

Untung Wa

Best
Networking
CISCO

Today Learner

|

Tomorrow Leader

ID-Workers

From Engineer to Engineer

PANDUAN MODUL

Assalamualaikum wr.wb.

Di dalam modul Cisco ini saya selaku penulis memberikan sedikit panduan tentang modul ini. Sebelum belajar menggunakan modul ini saya berharap anda sebagai pembaca sudah mengetahui sedikit banyak nya tentang Network Fundamental. Seperti halnya OSI Layer , TCP/IP dan Hardware Jaringan. Agar kedepannya lebih mudah dalam memahami buku ini.

Dan untuk penggunaan perangkat , di modul ini saya menggunakan Simulator seperti halnya **CISCO PACKET TRACER** dan juga **GNS3**. Saya berharap kalian sudah mempunyai basic tentang kedua alat simulator tersebut yaa gaess. Ini dilakukan karena saya sendiri belum mempunyai kesempatan untuk melakukan real config dengan alat nya langsung. Tapi tenang aja , alat simulator tersebut sudah mirip kok seperti aslinya. Di PACKET TRACER memiliki beberapa fitur IOS Cisco sendiri , jadi tidak sepenuhnya seperti real. Dan di GNS3 sudah menggunakan IOS Cisco secara langsung namun untuk IOS nya hanya ada untuk Router dan belum tersedia IOS CISCO untuk switch di GNS3. Yaa jadi saling melengkapi aja laah.

Di device cisco juga terdapat fitur “AutoCorrect” jadi semisal saya tidak lengkap mengetik Syntax nya itu pun masih bisa tetap jalan , karena adanya fitur Auto Correct itu. Tapi tidak semua sintaks autocorrect yaa , hanya sintaks yang sudah jelas saja yang bisa di autocorrect oleh device.

Materi 1. KONFIGURASI DASAR

Lab 1. Pengenalan Mode di Device CISCO

Assalamualaikum wr.wb

Sebagai pembuka di modul Cisco ini , kita akan memulainya dengan berkenalan dengan mode yang ada di setiap device Cisco. Jadi di setiap device Cisco memiliki tingkatan tersendiri dalam melakukan konfigurasi. Konfigurasi yang dapat dilakukan pun berbeda di setiap modenya. Di Cisco sendiri ada 3 Mode Umum yaitu :

Router>	:	User EXEC Mode
Router#	:	Privilege Mode
Router(config)	:	Global Configuration Mode

Setiap mode itu diwakili oleh tanda yang berbeda , seperti yang kalian lihat di atas , bahwa User Mode diwakili tanda ">" , Privilege = "#" , dan Global Configuration = "(config)". Oke setelah kalian tau tentang jenis mode nya , sekarang kita bahas cara untuk pindah dari 1 mode ke mode lainnya.

Perintah	Keterangan
Router> <i>enable</i>	Untuk berpindah dari User Mode ke Privilege Mode
Router# <i>disable</i>	Untuk berpindah dari Privilege ke User Mode
Router# <i>conf t</i>	Untuk berpindah dari Privilege ke Global Configuration
Router (config)#	Mode Global Configuration
Router (config)# <i>exit</i>	Untuk mundur ke 1 mode sebelumnya

Untuk mengetahui perintah yang ada di setiap mode kita bisa gunakan perintah "?". Maka device Cisco akan menampilkan perintah apa saja yang bisa digunakan di mode tersebut. Seperti contoh berikut :

Perintah yang ada di EXEC Mode berikut penjelasan tentang perintah nya.

```
Router>?  
Exec commands:  
  <1-99>      Session number to resume  
  
  connect     Open a terminal connection  
  
  disable     Turn off privileged commands  
  
  disconnect  Disconnect an existing network connection  
  
  enable      Turn on privileged commands  
  
  exit        Exit from the EXEC  
  
  logout      Exit from the EXEC  
  
  ping        Send echo messages  
  
  resume      Resume an active network connection  
  
  show        Show running system information  
  
  ssh         Open a secure shell client connection  
  
  telnet      Open a telnet connection  
  
  terminal    Set terminal line parameters  
  
  traceroute  Trace route to destination  
  
Router>
```

Oke demikian lah lab pertama ini , Sebenarnya mode di IOS Cisco bukan hanya 3 itu saja. Namun secara garis besar 3 Mode itulah yang mewakili semua nya.

Oke sekian dulu di lab ini , kurang lebih nya saya mohon maaf.

Wassalamualaikum wr.wb

Lab 2. Pengecekan Hardware

Assalamualaikum wr.wb

Lanjut lagi masih di konfigurasi dasar , sekarang kita akan masuk ke pembahasan kedua yaitu tentang cara mengecek Hardware dan IOS device CISCO. Seperti kita ketahui perangkat jaringan Cisco ini layaknya komputer yang biasa kita pakai , dalam Device Cisco terdapat CPU , Disk , Memori , dll. Di lab kali ini kita akan bahas tentang cara mengecek *dalem* atau spesifikasi dari Device Cisco.

Cara mengeceknya adalah dengan cara ketikkan perintah **show version**. Di dalam Privilege Mode , masih inget kan cara masuk ke privilege mode ?? . Kalo lupa kebangetan berarti.

```
Router#show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE
SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE
SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

Cisco 2620 (MPC860) processor (revision 0x200) with 253952K/8192K
bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)

32K bytes of non-volatile configuration memory. ----->
NVRAM
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Dari keterangan diatas dapat kita ketahui bahwa :

1. Tipe Router nya adalah **Cisco 2620**
2. Memory yang dimiliki adalah (253952 + 8192) Kb = **262.144 Kb** (256 MB)
3. Memiliki 1 buah Interface FastEthernet
4. NVRAM yang dimiliki adalah sebesar **32 kb**
5. Flash yang dimiliki adalah sebesar 63488 Kb (64 MB)

Mungkin dari informasi diatas ada kata yang masih asing di telinga kalian yaitu NVRAM dan Flash. Oke saya akan menjelaskan sedikit tentang hal itu

- ✓ Flash digunakan sebagai media penyimpanan IOS (Internetwork Operating System) yaitu system operasi yang digunakan oleh device CISCO.
- ✓ Memory/RAM digunakan sebagai media penyimpanan konfigurasi sementara. Kalo dibahasa cisco itu **Running-configuration**.
- ✓ NVRAM (Non-Volatile RAM) digunakan sebagai tempat penyimpanan konfigurasi utama. Ibaratnya ini adalah tempat penyimpanan semua konfigurasi secara permanen, layaknya hardisk namun hanya untuk konfigurasi. Kalo dibahasa cisco nya itu **Startup-Configuration**.

Oh ya perlu diingat masalah Running Config dan Startup Config , karena itu akan diperlukan di konfigurasi kedepannya. Intinya kalo ada kata “Run” artinya RAM , sedangkan “startup” artinya NVRAM (Utama).

Running Configuration = R A M , → Penyimpanan Sementara

Startup Configuration = NVRAM → Penyimpanan Utama

Oke sekian dulu lab kali ini. Semoga setelah lab ini kalian sudah mulai lebih dekat dengan Device Cisco. Dan tentunya setelah mengenal dan mulai dekat maka timbulah benih benih cinta diantara kalian , cieeeeee. *Lhoo ngawuurr*.

Wassalamualaikum wr.wb

Lab 3. Pengecekan Software / IOS

Assalamualaikum wr.wb

Oke setelah di lab sebelumnya kita sudah kenal sama hardware dari Device CISCO sekarang saatnya kita kenal sama Software atau IOSnya. Seperti yang dibahas di lab sebelumnya bahwa Perangkat Jaringan Cisco memiliki Sistem Operasi sendiri , sistem operasi itu bernama IOS atau Internetwork Operating System. Sama hal nya kayak PC kaan ???.

Oke di lab kali ini sebenarnya gak jauh berbeda sama di lab sebelumnya , dan perintah yang digunakan pun masih sama , Cuma “*Sesuatu*” yang dicek nya aja yang beda. Tentu saja kalimat dan baris yang di liat juga beda. Oke daripada bingung langsung aja kita cek , kita masih pake keterangan dari Router sebelumnya aja. Ini dia CEKIDOT

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE
SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

Cisco 2620 (MPC860) processor (revision 0x200) with 253952K/8192K
bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Oke seperti di lab sebelumnya , mari kita cari informasi dari keterangan diatas :

1. Versi IOS yang digunakan adalah version 12.2(28),
2. Nama File IOS nya adalah version 12.2(28),
3. Nilai dari Configuration registernya adalah 0x2102

Ada 2 nilai configuration register yang sering digunakan , yaitu

- 0x2102 : Artinya router akan membaca konfigurasi yang ada di startup (NVRAM) ketika dinyalakan
- 0x2142 : Artinya router akan mem-bypass konfigurasi startup ketika dinyalakan.

Oke sekian dulu tentang lab mengenal IOS Cisco. Diharap setelah kalian mencoba 2 lab ini maka kalian akan lebih dekaat lagi dengan Cisco , baik lewat Hardware maupun dari sisi IOS nya.

Wassalamualaikum !

Lab 4. Melakukan Verifikasi dengan perintah “Show”

Assalamualaikum wr.wb

Lanjut lagi di konfigurasi dasar , di lab ini saya akan mengajak kalian para pembaca setia modul ini untuk mencoba satu lagi perintah dasar yang ada di Cisco. Yaitu perintah “Show”. Perintah *Show* dapat dilakukan di privilege Mode. Oke mari kita kupas tuntas tentang masalah show ini

Hal yang harus diingat saat menggunakan show ini adalah kata “Show” artinya menampilkan , jadi ketika kita gunakan perintah show ini maka kita harus tambahkan sintak dibelakangnya. Hal ini dimaksudkan agar kita tahu apa yang mau kita liat. Untuk melihat apa saja yang bisa dilihat oleh perintah *show* ini dapat gunakan tanda “?” di belakangnya.

```
Router#show ?
  aaa                Show AAA values
  access-lists      List access lists
  arp               Arp table
  cdp               CDP information
  class-map         Show QoS Class Map
  clock             Display the system clock
  controllers       Interface controllers status
  crypto            Encryption module
  debugging         State of each debugging option
  dhcp              Dynamic Host Configuration Protocol status
  file              Show filesystem information
  flash:            display information about flash: file system
  frame-relay       Frame-Relay information
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host
table
  interfaces        Interface status and configuration
  ip                IP information
  line              TTY line information
  logging           Show the contents of logging buffers
```

```
login          Display Secure Login Configurations and State
ntp            Network time protocol
policy-map     Show QoS Policy Map
privilege      Show current privilege level
--More--
```

Seperti yang kalian lihat diatas adalah perintah yang dapat di kombinasikan dengan show. Sebagai contoh saya akan coba untuk melihat Jam yang ada di Router tsb. Dengan menggunakan perintah *show clock*.

```
Router#show clock
*2:24:51.342 UTC Mon Mar 1 1993
Router#
```

Dan untuk tambahan pula , Perintah *show* ini jug abisa dijalan di Global Configuration , yaitu dengan cara menambahkan sintak *do* di depannya. Seperti *do*

```
Router(config)#do show clock
*2:28:43.123 UTC Mon Mar 1 1993
Router(config)#
```

show
<option>

Bisa dilihat maka hasilnya akan tetap sama saja , namun yang perlu diketahui untuk perintah *do* maka kita tidak bisa menggunakan fitur “*AUTOCORRECT*” , jadi kita harus memasukkan sintaknya secara full.

Oke sekian dulu tentang perintah show ini.

Wassalamualaikum wr.wb

Lab 5. Mengubah Hostname

Assalamualaikum wr.wb

Masih kuat kaan ?? Pasti masih dong , baru juga lab 5 belum ada apa-apanya , hehehehe. Oke di lab ke 5 ini saya mau memberikan tutorial yang special , yaitu tentang cara merubah nama dari Device Cisco kesayangan kita. *Cuit cuit*.

Untuk merubah hostname caranya adalah dengan mengetikkan ketikkan perintah “hostname <nama_hostname>” di dalam mode Global configuration. Monggo di simak aja dibawah ini.

```
Router>enable
Router#conf t
Router(config)#
```

Kemudian masukkan sintak berikut :

```
Router(config)#hostname UNTUNG
UNTUNG(config)#
```

Bisa dilihat Hostname dari Router nya sudah berubah menjadi nama saya sendiri , yaitu UNTUNG.

Lab 6. Setting Password di Router

Assalamualaikum wr.wb

Sekarang kita masuki lab basic tentang kemanan di Router Cisco. Kalo masalah password kalian pasti udah tau lah , tujuan dari pembuatannya password. Yaps, tentu saja supaya Router kita tidak mudah di *bobol* sama orang yang tidak bertanggung jawab. Jadi hanya orang orang tertentu saja yang bisa mengakses Router kita , tentu nya orang orang yang tau password kita. Password ini nantinya akan diminta ketika kita **ingin masuk** ke **Mode Privilege** Oke langsung aja yuuk *cuuus*.

Di Cisco ada 2 tipe untuk pemberian password , 2 cara tersebut adalah :

1. Password : Memberikan password namun tidak memberikan Enkripsi , meskipun kita bisa membuatnya menjadi di-enkripsi.
2. Secret : Memberikan Password sekaligus di enkripsi

Oke sekarang kita akan mencoba kedua tipe diatas , dan kita akan coba apa hasil nya jika kita gunakan kedua tipe diatas.

```
UNTUNG#conf t
UNTUNG(config)#enable password untung    → Untuk key password
UNTUNG(config)#enable secret wahyudi     → Untuk key Secret
```

Kemudian kita verifikasi dengan perintah "*show run*". Kemudian cari baris enable password dan enable secret.

```
UNTUNG#show run
Building configuration...

Current configuration : 561 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```

!
hostname UNTUNG
!
!
!
enable secret 5 $1$mERr$.3LaD0DuVETbxV5XDYwc2. →DI ENKRIPSI
enable password untung → TIDAK DI ENKRIPSI
!
!

```

Dari hasil verifikasi diatas dapat kita ketahui bahwa tipe *secret* lah yang di enkripsi sedangkan untuk tipe *password* tidak ter-enkripsi. Sekarang kita akan buat agar tipe password tersebut ter-enkripsi. Caranya adalah dengan cara ketikkan perintah :

```

UNTUNG(config)# service password-encryption

```

Kemudian kita cek lagi dengan *show run* , maka akan tampil kalimat *Service password-encryption*, yang artinya tipe password juga akan ter-enkripsi. Bisa dilihat dibagian *enable password* akan muncul bagian enkripsinya.

```

UNTUNG#sh run
Building configuration...

Current configuration : 568 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname UNTUNG
!
!
!

```

```
enable secret 5 $1$mERr$.3LaD0DuVETbxV5XDYwc2.  
enable password 7 0834425A1C1702 → DI ENKRIPSI  
!  
!
```

Oke sekarang kita bahas lagi , diatas kan kita menggunakan 2 tipe password , yaitu Tipe Secret dan juga Tipe Password , lalu yang mana yang akan digunakan ketika ingin mengakses router ??? . Jika 2 nya kita pakai maka yang akan digunakan adalah yang tipe **Secret**. Kenapaa ??? karena tipe Secret lah yang ter-enkripsi , jadi router akan menganggap itu lah yang paling aman. Meskipun kita buat enkripsi di jenis password tetap saja akan **memilih yang Secret**. Untuk pembuktian silahkan coba exit ke Mode User EXEC Mode. Kemudian masuk ke mode Privilege seperti dibawah ini.

```
UNTUNG#disable  
UNTUNG>enable  
Password: >> masukkan untung (Tipe Password)  
Password: >> masukkan wahyudi (Tipe Secret),  
Maka akan berhasil  
UNTUNG#
```

Oke sekarang kalian sudah tau bagaimana cara membuat password di Router Cisco dengan 2 cara. Dan kalian juga udah tau yang mana yang lebih aman , dan yang mana yang lebih diutamakan oleh router cisco. Karena kalian sudah bisa maka saya tutup lab ini dengan mengucap , Alhamdulillah.

Oke sekian dulu

Wassalam !

Lab 7. Setting Banner MOTD (Message Of The Day)

Assalamualaikum wr.wb

Masih di lab lab dasar , di lab ini saya mau memberikan lab yang benar benar special. Ini serius beneran special , karena kita akan membuat banner saat kita mengakses Router Cisco. Nama kerennya itu MOTD atau *Message of The Day* , wuiih kereen kan. Jadi nantinya ketika kita menyalakan router Cisco maka akan muncul message ini. Tujuan dibuat ini sebenarnya Cuma untuk mempercantik tampilan aja ketika login , kalo untuk fungsi lainnya saya kurang paham.

Oke langsung aja , caranya adalah masuk ke mode Global Configuration , kemudian ketikkan perintah

```
UNTUNG(config)#banner motd z                ( TEKAN ENTER )
Enter TEXT message. End with the character 'z'.
  SELAMAT DATANG                            ( MASUKAN KALIMATNYA )
    DI                                        ( KALIMAT BOLEH DI ENTER )
  ROUTER ID-NETWORKERS
z                                             → DIAKHIRI DENGAN huruf "z"

UNTUNG(config)#exit
UNTUNG#exit
```

Kemudian kita coba test , dengan cara keluar dari privilege mode “#” ke EXEC Mode “>” , dengan cara ketikkan perintah *exit* Di Privilege mode. Maka seharusnya akan muncul kalimat banner nya setelah kita tekan Enter.

```
UNTUNG con0 is now available
```

```
Press RETURN to get started.
```

```
SELAMAT DATANG
```

```
DI
```

```
ROUTER ID-NETWORKERS
```

```
UNTUNG>
```

Oke gimana ?? Tampilannya login nya udah lebih menarik kan ?. Seengganya banner itu bisa jadi penyemangat kalian dalam melakukan konfigurasi , yaa disamping adanya kedua orang tua dan kekasih hati yang menyemangati kita juga perlu lho dapet semangat dari Router Cisco hehehe.

Oke sekian dulu yoo.

Wassalamualaikum wr.wb

Lab 8. Menyimpan Konfigurasi

Assalamualaikum wr.wb

Oke karena kalian sudah berhasil membuat banner sekarang saya mau ngebahas hal yang penting nih , saya mau ngasih tau bahwa semua konfigurasi kita dari lab awal itu akan hilang jika kita Matikan Device Cisco. Karena semua konfigurasi itu awalnya berada di Running Config (RAM) , maka dari itu kita harus menyimpan konfigurasi kita dengan cara memindahkannya ke dalam Startup Config (NVRAM). Caranya adalah dengan cara ketikkan perintah “*copy running-config startup-config*” atau cukup dengan “*copy run start*” Artinya kita akan memindahkan/copy semua yang ada di running config ke dalam startup config. Atau bisa juga dengan perintah *write* atau *wr* saja cukup . didalam Mode Privilege

```
UNTUNG#copy run start
Destination filename [startup-config]? → langsung
saja enter
Building configuration...
[OK]
UNTUNG#
```

ATAU

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

Nah dengan cara diatas maka konfigurasi kalian tidak akan hilang , meskipun router kita matikan.

Lab 9. Menghapus Konfigurasi

Karena sudah tau cara menyimpan konfigurasi sekarang kita bahas lawannya yaitu bagaimana cara menghapus konfigurasi yang sudah disimpan tadi. Tujuan dihapusnya konfigurasi tadi sebenarnya digunakan saat kita ingin mengembalikan keadaan Device menjadi default sebelum dikonfigurasi.

Oke berikut cara untuk menghapus file konfigurasi yang sudah kita simpan di dalam Startup.. Oke mari kita telisik lebih ringkas.

Untuk menghapus file konfigurasi di Cisco caranya adalah dengan cara ketikkan perintah *write erase*.

```
UNTUNG#write erase
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]    → (TEKAN ENTER)
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
UNTUNG#
```

Setelah kita hapus konfigurasi nya , selanjut nya kita harus me-reload Routernya.

Berikut caranya

```
UNTUNG#reload
Proceed with reload? [confirm] → TEKAN ENTER
```

Setelah device di Reload maka semua konfigurasinya akan hilang , dan device akan menjadi seperti sedia kala. Oke karena lab nya sudah selesai maka saya tutup dengan mengucapkan Alhamdulillah.

Materi 2. Lab Switching

Assalamualaikum wr.wb

Alhamdulillah sekarang kita sudah masuk ke Materi yang kedua , yaitu tentang Lab Switch. Jadi di Materi atau Bab ini saya akan lebih memfokuskan lab lab pada device Switch. Adapun materi yang akan dibahas meliputi :

1. Mac Address Table
2. Vlan
3. Trunk
4. STP (Spanning Tree Protocol)
5. VTP (Virtual Trunking Protocol)
6. DHCP Server
7. Switchport Security
8. Etherchannel
9. Multilayer Switch
10. Router On the Stick / Inter-Vlan routing

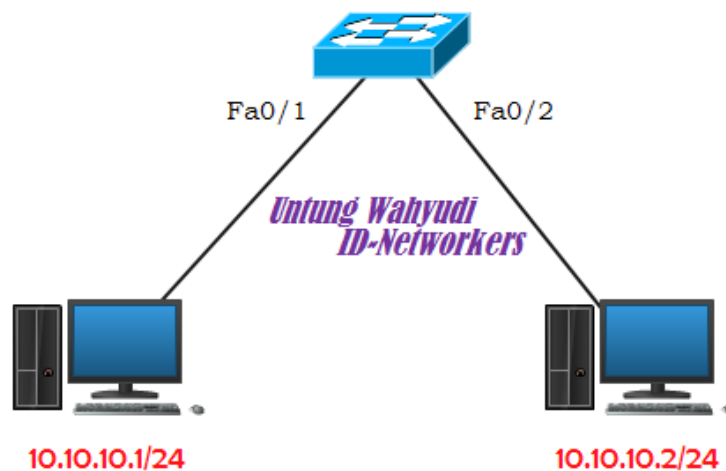
Lab 10. Mac Address Table Dynamic

Assalamualaikum wr.wb

Untuk membuka Lab pertama di materi Switch ini saya ingin memberikan konsep dasar dari Switch. Seperti yang kalian ketahui bahwa Switch itu bekerja di Layer 2 dan cara pendistribusian paket data adalah dengan cara membroadcast , Setelah paket data di broadcast maka Switch akan membuat Tabel Mac Address dari pengirim paket tersebut. Nah di Switch Cisco ada 2 metode untuk pembentukan Tabel Mac Address ini , yaitu :

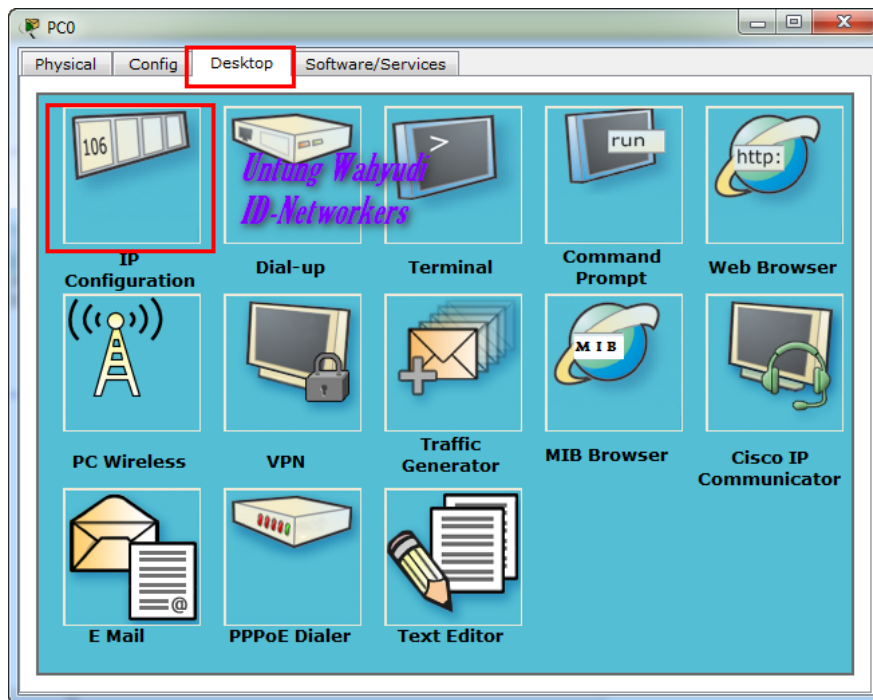
1. **Dynamic** : Artinya switch akan membuat secara otomatis table Mac Address nya. Tabel ini dibuat ketika komputer saling bertukar data
2. **Static** : Artinya kita sebagai Engineer memasukan secara otomatis mac address serta IP address dari setiap Host.

Oke langsung aja yuk cuss , pertama kita buat topologi seperti dibawah ini di packet Tracer. Pilih switch yang jenis **2950-24**.

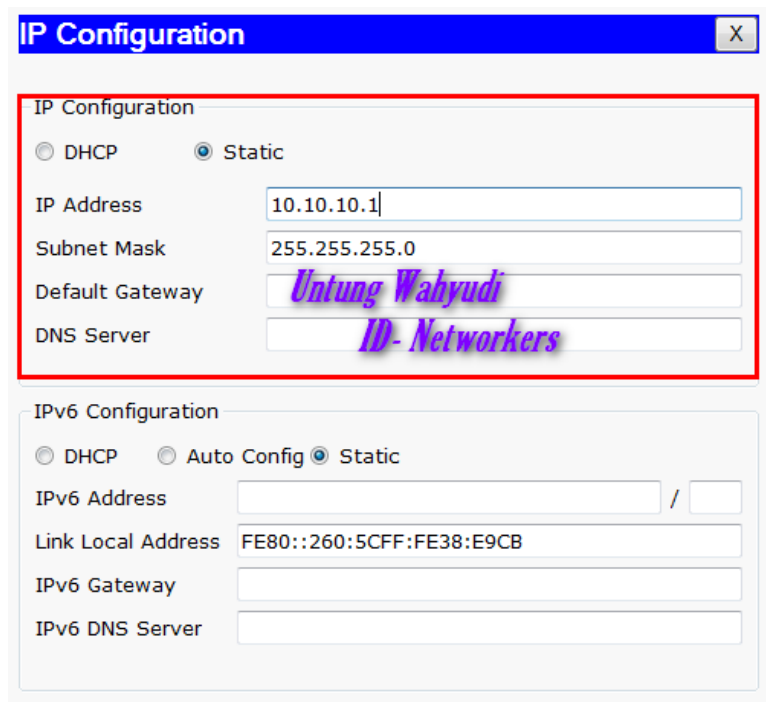


Selanjutnya kita berikan IP ke masing-masing PC yang terhubung ke switch, Ingaat yaa harus satu network , jika tidak maka Komputer tersebut tidak bisa saling ping. Cara setting IP PC di packet tracer adalah

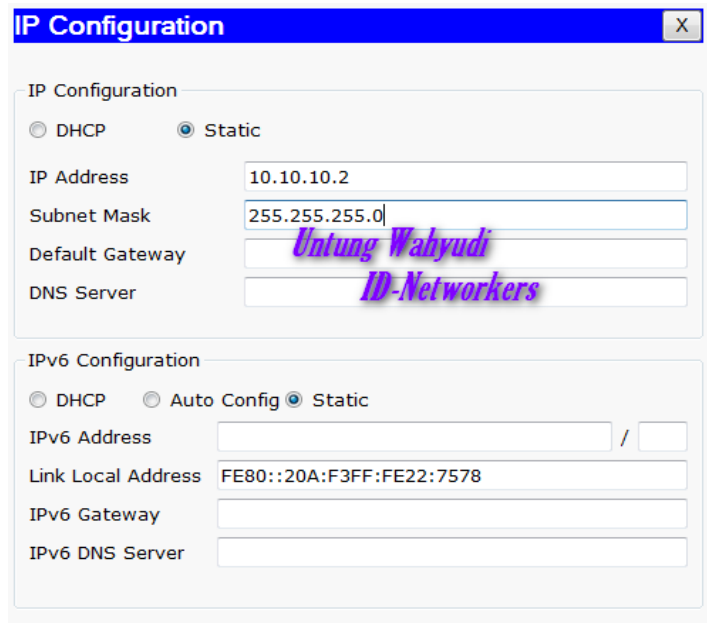
“Double Klik pada PC , lalu klik tab Config → IP Configuration”



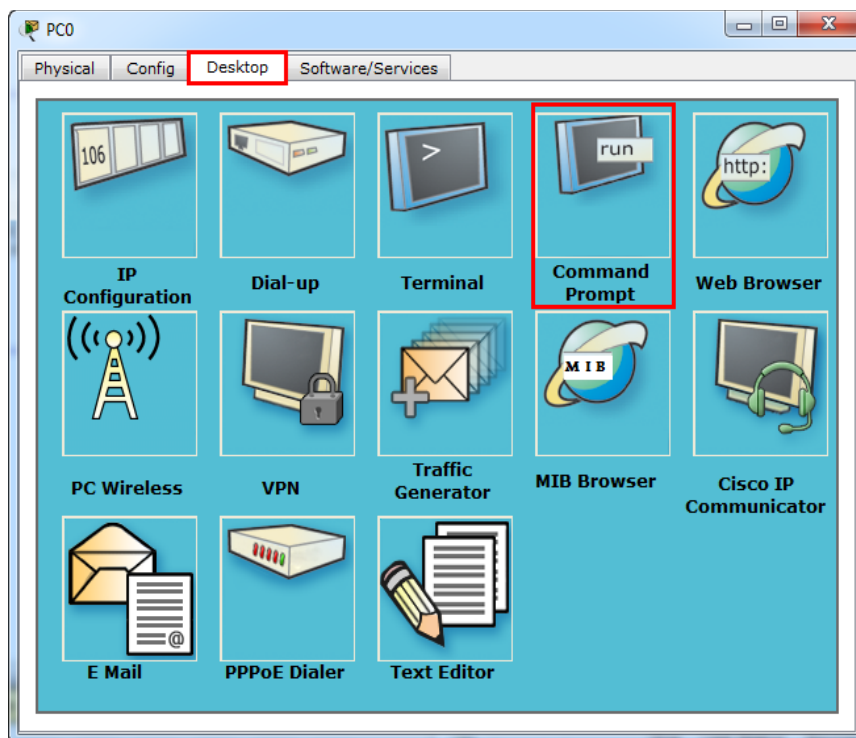
Setelah itu masukkan IP Address nya sesuka hati kalian , tapi ingat Harus satu network antar 1 Pc dengan Pc lainnya.



Lakukan hal yang sama di PC yang lain , namun dengan IP yang berbeda. Berikut IP yang saya berikan di PC kedua.



Setelah itu coba test Ping antar client, dengan cara masuk ke Tab Desktop yang tadi lalu klik Command Prompt , setelah itu lakukan ping seperti biasa.



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=2ms TTL=128
Reply from 10.10.10.2: bytes=32 time=0ms TTL=128
Reply from 10.10.10.2: bytes=32 time=0ms TTL=128
Reply from 10.10.10.2: bytes=32 time=0ms TTL=128

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Setelah kedua PC saling Ping , selanjutnya cek table mac address yang ada di Switch , dengan cara masuk ke mode privilege lalu ketikkan perintah *show mac-address-table*

```
Switch>enable
Switch#show mac-address-table

          Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       000a.f322.7578   DYNAMIC     Fa0/2
1       0060.5c38.e9cb   DYNAMIC     Fa0/1
Switch#
```

Bisa dilihat table mac address nya sudah terbuat , dan type nya adalah DYNAMIC , karena kita membuatnya dengan cara Ping.

Lab 11. Mac Address Table Static

Melanjutkan dari lab sebelumnya , setelah table nya sudah terbentuk menjadi Dynami sekarang kita akan buat menjadi STATIC. Lalu apa kelebihan dari STATIC ini ?? Jadi jika kita buat pemetaannya menjadi Static maka setiap host/PC tidak akan bisa saling bertukar port. Apa yang terjadi kalo kalo mereka mencoba bertukar port ?? Hasilnya adalah PC tidak akan terkoneksi ke switch.

Oke berikut caranya , setelah table mac address terbentuk secara DYNAMIC

```
Switch>enable
Switch#show mac-address-table
          Mac Address Table
-----
Vlan      Mac Address      Type        Ports
-----
1         000a.f322.7578   DYNAMIC     Fa0/2
1         0060.5c38.e9cb   DYNAMIC     Fa0/1
Switch#
```

Selanjutnya kita buat menjadi STATIC yaitu dengan cara masukkan sintak berikut di Mode Global Configuration :

```
“Switch (config)# mac-address-table static [MacAddress] [Vlan] interface [fao/1-24]”
```

Keterangan :

- **MacAddress** : Kita masukkan Mac Addres yang akan kita buat menjadi Static
- **Vlan** : Nomer vlan dari port PC (Kita akan bahas lebih dalam di Lab berikutnya)
- **Fao/1-24** : Nomer Interface dari Switch yg terhubung ke PC

Sekarang kita coba buat kedua mac-address diatas menjadi static dengan cara diatas


```
Switch#conf t
Switch(config)#mac-address-table static 0060.5c38.e9cb vlan 1 interface fa0/1
Switch(config)#mac-address-table static 000a.f322.7578 vlan 1 interface fa0/2
```

Setelah itu kita coba cek hasilnya , dengan perintah *show* , maka Type nya akan berubah menjadi Static

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type           Ports
----    -
1       000a.f322.7578   STATIC        Fa0/2
1       0060.5c38.e9cb   STATIC        Fa0/1
Switch#
```

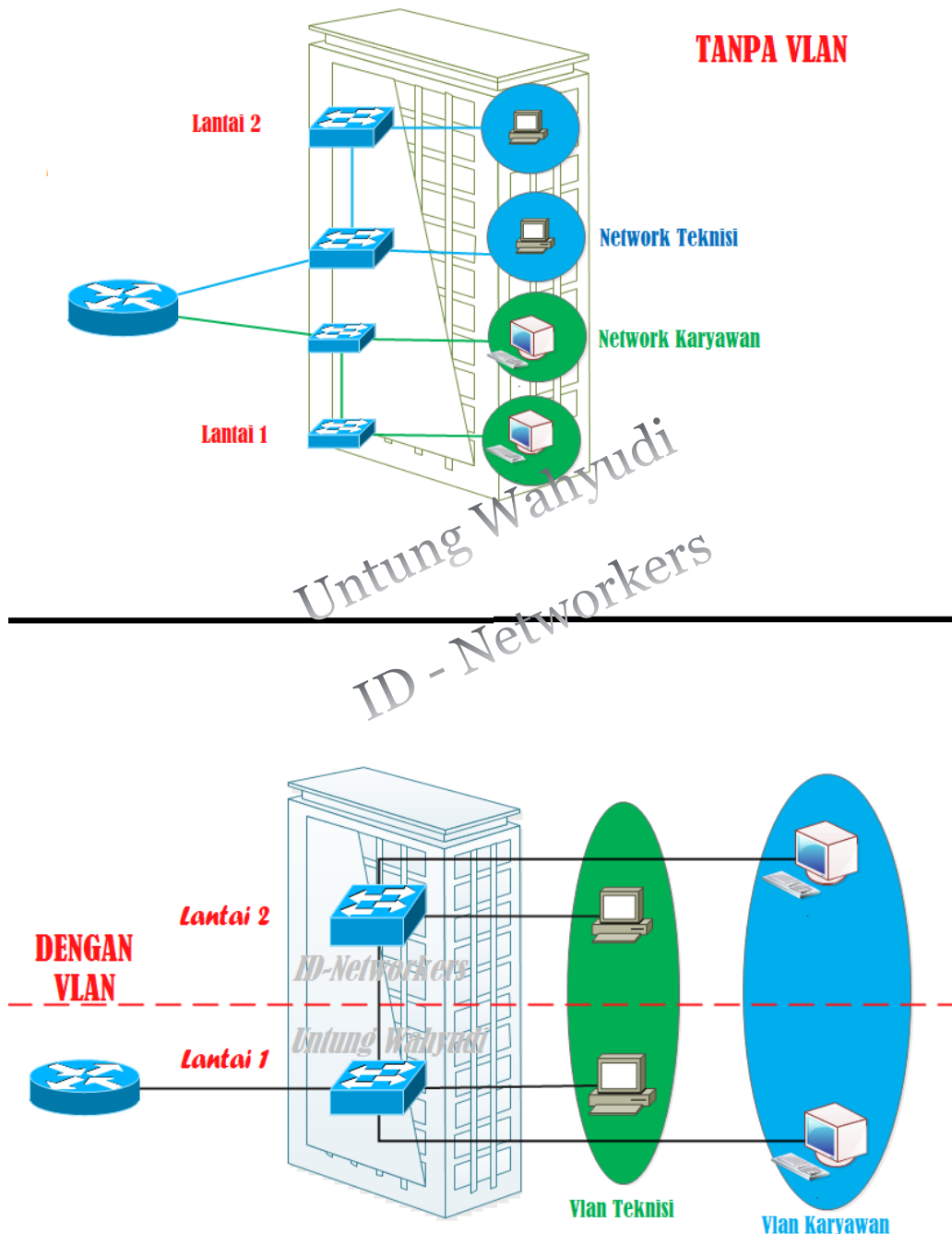
Kemudian untuk pengetasan lagi silahkan tukar port antar PC lalu coba test ping , pasti tidak akan berhasil. Karena Switch sudah mencatat bahwa port fao/1 adalah milik PC yang memiliki MAC Adres diatas.

VLAN

Assalamualaikum wr.wb

Sekarang kita sudah masuk ke BAB Vlan , jadi apa itu Vlan ??

Untuk dapat memiliki gambaran tentang Vlan , monggo simak dan perhatikan 2 topologi dibawah.



Dari gambar diatas kita bisa lihat ada beberapa perbedaan kan ?? Yaitu digambar pertama , jika kita menggunakan switch *unmanageable* yaitu switch seharga 100 atau 200 ribuan , maka semua port switchnya hanya bisa menghubungkan PC yang memiliki Network yang sama saja. Dan jika ingin membuat network yang baru maka harus membeli switch dan menarik kabel dari router lagi. Nah dengan menggunakan Switch *manageable* seperti switch cisco maka kita bisa membuat di satu switch itu menjadi beberapa network. Misal Network Teknisi dan Network Karyawan yang memiliki IP berbeda setiap network nya. Jadi pada **sebuah Switch** seolah seolah terdapat **beberapa LAN**.

Dengan adanya vlan ini , kita bisa memisahkan atau mengelompokkan user/PC sesuai kebutuhan masing-masing. Seperti Vlan Teknisi , Vlan Boss , Vlan Marketing , Vlan karyawan dll. Atau bisa juga berdasarkan lantai, missal vlan 10 untuk lantai 1 dan vlan 20 untuk lantai 2.

KEUNTUNGAN VLAN :

1. Lebih Hemat Switch , karena kita tidak perlu membeli 2 switch untuk memisahkan 2 network yang berbeda.
2. Hemat Resource , karena switch bekerja di layer 2 dan mengirim paket secara broadcast jadi setiap paket dikirim maka akan dibroadcast ke semua PC, bayangkan jika jumlah PC nya ada 100 , nah dengan ada nya Vlan maka broadcast domain hanya akan berbedar di setiap Vlan saja. Jadi lebih menguntungkan.

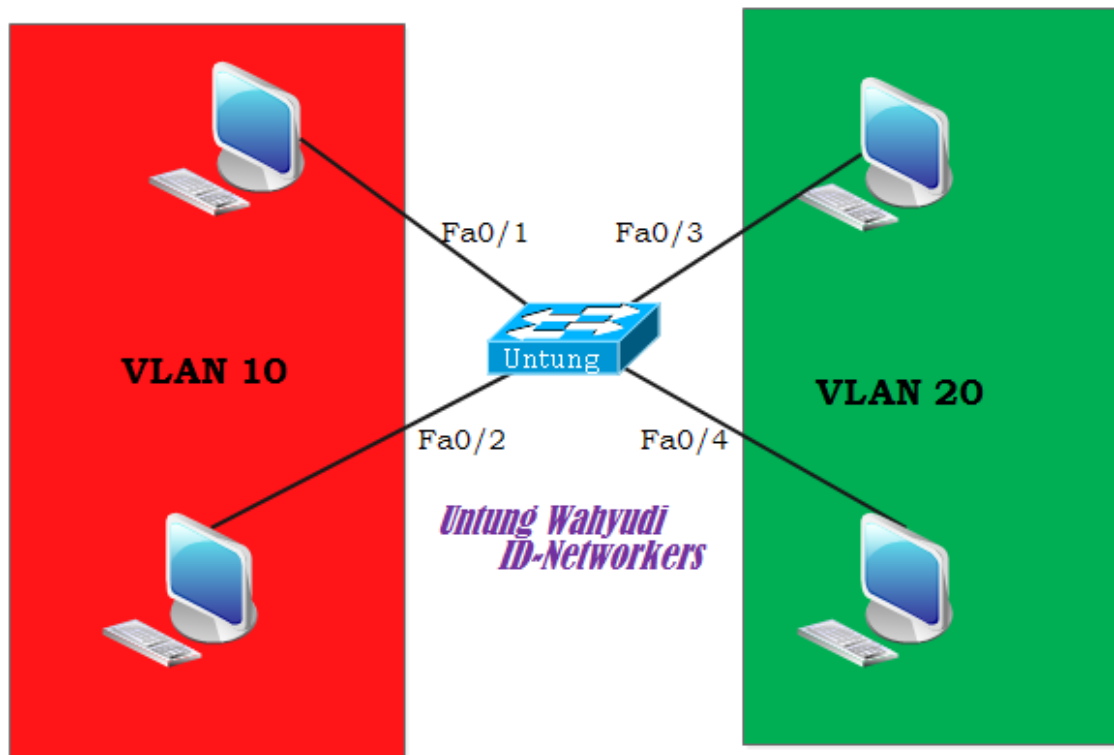
Lab 12. Konfigurasi Vlan di Switch

Assalamualaikum wr.wb .

Setelah kalian mulai paham dengan konsep Vlan , sekarang kita akan belajar membuat vlan dan mendaftarkan port ke vlan tersebut. Sebelum kita membuat vlan ada beberapa hal yang harus diketahui tentang vlan di switch cisco. Yaitu :

- Secara default , switch sudah memiliki 1 vlan , yaitu VLAN 1
- Secara default semua port yang ada di switch terdaftar di VLAN 1
- VLAN 1 TIDAK DAPAT DIHAPUS

Oke sekarang kita langsung masuk materi nya , pertama buat topologi seperti dibawah ini



Kemudian kita akan memastikan bahwa semua port itu terdaftar ke Vlan 1, caranya adalah dengan perintah *show vlan*

```
Switch#sh vlan
```

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 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Bisa dilihat , bahwa Switch secara default sudah memiliki VLAN 1 dengan nama default , lalu semua port yang dimiliki switch terdaftar di Vlan 1. Sekarang kita akan membuat Vlan 10 dan 20. Dan mendaftarkan PC sebelah kiri menjadi Vlan 10 dan PC sebelah Kanan menjadi Vlan 20.

Pertama kita akan buat terlebih dahulu Vlan beserta nama vlan nya. Caranya adalah masuk ke global configuration lalu buat seperti dibawah ini

```
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name UNTUNG
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name WAHYUDI
Switch(config-vlan)#ex
Switch(config)#
```

Setelah selesai membuat vlan selanjutnya daftarkan atau Bahasa kerennya itu *assign* port-port nya kedalam vlan nya. Oke karena sesuai skenario jadi PC sebelah kiri adalah Vlan 10 dan sebelah Kanan adalah Vlan 20 maka kita masukkan seperti ini :

- Fa0/1 & Fa0/2 => VLAN 10
- Fa0/3 & Fa0/4 => Vlan 20

Cara mendaftarkannya adalah dengan ketikkan perintah seperti dibawah ini,.
Pertama kita masuk ke mode global configuration lalu kita masuk ke mode Interface,
Setelah itu kita assign deh , gampang kan ?. Oke pertama kita assign dulu untuk vlan
10 yaitu fao/1 dan fao/2.

- Int = Interface
- Fa = FastEthernet

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
```

Selanjutnya kita assign PC yang sebelah kanan kedalam Vlan 20.

```
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex

Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
```

Selanjutnya kita cek vlan nya, apakah interfacenya sudah terdaftar didalam vlan 10 dan vlan 20 tadi. Jika konfigurasi nya benar maka hasilnya akan seperti dibawah ini interface nya sudah terdaftar dimasing – masing vlan.

```
Switch(config)#do show vlan
```

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
10	UNTUNG	active	Fa0/1, Fa0/2
20	WAHYUDI	active	Fa0/3, Fa0/4
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Setelah selesai meng-assign , sekarang waktunya pengujian. Untuk pengujiannya pertama kita setting IP terlebih dahulu di PC nya. Kita buat menjadi 2 Network. Yaitu **Network Vlan 10** dan **Network Vlan 20**. Untuk IP nya bisa dilihat sebagai berikut

- **VLAN 10 (PC Sebelah Kiri)** = 10.10.10.1/24 dan 10.10.10.2/24
- **VLAN 20 (PC Sebelah Kanan)** = 20.20.20.1/24 dan 20.20.20.2/24

Masih inget kan cara setting IP di PC ??? Jangan sampe lupa lhoo , itu konfig dasar yang penting. Kemudian utk pengujian silahkan test ping , untuk yang vlannya sama pasti akan berhasil , sedangkan yang berbeda vlan akan gagal saling ping. Itu lah fungsi vlan , jadi dia akan membatasi Broadcast Domain nya. Kemudian setelah saling ping , maka table mac-address nya pun akan muncul seperti berikut

Oke karena sesama vlan sudah saling ping dan yang beda vlan tidak bisa ping maka itu artinya sudah berhasil. Dan karena sudah berhasil maka saya tutup lab kali ini dengan mengucapkan Alhamdulillah.

Sekian dulu yoo

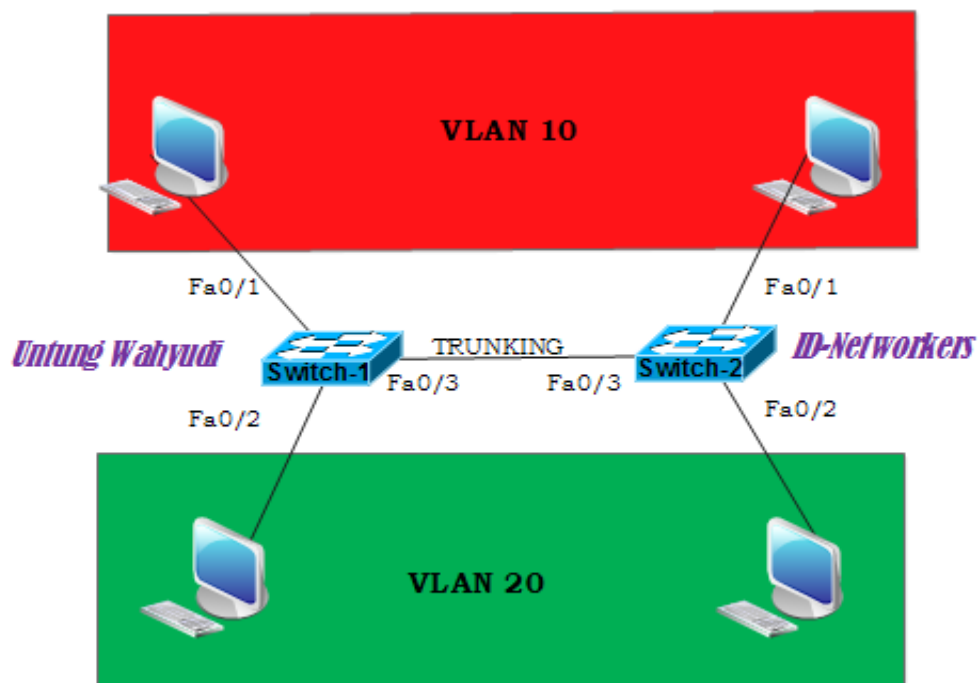
Wassalamualaikum wr.wb

Lab 13. Trunking Vlan.

Assalamualaikum wr.wb

Setelah dilab sebelumnya kita sudah belajar membuat vlan dan mendaftarkan port nya , sekarang kita coba untuk membuat vlan dengan 2 switch. Yang nantinya Vlan yang sama dapat saling ping , meskipun berbeda switch. Jadi intinya adalah kita akan membuat vlan yang sama antar switch dapat saling ping , namun tetap yang berbeda vlan tidak dapat saling ping.

Oke kita buat konfigurasinya dari ulang dengan topologi seperti ini. Untuk menghubungkan antar switch gunakan kabel Cross.



Langsung aja kita buat cepet , karena dilab sebelumnya kalian sudah belajar membuat vlan maka disini saya tidak akan membahas lebih dalam tentang pembuatan vlan , yang saya akan bahas adalah bagaimana cara membuat trunknya.

Pertama kita buat Vlan 10 dan 20 di masing – masing switch. Berikut pembuatan vlan di switch 1

```
##KONFIGURASI SWITCH 1 ##  
Switch-1(config)#vlan 10
```

```
Switch-1(config-vlan)#name UNTUNG
Switch-1(config-vlan)#ex
Switch-1(config)#vlan 20
Switch-1(config-vlan)#name WAHYUDI
Switch-1(config-vlan)#ex
```

Kemudian buat vlan yang sama di Switch 2 , untuk nama boleh beda , namun untuk nomer Vlan nya harus sama , yaitu vlan 10 dan vlan 20.

```
## KONFIGURASI SWITCH 2 ##
Switch-2(config)#vlan 10
Switch-2(config-vlan)#name UNTUNG
Switch-2(config-vlan)#ex
Switch-2(config)#vlan 20
Switch-2(config-vlan)#name WAHYUDI
Switch-2(config-vlan)#ex
```

Kemudian kita daftarkan port portnya sesuai dengan topologi yaitu , namun untuk port yang yang terhubung antar switch (fa0/3) kita akan buat trunk nantinya.

```
## KONFIGURASI SWITCH 1 ##
Switch-1(config)#int fa0/1
Switch-1(config-if)#switchport mode access
Switch-1(config-if)#switchport access vlan 10
Switch-1(config-if)#ex

Switch-1(config)#int fa0/2
Switch-1(config-if)#switchport mode access
Switch-1(config-if)#switchport access vlan 20
Switch-1(config-if)#ex
```

Selanjutnya kita assign juga port yang di switch 2, caranya sama seperti diatas

```
## KONFIGURASI SWITCH 2 ##
```

```
Switch-2(config)#int fa0/1
Switch-2(config-if)#switchport mode access
Switch-2(config-if)#switchport access vlan 10
Switch-2(config-if)#ex

Switch-2(config)#int fa0/2
Switch-2(config-if)#switchport mode access
Switch-2(config-if)#switchport access vlan 20
Switch-1(config-if)#ex
```

Selanjutnya kita akan menghubungkan vlan yang sama namun berbeda switch menggunakan Trunk. Pertama lihat dulu port yang menghubungkan switch itu berada di fastEthernet berapa. Kemudian kita konfigurasi di port tsb.

```
Switch-1(config)#int fa0/3
Switch-1(config-if)#switchport mode trunk
```

Lakukan hal serupa di switch satu nya.

```
Switch-2(config)#int fa0/3
Switch-2(config-if)#switchport mode trunk
```

Kemudian untuk pengujian silahkan setting IP di PC nya , seperti biasa yang satu vlan harus satu network. Vlan 10 = 10.10.10.0/24 dan vlan 20 = 20.20.20.0/24. Lalu test ping yang satu Vlan , maka hasilnya akan berhasil, namun tetap yang berbeda vlan tidak bisa saling ping. InsyaAllah di lab selanjutnya saya akan memberi tahu cara untuk menghubungkan vlan yang berbeda. Oh yaa topologi dan konfigurasi ini jangan dihapus ya, karena akan dipakai di lab selanjutnya.

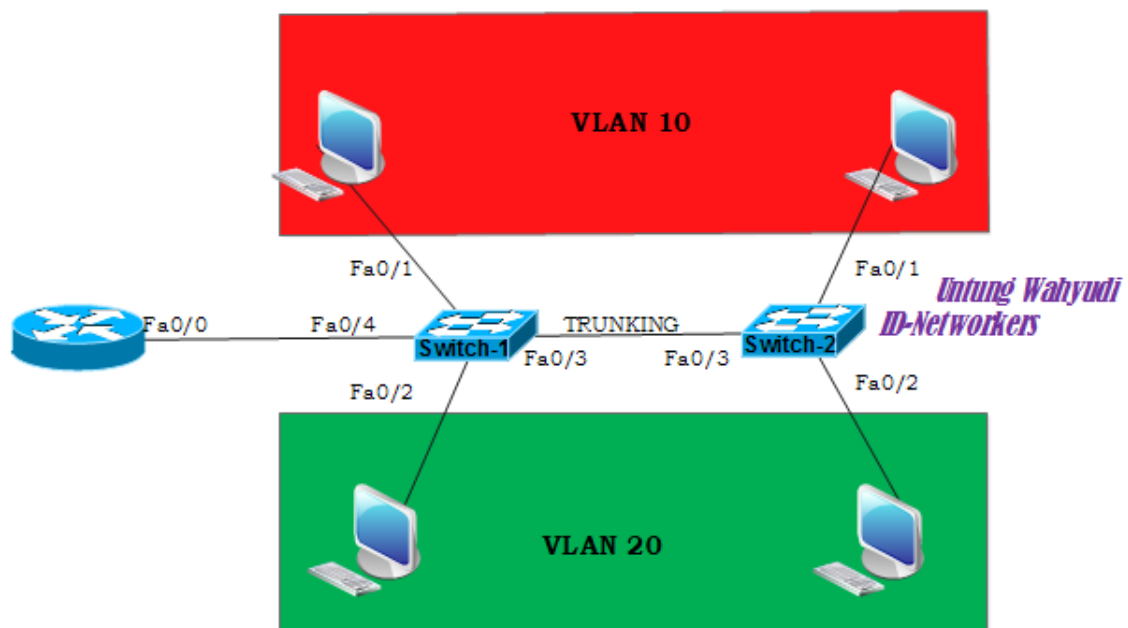
Oke sekian dulu yooo

Lab 14. Menghubungkan Beda Vlan / Router On The Stick

Assalamualaikum wr.wb

Sesuai janji saya dilab sebelumnya , saya akan memberitahu kepada kalian gimana caranya agar Komputer - komputer yang berbeda vlan dapat saling berkomunikasi. Untuk dapat menghubungkan antar vlan dapat dilakukan dengan beberapa cara , yang tentunya harus menggunakan device jaringan yang berada di layer 3 , seperti Router dan Switch layer 3. Fungsinya untuk dijadikan gateway ketika mengirim paket data.

Untuk cara yang pertama saya akan menggunakan Router terlebih dahulu. Kita masih menggunakan topologi dan konfigurasi sebelumnya , jadi konfigurasi sebelumnya jangan dihapus , kita hanya perlu menambahkan Router di atasnya , jadi topologinya akan berubah seperti dibawah ini.



Oke langsung aja kekonfigurasinya , setelah sesama vlan dapat saling berkomunikasi selanjutnya kita buat jalur trunk dari Switch-1 ke Router.

```
Switch-1#conf t
Switch-1(config)#int fa0/4
```

```
Switch-1(config-if)#switchport mode trunk
Switch-1(config-if)#exit
```

Setelah membuat jalur trunk di switch sekarang kita berpindah ke konfigurasi di Router. Selanjutnya kita akan memberikan gateway untuk masing-masing vlan. *Lho kan interface yang terhubung Cuma satu ?? gimana caranya dijadiin 2 gateway yang beda network ??*. Kalo ada yang nanya begitu berarti kalian sudah mulai paham konsep networking , dan juga device cisco tentunya. Sebelumnya kita cek dulu interface dari router tersebut. Dengan cara berikut

```
Router#sh 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

```
Router#
```

Nah lalu gimana caranya ?? Caranya adalah dengan membuat Sub interface sebanyak jumlah vlan yang ingin dilewatkan. Jadi nantinya IP dari Sub-Interface inilah yang akan dijadikan Gateway untuk masing-masing Vlan.

Untuk membuat sub interface caranya adalah sebagai berikut, kita masuk ke dalam Interface yang terhubung ke switch , kemudian kita tambahkan sub interface didalamnya.

```
## BUAT SUB-INTERFACE UNTUK VLAN 10 ##
Router#conf t
Router(config)#int fa0/0
Router(config-if)#int fa0/0.10          → SUB INTERFACE
Router(config-subif)#encapsulation dot1q 10
→ Enkapsulasi nya
```

```
Router(config-subif)#ip addr 10.10.10.1 255.255.255.0
```

→Pemberian Ip Address

```
Router(config-if)#no shutdown
```

→Perintah untuk

mengaktifkan Interface

```
Router(config-subif)#ex
```

Biar lebih jelas mari saya kasih keterangan :

- **No shutdown** = Yang berarti “Tidak Mati” , artinya kita akan menghidupkan interface tsb.
- **Int Fa0/0.10** = angka “10” itu adalah nomer dari vlan nya. Jadi kita akan membuat sub-interface untuk vlan 10
- **Encapsulation dot1q** = artinya kita akan membuat jenis enkapsulasi nya menjadi 802.1q. Dia Cisco terdapat 2 jenis enkripsi yaitu ISL dan 802.1q , namun jenis ISL tidak semua perangkat support dengan enkripsi itu , jadi enkapsulasi dot1q lah yang lebih banyak dipakai.

Kemudian buat juga Sub interface untuk vlan 20 , caranya masih sama seperti sebelumnya , kita konfigurasi kan didalam interface fa0/0.

```
Router(config)#int fa0/0
```

```
Router(config-if)#int fa0/0.20
```

```
Router(config-subif)#encapsulation dot1q 20
```

```
Router(config-subif)#ip addr 20.20.20.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-subif)#ex
```

Setelah itu kita cek lagi IP dari interface nya , dan pastikan di interface fa0/0 sudah terdapat sub-interface seperti dibawah ini

```
Router(config)#do show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up

```

FastEthernet0/0.10      10.10.10.1      YES manual      up      up
FastEthernet0/0.20      20.20.20.1      YES manual      up      up
FastEthernet0/1         unassigned       YES unset      administratively down
down
Vlan1                   unassigned       YES unset      administratively down
down
Router(config)#

```

Selanjutnya kita masuk ke pengujian , pertama kita setting IP di PC sesuai network vlan nya , lalu jangan lupa masukkan gatewaynya, untuk PC Kiri (VLAN 10) Gateway nya adalah 10.10.10.1 dan untuk PC Kanan (VLAN 20) Gateway nya adalah 20.20.20.1

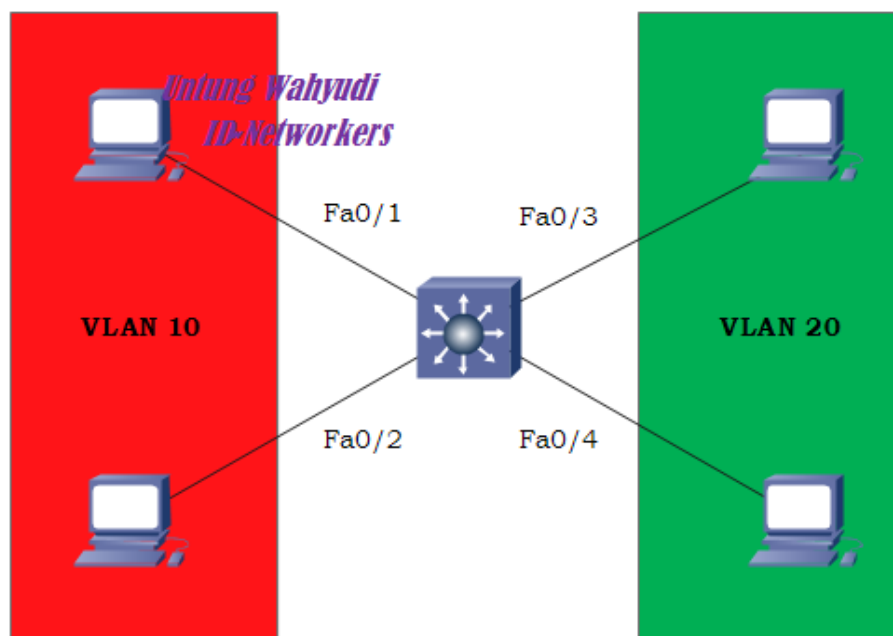
Oke selanjutnya tinggal test ping deh , pertama test dulu ping ke gateway/router dulu. Jika belum bisa , coba ping lagi dan lagi. Jika sudah dapat reply semua baru test ping antar Client yang beda Vlan. Jika belum berhasil berarti ada kesalahan dalam konfigurasi

Oke sekian dulu lab kali ini

Wassalamualaikum wr.wb

Lab 15. Menghubungkan Beda Vlan / Switch Layer 3

Oke lanjut lagi , materi di lab ini gak jauh beda dengan lab sebelumnya, yaitu bagaimana caranya menghubungkan Antar vlan. Kalo dilab sebelumnya kita menggunakan Router , nah di lab ini kita akan gunakan perangkat yang lain , yaitu switch layer 3. Switch layer 3 ini fungsinya hampir sama seperti Router , karena dia berjalan di Layer 3 OSI Model. Oke langsung aja buat topologinya seperti dibawah ini. Untuk jenis switch nya 3560-24ps.



Oke langkah pertama adalah kita buat terlebih dahulu vlan 10 dan vlan 20. Caranya sama seperti di switch yang lain.

```
Switch#conf t
```



```

Switch(config)#vlan 10
Switch(config-vlan)#name UNTUNG
Switch(config-vlan)#ex

Switch(config)#vlan 20
Switch(config-vlan)#name WAHYUDI
Switch(config-vlan)#ex

```

Selanjutnya kita assign port nya kedalam vlan , nah sekalian saya ingin ngasih tau cara cepat untuk melakukan konfigurasi terhadap lebih dari 1 interface , yaitu dengan cara menambahkan sintak *range* di konfigurasi interface. Berikut caranya

```

Switch(config)#int range fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit

```

Bisa dilihat , diatas saya menambahkan sintak *range* artinya kita akan menkonfigurasi range interface dari fao/1 sampai fao/2. Selanjutnya kita assign juga untuk vlan 20 nya.

```

Switch(config)#int range fa0/3-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit

```

Setelah sudah , pastikan setiap port nya sudah terdaftar di masing-masing vlan nya. Seperti dibawah ini.

```

Switch(config)#do show vlan

```

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 UNTUNG active Fa0/1, Fa0/2
```

```
20 WAHYUDI active Fa0/3, Fa0/4
```

```
1002 fddi-default act/unsup
```

```
1003 token-ring-default act/unsup
```

```
1004 fddinet-default act/unsup
```

```
1005 trnet-default act/unsup
```

Selanjutnya kita akan memberikan IP ke masing-masing interface vlan , IP ini lah yang nantinya akan dijadikan gateway dari PC untuk dapat saling berkomunikasi antar vlan.

```
Switch(config)#int vlan 10
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
Switch(config-if)#ex

Switch(config)#int vlan 20
Switch(config-if)#ip address 20.20.20.1 255.255.255.0
Switch(config-if)#ex
```

Kemudian cek IP dari interface vlan nya , dengan cara seperti biasa.

```
Switch(config)#do show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up

```

FastEtherneto/4    unassigned    YES unset up        up
FastEtherneto/5    unassigned    YES unset down      down
GigabitEtherneto/1 unassigned    YES unset down      down
GigabitEtherneto/2 unassigned    YES unset down      down

Vlan1              unassigned    YES unset administratively down down
Vlan10             10.10.10.1   YES manual up        up
Vlan20             20.20.20.1   YES manual up        up
Switch(config)#

```

Setelah itu kita masukkan perintah terakhir yaitu perintah yang sangat berguna. Karena perintah ini digunakan untuk menghubungkan antar vlan. Perintah nya cukup simple kok.

```
Switch(config)#ip routing
```

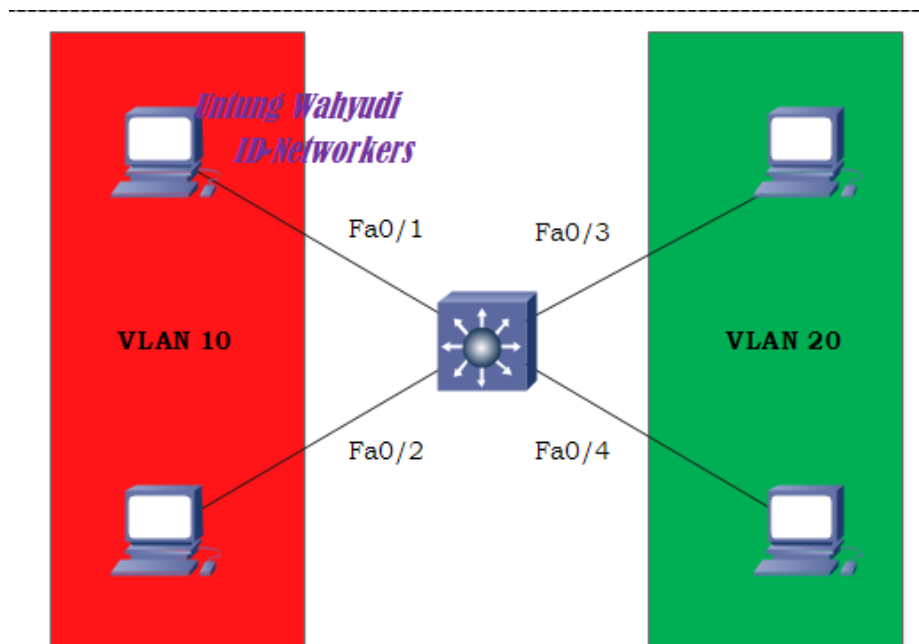
Setelah itu waktu nya pengujian , pertama setting IP nya terlebih dahulu. Seperti biasa , PC yang berada di vlan 10 kita beri gateway 10.10.10.1 dan untuk pc yang berada di vlan 20 kita beri gateway 20.20.20.1. Selanjutnya silahkan test ping antar vlan . InsyaAllah akan berhasil. Kemungkinan untuk ping pertama kali ke antar vlan akan gagal, namun yang kedua kalinya akan berhasil. Jika belum berhasil berarti ada kesalahan dalam konfigurasi mas broo.

Oke sekian dulu

Wassalam.

Lab 16. Membuat Switch menjadi DHCP Server

Oke masih kuaat?? Kita lanjut lagi nih masih dengan topolog yang sama seperti di lab sebelumnya , kali ini saya akan menjelaskan cara membuat DHCP Server di Switch. Jadi untuk membuat DHCP Server di switch hanya bisa dilakukan di switch layer 3 saja. Dan tidak bisa di switch layer2. Oh ya sebelumnya udah pada paham DHCP kan ?? DHCP itu sebuah sistem pengalokasian/pemberian IP secara otomatis kepada client yang membutuhkan.



Oke yuk cuss ke langkah-langkah nya , yaitu langsung masuk ke inti nya. Konfigurasi DHCP server untuk setiap Vlan nya. Berikut caranya

```
Switch#conf t
Switch(config)#ip dhcp pool DHCP-A → Nama dari DHCP
nya
Switch(dhcp-config)#network 10.10.10.0 255.255.255.0
Switch(dhcp-config)#default-router 10.10.10.1 → Gateway
Switch(dhcp-config)#ex

Switch(config)#ip dhcp pool DHCP-B
```

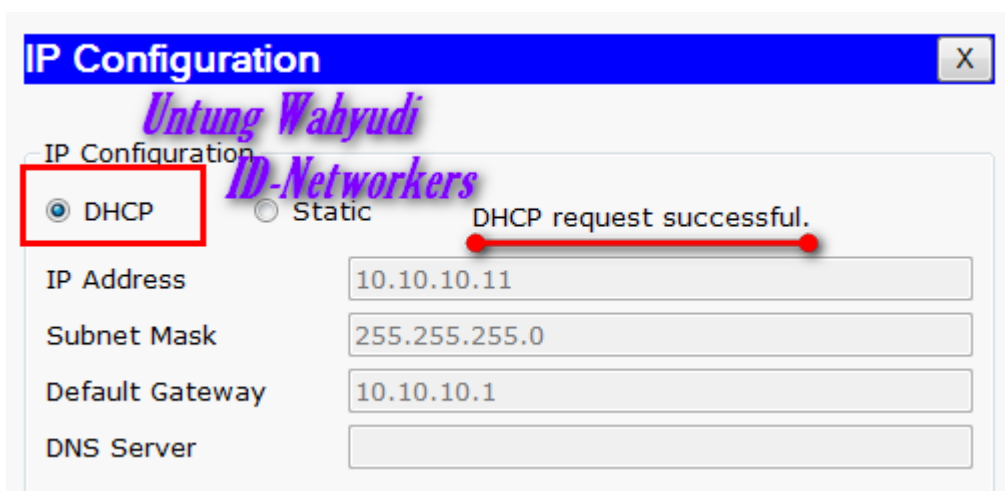
```
Switch(dhcp-config)#network 20.20.20.0 255.255.255.0
Switch(dhcp-config)#default-router 20.20.20.1
Switch(dhcp-config)#ex
Switch(config)#
```

Kita juga bisa memberikan batasan IP berapa saja yang TIDAK BOLEH diberikan ke client dengan perintah *ip dhcp excluded-address <IP awal> <IP Akhir>*

```
Switch(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.10
Switch(config)#ip dhcp excluded-address 20.20.20.1 20.20.20.10
```

Dengan perintah diatas , maka VLAN 10 akan mendapat IP mulai dari 10.10.10.11 dan VLAN 20 akan mendapat IP mulai dari 20.20.20.11.

Selanjutnya kita test di sisi client, dibagian konfigurasi IP kita pilih tab yang DHCP maka secara otomatis client akan mendapatkan IP dari Switch



Oke karena client sudah mendapat IP secara otomatis berarti lab kali ini sudah berhasil. Sekian dulu yoo

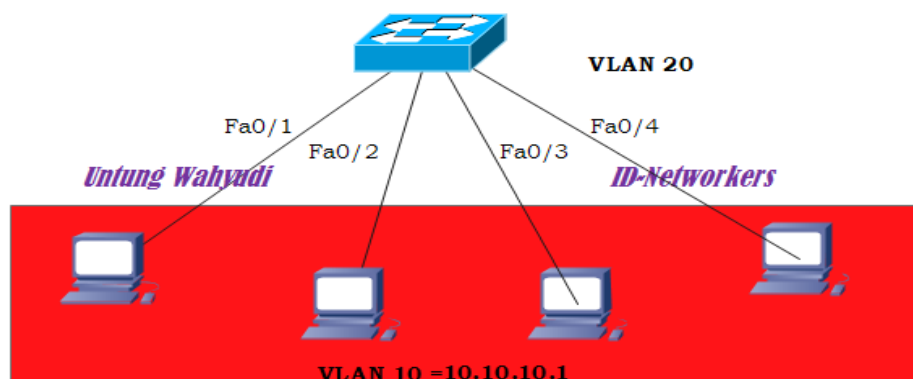
Wassalamualaikum.

Lab 17. Cara membuat switch dapat diremote lewat Telnet

Assalamualaikum wr.wb

Lanjut lagi yuk , sekarang kita masuk ke lab tentang cara meremote switch. Selama ini kan kita pake packet tracer , dan untuk melakukan konfigurasi terhadap switch/router kita hanya tinggal klik router nya lalu tampilan terminal akan muncul. Namun di real device nya kita harus me-remote device tersebut dari sebuah PC atau Laptop. Nah untuk meremotinya ada banyak cara . di Lab ini saya akan menjelaskan cara remote nya lewat telnet, masih tetap pakai Packet Tracer tentunya, karena disini tidak ada real device nya :v.

Oke langsung aja buat topologi seperti ini , switchnya bebas mau pakai yang layer 2 atau layer 3 sama saja.



Seperti biasa hal yang harus dilakukan adalah membuat vlan untuk port port nya. Disini kita hanya perlu membuat 1 vlan saja , dan mendaftarkan semua PC kedalam Vlan 10.

```
Switch>enable
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name TELNET
Switch(config-vlan)#ex
```

```
Switch(config)#int range fa0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#ex
Switch(config)#
```

Setelah itu kita setting IP untuk VLAN 10 , yang nantinya akan dijadikan gateway sekaligus IP untuk diremote oleh client. Caranya sebagai berikut

```
Switch(config)#int vlan 10
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
Switch(config-if)#ex
```

Jika sudah selanjutnya kita akan mengaktifkan dan memberikan password untuk remote telnet (Virtual Terminal). Caranya adalah sebagai berikut

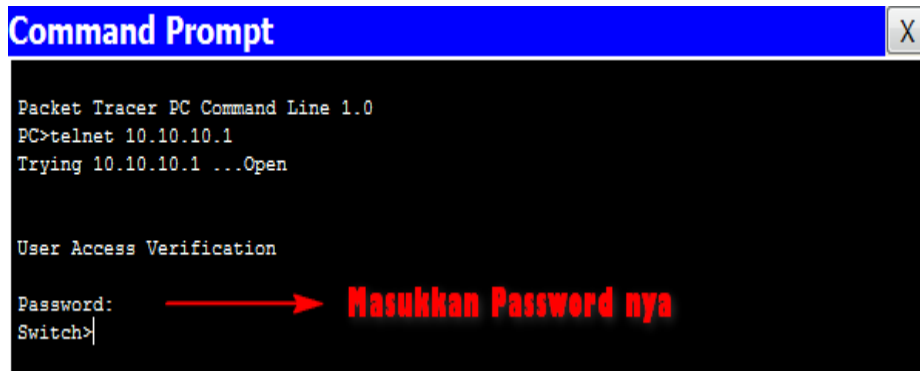
```
Switch(config)#line vty 0 2
Switch(config-line)#password untung
Switch(config-line)#exit
```

Yuk kita bahas sintaks diatas , jadi berikut keterangannya :

- **Line** artinya kita akan mengkonfigurasi Terminal Configure
- **Vty** artinya jenis terminal yang akan diaktifkan adalah *Virtual Terminal* , seperti telnet , ssh dll.
- **0 2** , artinya id yang akan diberikan ke user yg meremote. Ini juga menggambarkan jumlah Client yg dapat meremote. Angka “0” adalah angka awal yg diberikan ke client dan “2” adalah id/angka terakhir yang diberikan ke client. Jadi nanti client akan mendapatkan ID 0 - 2. Jadi User yang dapat meremote adalah sejumlah 3 Client (ID 0, 1, dan 2).

Jika sudah selanjutnya setting IP di client dan masukan gateway nya dengan IP dari switch yaitu 10.10.10.1 ,

Selanjutnya kita test remote , ketikkan perintah *telnet <IP SWITCH>* . Maka hostname yang tadi nya PC akan berubah menjadi Switch>

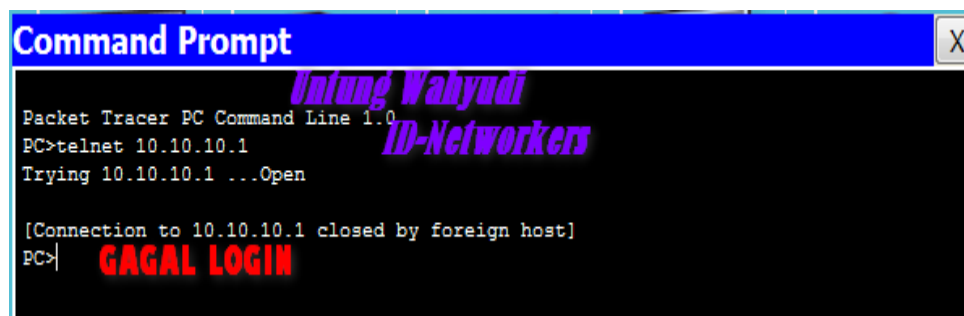


```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>telnet 10.10.10.1
Trying 10.10.10.1 ...Open

User Access Verification

Password: → Masukkan Password nya
Switch>
```

Dan untuk memastikan bahwa jumlah client yang dapat meremote adalah 3 client , maka semua client cobalah untuk meremote , pasti yang ke-4 akan gagal. Berikut gambar nya.



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>telnet 10.10.10.1
Trying 10.10.10.1 ...Open

[Connection to 10.10.10.1 closed by foreign host]
PC> GAGAL LOGIN
```

Oke sekian dulu yaa tentang lab meremote ini.

Wassalamualaikum wr.wb

Lab 18. VTP (Vlan Trunking Protocol)

Assalamualaikum wr.wb

Sekarang kita ke tahap lebih lanjut tentang Vlan. Setelah kita belajar membuat dan menghubungkan vlan di lab ini saya akan membahas cara meng-advertise vlan. Yaitu dengan menggunakan VTP atau Vlan Trunking Protocol. Didalam VTP ini ada 3 mode untuk setiap switch nya , yaitu :

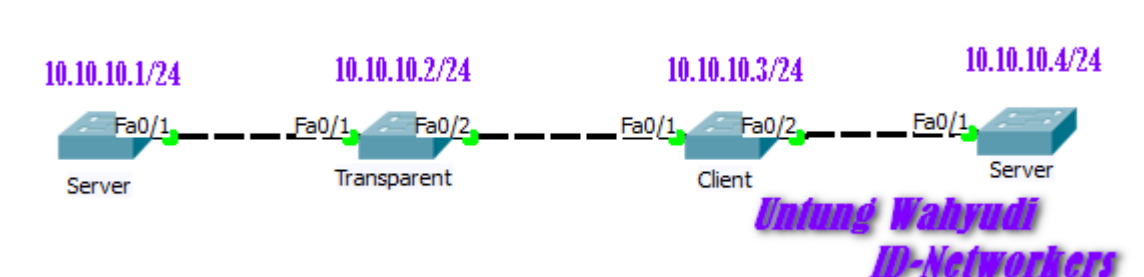
1. VTP Server
2. VTP Tranparent
3. VTP Client.

Secara default semua switch merupakan VTP Server.

Yang perlu diketahui tentang 3 mode itu adalah sebagai berikut :

VTP SERVER	VTP TRANSPARENT	VTP CLIENT
Dapat membuat dan menghapus vlan	Hanya bersifat independent , Jika membuat vlan maka hanya untuk dirinya sendiri	Tidak bisa membuat vlan , hanya bisa menerima VTP Update dari Server
Memforward dan menerima VTP Update	Hanya mem-forward semua VTP update , tapi tidak dimasukkan ke databasenyanya	Menerima dan mem-forward VTP Update
SEMUA VTP APAPUN YANG SATU DOMAIN AKAN MENERUSKAN / MEM-FORWARD VTP UPDATE KE SWITCH LAINNYA		

kita masuk ke tahap lab nya , buatlah topologi seperti dibawah ini ,



Oke langsung kita mulai konfigurasi nya , hal pertama yang harus dilakukan adalah mengaktifkan fitur Trunk pada Interface VLAN 1 pada semua Switch , agar dapat saling terkoneksi. INGAAT SEMUA SWITCH !

```
Switch#conf t
Switch(config)#int range fa0/1-2
Switch(config-if-range)#switchport mode trunk
```

Lakukan konfigurasi diatas untuk semua switch , kemudian kita setting IP untuk interface Vlan 1 untuk masing-masing switch. Kita buat IP nya sesuai dengan topologi diatas yo.

KONFIGURASI SWITCH-A

```
Switch-A(config)#int vlan 1
Switch-A(config-if)#ip addr 10.10.10.1 255.255.255.0
Switch-A(config-if)#no shutdown
Switch-A(config-if)#exit
```

KONFIGURASI SWITCH-B

```
Switch-B(config)#int vlan 1
Switch-B(config-if)#ip addr 10.10.10.2 255.255.255.0
Switch-B(config-if)#no shutdown
Switch-B(config-if)#exit
```

KONFIGURASI SWITCH-C

```
Switch-C(config)#int vlan 1
Switch-C(config-if)#ip addr 10.10.10.3 255.255.255.0
Switch-C(config-if)#no shutdown
Switch-C(config-if)#exit
```

KONFIGURASI SWITCH-D

```
Switch-D(config)#int vlan 1
Switch-D(config-if)#ip addr 10.10.10.4 255.255.255.0
Switch-D(config-if)#no shutdown
Switch-D(config-if)#exit
```

Sekarang kita masuk ke konfigurasi VTP nya , pertama yang harus diperhatikan adalah kita harus membuat VTP Domain yang sama dan juga Password nya. Dan tentunya jenis dari VTP untuk setiap switchnya.

VTP SWITCH-A

```
Switch-A(config)#vtp mode server
Switch-A(config)#vtp domain UNTUNG
Switch-A(config)#vtp password rahasia
```

VTP SWITCH-B

```
Switch-B(config)#vtp mode transparent
Switch-B(config)#vtp domain UNTUNG
Switch-B(config)#vtp password rahasia
```

VTP SWITCH-C

```
Switch-C(config)#vtp mode client
Switch-C(config)#vtp domain UNTUNG
Switch-C(config)#vtp password rahasia
```

VTP SWITCH-D

```
Switch-D(config)#vtp mode server
Switch-D(config)#vtp domain UNTUNG
Switch-D(config)#vtp password rahasia
```

Setelah sudah kemudian test dengan membuat Vlan di setiap Switch. Seperti berikut

```
Switch-A(config)#vlan 10
Switch-A(config-vlan)#name VLAN-A
```

```
Switch-B(config)#vlan 20
Switch-B(config-vlan)#name VLAN-B
```

```
Switch-C(config)#vlan 30
VTP VLAN configuration not allowed when device is in CLIENT
mode.
Switch-C(config)#
```

“(SWITCH VTP CLIENT TIDAK BISA MEMBUAT VLAN)”

```
Switch-D(config)#vlan 40
```

```
Switch-D(config-vlan)#name VLAN-D
```

Dari gambar diatas bisa dilihat bahwa semuanya dapat membuat vlan kecuali yang ber-mode CLIENT. Selanjutnya kita lakukan verifikasi , dengan cara lihat jumlah Vlan yang ada di setiap switch , jika berhasil maka semua switch **KECUALI** SwitchB atau switch yang bermode Transparent akan memiliki jumlah Vlan yang sama. Jumlah vlannya adalah 2 Vlan , yang dibuat oleh Switch-A dan Switch-B. Berikut contoh nya

```
Switch-A#show vlan
```

VLAN Name	Status	Ports
1 default	active	FaO/2, FaO/3, FaO/4, FaO/5 FaO/6, FaO/7, FaO/8, FaO/9 FaO/10, FaO/11, FaO/12, FaO/13 FaO/14, FaO/15, FaO/16, FaO/17 FaO/18, FaO/19, FaO/20, FaO/21 FaO/22, FaO/23, FaO/24
10 VLAN-A	active	
40 VLAN-D	active	

Namun untuk jumlah vlan yang ada di Transparent hanya satu yaitu vlan yang dibuatnya sendiri. Dan vlan ini tidak disebar ke Switch lain , makanya kita tidak melihat VLAN-B atau vlan dari switch-B.

```
Switch-B#show vlan
```

VLAN Name	Status	Ports
1 default	active	FaO/3, FaO/4, FaO/5, FaO/6 FaO/7, FaO/8, FaO/9, FaO/10 FaO/11, FaO/12, FaO/13, FaO/14 FaO/15, FaO/16, FaO/17, FaO/18 FaO/19, FaO/20, FaO/21, FaO/22 FaO/23, FaO/24
20 VLAN-B	active	
1002 fddi-default	act/unsup	

Oke sekian dulu tentang VTP yoo ,

Wassalam !

Lab 19. Spanning Tree Portfast

Assalamualaikum wr.wb

Di lab kali saya akan memberikan sedikit tips untuk switch. Bila kita colokkan kabel ke switch biasanya butuh waktu yang agak lama untuk switch dapat aktif, kalo di packet tracer maka simbolnya akan berwarna dari orange hingga ke hijau. Kira kira dibutuhkan waktu sekitar 40 - 50 detik. Berikut tahapan port switch agar menjadi aktif

```
Blocking -----> Listening -----> Learning -----> Forwarding (lampu
hijau)
20 detik           15 detik           15 detik
<optional>
```

Kita bisa buat lebih cepat dengan menggunakan Spanning Tree Portfast, kita bisa buat lebih cepat. Karena status port nya akan akan *jumping* dari Blocking langsung ke forwarding. Dengan menggunakan **topologi sebelumnya** kita langsung ke konfigurasinya, sebagai berikut

```
Switch(config)# interface range fa0/1-4
Switch(config-if)# spanning-tree portfast.
```

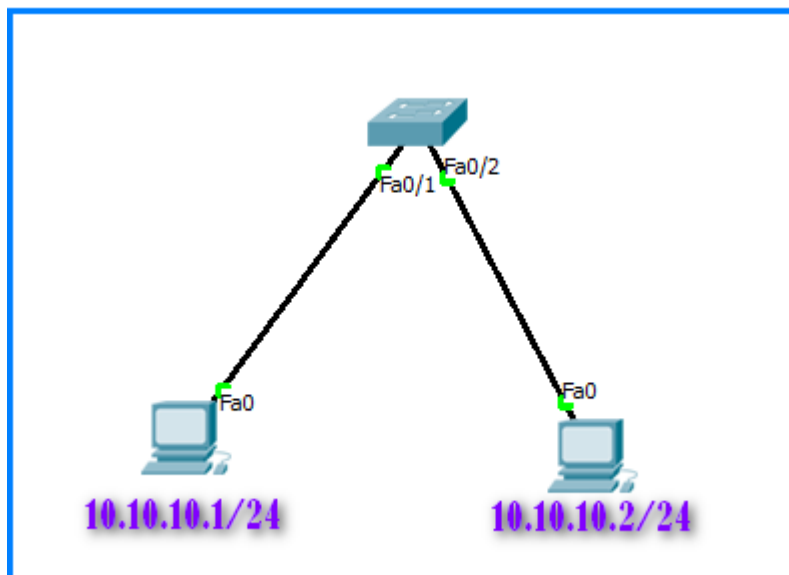
Selanjutnya silahkan test dengan mencabut dan pasang lagi kabel nya dari PC, dan pastikan kali ini proses nya akan lebih cepat dari warna orange sampe ke hijau.

Untuk tambahan Spanning Portfast ini lebih cocok jika di pasang di Switch yang terhubung ke End Device / ke Client PC. Karena jika dipasang di switch yang terhubung antar switch maka akan terjadi error karena switch tidak membacanya,

Lab 20. Port Security Static

Sekarang kita masuk ke awal dari keamanan. Kita bisa membuat agar port yang digunakan oleh PC tidak dapat ditukar oleh pc lain. Jadi kita ada yang nekat menukarnya maka pc tersebut tidak bisa terkoneksi ke switch. Konsepnya sama seperti di lab Mac Address Static , namun di lab ini kita akan menggunakan Switch Port Security. Ada 2 cara dalam membuat port security ini , yaitu dengan static dan sticky. Kalo Static kita akan masukan secara manual mac-address dari pc nya ,kalo sticky dia akan otomatis menggunakan mac-address yg sudah terdaftar.

Langsung aja , pertama kita akan buat yang static terlebih dahulu. Yang harus dilakukan adalah buat topologi seperti dibawah ini, kemudian tanpa konfigurasi switch , atur IP di PC nya , PC-A = 10.10.10.1/24 dan PC-B = 10.10.10.2/24.



Jika sudah selanjunya test ping antar client , sehingga terbentuk table mac-address di Switch. Pastikan Ping nya berhasil yaaa

```
Switch>enable
Switch#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -

```

```
1      0000.0cc8.69aa    DYNAMIC    Fa0/1
1      00e0.a302.b27c    DYNAMIC    Fa0/2
Switch#
```

Selanjutnya kita atur port-security di kedua Interface tersebut. Seperti yang dibilang sebelumnya , karena kita menggunakan static maka kita masukkan Mac-Address nya secara manual.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0000.0cc8.69aa
Switch(config-if)#exit
```

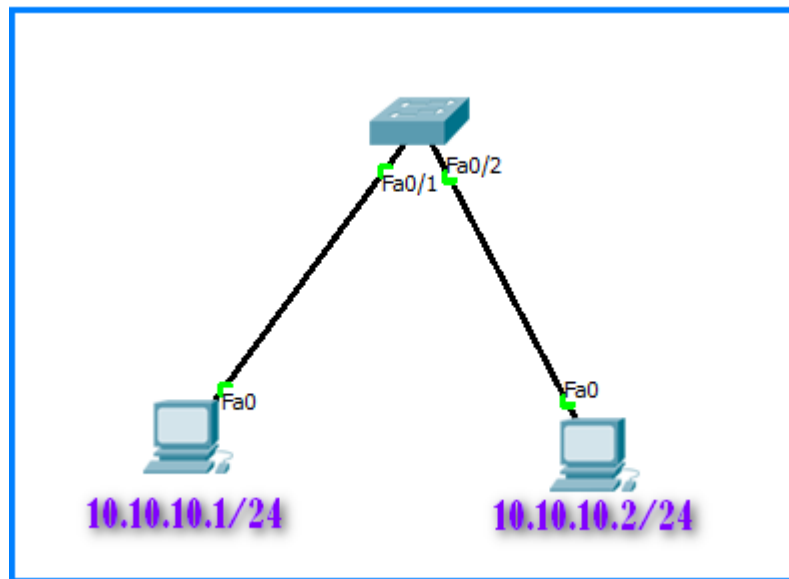
Lakukan juga untuk interface fao/2 nya.

```
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 00e0.a302.b27c
Switch(config-if)#exit
```

Untuk pengujian cabut dan tukar port nya , jadi tadi yang PC kiri pindahkan ke fao/2 , dan yang PC kanan pindahkan ke Fa0/1. Lalu lakukan test ping , maka hasilnya akan tidak berhasil dan link akan tershutdown. Itulah fungsi dari Port Security. Di Lab selanjutnya akan saya bahas tentang Port Security Sticky

Lab 21. Port Security Sticky

Karena dilab sebelumnya kita sudah praktek tentang port security static yakni kita harus mendaftarkan secara otomatis sekarang kita akan menggunakan cara yang kedua yaitu dengan cara Sticky , jadi kita tidak perlu lagi mendaftarkan mac address nya secara manual. Langsung aja yuk, kita pakai topologi yang sama , tapi tidak harus melanjutkan konfigurasi yang sebelumnya.



Seperti biasa atur dulu IP di PC kanan dan kiri , kemudian kita masuk ke konfigurasi Switch nya. Cara nya tidak jauh berbeda dengan dengan static kok malah yang ini lebih simple.

```
Switch(config)#int range fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#ex
Switch(config)#
```

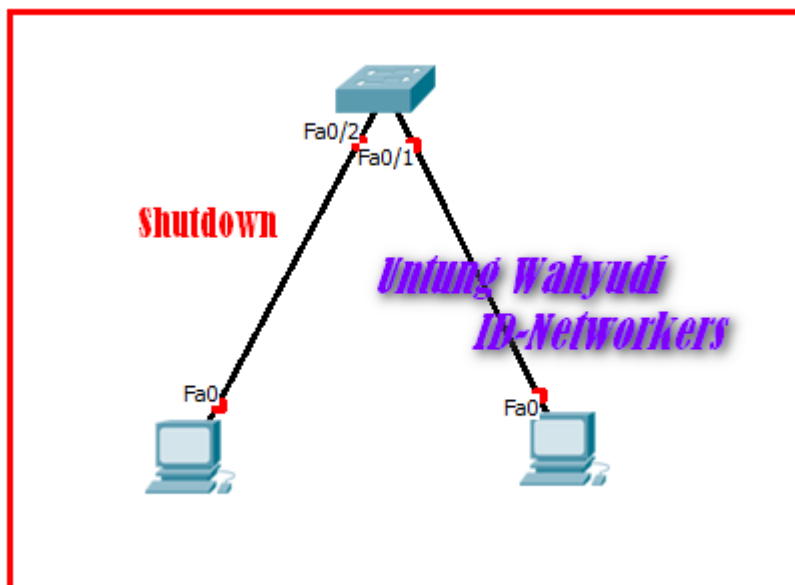
Jika sudah selanjutnya test ping dari client , agar table mac-address di switch terbentuk , jika sudah maka akan muncul seperti berikut

```
Switch(config)#do show mac-address-table
Mac Address Table
```


Vlan	Mac Address	Type	Ports
1	0000.0c06.a985	STATIC	Fa0/2
1	0009.7c26.176e	STATIC	Fa0/1

Switch(config)#

Setelah itu silahkan lepas dan tukar kan portnya seperti di lab sebelumnya. Maka hasilnya port akan ter-shutdown. Sama seperti sebelumnya.



Bisa dilihat bahwa port nya ter-shutdown , untuk mengaktifkan nya kembali kita tinggal pindah port nya , lalu kita matikan dan nyalakan kembali

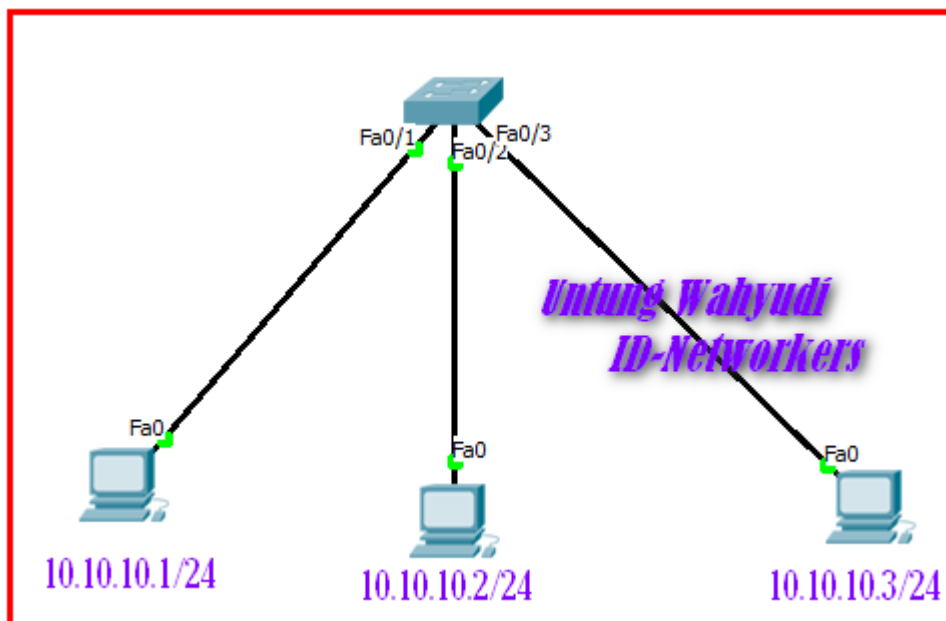
“Shutdown dan no shutdown” kembali

Lab 22. Port Security Violation

Masih di port security nih , sekarang kita bahas yang lebih mudah dan gampang lagi. Sebenarnya ini adalah terusan dari lab sticky namun saya buat menjadi beda lab. Kalo di Sticky ketika PC bertukar port maka akan otomatis tershutdown , namun di violation ini kita bisa memilih action yang diberikan. Ada 3 Action di Violation :

1. Shutdown : Port nya akan otomatis ter-shutdown seperti dilab sebelumnya
2. Protect : Data yang dikirim akan dibiarkan alias tidak dikirim ke tujuan
3. Restrict : hampir sama seperti Protected dengan mengirimkan notifikasi SNMP.

Kita buat topologi nya seperti ini , dengan 3 PC sebagai client. Nantinya port fao/1 mendapat action shutdown , fao/2 = Protected , fao/3 = Restrict.



Seperti biasa , kalian setting dulu IP di masing-masing PC. Kemudian kita konfigurasi Violation nya seperti berikut. Yang pertama kita akan buat untuk Fa0/1 dengan action Shutdown.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
```

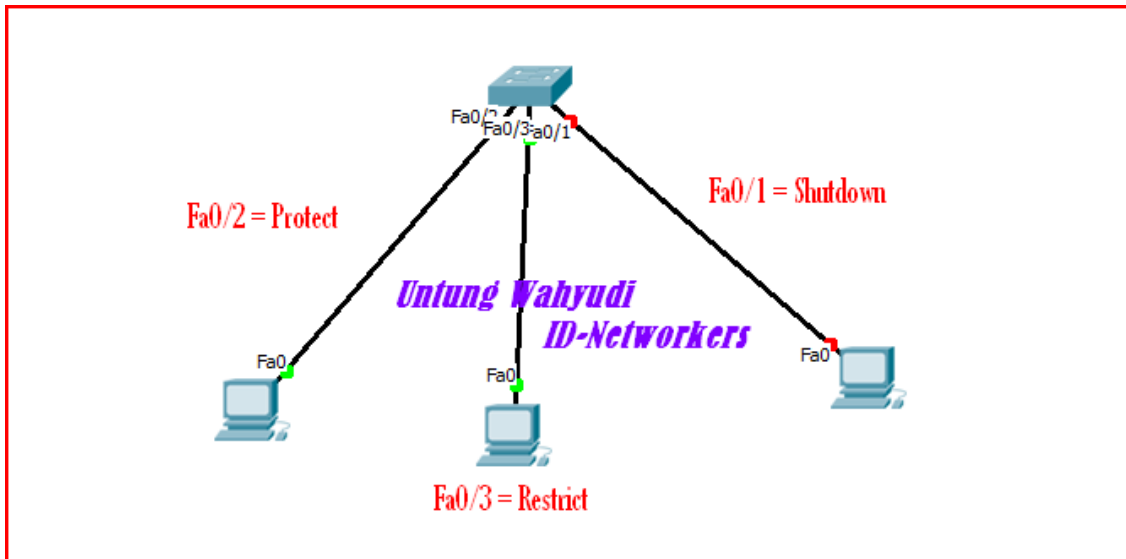
```
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#
```

Kemudian kita buat juga untuk Fa0/2 dan fa0/3 dengan action yang berbeda tentunya.

```
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#

Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#exit
Switch(config)#
```

Untuk pengujian caranya masih sama , pertama test ping antar client sampai mendapat reply , kemudian cabut dan tukarkan port nya, setelah itu test ping lagi. Maka hasilnya akan seperti ini



Ketika kita pakai Action Shutdown , maka paket data tidak dikirim dan portnya langsung ter-shutdown. Namun jika kita gunakan Protect atau Restrict . Paket data tidak akan terkirim (Tidak bisa di Ping) , namun port nya tidak mati alias masih tetap hidup.

Kita juga bisa memonitoring port yang terkena Port-Security. Caranya sebagai berikut

```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security
Action
                (Count)          (Count)          (Count)
-----
    Fa0/1         1             1             1         Shutdown
    Fa0/2         1             1             0         Protect
    Fa0/3         1             1             6         Restrict
Switch#
```

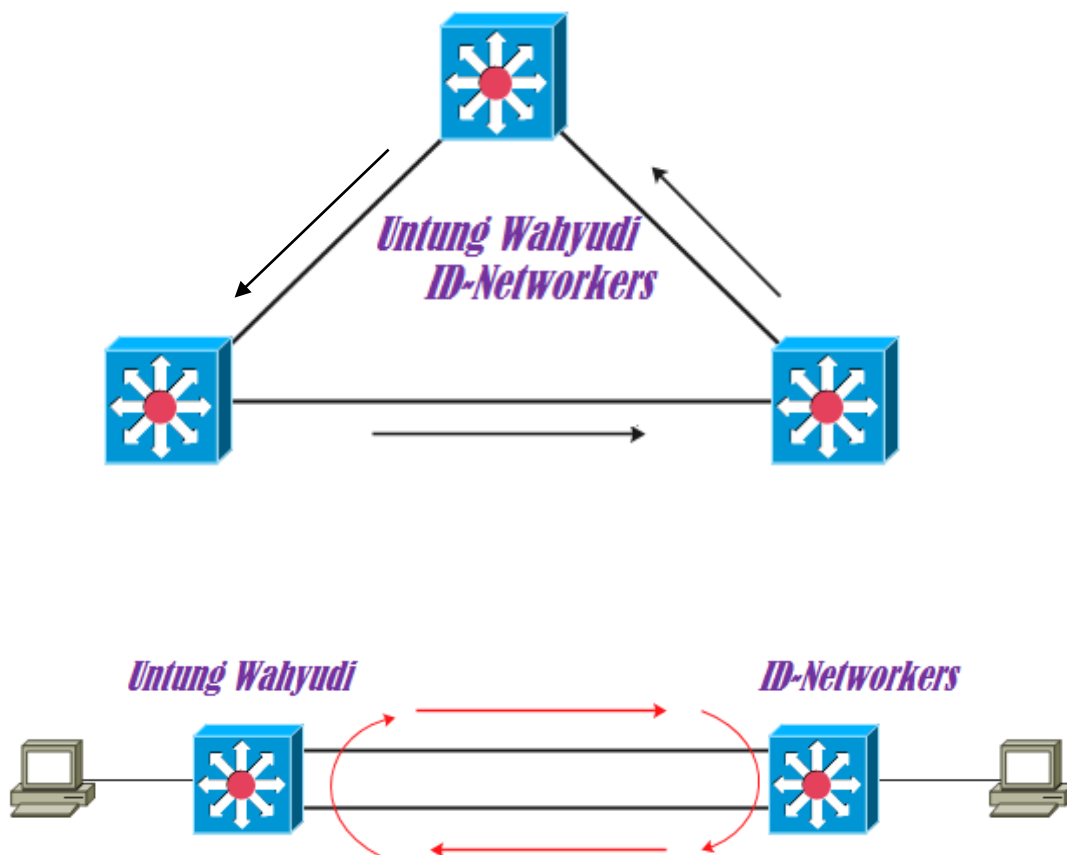
Semua port security udah saya bahas , sekarang kita beralih materi nih guys.

Sekian dulu yo.

Wassalam.

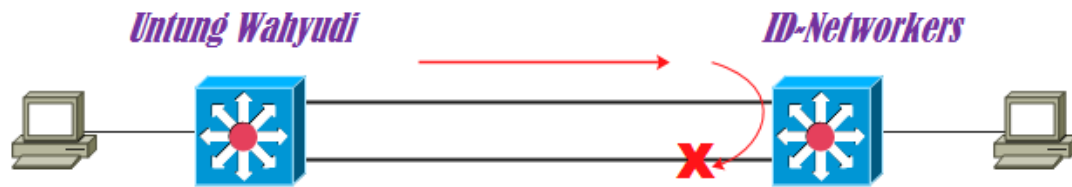
Spanning Tree Protocol

Untuk menghubungkan beberapa perangkat jaringan baik point to point maupun skala lebih luas , ada yang namanya Redudant Link , yaitu link cadangan / backup ketika link yang satu putus. Jadi demi keamanan dan kelancaran 2 device tersebut di hubungkan dengan 2 atau lebih link/kabel. Atau bahkan membuat 2 jalur untuk sampai ketujuan. Namun dengan adanya Redudant link tersebut maka Paket data yang dikirim hanya akan berputar-putar saja Bahasa kerennya itu “**Looping**”, karena device tidak tau harus dikirim kemana dan menggunakan link yang mana. Seperti berikut :



Untuk menghentikan looping tadi maka dibuatlah sebuah protocol yang bernama **Spanning Tree Protocol**. Cara kerja protocol ini adalah memblock salah satu port yang tidak digunakan, jadi hanya satu link saja yang digunakan. Namun ketika link

utama mati maka port yg tadi diblok akan dibuka sehingga , Link cadangan akan aktif.



Nah bab ini saya akan menjelaskan tentang Spanning Tree Protocol di Switch Cisco .
Sebenarnya untuk STP (Spanning Tree Protocol) sudah otomatis dijalankan ketika kita membuat redundant link. Jadi kita tidak perlu melakukan konfigurasi yang terlalu banyak.

Untuk lebih lanjutnya silahkan baca di lab lab berikutnya.

Lab 23. Spanning Tree Protocol

Di lab ini saya akan menjelaskan lebih dalam tentang STP di Cisco, seperti dibahas sebelumnya, secara default Switch di Cisco sudah menjalankan fitur STP ketika kita menggunakan Redundancy. Yang perlu diketahui tentang istilah-istilah yang ada di STP ini adalah :

- BPDU (Bridge Protocol Data Unit), berisi tentang Informasi Priority dan Mac-Address dari Switch itu sendiri.

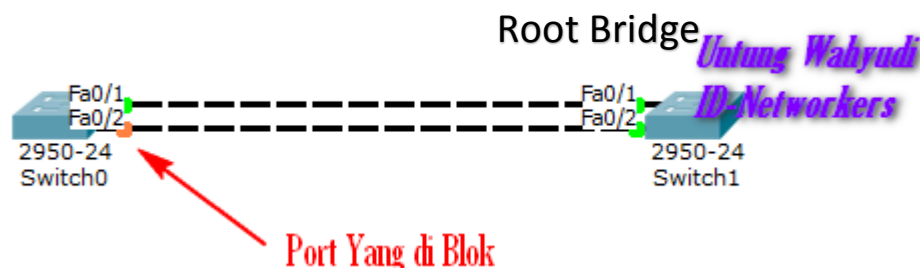
Jenis Switch yang berada di STP :

- Root Bridge : Yaitu switch yang terbaik diantara switch yg lain. Root bridge dipilih berdasarkan **Priority terendah** (default = 32768), jika priority nya sama maka akan dipilih berdasarkan **MAC-Address Terendah**. *Semua portnya adalah Designated Port*. Hanya ada 1 Root Bridge dalam 1 jaringan STP.
- Non-Root Bridge : Yaitu switch switch yang lain, selain Root Bridge.

Jenis Port yang ada di STP :

- Designated Port : Yaitu port yang terbaik, port yang memiliki Cost terbaik (priority terendah). Port ini digunakan untuk mem-forward paket data.
- Root Port : Yaitu port milik switch yang terhubung ke Root Bridge.
- Blocking Port : Yaitu Port yang akan diblok, dipilih berdasarkan priority dan MAC-Address Terbesar dari Switch itu.

Sekarang kita cek menggunakan Device Switch di Cisco Packet Tracer. Masukkan 2 Switch kemudian buat topologi seperti dibawah ini menggunakan 2 Link.



Dari gambar diatas bisa kita lihat bahwa Switch Cisco akan secara otomatis menjalankan fitur STP ketika kita membuat Link Redundancy. Di Lab ini saya hanya

akan memberitahukan cara mengecek nya saja. Untuk pengecekan lebih lanjut kalian dapat gunakan perintah berikut.

PENGECEKAN DI SWITCH - 1 :

```
SW-1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority      32769
                Address      0060.47C3.CD33
                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      0090.2BBB.7EDD
  Hello Time   2 sec    Max Age 20 sec    Forward Delay 15
sec

                Aging Time   20

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

Bisa kita lihat diatas , bahwa Interface fao/2 di switch 1 lah yang mengalami Blocking. Dan Interface Fa0/1 lah yang menjadi Forward. Kemudian kita cek di Switch yang kedua.

```
SW-2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority      32769
                Address      0060.47C3.CD33
                This bridge is the root
  Hello Time   2 sec    Max Age 20 sec    Forward Delay 15
```



```

sec

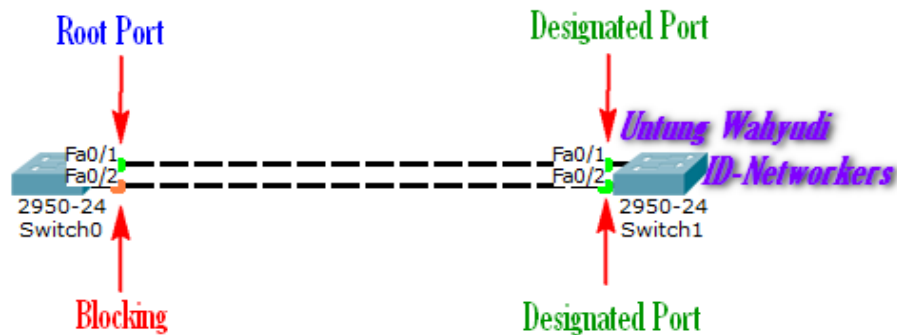
Bridge ID   Priority   32769   (priority 32768 sys-id-ext 1)
           Address   0060.47C3.CD33
           Hello Time 2 sec   Max Age 20 sec   Forward Delay 15
sec

           Aging Time 20

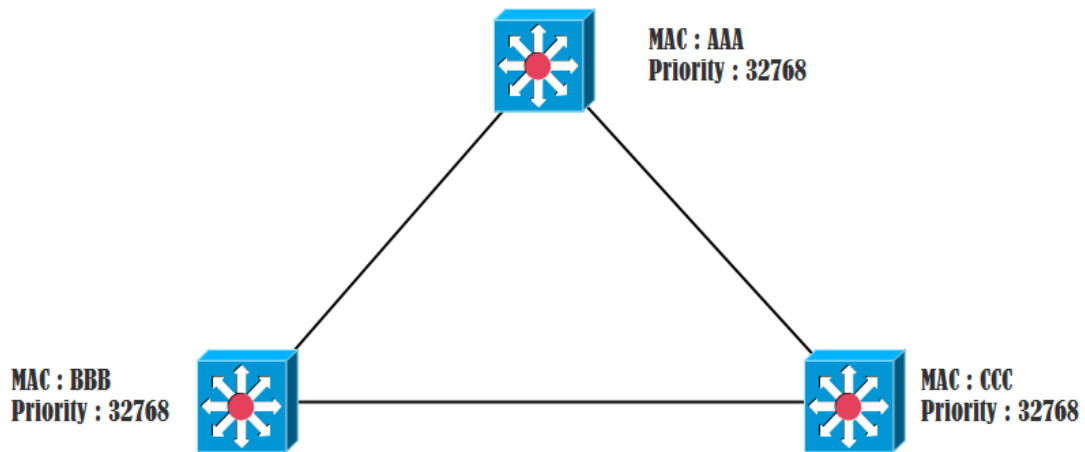
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

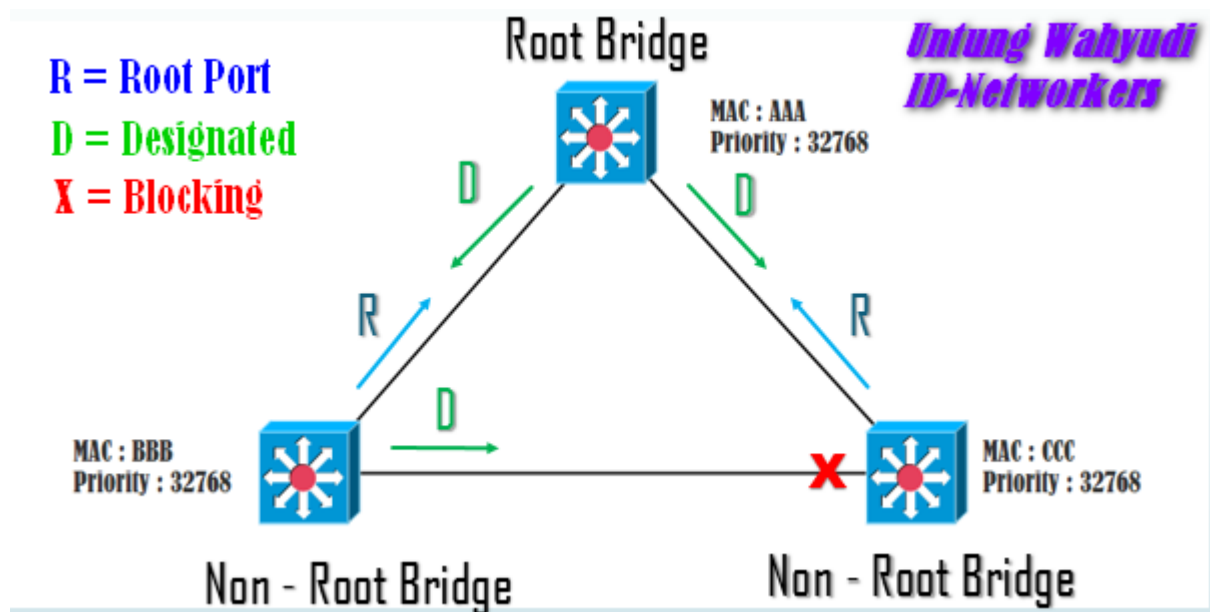
Kita bisa lihat perbedaan di Antara keduanya , di switch 2 akan ada kalimat *“This Bridge is Root”* yang artinya bahwa Switch ini lah menjadi Root Bridge. Karena memiliki MAC-Address yang ter-rendah. Dan semua Port nya berstatus Forward. Untuk lebih jelas mengenai jenis Port di setiap Interface maka gambar nya akan ane jelasin seperti dibawah ini.



Untuk lebih dalam mempelajari STP ini , silahkan kalian Simak gambar berikut. Dan coba selidiki dan tentukan Jenis switch dan Port nya, sesuai dengan Priority dan Mac-Address dari Switch tersebut.

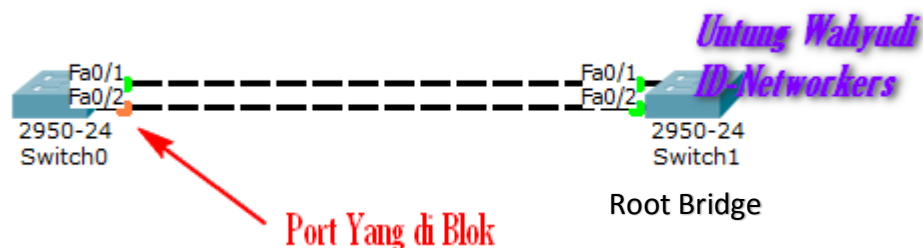


Kalo kalian udah mulai pusing dan bete , nyari jawabannya saya sebagai pengarang modul yang baik akan memberikan jawabannya secara free , hehehe. Kalian tinggal selidiki saja. Gambar dibawah sudah benar dalam penentuan Jenis Switch dan Port nya.



Lab 24. Mengganti Root Bridge pada STP

Setelah kalian sudah tau tentang penentuan Root Bridge dan Port yang di blok , sekarang kita lanjutkan cara merubah Switch Root Bridge nya. Seperti yang kita tahu bahwa Switch yang berstatus sebagai ROOT BRIDGE maka Semua PORTNYA FORWARD. Jadi dengan topologi yang sama kita akan ubah Root Bridge nya menjadi Switch yang sebelah kiri , sehingga port yang blocking akan berubah menjadi di switch yang kanan. Ini topologi sebelumnya



Untuk mengubah Root Bridge bisa menggunakan 2 cara yaitu Priority dan Bandwidth. Seperti yang kita tahu bahwa switch dengan priority terkecil akan menjadi Root Bridge. Maka dari itu kita akan mengubah priority di Switch 1 menjadi lebih kecil dari Switch yang sebelah kanan.

Untuk yang Priority bisa gunakan perintah berikut

```
SW-1(config)#spanning-tree vlan 1 priority 0
```

Yang perlu diingat bahwa priority hanya bisa menggunakan kelipatan 4096. Selain itu maka tidak bisa. Jika sudah selanjutnya kita cek lagi Spanning Tree nya , maka status Blok Port dan Root Bridge akan berpindah.

PADA SW-1 , akan berubah menjadi Root Bridge dan semua port nya akan menjadi Forward (Designated). Tambahan lagi , jika kita atur Priority nya maka secara otomatis dia kan bertambah 1, sebagai contoh tadi kita masukkan priority nya 0 maka ditambah 1 menjadi 1 (0+1=1)

```

SW-1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0090.2BBB.7EDD
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority    1 (priority 0 sys-id-ext 1)
             Address     0090.2BBB.7EDD
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

             Aging Time  20

Interface          Role Sts Cost          Prio.Nbr Type
-----
Fa0/1              Desg FWD 19           128.1    P2p
Fa0/2              Desg FWD 19           128.2    P2p

```

Kemudian pada SW-2 , tidak akan lagi menjadi Root Bridge , dan salah satu port nya akan ter-Blok. Silahkan bandingkan dengan 2 sintak sebelumnya Gaessss

```

SW-2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0090.2BBB.7EDD
             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     0060.47C3.CD33
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

```

```

Aging Time 20

```

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

Dan topologinya pun akan berubah seperti gambar dibawah ini , Port yang berwarna oranye berubah menjadi di sebelah kanan dan di **Interface Fa0/2**



Selanjutnya kita lakukan percobaan lagi , kita akan buat yang diblok pindah ke atas atau ke Interface Fa0/1. Caranya adalah dengan mengubah bandwidth dari Link tersebut. Semakin besar bandwidth nya maka semakin diutamakan link tersebut. Default nya adalah 100 Mbps. Jadi kita akan mengubah Speed Fa0/1 menjadi 10 Mbps agar port nya berubah keatas (Fa0/1). Berikut caranya

```

SW-2(config)#int fa0/1
SW-2(config-if)#speed 10 → 10 Mbps

```

Kemudian kita cek lagi , port yang diblok pasti akan berubah ke Fa0/1. Seperti berikut

```

SW-2#sho spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    1
              Address     0090.2BBB.7EDD
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

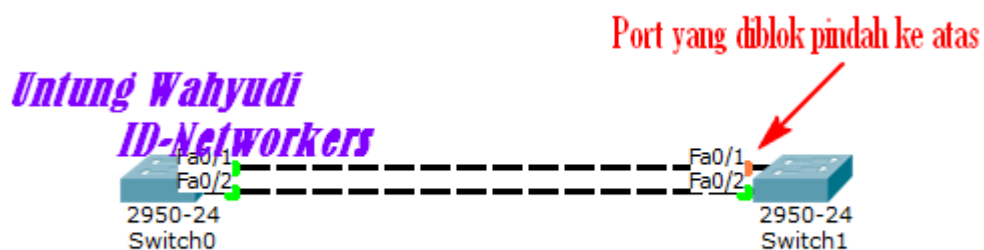
  Bridge ID    Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0060.47C3.CD33
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

              Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Altn BLK 100      128.1   P2p
Fa0/2          Root FWD 19       128.2   P2p

```

Topologinya juga pasti berubah dong port yang warnanya oranye akan menjadi diatas atau di Fa0/1.



Oke kita sudahi dulu tentang Spanning Tree Protocol di Cisco yoo, Kita lanjut ke materi yang lain. Wassalamualaikum.

Etherchannel

Etherchannel ini digunakan untuk menghubungkan atau membundle beberapa link seolah olah menjadi 1 link. Teknik ini berbeda dengan Spanning tree yang akan memblok beberapa link , dan hanya menggunakan 1 link. Kalau menggunakan Etherchannel maka semua link akan menjadi aktif , dan semuanya akan digunakan untuk mengirim paket. Dengan metode ini maka proses pengiriman paket data akan lebih cepat , semisal kita gunakan 3 link maka kecepatannya akan menjadi 3x lipat, apabila kita menggunakan 5 link maka kecepatannya akan mejadi 5x lipat. Jika salah satu link mati maka kecepatannya akan menjadi 4x lipat. Begitu seterusnya. Maksimal link yang dapat di gabungkan adalah **8 Link**.

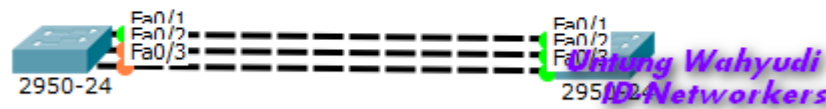
Ada 3 Jenis Etherchannel yang dapat kita konfigurasi :

- PaGP (Port Aggregation Protocol) : Cisco Proprietary , artinya hanya bisa dikonfigurasi di perangkat Cisco saja.
- LaCP (Link Aggregation Control Protocol) : Jenis ini bisa digunakan untuk semua perangkat , istilahnya itu **Open Standar**
- Layer 3 Etherchannel : Dikonfigurasikan di Switch layer 3

Ketiga jenis itu akan kita konfigurasi kan di lab lab kedepannya.

Lab 25. Etherchannel LaCP

Untuk lab pertama Etherchannel ini saya buka dengan jenis LaCP ini , seperti yang dibahas sebelumnya bahwa LaCP ini bisa digunakan oleh perangkat lain , jadi tidak hanya perangkat Cisco saja yang menggunakan. Untuk Lab nya langsung saja buat topologi seperti dibawah ini.



Kemudian kita konfigurasi PaCP di semua interface Switch diatas. Untuk Mode LACP kita gunakan mode perintah “**active**”

```
SW-1(config)#int range fa0/1-3
SW-1(config-if-range)# channel-group 1 mode active
```

```
SW-2(config)#int range fa0/1-3
SW-2(config-if-range)# channel-group 1 mode active
```

Setelah kita konfigurasi seperti diatas , maka akan muncul 1 interface baru , yaitu interface **Port-Channel 1**. Selanjutnya kita konfigurasi interface port-channel nya menjadi mode Trunk. Kita juga bisa langsung konfigurasi trunk di interface Fa0/1-3.

```
SW-1(config)#int port-channel 1
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#exit
```

```
SW-2(config)#int port-channel 1
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#exit
```


Kemudian silahkan cek port-channelnya maka setiap interfacenya akan berubah menjadi type active , dan protocolnya akan menjadi LACP

```
SW-1#show etherchannel port-channel
Channel-group listing:
-----

Group: 1
-----
Port-channels in the group:
-----

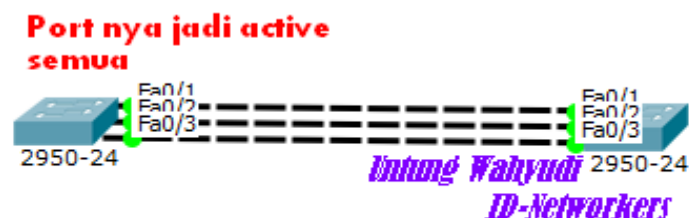
Port-channel: Po1
-----

Age of the Port-channel = 00d:00h:11m:43s
Logical slot/port = 2/1 Number of ports = 3
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel
Protocol = PAGP
Port Security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits
-----+-----+-----+-----+-----+-----
0 00 Fa0/3 Active 0
0 00 Fa0/2 Active 0
0 00 Fa0/1 Active 0
Time since last port bundled: 00d:00h:02m:44s Fa0/1
SW-1#
```

Setelah beberapa lama , maka lampu indikator di switch akan berubah menjadi hijau semua



Lab 26. Etherchannel PaCP

Selanjutnya kita ganti mode nya menjadi PaCP , untuk lab nya kita harus buat dari awal lagi . Tapi kita tetap menggunakan topologi yang sama seperti sebelumnya. Sekarang kita masuk lab nya saja.

Konfigurasikan etherchannel PaCP di semua interface Switchnya, untuk tipe PaCP kita gunakan mode “**desirable**”.

```
SW-1(config)#int range fa0/1-3
SW-1(config-if-range)# channel-group 1 mode desirable
SW-1(config-if-range)#exit

SW-1(config)#int port-channel 1
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#exit
```

Lakukan juga untuk Switch 2.

```
SW-2(config)#int range fa0/1-3
SW-2(config-if-range)# channel-group 1 mode desirable
SW-2(config-if-range)#exit

SW-2(config)#int port-channel 1
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#exit
```

Selanjutnya kita cek port-channel nya , maka jenisnya akan menjadi desirable, seperti berikut

```
SW-1#show etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----

Port-channel: Po1
-----

Age of the Port-channel = 00d:00h:03m:34s
Logical slot/port = 2/1 Number of ports = 3
GC = 0x00000000 HotStandBy port = null
```

```

Port state = Port-channel
Protocol = PAGP → PROTOCOL NYA MENJADI PAGP
Port Security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits
-----+-----+-----+-----+-----
0 00 Fa0/1 Desirable-S1 0
0 00 Fa0/2 Desirable-S1 0
0 00 Fa0/3 Desirable-S1 0
Time since last port bundled: 00d:00h:02m:25s Fa0/3
SW-1#

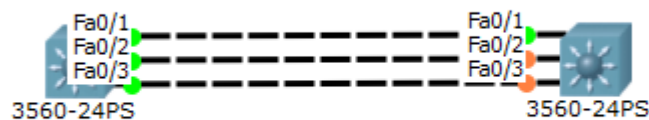
```

Dan portnya akan berubah menjadi hijau semua , sama seperti sebelumnya



Lab 27. Layer 3 Etherchannel

Sesuai namanya untuk layer 3 etherchannel ini kita konfigurasi di Switch Layer 3. Untuk konfigurasi mungkin sedikit berbeda, karena kita harus mematikan switchportnya, daripada bingung langsung aja ke konfigurasi. Untuk topologinya masih sama, namun kita ubah switchnya menjadi switch layer 3



Selanjutnya kita konfigurasi etherchannelnya, untuk mode L3 ini kita gunakan mode **“on”**, dan matikan switchport di setiap interfacenya.

```
SW-1(config)#int range fa0/1-3
SW-1(config-if-range)#no switchport
SW-1(config-if-range)#channel-group 1 mode on
SW-1(config-if-range)#exit
```

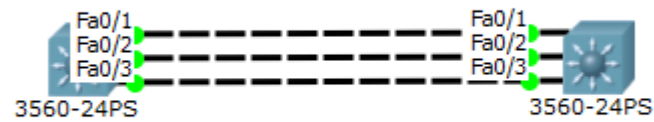
```
SW-2(config)#int range fa0/1-3
SW-2(config-if-range)#no switchport
SW-2(config-if-range)#channel-group 1 mode on
SW-2(config-if-range)#exit
```

Setelah itu kita setting IP untuk interface port-channelnya. Setting ip menjadi 1 network antara Sw1 dan Sw2.

```
## UNTUK SWITCH PERTAMA ##
SW-1(config)#int port-channel 1
SW-1(config-if)#ip address 10.10.10.1 255.255.255.0

## UNTUK SWITCH KEDUA ##
SW-2(config)#int port-channel 1
SW-2(config-if)#ip address 10.10.10.2 255.255.255.0
```

Kemudian cek lampu indikatornya ,pastikan semuanya berwarna hijau dan silahkan test ping antar switch.



```
SW-1#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 =
0/0/1 ms

SW-1#
```

Oke karena sudah berhasil maka saya tutup lab etherchannel kali ini yoo

Kita langsung masuk ke Bab yang lain.

Materi 3. Lab Router

Alhamdulillah sekarang kita sudah masuk ke Materi/BAB ke 3 yaitu tentang Router. Di Bab ini akan banyak dibahas mengenai Routing , baik Static maupun Dynamic. Selain Routing di BAB ini juga akan dibahas tentang jaringan WAN di Cisco. Adapun materi dari BAB 3 ini meliputi :

1. Static Routing
2. RIP
3. EIGRP
4. OSPF
5. OSPFv3
6. EIGRP IPv6
7. Access List Standard and Extended
8. NAT Static , Dynamic dan Dynamic with Overload
9. HSRP
10. VRRP
11. GLBP
12. HDLC
13. PPP

PANDUAN DALAM BAB INI :

Ada tambahan panduan di bab ini , yaitu dalam pengalamatan IP. Saya akan membuatnya menjadi lebih mudah , yakni jika ada 2 router yang terhubung maka IP nya akan sesuai dengan nomer dari 2 router tsb. Sebagai contoh R1 terhubung ke R2 maka IP nya adalah **12.12.12.1**(R1) dan **12.12.12.2**(R2). Kemudian jika R2 terhubung ke R3 maka IPnya **23.23.23.2**(R2) dan **23.23.23.3**(R3). Jika R3 dengan R4 maka **34.34.34.3** dan **34.34.34.4** begitu seterusnya okee. Ini digunakan agar lebih mudah dalam pengalamatan dan Tshoot nantinya.

Lab 28. Routing Static

Assalamualaikum wr.wb

Sebagai pembukaan di Lab Routing ini saya akan mulai dengan sebuah lab yang berjudul Routing Static. Sebelum memulai lab ada baiknya kita kenalan dulu sama yang namanya Routing, tapi saya tidak akan memperdalam pengertiannya karena modul ini adalah modul Practice. Jadi Routing adalah sebuah proses yang digunakan untuk menghubungkan PC atau host yang berbeda network, alat yang biasa digunakan adalah Router dan Switch layer 3.

Kemudian apa itu Routing Static ??, Routing Static adalah routing yang pemilihan jalur untuk sampai ke tujuan ditentukan secara manual oleh Administrator Jaringan. Jadi nantinya sang admin lah yang memasukan network tujuan dan jalur yang akan dilewatkan oleh paket. Untuk konfigurasi nya pakai saja panduan dari kalimat berikut:

“Mau kemana ?? Dan Lewat mana ??”

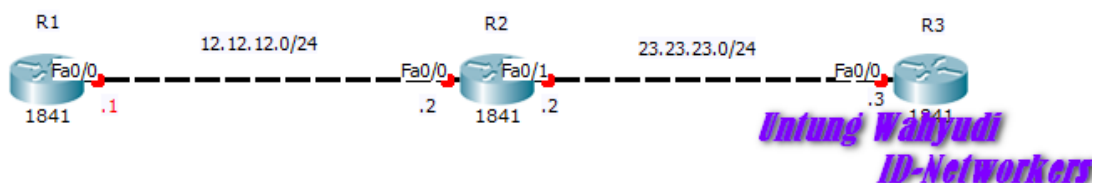
Untuk Routing Static di Cisco kita bisa gunakan sintak berikut

```
Router(config)# ip route X.X.X.X ( Network Tujuan) Y.Y.Y.Y ( Subnet Mask) A.B.C.D ( Gateway )
```

Sebagai Contoh :

```
Router(config)# ip route 192.168.1.0 255.255.255.0 12.12.12.2
```

Untuk lab nya buat topologi dengan 3 router seperti ini. Dan Goal nya adalah semua Router dapat saling ping menggunakan Routing Static.



Yang pertama harus dilakukan adalah atur IP di setiap interface yang ada di Router, seperti diawal BAB ini sudah saya jelaskan tentang pengalamatan IP yang akan saya gunakan.

Untuk R1 :

```
R1(config)#int fa0/0
R1(config-if)#ip address 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Untuk R2 :

```
## Untuk Interface ke R1 ##
R2(config)#int fa0/0
R2(config-if)#ip addr 12.12.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ex

## Untuk Interface ke R3 ##
R2(config)#int fa0/1
R2(config-if)#ip addr 23.23.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ex
```

Untuk R3 :

```
R3(config)#int fa0/0
R3(config-if)#ip addr 23.23.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#ex
```

Jika sudah silahkan test ping antar router , pasti yang bisa ping hanya R1 ke R2 , atau R2 ke R3. Sedangkan R1 tidak bisa ping ke R3. Karena kedua Router tersebut tidak

terhubung secara langsung. Untuk itu diperlukan yang namanya Routing. Sekarang kita konfigurasi Routing Static nya sesuai dengan Perintah sebelumnya.

Daftarkan Network Tujuan 23.23.23.0 (R3):

```
R1(config)#ip route 23.23.23.0 255.255.255.0 12.12.12.2
```

Keterangan :

23.23.23.0 255.255.255.0 = IP Network Tujuan (23.23.23.0/24)

12.12.12.2 = Gateway yang digunakan untuk sampai Tujuan

Untuk di R2 tidak perlu di konfigurasi Static Routing, karena dia sudah terhubung langsung dengan R1 dan R3. Jadi dia secara otomatis dapat ping ke 2 Router tsb.

Daftarkan Network Tujuan 12.12.12.0 (R1) :

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

Kemudian silahkan test ping dari Router 2 ke Router 3.

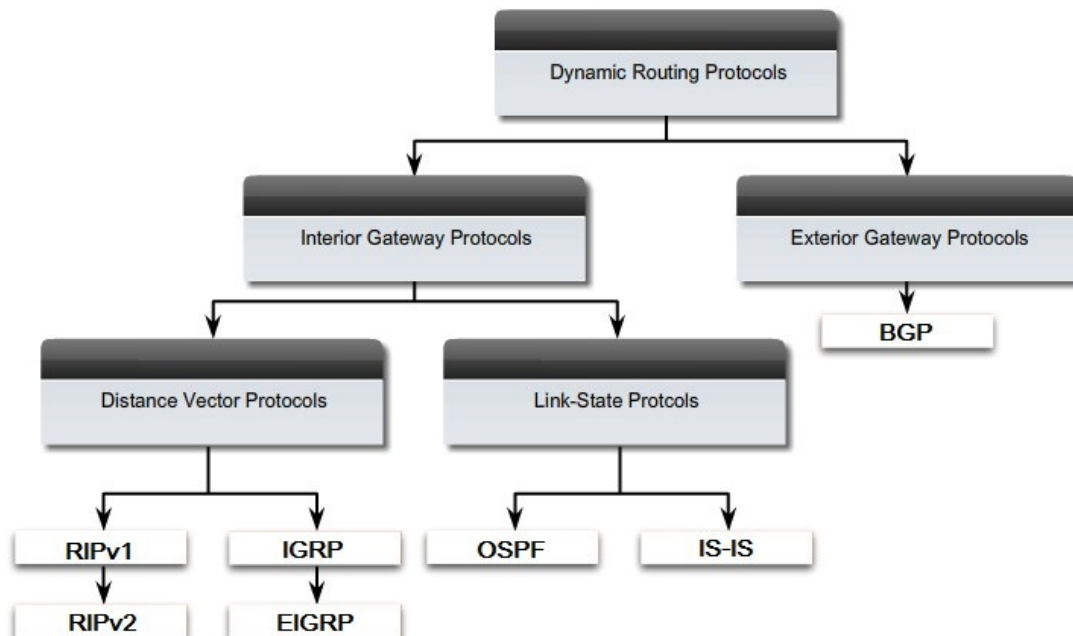
```
R1#ping 23.23.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/0 ms
R1#
```

Karena hasilnya sudah berhasil maka kita tutup Lab Static Routing kali ini.

Wassalam !

DYNAMIC ROUTING

Setelah dilab sebelumnya kita sudah bahas tentang Static Routing maka di lab ini sya akan bahas tentang Dynamic Routing. Apa bedanya ?? Jelas sangat berbeda , kalau Static Routing kita harus daftarkan Network tujuan beserta gatewaynya secara manual maka di Dynamic Routing ini kita hanya perlu mendaftarkan network masing – masing dan nantinya Router lah yang akan memilih/mencari jalur untuk sampai ketujuan. Untuk lebih jelas tentang jenis Routing Dynamic ini bisa liat gambar dibawah ini.



ROUTING DYNAMIC dibagi menjadi 2 :

IGP = Untuk melakukan routing dalam 1 AS atau satu kepemilikan

EGP = Untuk melakukan routing Antar AS

IGP Dibagi lagi menjadi 2 :

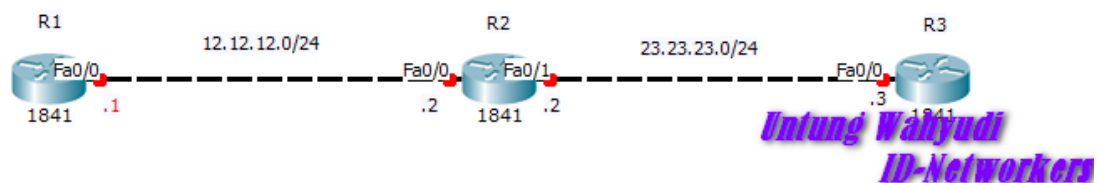
Distance Vector = Pemilihan Jalur berdasarkan Next Hop / jarak antar router

Link-State = Pemilihan jalur berdasarkan Kondisi Link.

Lab 29. Routing RIPv2

Sebagai pembuka di lab dynamic routing ini saya akan mulai dengan lab RIP (Routing Information Protocol). Sebenarnya Routing RIP ini sudah jarang digunakan karena dia pemilihan jalur berdasarkan jarak lompatan terdekat, dan tidak memperdulikan bandwidth, ditambah lagi maksimal next hop nya cuma 15 Next Hop. Tapi disini saya ingin menjelaskan saja bagaimana cara konfigurasi Routing RIP ini agar setidaknya kalian tau tentang RIP ini. Dan juga RIP versi 1 ini benar benar masih *Jaduil*, jadi dia hanya bisa merouting network yang memiliki Netmask yang sama, contoh /24 dengan /24 saja. Selain itu maka tidak bisa di routing. Maka dari itu disini saya menggunakan RIP Versi 2

Buat topologi 3 Router seperti ini



Selanjutnya konfigurasi IP seperti di lab sebelumnya.

R1 :

```
R1(config)#int fa0/0
R1(config-if)#ip address 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

R2 :

```
R2(config)#int fa0/0
R2(config-if)#ip addr 12.12.12.2 255.255.255.0
```

```
R2(config-if)#no shutdown
R2(config-if)#ex

R2(config)#int fa0/1
R2(config-if)#ip addr 23.23.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ex
```

R3 :

```
R3(config)#int fa0/0
R3(config-if)#ip addr 23.23.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#ex
```

Setelah selesai men-setting ip address pada interface Ethernet , kita juga harus setting IP di interface loopback , yang fungsinya seolah-olah jaringan local dari Router tsb. Tapi jika tidak ingin membuatnya juga tidak masalah , ini kan Cuma buat pengibaratan jaringan local nya , dan biasanya menggunakan IP dengan /32.

```
R1(config)#int loopback0
R1(config)#ip address 1.1.1.1 255.255.255.255
```

```
R2(config)#int loopback0
R2(config)#ip address 2.2.2.2 255.255.255.255
```

```
R3config)#int loopback0
R3(config)#ip address 3.3.3.3 255.255.255.255
```

Selanjutnya kita konfigurasi Routing RIP nya, tambahan nih kalo di Routing Dynamic itu kita hanya perlu memasukkan Network Router **masing-masing**. Nanti untuk routing nya biarlah si Router yang mengerusunya.

```
R1(config)#router rip
R1(config-router)#version 2           →Kita gunakan
ver.2
R1(config-router)#network 12.12.12.0  Daftarkan
networknya
R1(config-router)#network 1.1.1.1     Daftarkan
networknya
R1(config-router)#no auto-summary
R1(config-router)#exit
```

Daftarkan juga Network di Router 2 :

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 12.12.12.0
R2(config-router)#network 23.23.23.0
R2(config-router)#network 2.2.2.2
R2(config-router)#no auto-summary
R2(config-router)#exit
```

Jangan lupakan di Router 3 :

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 23.23.23.0
R3(config-router)#network 3.3.3.3
R3(config-router)#no auto-summary
R3(config-router)#exit
R3(config)#
```

Selanjutnya silahkan cek table Routing nya , maka akan muncul table routing yang dibuat oleh routing RIP , ditandai dengan huruf “**R**” di depannya.

```

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
R    2.2.2.2 [120/1] via 12.12.12.2, 00:00:23, FastEthernet0/0
    3.0.0.0/32 is subnetted, 1 subnets
R    3.3.3.3 [120/2] via 12.12.12.2, 00:00:23, FastEthernet0/0
    12.0.0.0/24 is subnetted, 1 subnets
C    12.12.12.0 is directly connected, FastEthernet0/0
    23.0.0.0/24 is subnetted, 1 subnets
R    23.23.23.0 [120/1] via 12.12.12.2, 00:00:23, FastEthernet0/0

```

Kemudian test ping antar client , kita bisa ping IP loopback nya ataupun IP interfacenya, tidak ada bedanya. Asal bisa reply artinya berhasil

```

R1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms

R1#

```

Jika sudah reply artinya berhasil.

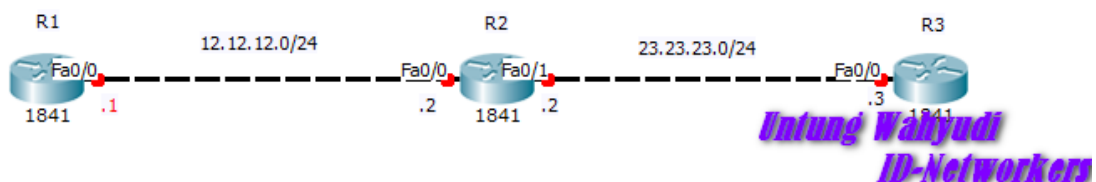
Saya tutup lab kali ini tentang RIP versi 2 , silahkan dipelajari lagi yaa

Wassalam.

Lab 30. Routing EIGRP (Enhanced Interior Gateway Routing Protocol)

Sekarang kit masuk lab EIGRP , jadi Routing EIGRP in adalah protocol Routing Cisco Proprietary , artinya hanya bisa dijalankan di Router Cisco saja. Kelebihan utama dari routing EIGRP ini adalah routing protocol satu satunya yang menyediakan fitur backup route , dimana jika terjadi perubahan pada network maka EIGRP tidak akan meng-kalkulasi ulang untuk pemilihan jalur routingnya , karena dia langsung menggunakan backup route ini.

Langsung aja ke lab nya , buat topologi seperti sebelumnya.



Kemudian setting IP di Interface dan loopback sama seperti sebelumnya

```
R1(config)#int fa0/0
R1(config-if)#ip address 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#int loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#exit
```

PADA ROUTER 2 :

```
R2(config)#int fa0/0
R2(config-if)#ip addr 12.12.12.2 255.255.255.0
R2(config-if)#no shutdown
```

```
R2(config-if)#ex

R2(config)#int fa0/1
R2(config-if)#ip addr 23.23.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ex

R2(config)#int loopback0
R2(config-if)#ip addr 2.2.2.2 255.255.255.255
R2(config-if)#ex
```

PADA ROUTER 3 :

```
R3(config)#int fa0/0
R3(config-if)#ip addr 23.23.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#ex

R3(config)#int loopback0
R3(config-if)#ip addr 3.3.3.3 255.255.255.255
R3(config-if)#ex
```

Sekarang kita konfigurasi EIGRP nya , sebenarnya konfigurasinya sama saja seperti RIP , hanya saja protocol yang digunakan kita rubah menjadi EIGRP. Dan kita buat EIGRP ID nya sama satu sama lain.

Pada R1 :

```
R1(config)#router eigrp 10 → EIGRP ID , harus sama
R1(config-router)#network 12.12.12.0
R1(config-router)#network 1.1.1.1
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#
```


Pada R2 :

```
R2(config)#router eigrp 10
R2(config-router)#network 12.12.12.0
R2(config-router)#network 23.23.23.0
R2(config-router)#network 2.2.2.2
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#
```

Pada R3 :

```
R3(config)#router eigrp 10
R3(config-router)#network 23.23.23.0
R3(config-router)#network 3.3.3.3
R3(config-router)#no auto-summary
R3(config-router)#exit
R3(config)#
```

Kemudian cek table routing nya , maka akan muncul tabel routing yang dibuat oleh EIGRP , yang ditandai dengan huruf “D”.

```
R1#show ip route

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       1.0.0.0/8 [90/158720] via 12.12.12.2, 00:02:55,
FastEthernet0/0
C       1.1.1.0/24 is directly connected, Loopback0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       2.0.0.0/8 [90/161280] via 12.12.12.2, 00:01:59,
FastEthernet0/0
D       2.2.2.2/32 [90/156160] via 12.12.12.2, 00:02:55,
FastEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
D       3.3.3.3 [90/158720] via 12.12.12.2, 00:01:59,
FastEthernet0/0
```

```
12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D      12.0.0.0/8 [90/35840] via 12.12.12.2, 00:01:59,
FastEthernet0/0
C      12.12.12.0/24 is directly connected, FastEthernet0/0
      23.0.0.0/24 is subnetted, 1 subnets
D      23.23.23.0 [90/30720] via 12.12.12.2, 00:02:55,
FastEthernet0/0
R1#
```

Kemudian test ping antar router.

```
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/1 ms

R1#
```

Oke karena sudah berhasil maka saya tutup lab kali ini oke.

Wassalam

Routing OSPF

Sekarang kita masuk ke Routing Dynamic yang lain yaitu tentang OSPF (Open Shortest Path First). OSPF merupakan Routing Dynamic yang menggunakan protocol Link State, artinya dia akan memilih jalur berdasarkan kondisi link. Jika kondisi link itu bagus dan bandwidth nya juga bagus maka link itu lah yang akan digunakan. Berikut fitur fitur lain dari OSPF :

- Membagi berdasarkan Area dan Autonomous System (AS).
- Meminimalkan Routing Update Traffic
- Scalability
- Support VLSM/CIDR
- Unlimited Hop Count
- Open Standar / Bisa digunakan banyak vendor

OSPF menggunakan algoritma Djikstra atau SPF (Shortest Path First) , yang mana algoritma ini memperbaiki informasi database dari informasi topologi , jadi OSPF ini akan mengetahui dengan pasti topologi yang kita buat, sehingga dalam pemilihan jalur akan lebih baik. Dalam penentuan jalur terbaik OSPF menggunakan “Cost” sebagai acuannya. Untuk rumus menghitung Cost ini adalah

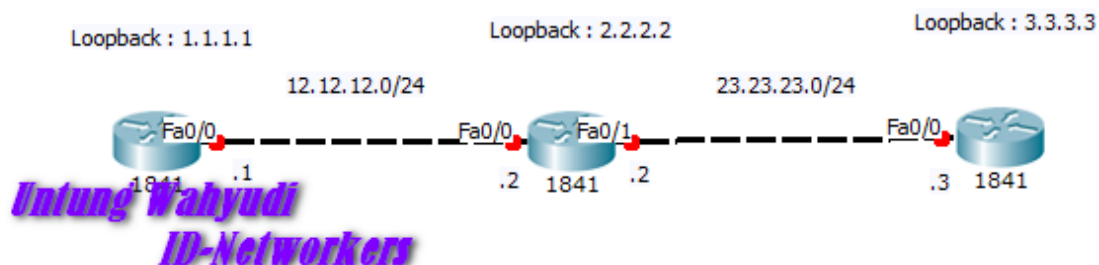
Reference bandwidth / bandiwidth , yang dikonfigurasi di interface router nya.

Lab 31. Routing OSPF Single Area

Sekarang kita masuk ke lab nya, seperti yang kita bahas sebelumnya bahwa OSPF akan membagi router-router berdasarkan Area – Area dan AS. Yang perlu diketahui tentang Area di OSPF adalah :

- Dalam membentuk Jaringan OSPF harus ada Area “0”
- Area 0 biasa disebut dengan Area Backbone
- Semua area harus terhubung dengan Area Backbone untuk dapat saling bertukar informasi antar area.
- Untuk menghubungkan area backbone dan area lain harus ada Router ABR yaitu router yang menjadi penengah (1 interfacenya terhubung ke area backbone dan interface lainnya terhubung ke area lain).

Setelah mengetahui hal diatas , sekarang kita akan membuat lab OSPF menggunakan 1 area saja. Tentu saja area tersebut adalah Area Backbone. Untuk lab nya buat topologi dengan 3 Router seperti sebelumnya.



Selanjutnya kita setting IP di setiap Router sama seperti di lab sebelumnya. **Untuk setting IP Interface dan Loopback tidak saya jelaskan lagi yaa.** Kalian juga udah pasti bisa kan , tinggal ikutin aja langkah di lab sebelumnya.

Kita langsung aja ke lab konfigurasi nya,

```
R1(config)#router ospf 10 → OSPF ID
R1(config-router)#network 12.12.12.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#exit
```

Keterangan :

Yang saya beri tanda merah itu namanya Wildcard , yang digunakan untuk mencocokkan IP nya. Angka itu didapat dari rumus :

255.255.255.255 - Netmask yang digunakan.

Jadi karena kita pakai netmask 255.255.255.0 (IP Interface) dan 255.255.255.255 (IP Loopback) maka

255.255.255.255 - 255.255.255.0 = 0.0.0.255 Network interface

255.255.255.255 - 255.255.255.255 = 0.0.0.0 Network Loopback.

Oke sekarang lanjut , kita konfigurasi OSPF di Router selanjutnya , karena kita menggunakan 1 Area saja , maka semua interface di router kita masukkan ke Area 0

```
R2(config)#router ospf 10
R2(config-router)#network 12.12.12.0 0.0.0.255 area 0
R2(config-router)#network 23.23.23.0 0.0.0.255 area 0
R2(config-router)#network 2.2.2.2 0.0.0.0 area 0
R2(config-router)#exit
```

```
R3(config)#router ospf 10
R3(config-router)#network 23.23.23.0 0.0.0.255 area 0
R3(config-router)#network 3.3.3.3 0.0.0.0 area 0
R3(config-router)#exit
R3(config)#
```

Selanjutnya kita cek tabel routing nya , maka akan muncul informasi Routing OSPF , yang di depannya ditandai huruf "O".

```
R1#show ip route

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 12.12.12.2, 00:02:42, FastEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
```

```
○      3.3.3.3 [110/3] via 12.12.12.2, 00:01:08, FastEthernet0/0
      12.0.0.0/24 is subnetted, 1 subnets
C      12.12.12.0 is directly connected, FastEthernet0/0
      23.0.0.0/24 is subnetted, 1 subnets
○      23.23.23.0 [110/2] via 12.12.12.2, 00:01:08,
FastEthernet0/0
R1#
```

Kemudian silahkan test ping antar router ,

```
R1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/0 ms

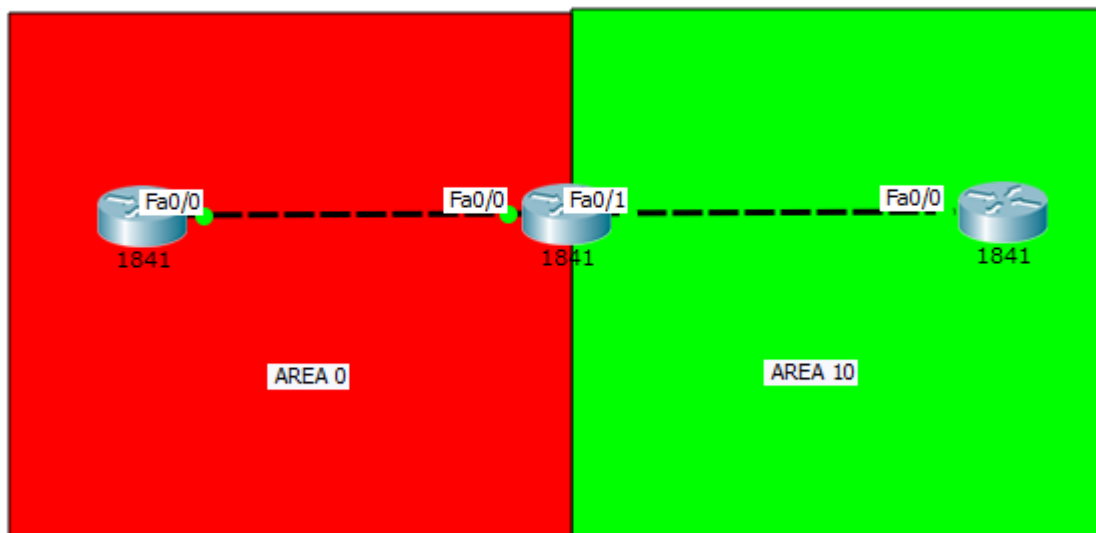
R1#
```

Karena sudah berhasil maka artinya sudah berhasil Gaess.

Sekian dulu ya !

Lab 32. Routing OSPF Multi Area

Karena dilab sebelumnya kita sudah konfigurasi OSPF dalam 1 area , sekarang kita akan membuatnya menjadi 2 area. Yaitu area 0 dan area 10. Untuk penomoran area kita bisa gunakan angka sesuka kita , namun untuk area backbone tidak bisa kita ubah. Oke langsung saja kita lanjutkan lab sebelumnya yaa, Topologi nya akan berubah secara logical menjadi seperti ini :



Pertama hapus dulu konfigurasi OSPF di lab sebelumnya. Gunakan perintah ini untuk semua router.

```
R1(config)#no router ospf 10
R2(config)#no router ospf 10
R3(config)#no router ospf 10
```

Selanjutnya kita buat lagi konfigurasi OSPF nya, kita akan masukkan interface setiap router kedalam area nya masing-masing , sesuai dengan topologi diatas.

```
R1(config)#router ospf 90
R1(config-router)#network 12.12.12.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#exit
R1(config)#
```

```
R2(config)#router ospf 90
R2(config-router)#network 12.12.12.0 0.0.0.255 area 0
R2(config-router)#network 23.23.23.0 0.0.0.0 area 10
R2(config-router)#network 2.2.2.2 0.0.0.0 area 10
R2(config-router)#exit
R2(config)#
```

```
R3(config)#router ospf 90
R3(config-router)#network 23.23.23.0 0.0.0.255 area 10
R3(config-router)#network 3.3.3.3 0.0.0.0 area 10
R3(config-router)#exit
R3(config)#
```

Selanjutnya silahkan cek tabel routing , dan pastikan sudah muncul tabel routingnya seperti sebelumnya. Kemudian test ping antar router

```
Router#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/0 ms

Router#
```


ACCESS LIST

Access List digunakan untuk mem-filter paket yang akan masuk maupun keluar dari Router. Dimana ada paket ingin masuk/keluar maka akan diproses terlebih dahulu di Access List ini. Maka jika ada paket yang tidak sesuai kriteria maka akan di drop , sesuai dengan kebijakan yang kita buat.

Yang perlu diketahui tentang Access List ini adalah :

Metode dalam penerapan ACL :

- Inbound access-list : Paket akan difilter ketika masuk.
- Outbound access-list : Paket akan difilter ketika ingin keluar.

ACL dibagi menjadi 2 Jenis :

- Standard Access List : Melakukan filtering berdasarkan IP Host atau network Source nya saja. Standar ACL menggunakan nomer ACL 1 – 99.
- Extended Access List : Penerapan Filteringnya lebih spesifik, bisa melakukan filtering berdasarkan destination , protocol dan port yang digunakan. Extended ACL menggunakan Nomer ACL 100 – 199 .

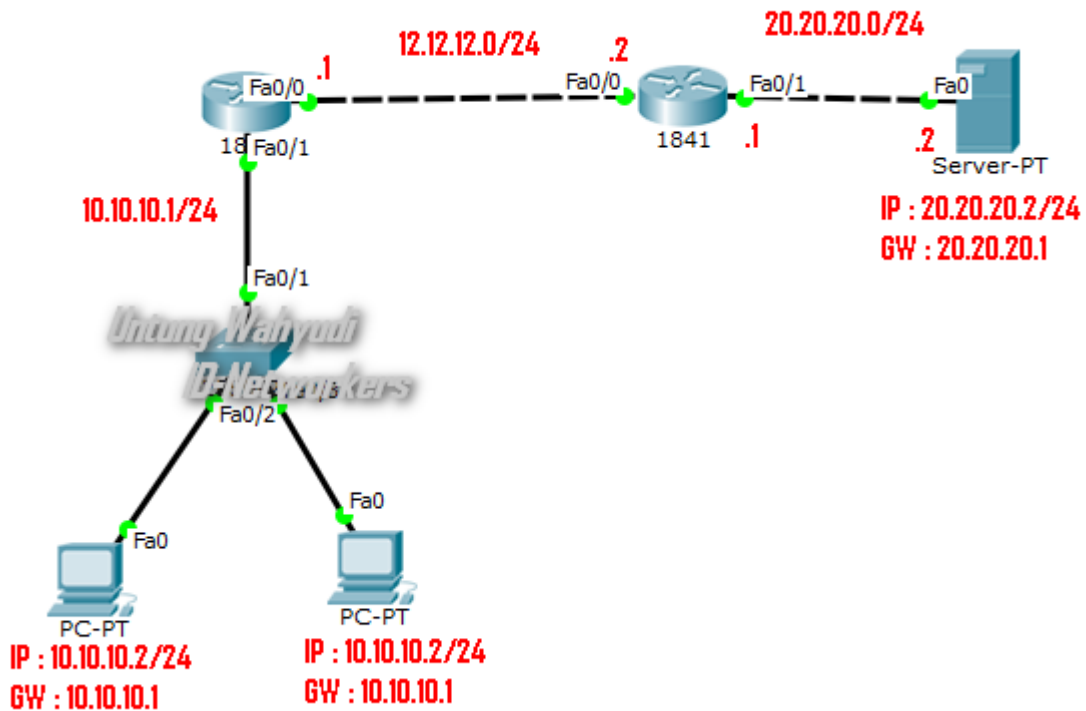
Terdapat 3 Opsi dalam penerapan ACL :

- Permit : Mengizinkan
- Deny : Menolak
- Remark : Memberikan komentar

Lab 33. Standard Access List

Sekarang kita masuk lab konfigurasi Standard Access List. Untuk konfigurasi Standard Access List ini kita harus membuat rule nya di **Interface TERDEKAT** **dengan TUJUAN**

Untuk lab nya silahkan buat topologi seperti dibawah ini :



Silahkan kalian konfigurasi IP nya sesuai dengan topologi diatas. Karena saya tidak akan mengkonfigurasinya dari awal. Setelah mengkonfigurasi IP seperti diatas selanjutnya konfigurasi Default Route di setiap routernya.

```
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 12.12.12.1
```

Jika sudah silahkan ping dari PC ke Server , dan pastikan akan berhasil karena sudah di routing.

```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms 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 = 1ms, Average = 0ms
```

Jika sudah berhasil , sekarang kita akan men-filter traffic yang akan masuk ke Server dengan menggunakan Standard Access List. Kita akan buat rule nya agar PC **10.10.10.2 TIDAK dapat mengakses web server**. Untuk topologi diatas berarti kita akan konfigurasi kan di **Interface Fa0/1 Router 2**. Kita gunakan 2 rule , rule yang pertama untuk menolak IP 10.10.10.2 , dan rule kedua akan membolehkan semua traffic.

```
R2(config)#access-list 1 deny 10.10.10.2 0.0.0.0
R2(config)#access-list 1 permit any
R2(config)#int fa0/1
R2(config-if)#ip access-group 1 out
```

Keterangan :

- Untuk men-deny 1 host saja , wild card nya gunakan /32 , artinya wildcardnya menjadi 0.0.0.0. Sedangkan untuk mendeny 1 network , bisa gunakan netmask sesuai dengan netmask IP nya.
- Di bagian Fa0/1 kita konfigurasi Out. Karena interface itu yang terdekat dengan web server.

Untuk verifikasi nya , silahkan ping dari PC 10.10.10.2 (PC 1) maka tidak akan berhasil , karena paketnya di drop.

```
PC>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),
PC>
```

Kemudian silahkan test ping dari PC 2 (10.10.10.3) maka hasilnya akan berhasil , karena IP 10.10.10.3 tidak terkena Access List.

```
PC>ping 20.20.20.2
Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=9ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms 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 = 9ms, Average = 2ms
PC>
```

Kita juga bisa memblokir menggunakan Networknya , jadi kita ingin semua IP 10.10.10.0/24 tidak bisa ping ke web server. Tinggal buat access list nya ,
NOTE : “*Jika kita membuat access List baru , maka access list yang lama akan terhapus*” Jadi tidak masalah kalo nomer access listnya kita ganti asal nomernya 1-99 ini kan masih Standard access list.

```
R2(config)#access-list 10 deny 10.10.10.0 0.0.0.255
R2(config)#access-list 10 permit any
R2(config)# int fa0/1
R2(config-if)#ip access-group 10 out
```

Untuk verifikasi nya silahkan test ping dari kedua client maka hasilnya akan gagal, seperti ini

```
PC>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),

PC>
```

Kita juga bisa cek ACL nya , untuk melihat berapa banyak paket yang di drop dan di permit.

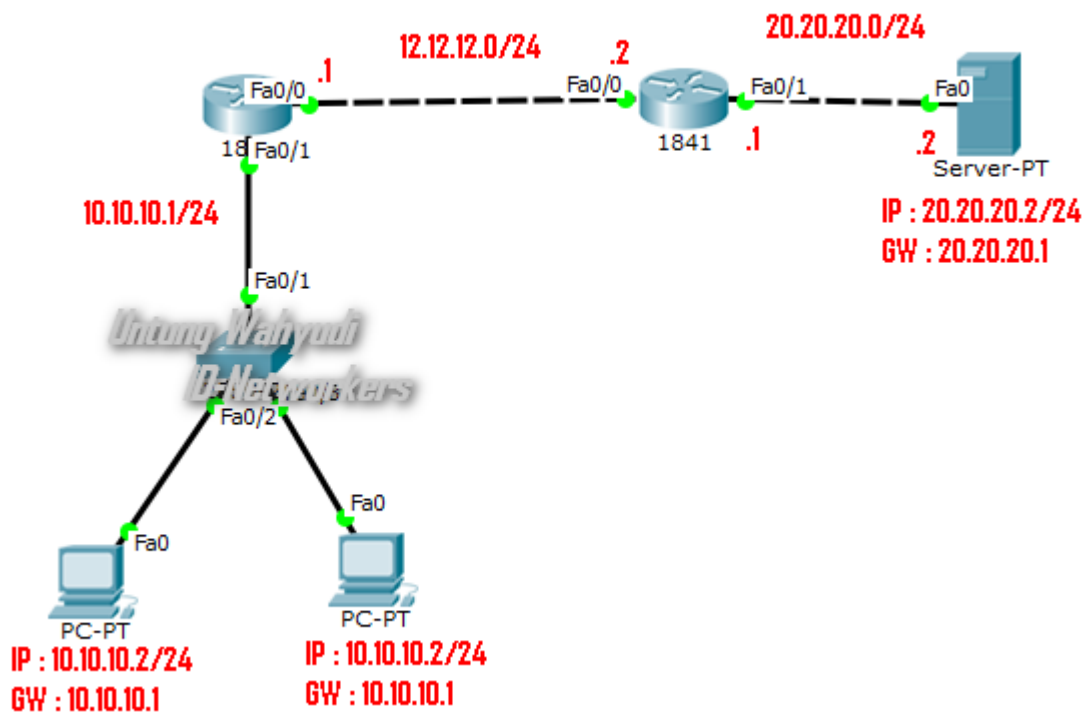
```
R2#show access-lists 10
Standard IP access list 10
deny 10.10.10.0 0.0.0.255 (4 match(es))
permit any
R2#
```

Bisa dilihat ada 4 paket yang di drop , dan belum ada paket yang di ijin masuk.

Untuk manajemen traffic nya bisa kalian atur sesuai kebutuhan dan keinginan kalian , silahkan kembangkan lagi.

Lab 34. Extended Access List

Selanjutnya kita masuk ke bagian Extended nya , dengan extended ini kita bisa menfilter paket lebih spesifik , baik dari port , protocol dan destinationnya. Kalau standard hanya bisa mentraffic berdasarkan source saja. Extended ini menggunakan nomer ACL 100 – 199. Kita masih melanjutkan lab sebelumnya jadi , topologi nya masih sama.



Pertama kita hapus dulu konfigurasi ACL di lab sebelumnya.

```
R2(config)#no access-list 1
R2(config)#no access-list 10
R2(config)#int fa0/1
R2(config-if)#no ip access-group 10 out
R2(config-if)#exi
```

Untuk kasus di lab ini , kita akan buat IP 10.10.10.2 tidak dapat mengakses web server, tetapi dia masih bisa melakukan Ping. Jadi kita akan drop **www** nya.

Langsung aja kita buat rule access list seperti dibawah ini , ingat nomer ACL nya harus antara 100-199.

Konfigurasi di Interface yang TERDEKAT dengan SOURCE , karena dari topologi diatas yang terdekat adalah Interface Fa0/1 dari Router 1

```
R1(config)#access-list 100 deny tcp 10.10.10.2 0.0.0.0 host
20.20.20.2 eq 80
R1(config)#access-list 100 permit ip any any
```

Keterangan :

- TCP : artinya kita akan memblok protocol TCP
- 10.10.10.2 0.0.0.0 : IP Source
- Host : Kita akan memblok tujuan yg memiliki 1 IP address
- 20.20.20.2 : IP Destination
- Eq : Kita akan blok berdasarkan port
- 80 : Nomer port nya (HTTP) atau bisa kita ubah menjadi www.

Selanjutnya pasang ACL nya di interface terdekat dengan source , dan modenya kita buat IN , jadi kita akan memfilter paket yang akan masuk ke R1.

```
R1(config)#int fa0/1
R1(config-if)#ip access-group 100 in
R1(config-if)#
```

Untuk verifikasi silahkan test ping dari client , pasti akan berhasil baik PC 1 maupun PC 2.

```
PC>ping 20.20.20.2

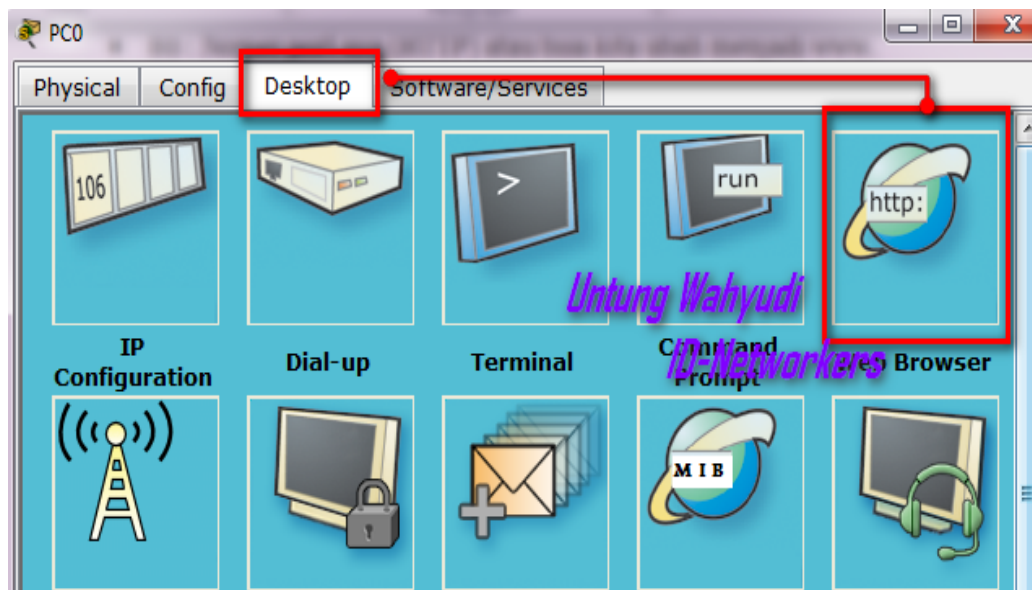
Pinging 20.20.20.2 with 32 bytes of data:

Reply from 20.20.20.2: bytes=32 time=1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=1ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126

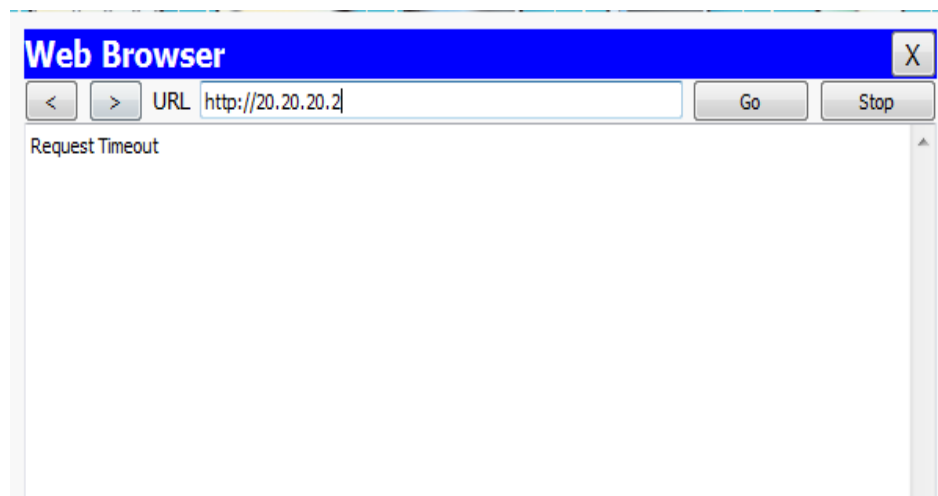
Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

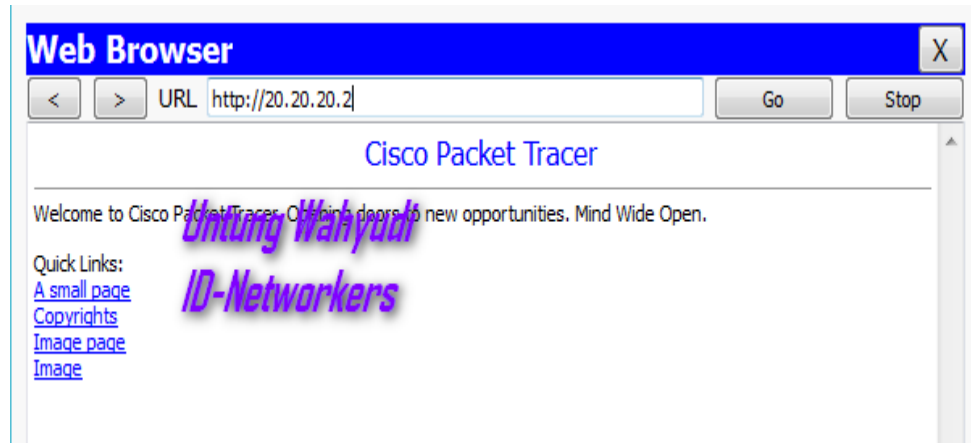
Selanjutnya silahkan test akses web servernya dari PC 1 (10.10.10.2). Caranya adalah dengan ke menu Config kemudian klik Web Browser seperti gambar dibawah ini.



Selanjutnya ketikkan IP Server di bagian search , maka hasilnya akan gagal.



Kemudian test lagi akses web servernya menggunakan PC 2 , dan pastikan hasilnya akan berhasil seperti gambar dibawah ini.



Silahkan cek ACL nya untuk melihat jumlah paket yang di deny dan di permit.

```
R1#show access-lists 100
Extended IP access list 100
deny tcp host 10.10.10.2 host 20.20.20.2 eq www (12 match(es))
permit ip any any (14 match(es))
R1#
```

Maka akan terlihat ada 12 paket yang di drop dan ada 14 paket yang di permit , jumlah ini pasti akan selalu berbeda setiap kita lab , tergantung banyaknya paket yang kita kirim.

NAT

Network Address Translation

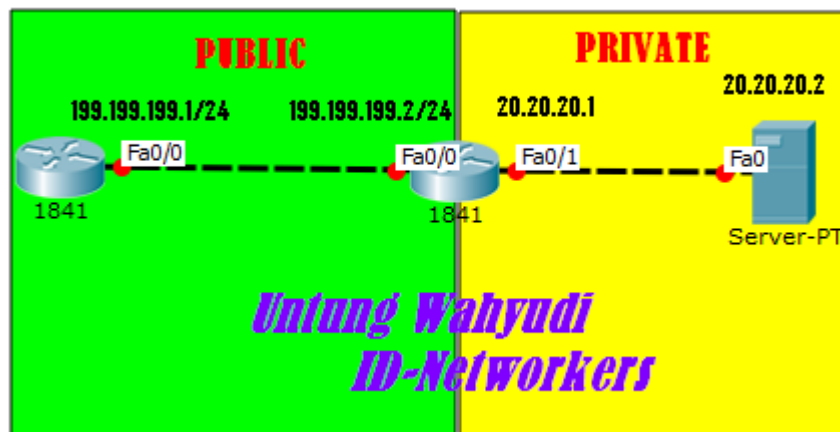
NAT (Network Address Translation) digunakan untuk menterjemahkan suatu IP ke Alamat IP yang lain. IP sendiri dapat kita bagi menjadi 2 yaitu IP Public dan IP Local/Private. IP local digunakan hanya untuk jaringan local saja , sedangkan IP Public digunakan secara umum , IP Public inilah yang digunakan untuk berkomunikasi di dunia internet karena dapat diakses dari manapun. Tapi IP Public juga memiliki batasan , jadi tidak semua memiliki IP Public , hanya kalangan tertentu saja yang memilikinya , seperti ISP. Karena dalam internet untuk berkomunikasi harus menggunakan IP Public , dengan NAT ini kita bisa membuat IP Local juga bisa menggunakan Internet. Yang mana prosesnya itu IP Local akan diterjemahkan menjadi IP Public.

Di Cisco ada 3 jenis NAT , yaitu :

1. Static NAT : Penggunaan 1 IP Public untuk 1 IP Private (One to One Mapping). Sebagai contoh ada sebuah server yang ingin diakses melalui internet , sedangkan Server tsb menggunakan IP Private. Dengan menggunakan Static NAT maka server dapat diakses melalui IP Public.
2. Dynamic NAT Overloading : Penggunaan 1 IP Public untuk beberapa IP Private. Sebagai contoh ada lebih dari 1 client ingin mengakses internet , namun hanya ada 1 IP Public , maka kita bisa gunakan Dynamic Nat Overloading ini.
3. Dynamic NAT : Penggunaan IP Public untuk IP Private yang memiliki jumlah yang sama. Jadi untuk menggunakannya membutuhkan jumlah IP Public dan IP Private yang sama , misal kita ada 5 client maka kita harus memiliki 5 IP Public , maka dari itu Dynamic NAT ini jarang digunakan.

Lab 35. Static NAT

Untuk pembahasan NAT yang pertama kita mulai dari Static NAT. Static NAT ini digunakan untuk menterjemahkan 1 IP Private ke 1 IP Public. Implementasi nya misalnya di sebuah kantor memiliki Server yang ingin diakses melalui internet , sedangkan Server tersebut menggunakan IP Private. Kita buat contoh kasus seperti diatas , buat topologi serperti dibawah ini.



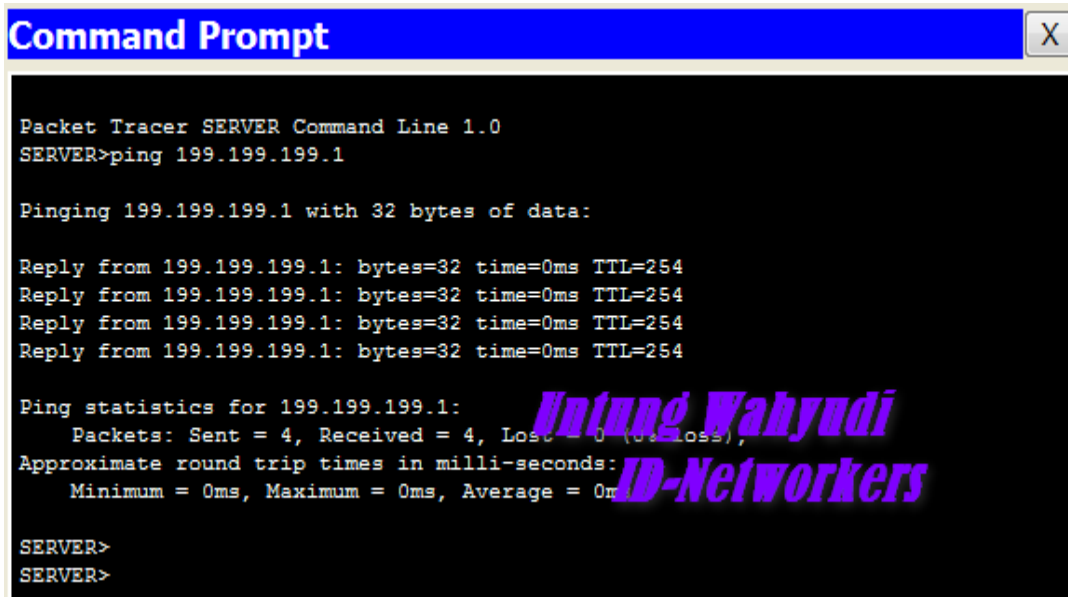
Langkah pertama adalah konfigurasi IP sesuai dengan topologi diatas ,kemudian setting NAT di Router 2 (Dekat Server). Seperti berikut

```
R2(config)#ip nat inside source static 20.20.20.2 199.199.199.2
R2(config)#int fa0/0
R2(config-if)#ip nat outside
R2(config-if)#int fa0/1
R2(config-if)#ip nat inside
R2(config-if)#ex
```

Keterangan :

- 20.20.20.2 = IP Private yang ingin ditranslate menjadi IP Public
- 199.199.199.2 = IP Public
- IP NAT Outside = kita pilih interface yang menjadi IP Public
- IP NAT Inside = kita pilih interface yang menjadi IP Private

Selanjutnya silahkan test ping dari Server ke Router 1 , maka hasilnya akan berhasil akan tetapi R1 tidak dapat test ping ke Server , karena IP Private tidak akan bisa diping kecuali kita routing.



```
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 199.199.199.1

Pinging 199.199.199.1 with 32 bytes of data:

Reply from 199.199.199.1: bytes=32 time=0ms TTL=254
Reply from 199.199.199.1: bytes=32 time=0ms TTL=254
Reply from 199.199.199.1: bytes=32 time=0ms TTL=254
Reply from 199.199.199.1: bytes=32 time=0ms TTL=254

Ping statistics for 199.199.199.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

SERVER>
SERVER>
```

Untuk cek IP NAT gunakan perintah berikut

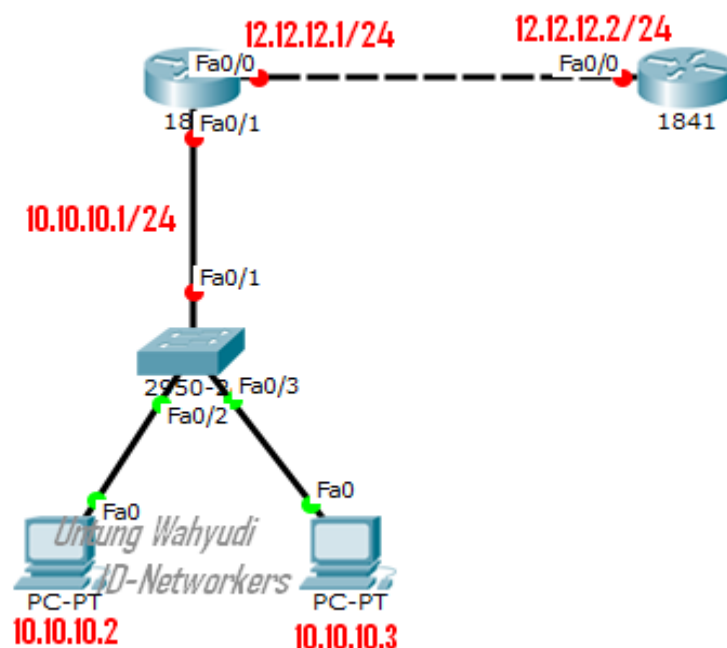
```
R2#show ip nat translation

Pro Inside global      Inside local Outside local   Outside global
icmp 199.199.199.2:6 20.20.20.2:6 199.199.199.1:6 199.199.199.1:6
icmp 199.199.199.2:7 20.20.20.2:7 199.199.199.1:7 199.199.199.1:7
icmp 199.199.199.2:8 20.20.20.2:8 199.199.199.1:8 199.199.199.1:8
--- 199.199.199.2      20.20.20.2      ---                ---
```

Lab 36. Dynamic NAT

Untuk Dynamic NAT sebenarnya sudah jarang atau bahkan sudah tidak pernah dipakai lagi, karena untuk menterjemahkan alamat IP maka “Jumlah IP Public Harus sama dengan Jumlah IP Private”. Cara ini sangat tidak efektif makanya sudah tidak ada yang menggunakan Dynamic NAT. Namun saya sebagai penulis , ingin memperkenalkan Dynamic NAT ini , sehingga kita bisa lebih dekat dengan semua jenis NAT di Cisco.

Langsung saja buat topologi seperti dibawah ini , dengan kasusnya R1 hanya memiliki 1 IP public dari ISP , sedangkan dia memiliki 2 client untuk terkoneksi ke Internet (ISP). Nantinya hanya 1 client saja yang dapat terkoneksi karena kita menggunakan Dynamic NAT.



Pertama silahkan Setting IP sesuai dengan topologi diatas , baik interface router maupun di PC , untuk yang di PC jangan lupa gateway nya. Jika sudah selanjutnya kita konfigurasi Dynamic NAT nya , seperti dibawah ini

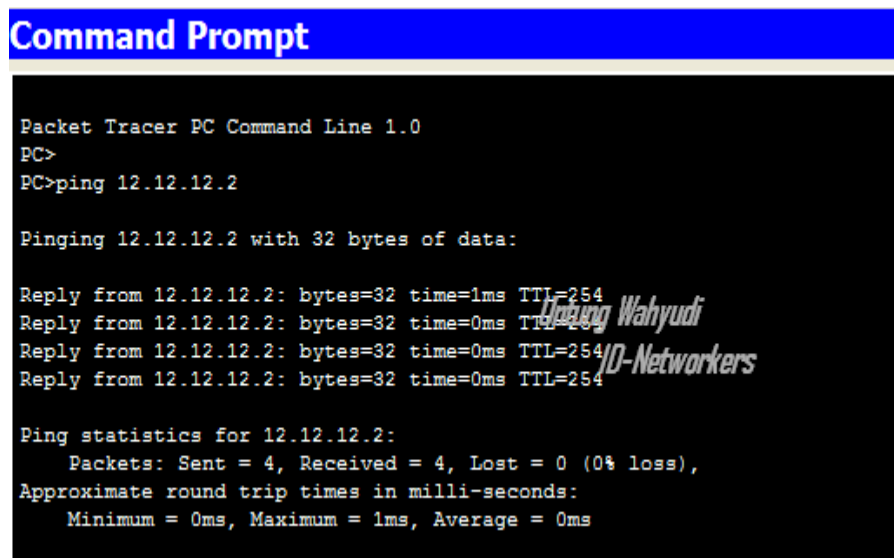
```
R1(config)#ip nat pool UNTUNG 12.12.12.1 12.12.12.1 netmask 255.255.255.0
R1(config)#access-list 1 permit 10.10.10.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool UNTUNG
R1(config)#int fa0/0
```

```
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#int fa0/1
R1(config-if)#ip nat inside
R1(config-if)#ex
```

KETERANGAN :

- IP 12.12.12.1 yang pertama adalah IP Public awal
- IP 12.12.12.2 Yang KEDUA adalah IP Public Akhir , karena kita hanya menggunakan 1 IP Public maka kita masukan awal dan akhirnya sama.
- Pool UNTUNG adalah penamaan dari range IP Public nya , bisa di isi dengan nama yang lain

Setelah itu silahkan test ping dari kedua PC ke Router 2 , pasti hanya ada 1 yang berhasil , dan yang satu lagi tidak akan berhasil.



```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>
PC>ping 12.12.12.2

Pinging 12.12.12.2 with 32 bytes of data:

Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254

Ping statistics for 12.12.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 12.12.12.2

Pinging 12.12.12.2 with 32 bytes of data:

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

Ping statistics for 12.12.12.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

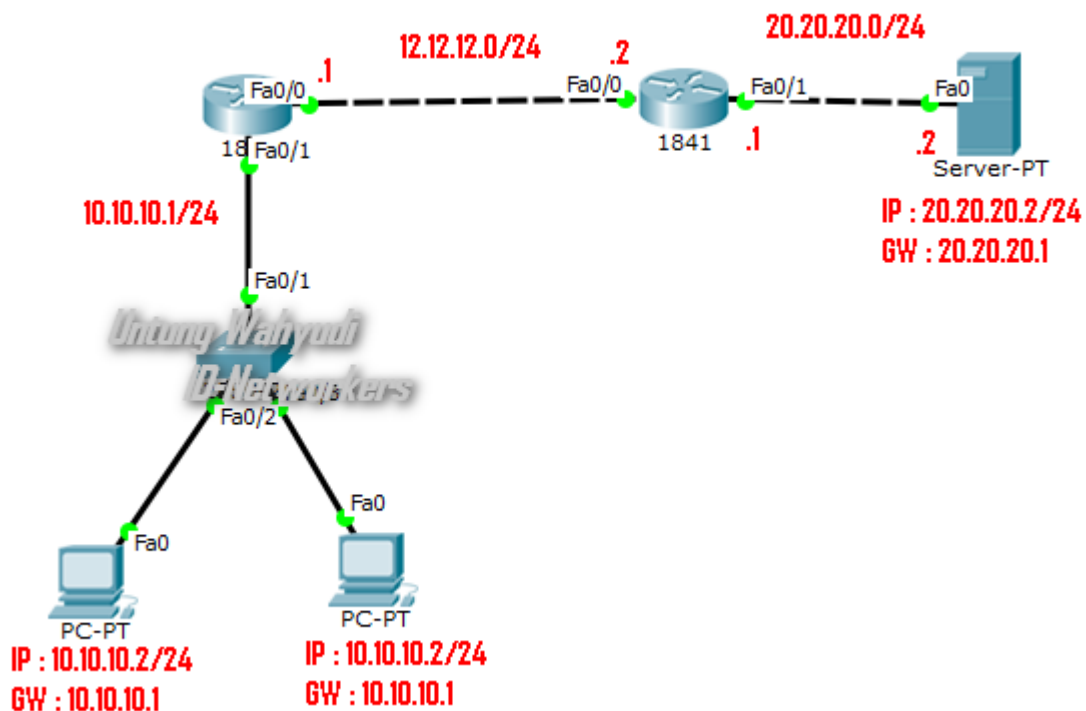
PC>
```

Kenapa hanya satu saja yang dapat ping ?? . Ini karena fungsi dari Dynamic NAT itu sendiri , jumlah IP Public harus sama dengan IP Private , sedangkan diskenario diatas kita hanya memiliki 1 IP public maka hanya 1 IP Private saja yang bisa di translate.

Lab 37. Dynamic NAT Overloading

Sebagai pembahasan terakhir di NAT ini , saya akan membuat lab tentang Dynamic NAT Overloading. NAT Overloading ini lebih banyak digunakan daripada Dynamic NAT , karena dengan NAT Overloading ini kita bisa menterjemahkan beberapa IP Private hanya dengan 1 IP Public , biasanya dikenal dengan Istilah PAT (Port Address Translation) , karena dia akan menterjemahkan IP Private ke 1 IP Public dengan berbeda jalur/port. Biasanya digunakan agar Client yang cukup banyak dapat menikmati koneksi internet.

Langsung aja kita buat topologi seperti dibawah ini , topologi yang sama seperti di lab access list.



Langkah pertama seperti biasa konfigurasi IP Pada setiap interface router , PC dan server nya sesuai dengan topologi diatas , Kemudian konfigurasi default route di kedua Router.

```
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 12.12.12.1
```

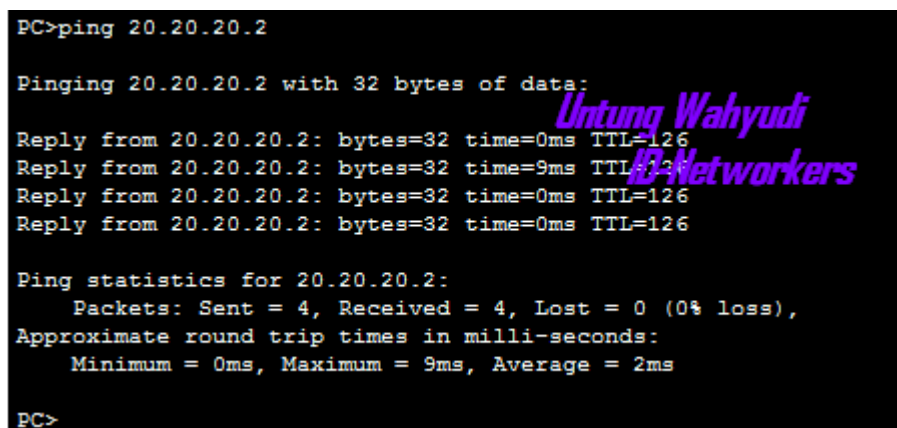

selanjutnya kita akan konfigurasi Dynamic NAT Overload nya.

```
R1(config)#ip nat inside source list 1 interface fa0/0 overload
R1(config)#access-list 1 permit 10.10.10.0 0.0.0.255
R1(config)#int fa0/0
R1(config-if)#ip nat outside
R1(config-if)#ex
R1(config)#int fa0/1
R1(config-if)#ip nat inside
R1(config-if)#ex
```

Dibagian interface overload , kita pilih interface yang Outside , atau interface yang memiliki IP Public. Selanjutnya kita jalankan debug di R1 , untuk mengecek paket data yang lewat.

```
R1#debug ip nat
```

Kemudian test ping dari PC 1 dan 2 ke Server. Dan pastikan hasilnya berhasil karena sudah kita routing.



```
PC>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=9ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms TTL=126
Reply from 20.20.20.2: bytes=32 time=0ms 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 = 9ms, Average = 2ms

PC>
```

Kemudian cek di R1 , setelah di ping maka Debug akan berjalan , dan dapat kita lihat bahwa IP Private nya sudah diterjemahkan menjadi IP Public. Dari 10.10.10.2 dan 10.10.10.3 diubah menjadi 12.12.12.1.

```
R1#
NAT: s=10.10.10.3->12.12.12.1, d=20.20.20.2 [6]
NAT*: s=20.20.20.2, d=12.12.12.1->10.10.10.3 [2]
NAT: s=10.10.10.2->12.12.12.1, d=20.20.20.2 [1]
NAT*: s=20.20.20.2, d=12.12.12.1->10.10.10.2 [3]
```

Kemudian cek IP NAT nya , maka di bagian inside global hanya akan ada 1 IP yaitu 12.12.12.1 , namun dengan port yang berbeda (12.12.12.1:1 dan 12.12.12.1:5).

```
Router#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	12.12.12.1:1	10.10.10.2:1	20.20.20.2:1	20.20.20.2:1
icmp	12.12.12.1:5	10.10.10.3:5	20.20.20.2:5	20.20.20.2:5