yang akan kita deny adalah IP dari PC0 yaitu 10.10.10.2 dan untuk PC yang lainnya tetap dapat mengakses network 20.20.20.0

Karna default dari access-list ini adalah deny maka apabila kita tidak membuat konfigurasi ACL untuk mem-permit yang lainnya, secara otomatis smua juga akan di deny. Oleh karna itu kita juga harus membuat konfigurasi ACL untuk mempermit

Konfigurasi ACL

```
R2(config)#access-list 1 deny host 10.10.10.2
R2(config)#access-list 1 permit any
R2(config)#int gig0/1
R2(config-if)#ip access-group 1 out
```

Lakukan verifikasi

```
R2(config-if)#do show access-list
Standard IP access list 1
    10 deny host 10.10.10.2
    20 permit any
```

Dapat di lihat rule untuk ACL yang sudah di pilah-pilah tadi. Perhatikan bahwa ACL akan membaca rule dari atas ke bawah jadi apabila kita membuat konfigurasi untuk mempermit terlebih dahulu maka konfiguraasi denynya tidak akan dibaca oleh ACL karna sudah tertiban oleh konfigurasi permit yang tadi.

Maka setelah itu kita dapat mencoba test ping dari PC1 dengan IP 10.10.10.2 menuju network 20.20.20.0

PC0

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

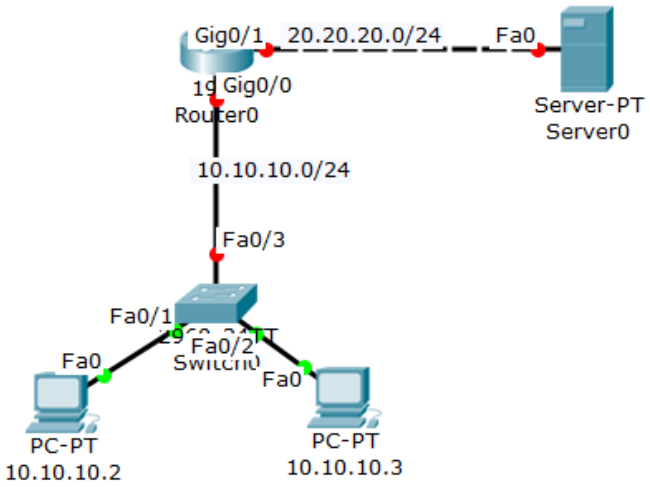
PC1

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 20.20.20.2: bytes=32 time=1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=10ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=10ms TTL=126

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms
```

# EXTENDED ACL

Pada lab kali ini kita akan membahas salah satu jenis access-list yaitu extended access-list yang mana salah satu perbedaan extended acl ini memiliki fiutr yang lebih mendalam dari pada standard access – list, apabila dalam standard acl kita hanya dapat memfilter yang berasal dari source saja, maka pada extended acl ini dapat memfilter seperti destination, protocol, port dan lain sebagainya atau dapat di katakan extended acl ini merupakan acl yang lebih spesifik dari pada standard acl

Berikut topologinya :




Pada topologi kali ini kita akan memfilter salah sartu client dengan IP 10.10.10.2, agar tidak dapat melakukan ping ke network server, dan untuk client ip 10.10.10.3 kita akan memfilter agar tidak dapat mengakses http.

Jadi kita akan memfilter menggunakan ACL extended untuk source address 10.10.10.2 tidak dapat melakukan ping maka kita konfigurasikan deny protocol ICMP kemudian untuk client 10.10.10.3 kita akan konfigurasikan deny http/tcp 80.

Sebelum kita mengonfigurasi kan kita dapat mengkonfigurasi kan ip address terlebih dahulu pada setiap interface pada masing-masing device sesuai pada topologi

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gig0/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int gig0/1
R1(config-if)#ip add 20.20.20.1 255.255.255.0
R1(config-if)#no sh
```

SW1  Konfigurasikan trunk yang mengarah ke R1

```
Switch>en
Switch#conf t
Switch(config)#host SW1
SW1(config)#int fa0/3
SW1(config-if)#sw mode trunk
```

Setelah mengkonfigurasikan ip address kita dapat memulai dengan mengkonfigurasikan ACL extended untuk client dengan ip 10.10.10.2 deny icmp dan client 10.10.10.3 deny tcp 80

```
R1(config)#access-list 100 deny icmp host 10.10.10.2 20.20.20.0 0.0.0.255
R1(config)#access-list 100 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq 80
R1(config)#access-list 100 permit ip any any
```

Beberapa keterangan di atas :

**100** = pengklasifikasian access – list extended(100–199) atau standard(1-99)

**Deny** = action dari ACL permit(izinkan) ataukah deny(dilarang)

**Icmp** = protocol yang akan di filter

**Host** = jenis yang akan kita filter perhost atau network dan lain sebagainya

**10.10.10.2** = source address (sumber ip address)

**20.20.20.2** = destination (tujuan ip address)

**0.0.0.0255** = wilcard mask

**Eq** = untuk penghususan port dalam tcp atau udp

**Permit ip any any** = di karna kan default dari ACL deny maka agar apabila terdapat client lain yang terhubng tidak ikut terfilter atau deny maka kita harus menambahkan permit ip any any

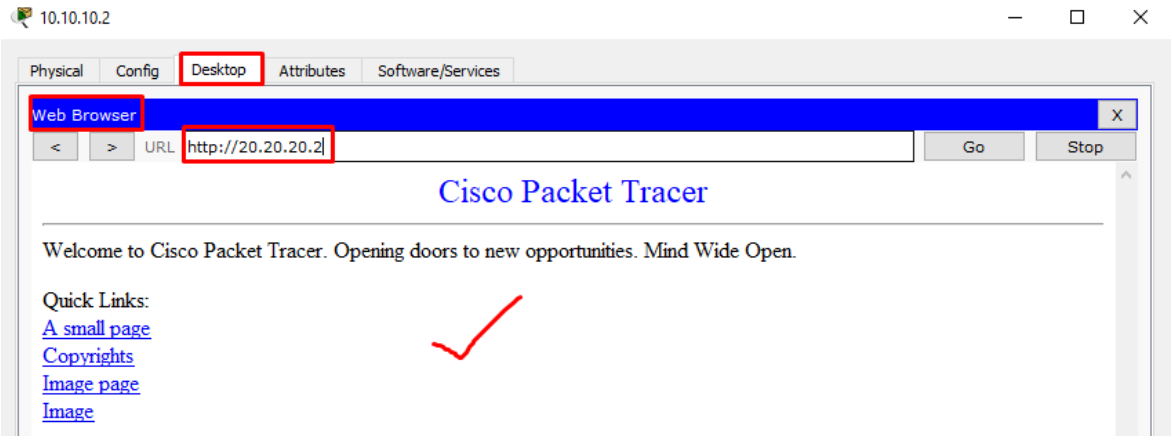
Setelah kita mengkonfigurasi kan ACL kita dapat  tanamkan konfigurasi ACL ke dalam interface

```
R1(config)#int gig0/1
R1(config-if)#ip access-group 100 out
```

Untuk verifvikasi kita dapat melakukan test ping dari client 10.10.10.2 ke 20.20.20.2 kemudian test akses web

PC dengan ip 10.10.10.2

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

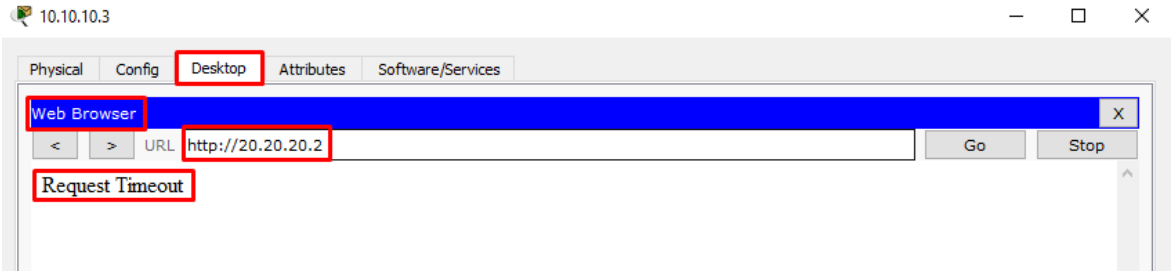



Jika hasilnya seperti di atas, PC dengan ip 10.10.10.2 tidak bisa mengakses 20.20.20.0/24 dengan icmp, akan tetapi masih bisa mengakses network 20.20.20.0 dengan browser.

Sekaran ujicoba PC dengan ip 10.10.10.3

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 20.20.20.2: bytes=32 time=1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127
Reply from 20.20.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

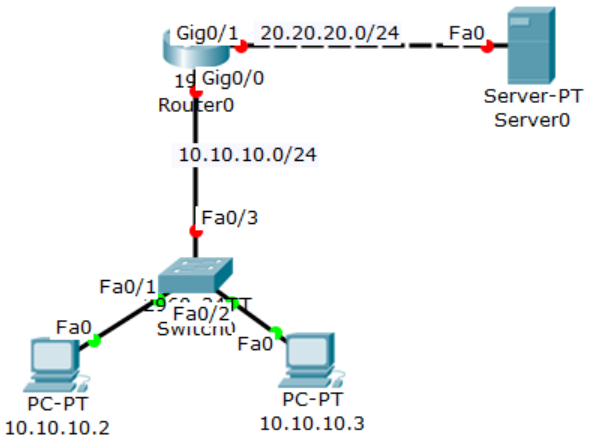
Lalu coba menggunakan browser



## Extended Access-list (contoh-2)

Pada lab kali ini kita akan mengkonfigurasikan dengan manggunkan range yang mana pada lab kali ini kita akan mendeny 2 protocol sekaligus yaitu http dan https

Untuk lab kali ini kita masih menggunakan topologi pada lab sebelumnya.




Kita akan mendeny HTTP pada client1 10.10.10.2 dan mendeny HTTP dan HTTPS pada ip 10.10.10.3 menggunakan range pada ACL.

Sebelum mengkonfigurasikan ACL kita hapus terlebih dulu konfigurasi acl pada lab sebelumnya.

```
R1(config)#no access-list 100 deny icmp host 10.10.10.2 20.20.20.0 0.0.0.255
R1(config)#no access-list 100 deny tcp host 10.10.10. 20.20.20.0 0.0.0.255 eq 80
R1(config)#no access-list 100 permit ip any any
R1(config)#int gig0/1
R1(config-if)#no ip access-group 100 out
```

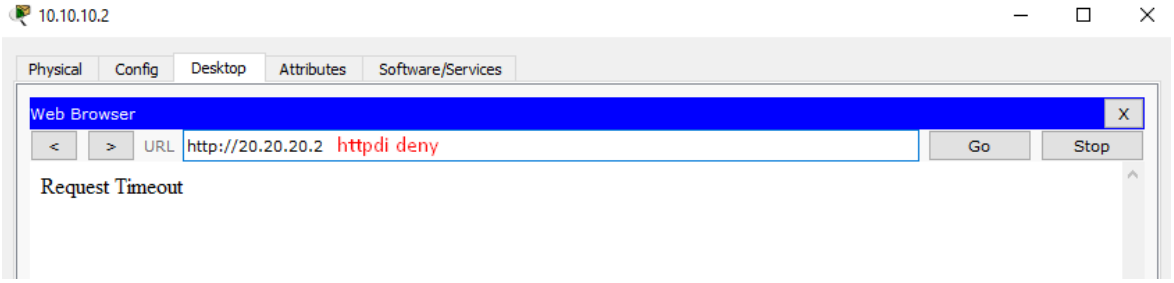
Kemudian kita dapat lanjut dengan mengkonfigurasikan ACL extended dengan memulai dengan mengkonfigurasiakn rule untuk memfilter client 10.10.10.2 dengan deny HTTP dan dilanjutkan 10.10.10.3 deny HTTP dan HTTP dengan menggunakan range

```
R1(config)#access-list 100 deny tcp host 10.10.10.2 20.20.20.0 0.0.0.255 eq 80
R1(config)#access-list 100 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 range 80
443
R1(config)#access-list 100 permit ip any any
```

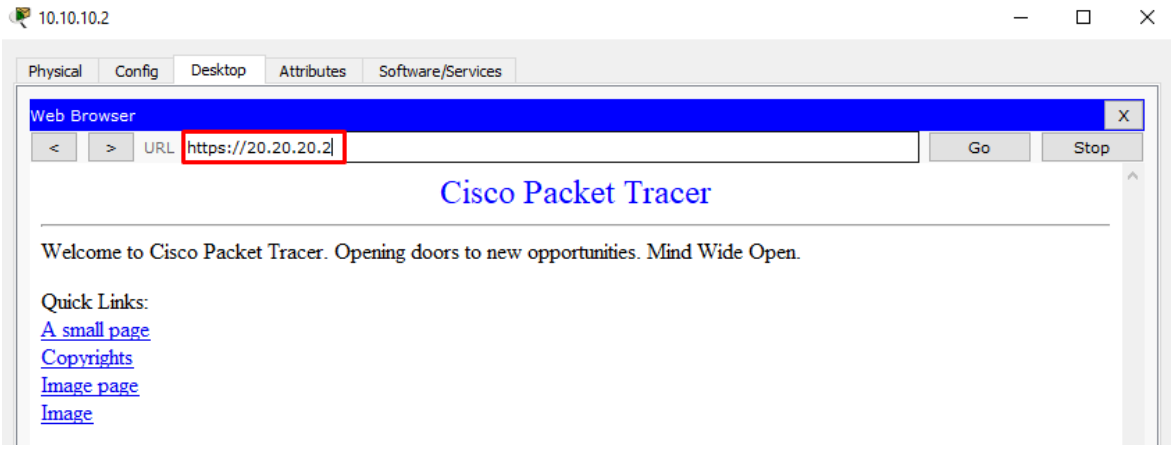
Setelah itu kita dapat konfigurasi kan ACL yang telah kita buat tadi kedalam interface router apakah itu in ataukah out

```
R1(config)#int gig0/1
R1(config-if)#ip access-group 100 out
```

Untuk verifikasi kita dapat lakukan akses HTTP pada PC1

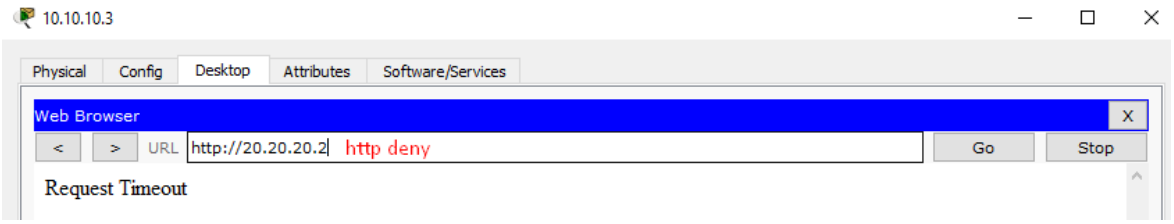


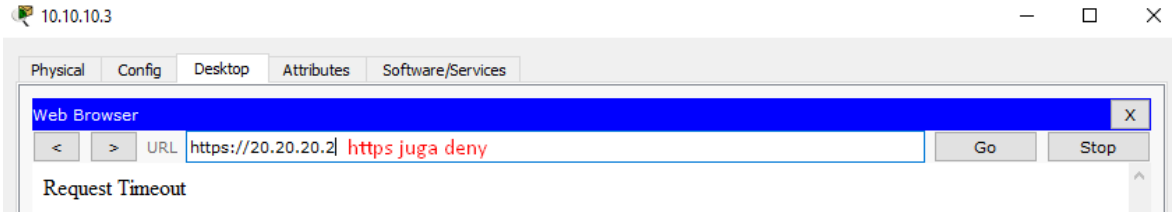

Lalu verifikasi menggunakan https




Terlihat disana bahwa PC1 ketika mengakses http secara otomatis sudah deny, tapi tidak jika mengaksesnya menggunakan https PC ini masih bisa mengakses network tsb.

Untuk selanjutnya kita akan verifikasi/ujicoba menggunakan PC dengan host 10.10.10.3 sesuai dengan konfigurasi kita tadi yaitu kita men-deny http dan https



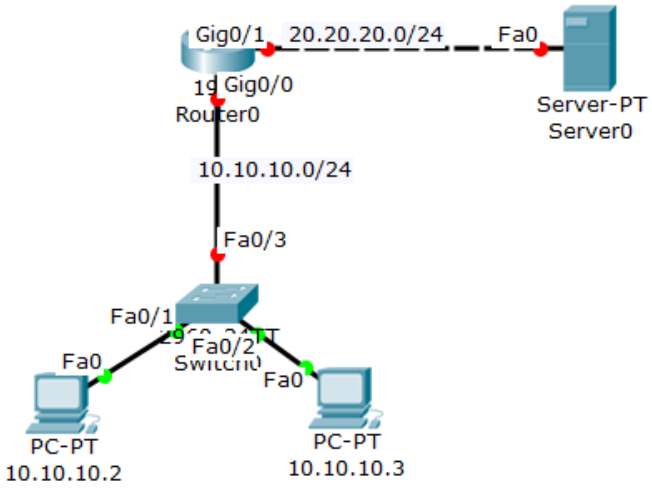

Jika hasilnya seperti ini, maka kita telah berhasil mengkonfigurasi sesuai dengan topologi yang sudah direncanakan.

# NAMED ACL

Pada lab kali ini kita akan mengkonfigurasikan ACL dengan menggunakan name, yaitu pada ACL ini kita dapat menetukan sequenece number atau dalam kata lain kita dapat mencustome urutan rule kita sendiri.

Apabila pada lab sebelum nya kita *"sh ip access-list"* maka ia akan terlihat rule pada ACL, yang mana ACL ia akan membaca rule dari atas ke bawah, maka apabila terdapat salah satu konfigurasi yang kurang maka kita tidak dapat menghapus salah satu konfigurasi dalam ACL tersebut, kecuali kita menghapus ACL tersebut dan mengkonfigurasi nya dari awal kembali.

Topologi yang akan kita gunakan masih sama seperti lab sebelumnya, hanya saja sekarang kita akan reload/hapus seluruh konfigurasinya (agar terbiasa dalam konfigurasi).




Pastikan sudah tidak ada konfigurasi apapun pada router (kecuali ip pc)

Kita akan mengkonfigurasikan extended ACL dengan menggunakan ACL name, dengan mendeny client1 yaitu 10.10.10.2 dan deny ICMP serta client2 10.10.10.3 deny HTTP dan HTTPs, disini kita tidak menggunakan range akan tetapi hanya menambahkan rule

Berikan ip address di setiap interface

```
R1(config)#int gig0/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int gig0/1
R1(config-if)#ip add 20.20.20.1 255.255.255.0
R1(config-if)#no sh
```

Kita akan mendeny ICMP dan HTTP pada client1, kemudian untuk client2 permit any setelah itu kita dapat menyisipkan rule untu k deny HTTPS pada client2

```
R1(config)#ip access-list extended zaky
R1(config-ext-nacl)#10 deny icmp host 10.10.10.2 20.20.20.0 0.0.0.255
R1(config-ext-nacl)#15 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq 80
R1(config-ext-nacl)#20 permit ip any any
```

Beberapa keterangan di atas :

**Extended :** ACL yang akan di gunakan standard atau extended

**zaky :** nama ACL yang kita gunakan (bebas)

**10 :** sequence number (urutan rule)

**Deny :** action ACL (deny/permit)

**ICMP :** protocol yang ingin di filter (tcp/udp, ICMP dll)

**Host :** jenis filter host, network dan lain sebagai nya

**10.10.10.2 :** source address

**20.20.20.2 :** destination address

**0.0.0.255 :** wilcard mask

**Eq 80 :** identifikasi number port

Dengan ini kita telah mengkonfigurasi kan deny ICMP (ping), HTTTP, dan permit any, tetapi kita belum mengkonfigurasikan deny untuk HTTPS.

pada dasar nya apabila kita menggunakan ACL dengan konfigurasi biasaseperti pada lab sebelum nya kita tidak dapat menyisipkan rule di antara rule-rule yang lain dan apabila kita menambahkan rule dengan ACL maka rule tersebut sudah tidak terbaca di karna kan ACL membaca dari atas kebawah dan rule tersebut berada pada rule "*permit ip any any"* maka rule deny sudah tidak dapat terbaca kembali oleh ACL

Show ip access-list

```
R1#show ip access-list
Extended IP access list zaky
    10 deny icmp host 10.10.10.2 20.20.20.0 0.0.0.255
    15 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq www
    20 permit ip any any
```

Selanjutnya kita akan menyisipkan rule di antara sequence 10 dan 15 untuk deny HTTPS

```
R1(config)#ip access-list extended zaky
R1(config-ext-nacl)#13 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq 443
```

Show ip access-list

```
R1#sh ip access-lists
Extended IP access list zaky
    10 deny icmp host 10.10.10.2 20.20.20.0 0.0.0.255
    13 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq 443
    15 deny tcp host 10.10.10.3 20.20.20.0 0.0.0.255 eq www
    20 permit ip any any
```

Maka kita telah menyisipkan salah satu rule kedalam ACL , yang mana merupakan salah satu kelebihan dalam penggunaan ACL name

Setelah itu jangan lupa ACL yang telah kita konfigurasikan di tanamkan  dalam interface router

```
R1(config)#int gig0/1
R1(config-if)#ip access-group zaky out
```

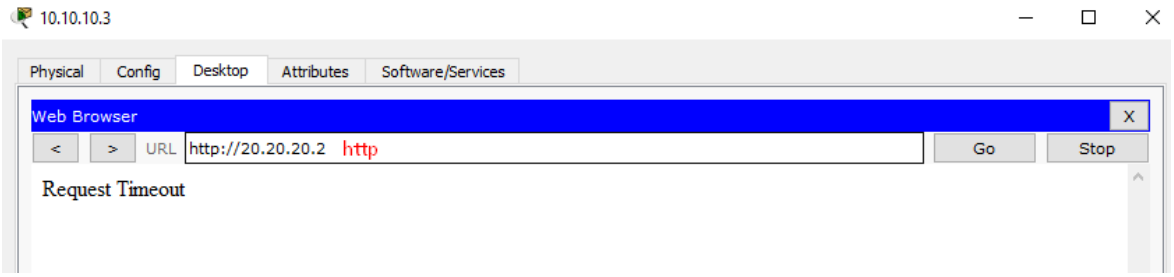
Kalau pada ACL biasa kita menggunakan number ACL nya, pada ACL name kita menggunakan nama dari ACL tersebut yang telah kita konfig

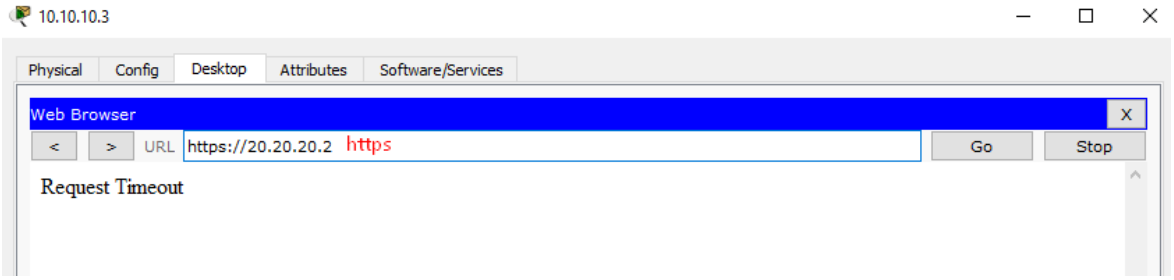
Untuk verivikasi dapat di lakukan dengan test ping dari client1 dan aksess HTTP dan HTTPS pada client2

PC1 (ip 10.10.10.2)

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC2 (ip 10.10.10.3)



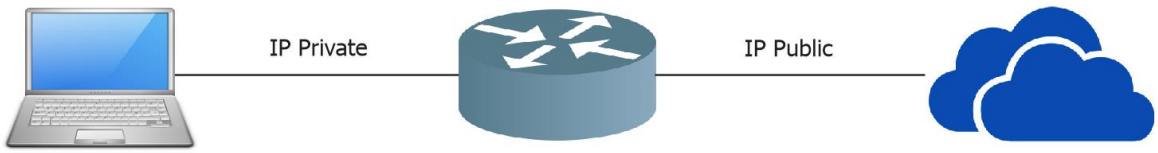



# NETWORK ADDRESS TRANSLATION (NAT)

**NAT** adalah sebuah proses pemetaan alamat IP dimana perangkat jaringan komputer akan memberikan alamat IP public ke perangkat jaringan local sehingga banyak IP private yang dapat mengakses IP public.

Dengan kata lain NAT akan mentranslasikan alamat IP sehingga IP address pada jaringan local dapat mengakses IP public pada jaringan WAN. NAT mentranslasikan alamat IP private untuk dapat mengakses alamat host diinternat dengan menggunakan alamat IP public pada jaringan tersebut. Tanpa hal tersebut (NAT) tidaka mungkin IP private pada jaringan local bisa mengakses internet.

- Berfungsi untuk menerjemahkan atau merubah IP seperti dari IP privat menjadi IP public
- Ip privat sendiri tidak dapat di gunakan dalam internet, maka dari itu kita harus menerjemahkan Ip privat tersebut ke dalam ip public dengan menggunakan NAT
- Dapat digunakan apabila terdapat suatu server local yang ingin diakses mengunakan internet maka digunakan IP public
- Dapat digunakan apabila ingin koneksi VPN menuju kantor mengunakan IP public




Dalam konfigurasi NAT interface dibagi mejadi 2 kategori :

- Inside : traffic yang masuk ke interface yang berasal dari local network
- Outside : traffic yang keluar dari interface router yang menuju ke destination (internet).

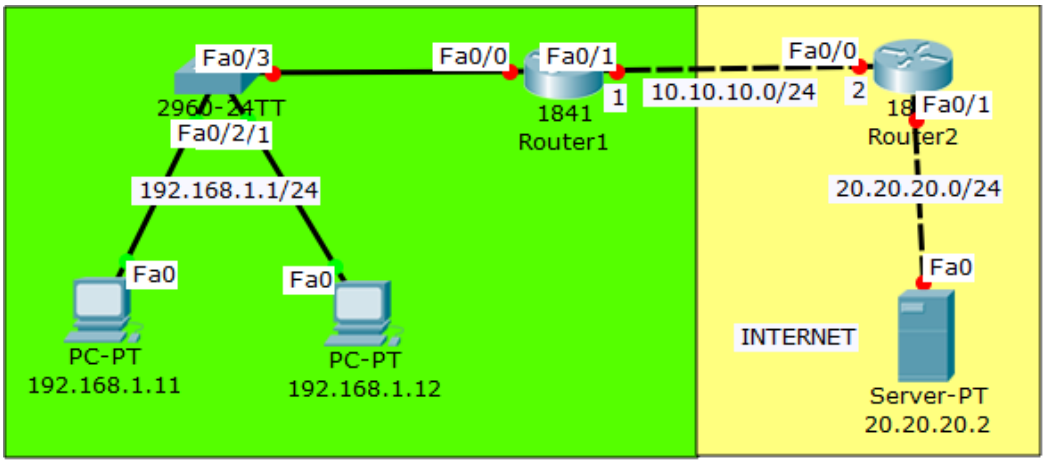
Nat pada cisco terbagi dari beberapa tipe :

- Static NAT : satu IP privat yang ditranslasikan ke satu IP public (one to one mapping)
- Dynamic NAT : jumlah IP public yang di sediakan harus sejumlah ip privat yang ditranslasikan, dan NAT jenis ini jarang di gunakan
- Overloading/port address translation (PAT) : Akses ineternet menggunakan 1 IP public, dan ini yang sedang banyak di gunakan pada saat ini

# STATIC NAT

Pada static NAT kita akan mentranslasikan ip privat ke ip public secara static, yang mana kita akan mengkonfigurasikan satu ip privat yang kita ubah ke ip public secara manual sesuai ip yang kita inginkan, atau dapat diartikan static nat itu merupakan one to one mapping.

Dalam static NAT, hanya 1 ip privat yang ditranslasikan ke 1 ip public. Artinya hanya 1 PC LAN yang dapat mengakses internet.




Konfigurasikan IP address di smua interface

R1

```
Router>en
Router#conf t
Router(config)# host R1
R1(config)#int fa0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int fa0/1
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa0/0
R2(config-if)#ip add 10.10.10.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int fa0/1
R2(config-if)#ip add 20.20.20.1 255.255.255.0
R2(config-if)#no sh
```

Konfigurasi static NAT dan default route pada R1 PC LAN 192.168.1.11 akan ditranslasikan ke ip public 10.10.10.10

```
R1(config)#ip nat inside source static 192.168.1.11 10.10.10.10
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config-if)#int fa0/1
R1(config-if)#ip nat outside
R1(config-if)#ex
R1(config)#ip route 0.0.0.0 0.0.0.0 fa0/1
```

Ping static NAT melalui server dan sebaliknya. Alamat PC LAN tidak akan pernah dapat diping dari internet.

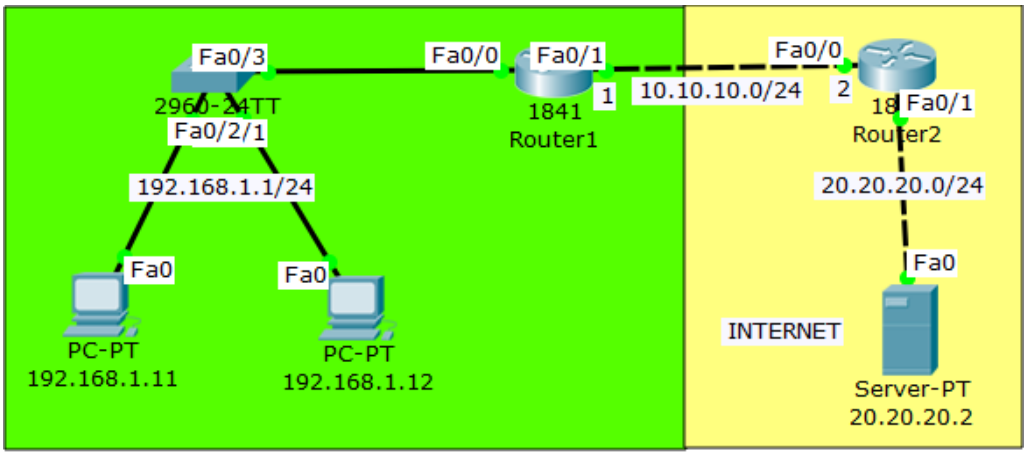
```
SERVER:\>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126
Reply from 10.10.10.10: bytes=32 time<1ms TTL=126
Reply from 10.10.10.10: bytes=32 time=11ms TTL=126
Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

```
SERVER:\>ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:
Reply from 20.20.20.1: Destination host unreachable.
Reply from 20.20.20.1: Destination host unreachable.
Reply from 20.20.20.1: Destination host unreachable.
Reply from 20.20.20.1: Destination host unreachable.
Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 20.20.20.2
Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=10ms TTL=126
Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

# OVERLOAD NAT (PAT)

PAT (Port Address Translation) digunakan agar banyak PC local dapat mengakses internet secara bersamasama hanya dengan menggunakan 1 ip public




masih melanjutkan konfigurasi sebelumnya, hapus dulu konfigurasi static nat pada R1

```
R1(config)#no ip nat inside source static 192.168.1.11 10.10.10.10
```

Buat access list untuk mendefinisikan network yang akan ditranslasikan dan konfigurasi dynamic nat overload pada R1.

```
R1(config)#ip nat inside source list 1 interface fa0/1 overload
```

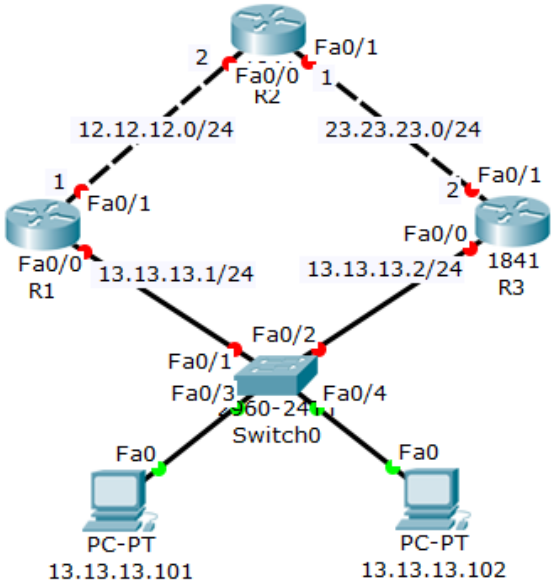
Sekarang ping server melalui PC0 dan PC1 pastikan reply

```
C:\>ping 20.20.20.2
Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time<1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=10ms TTL=126
Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

# HIGH AVAILABILITY (HSRP)

High Availibility digunakan dengan maksud redundancy, yaitu menggunakan beberapa router, yang satu menjadi link utama dan yang lain sebagai backup. Satu virtual gateway akan dipasang di PC local sehingga ketika pindah router tidak perlu mengeset gateway lagi.

HSRP (Hot Standby Redudancy Protocol)




Seperti biasa, silahkan konfigurasikan ip addres disetiap interface router

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa0/0
R1(config-if)#ip add 13.13.13.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int fa0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int lo0
R2(config-if)#ip add 1.1.1.1 255.255.255.255
R2(config-if)#int fa0/1
R2(config-if)#ip add 23.23.23.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int fa0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh
```

Perhatikan disana terdapat ip loopback yang fungsinya sebagai barometer R1 dan R3 nantinya sebelum di konfigurasi HSRP.

R3

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int fa0/0
R3(config-if)#ip add 13.13.13.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int fa0/1
R3(config-if)#ip add 23.23.23.2 255.255.255.0
R3(config-if)#no sh
```

Agar semua ip/network bisa saling komunikasi, kita akan tambahkan routing eigrp di setiap router.

```
R1(config)#router eigrp 10
R1(config-router)#no auto-summary
R1(config-router)#network 13.13.13.0 0.0.0.255
R1(config-router)#network 12.12.12.0 0.0.0.255

R2(config-if)#router eigrp 10
R2(config-router)#no auto-summary
R2(config-router)#net 1.1.1.1 0.0.0.0
R2(config-router)#net 12.12.12.0 0.0.0.255
R2(config-router)#net 23.23.23.0 0.0.0.255

R3(config)#router eigrp 10
R3(config-router)#no auto-summary
R3(config-router)#net 13.13.13.0 0.0.0.255
R3(config-router)#net 23.23.23.0 0.0.0.255
```

Pastikan R1 dan R3 dapat melakukan ping ke 1.1.1.1 baru lakukan konfigurasi HSRP.

```
R1#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

```
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

Konfigurasikan HSRP

```
R1(config)#int fa0/0
R1(config-if)#sta
R1(config-if)#standby ?
  <0-4095>  group number
  ip        Enable HSRP and set the virtual IP address
  ipv6      Enable HSRP IPv6
  preempt   Overthrow lower priority Active routers
  priority  Priority level
  timers    Hello and hold timers
  track     Priority Tracking
  version   HSRP version
R1(config-if)#standby 1 ip 13.13.13.13
R1(config-if)#standby 1 preempt
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
R1(config-if)#standby 1 priority 105
R1(config-if)#standby 1 track fa0/1
```

```
R3(config)#int fa0/0
R3(config-if)#standby 1 ip 13.13.13.13
R3(config-if)#standby preempt
```

Selanjutnya silahkan isi ip di masing-masing pc dengan gateway 13.13.13.13, kemudian lakukan ping dan tracert ke 1.1.1.1

Verifikasi :

```
C:\>ping 1.1.1.1
Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=1ms TTL=254
Reply from 1.1.1.1: bytes=32 time<1ms TTL=254
Reply from 1.1.1.1: bytes=32 time=1ms TTL=254
Reply from 1.1.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 1.1.1.1
Tracing route to 1.1.1.1 over a maximum of 30 hops:
  1   0 ms      0 ms      0 ms      13.13.13.1
  2   1 ms      0 ms      0 ms      1.1.1.1

Trace complete.
```

Untuk memastikan, silahkan cek standby di R1 dan R3

```
R1#sh standby br
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    105 P Active   local           13.13.13.2      13.13.13.13
```

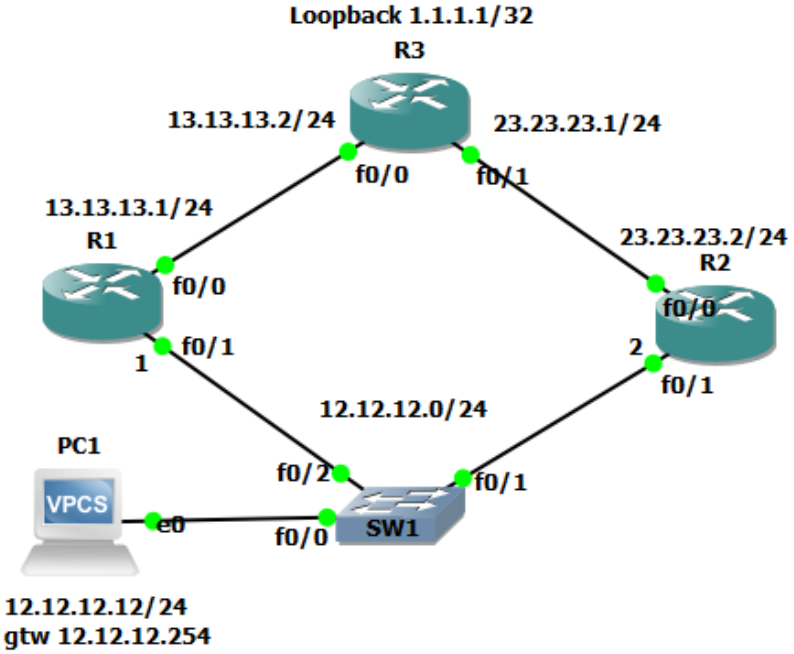
```
R3#sh standby br
                P indicates configured to preempt.
                |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    100   Standby  13.13.13.1      local           13.13.13.13
```

```
R3(config)#int fa0/0
R3(config-if)#standby 1 ip 13.13.13.13
R3(config-if)#standby preempt
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
```

# HIGH AVAILABILITY (VRRP)

**VRRP (Virtual Router Redudancy Protocol)** hampir sama seperti HSRP yang membedakan adalah HSRP adalah **Cisco Propriety** sedangkan VRRP adalah standar internasional IEEE. Di HSRP juga mendukung authentication sedangkan VRRP tidak. Oleh karena itu, sebelum memasuki lab VRRP lebih baik mengerti terlebih dahulu HSRP yang dapat di buka pada link di atas.

Langsung ke konfigurasi saja. Buatlah Topologi Persis seperti lab sebelumnya, kali ini kita pakai 1 pc saja dan ipnya kita bedakan. Dan sekarang kita akan menggunakan **GNS3** karena di GNS3 mendukung vitur vrrp.




Dari topologi di atas, silahkan masukkan ip di masing-masing port lalu buatkan routing stati di setiap router

R1

```
R1#conf t
R1(config)#int fa0/0
R1(config-if)#ip add 13.13.13.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int fa0/1
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
```

R2

```
R2#conf t
R2(config)#int fa0/0
R2(config-if)#ip add 23.23.23.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int fa0/1
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh
```

R3

```
R3#conf t
R3(config)#int fa0/0
R3(config-if)#ip add 13.13.13.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int fa0/1
R3(config-if)#ip add 23.23.23.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int loopback0
R3(config-if)#ip add 1.1.1.1 255.255.255.255
```

Buatkan routing static di setiap router

```
R1(config)#ip route 1.1.1.0 255.255.255.255 13.13.13.2

R2(config)#ip route 1.1.1.0 255.255.255.255 23.23.23.1

R3(config)#ip route 12.12.12.0 255.255.255.0 23.23.23.2
```

Jika sudah, maka kita langsung konfigurasikan vrrp. Sebenarnya sama saja dengan hsrp, hanya beda perintahnya saja :-D

R1

```
R1(config)#int fa0/1
R1(config-if)#vrrp 1 ip 12.12.12.254
*Mar  1 00:19:35.307: %VRRP-6-STATECHANGE: Fa0/1 Grp 1 state Init -> Backup
R1(config-if)#
*Mar  1 00:19:38.919: %VRRP-6-STATECHANGE: Fa0/1 Grp 1 state Backup -> Master
```

R2

```
R2(config)#int fa0/1
R2(config-if)#vrrp 1 ip 12.12.12.254
*Mar  1 00:21:21.119: %VRRP-6-STATECHANGE: Fa0/1 Grp 1 state Init -> Backup
R2(config-if)#
*Mar  1 00:21:24.731: %VRRP-6-STATECHANGE: Fa0/1 Grp 1 state Backup -> Master
```

Disinilah letak perbedaanya, jika di HSRP ada yang namanya active dan standby. Di VRRP namanya adalah Backup dan Master. Backup sebagai cadangan dan Master sebagai jalur utama. Dan sama seperti di HSRP penentuannya adalah IP address tertinggilah yang akan menjadi Master. Dalam Kasus ini berarti masternya adalah R2 (12.12.12.2)

Selanjutnya, untuk verifikasi kita lakukan show vrrp brief pada R2

```
R2#show vrrp br
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/1              1   100 3609       Y  Master  12.12.12.2      12.12.12.254
```

Terlihat disana ada ip 12.12.12.2 yang menjadi jalur utama (master). Setelah itu silahkan konfigurasikan ip di PC1 dengan gateway 12.12.12.254

```
PC1> ip 12.12.12.12/24 12.12.12.254
Checking for duplicate address...
PC1 : 12.12.12.12 255.255.255.0 gateway 12.12.12.254
```

Jika semuanya sudah dikonfigurasi, sekarang kita tinggal ujicoba dengan cara ping dari PC ke loopback

```
PC1> ip 12.12.12.12/24 12.12.12.254
Checking for duplicate address...
PC1 : 12.12.12.12 255.255.255.0 gateway 12.12.12.254
```

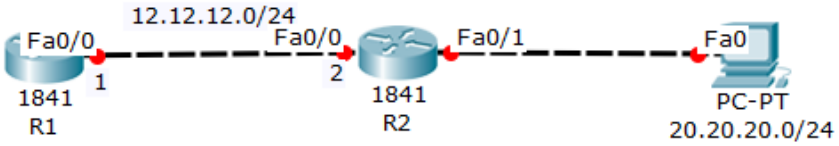
# DHCP RELAY

DHCP Relay hanyalah sebuah proxy yang bisa atau dapat menerima permintaan DHCP (Client) dan mengirimkannya kembali ke DHCP Server sesungguhnya"

Jadi, DHCP Relay ini berfungsi untuk meneruskan service dari DHCP Server menuju ke client

DHCP Relay akan meneruskan IP Address yang diberi Server ke clien yang memintanya. Jadi biasanya kita mendapatkan IP address dengan gateway yang satu segment. Jika dengan DHCP Relay maka IP Address dan gatewaynya berbeda.

Buat topologi berikut :




R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa0/0
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh

R1(config)#ip dhcp pool it-ndeso
R1(dhcp-config)#net 20.20.20.0 255.255.255.0
R1(dhcp-config)#def 20.20.20.1
R1(dhcp-config)#dns 100.100.100.100
R1(dhcp-config)#
R1(dhcp-config)#ip route 20.20.20.0 255.255.255.0 12.12.12.2
```

It-ndeso merupakan nama pool nya saja. Bisa di isi nama apa aja.

Default-router merupakan IP Gateway yang akan diberikan ke client.

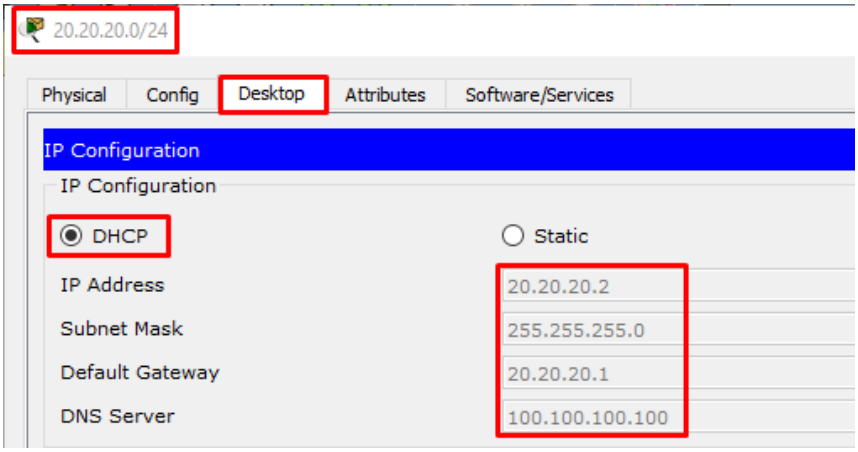
DNS-Server merupakan IP dns server jika ada.

Perlu ditambah routing agar R1 dapat mengetahui network yang dibagikannya

Setelah itu konfigurasi IP Address dan DHCP Relay pada R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh

R2(config-if)#int fa0/1
R2(config-if)#ip add 20.20.20.1 255.255.255.0
R2(config-if)#no sh

R2(config-if)#ip helper-address 12.12.12.1
```

Perintah **helper-address** akan mengaktifkan fitur DHCP Relay 12.12.12.1 merupakan alamat DHCP Server. Sekarang liat pada Client apakah sudah mendapatkan IP Address atau belum.

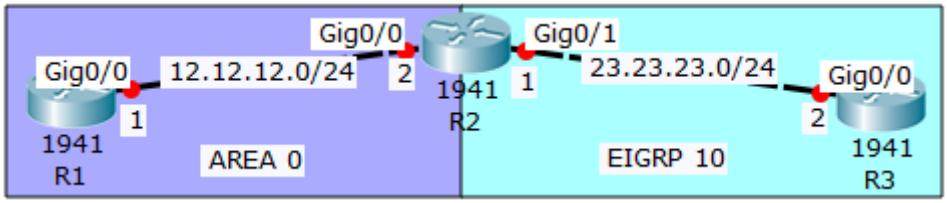


# REDISTRIBUTE

Sebelum kita masuk ke lab redistribute, kita harus faham dulu apa itu redistribute, bagaimana cara kerjanya.

Redistribute adalah sebuah metode untuk menghubungkan routing protocol yang berbeda dalam sebuah topologi, contohnya ada routing OSPF dan EIGRP dalam satu topologi.

Buat topologi berikut :




Konfigurasikan ip address sesuai dengan interfacenya, dan lanjutkan dengan masing-masing routing protocolnya sesuai dengan topologi.

R1

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int gi0/0
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#ex
R1(config)#router ospf 10
R1(config-router)#net 12.12.12.0 0.0.0.255 area 0
```

R2

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int gig0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int gi0/1
R2(config-if)#ip add 23.23.23.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#ex
R2(config)#router ospf 10
R2(config-router)#net 12.12.12.0 0.0.0.255 area 0
R2(config-router)#ex
R2(config)#router eigrp 10
R2(config-router)#no auto-summary
Router(config-router)#net 23.23.23.0 0.0.0.255
```

R3

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int gig0/0
R3(config-if)#ip add 23.23.23.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#ex
R3(config)#router eigrp 10
R3(config-router)#no auto-summary
R3(config-router)#net 23.23.23.0 0.0.0.255
```

Jika sudah dibuatkan routing, lakukan ping untuk memastikan bahwa antar routing protocol yang di buat tadi belum bisa komunikasi

```
R1#ping 23.23.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Ketika R1 ping kw R3 (23.23.23.2) belum bisa terhubung, karna masih beda protocol dan belum ada redistribute antara keduanya.

Selanjutnya kita akan konfigurasikan redistribute pada R2 agar kedua routing protocol itu bisa saling komunikasi

```
R2(config )#router eigrp 10
R2(config-router)#redistribute ospf 10 metric 1 1 1 1 1
R2(config-router)#ex
R2(config )#router ospf 10
R2(config-router)#redistribute eigrp 10 subnet
```

Keterangan :

Ketika akan melakukan redistribute dari ospf ke eigrp, maka posisi konfigurasi harus masuk ke ospf terlebih dahulu, begitupula sebaliknya.

Metric 1 1 1 1 1 ini adalah cost yang digunakan oleh protocol ospf untuk menentukan best-pathnya.

Jika sudah dibuatkan redistributenya, sekarang lakukan ping lagi antar router dan pastikan hasilnya reply.

```
R1#ping 23.23.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
R2#ping 12.12.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R2#ping 23.23.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
R3#ping 12.12.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

*Remember me in your pray*