Feriansyah

ID-Networkers
INDONESIAN EXPERT FACTORY

CISCO

CCNA JobSheet

30 Lab Cisco

VLAN, Trunk, InterVLAN, Native, DTP,
STP, VTP, DHCP Server, Port-security
Etherchannel, Static Routing, OSPF,
EIGRP, Redistribute, Standard Access-List
Extended Access-list, SNAT, DNAT, NAT PAT,
HSRP, VRRP, GLBP, HDLC, PPP

Feriansyah
0815-4515-2905
Jl. H. Jahrah
feriansyah.ms@gmail.com
feri.ms

DAFTAR ISI

LAB 1 - Preparation Cisco (GNS3)

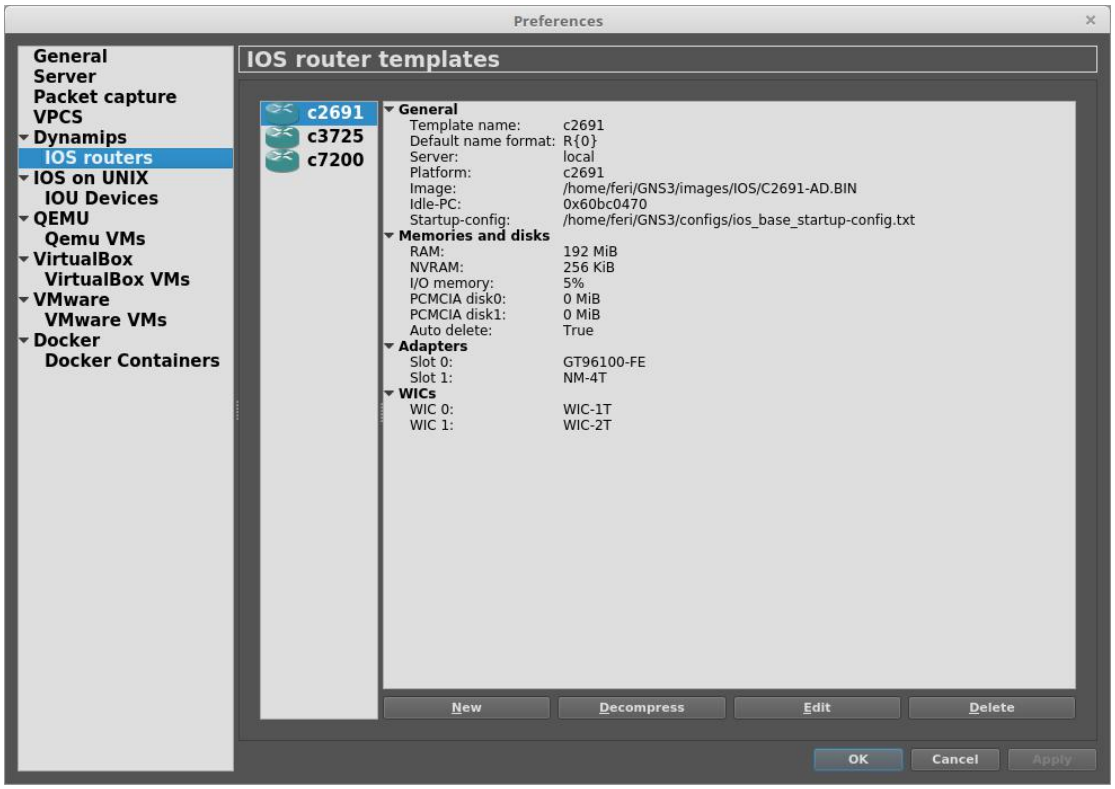
Untuk belajar cisco dapat menggunakan virtual yaitu GNS3 ataupun Cisco Packet Tracer. Namun di sarankan memakai GNS3 karena GNS3 memakai Cisco IOS asli dan lebih disarankan memakai alat yang asli walaupun hanya untuk belajar.

Yang harus disiapkan

Aplikasi GNS3 yang kudu di install dulu di laptop/pc yang antum gunain bisa check di web resminya dulu (https://www.gns3.com/)

Persiapin Cisco IOS nya juga yang bakal digunakan nanti yang bisa di cari di google.

1. Jika GNS3 sudah di install
2. Buka aplikasi GNS3 nya
3. Lalu tambahkan Cisco IOS

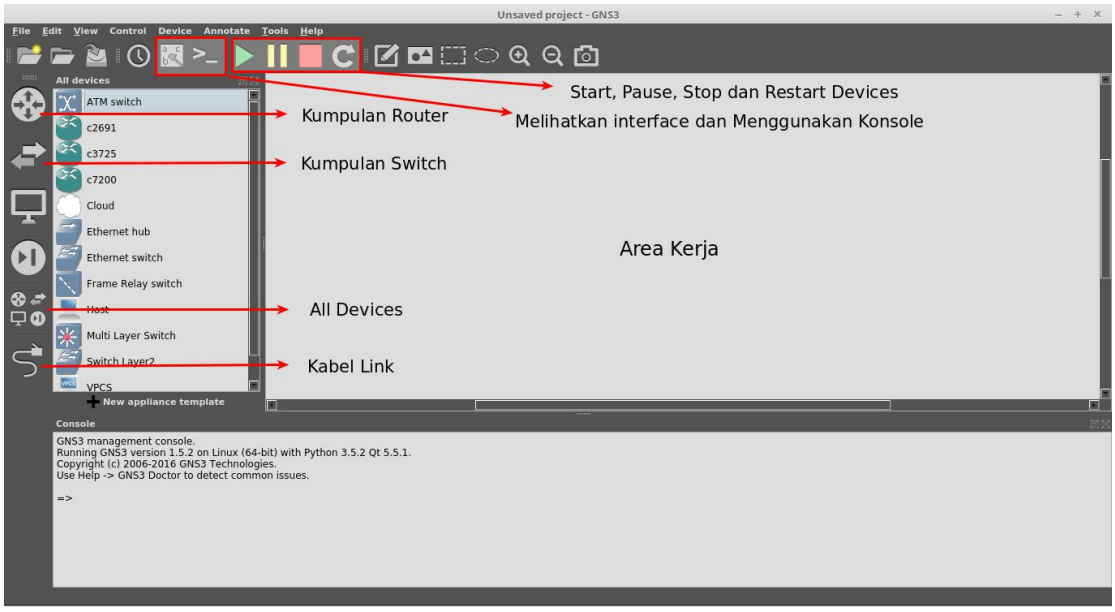


Gambar 1.1 GNS3 > Preference

Cisco Router = buka tab >> edit >> preferences >> Dynamips >> IOS routers >> New.

1. Maka nanti akan muncul tab baru, lalu pilih new image lalu klik Browse dan pilih Cisco Router IOS entah itu c2691, atau c3660 ataupun c7200 lalu Next
2. Pilih nama dari routernya, isi defaultnya aja lalu Next
3. Lalu masukkan alokasi untuk RAM terserah aja tergantung kemampuan laptop, semakin tinggi semakin baik.
4. Lalu penambahan interface, di Slot 1 tambah NM-4E lalu Next
5. Lalu klik Idle-PC finder, maka GNS3 akan otomatis mencari Idle-PC agar tidak bekerja 100%. Ketika sudah ketemu lalu klik Finish
6. Untuk Cisco Switch = buka tab >> edit >> preferences >> IOS on UNIX >> IOU Devices >> New
7. Maka akan muncul tab baru lalu, Beri nama untuk Switchnya. Lalu pilih New Image. Lalu pilih apakah Layer2 atau Layer3 dan masukkan IOU image jika type yang dipilih Layer2 maka IOU imagenya pun Layer2
8. Lalu klik Finish
9. Jika ingin menambahkan network pada router maupun switch klik edit lalu klik slot untuk router. klik network untuk switch.
10. Setelah Cisco IOS sekarang kita sudah bisa menggunakan Cisco router maupun Cisco switch

Untuk menambahkan Cisco router atau Switch ikuti langkah berikut



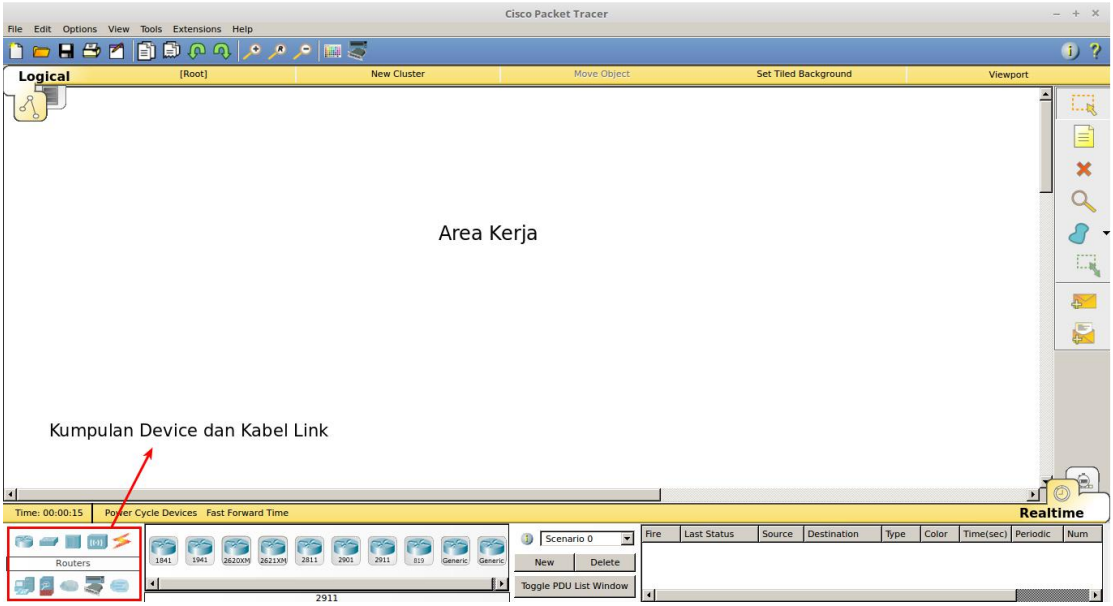
Gambar 1.2 Tampilan GNS3

Beberapa keterangan diatas adalah :

1. Kumpulan Router device yang bisa kita gunakan
2. Kumpulan Switch device yang bisa kita gunakan
3. Kumpulan Semua device yang kita masukkan IOS dan IOU nya
4. Kabel penghubung
5. Start, yang akan menyalakan semua device
6. Untuk membuka terminal CLI yang akan kita gunakan untuk konfigurasi
7. Akan memperlihatkan interface yang digunakan setiap device
8. Untutk menambahkan device cukup drag and drop device ke halaman tengah, lalu sambungkan setiap device dengan kabel.

LAB 2 - Preparation Cisco (Cisco Packet Tracer)

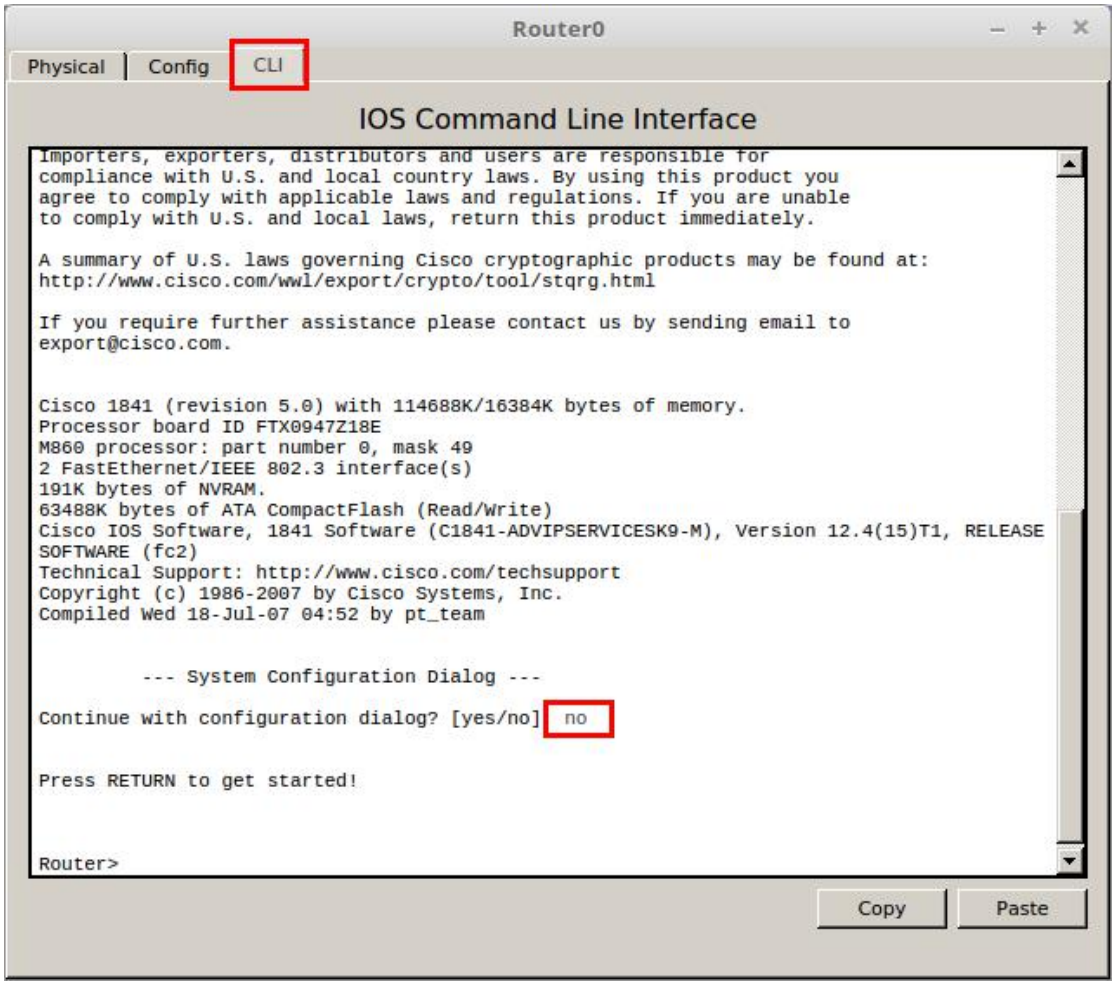
Selain menggunakan GNS3 kita juga dapat menggunakan aplikasi Cisco Packet Tracer. GNS3 memakan memory yang lumayan banyak, jadi menggunakannya agak berat. Sedangkan, pada Cisco Packet Tracer lebih ringan. Aplikasi yang saya gunakan menggunakan Cisco Packet Tracer 7.3. Tampilannya kira-kira seperti ini.



Gambar 2.1 Tampilan Cisco Packet Tracer

Hampir sama seperti menggunakan GNS3 ada beberapa device yang bisa di lihat pada kotak di bawah kiri. Dan untuk menggunakannya tinggal **Drag & Drop** saja ke area kerja. Klik dua kali pada devicenya lalu klik CLI untuk menggunakan konsole atau terminalnya.

Tampilannya kira-kira seperti gambar di bawah ini



Gambar 2.2 Tampilan terminal pada Router0

Jika pilih **yes** maka kita akan mengkonfigurasinya secara otomatis tidak menggunakan perintah.

LAB 3 - User, Privileged dan Global Configuration Mode

Pada cisco juga memiliki beberapa mode :

1. User mode
2. Privileged mode
3. Global Configuration mode

User Mode

User mode tandanya adalah **“hostname>”** dan sedikit saja yang kita lakukan pada mode ini. Tidak bisa mengkonfigurasi router pada mode ini. Kita bisa menggunakan **?** Jika tidak mengetahui perintah apa saja yang dapat digunakan.

```
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
```

Priviliged Mode

Tandanya adalah **“hostname#”.** Pada mode ini kita bisa untuk masuk ke mode ini ketik perintah **enable.** Pada mode ini kita bisa melihat konfigurasi yang telah di konfigurasi pada router. Gunakan perintah **?** Untuk melihat apa saja perintah yang dapat digunakan.

```
Router>enable

Router#?

Exec commands:

  <1-99>      Session number to resume

  auto        Exec level Automation

  clear       Reset functions

  clock       Manage the system clock

  configure   Enter configuration mode

  connect     Open a terminal connection

  copy        Copy from one file to another

  debug       Debugging functions (see also 'undebug')

  delete      Delete a file

  dir         List files on a filesystem

  disable     Turn off privileged commands

  disconnect  Disconnect an existing network connection

  enable      Turn on privileged commands

  erase       Erase a filesystem

  exit        Exit from the EXEC

  logout      Exit from the EXEC

  mkdir       Create new directory

  more        Display the contents of a file

  no          Disable debugging informations

  ping        Send echo messages

  reload      Halt and perform a cold restart

  resume      Resume an active network connection

  rmdir       Remove existing directory
```

```
  send        Send a message to other tty lines
  setup       Run the SETUP command facility
  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
  undebug     Disable debugging functions (see also 'debug')
  vlan        Configure VLAN parameters
  write       Write running configuration to memory, network, or terminal
```

Misal kita ingin melihat konfigurasi IP Address,

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method  Status
Protocol

FastEthernet0/0        unassigned      YES unset  administratively down down

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
```

Dan beberapa perintah yang dapat digunakan pada show

```
Router#show ?
  aaa               Show AAA values
  access-lists       List access lists
  arp               Arp table
  cdp               CDP information
  class-map          Show QoS Class Map
....
```

Global Configuration Mode

Pada mode inilah kita mengkonfigurasi router atau switch. Tandanya adalah **“hostname(config)#”** untuk masuk ke mode ini menggunakan perintah **configuration terminal.**

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Pada cisco mudahnya kita dapat menyingkat perintahnya seperti berikut. Dan kita juga bisa menggunakan **TAB** untuk menyelesaikan perintahnya.

```
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Dari mode ini kembali ke mode privileged bisa menggunakan CNTRL + Z

LAB 4 - Konfigurasi Dasar

Pada saat perintah salah maka akan muncul dulu. Biar cepet bisa menekan CNTRL + SHIFT + 6

```
Router>em

Translating "em"...domain server (255.255.255.255) % Name lookup aborted
```

Melihat versi cisco dengan perintah **show version**

```
Router#show version

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team


ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)


System returned to ROM by power-on

System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.


A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Mengkonfigurasi IP Address pada interface

```
Router(config)#int fa0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 12.12.12.1 255.255.255.0
```

Perintah **no shutdown** digunakan untuk menyalakan interface karena pada posisi awalnya interface tersebut dalam keadaan mati (**shutdown**).

Untuk melihat IP Address yang sudah di konfigurasi dengan perintah **show**

```
Router#show ip int br
Interface                  IP-Address      OK? Method  Status
Protocol

FastEthernet0/0        12.12.12.1      YES manual up                    down

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
```

Status port yang dapat di temui adalah :

1. Administratively down down = Status port dalam keadaan mati
2. Down down = Masalah pada Layer 1
3. Up down = Masalah pada Layer 2
4. Up up = Layer 1 dan 2 udah bagus.

Pada contoh di atas statusnya adalah **up** dan **down** ini dikarenakan interface lawannya tidak di konfigurasi.

Mengubah hostname (nama route) dengan perintah **hostname** *nama-router.*

```
Router(config)#hostname Feri-R1
Feri-R1(config)#
```

Untuk melihat seluruh konfigurasi dapat menggunakan **show run**

```
Feri-R1#show running-config
Building configuration...

Current configuration : 564 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Feri-R1
.....
```

Mengkonfigurasi password pada router

```
Feri-R1(config)#enable password 123
atau
Feri-R1(config)#enable secret 123
```

Jika menggunakan password maka bentuknya plain-text jika di lihat pada running-config. Jika menggunakan secret maka akan terenkripsi.

Pada cisco, setiap konfigurasi akan tersimpan pada running-config, maka pada saat kita menreboot atau menshutdown device, konfigurasinya akan hilang. Maka kita perlu menyimpannya ke startup-config, dengan perintah **write.**

```
Feri-R1#write
Building configuration...
[OK]
Atau
Feri-R1#copy running-config startup-config
Destination filename [startup-config]? enter
Building configuration...
[OK]
```

Dan jika kita menggunakan perintah pada privileged pada mode konfig maka hasilnya seperti berikut

```
Feri-R1(config)#write
               ^
% Invalid input detected at '^' marker.
```

Dan jika ingin menggunakan perintah tersebut maka harus menambahkan **do**

```
Feri-R1(config)#do write
Building configuration...
[OK]
```

Dan untuk mengembalikan ke konfigurasi awal kita, perintahnya **write erase.** Dan perlu di reboot dulu dengan perintah **reload.**

```
Feri-R1#write erase
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Feri-R1#reload
Proceed with reload? [confirm]enter
```

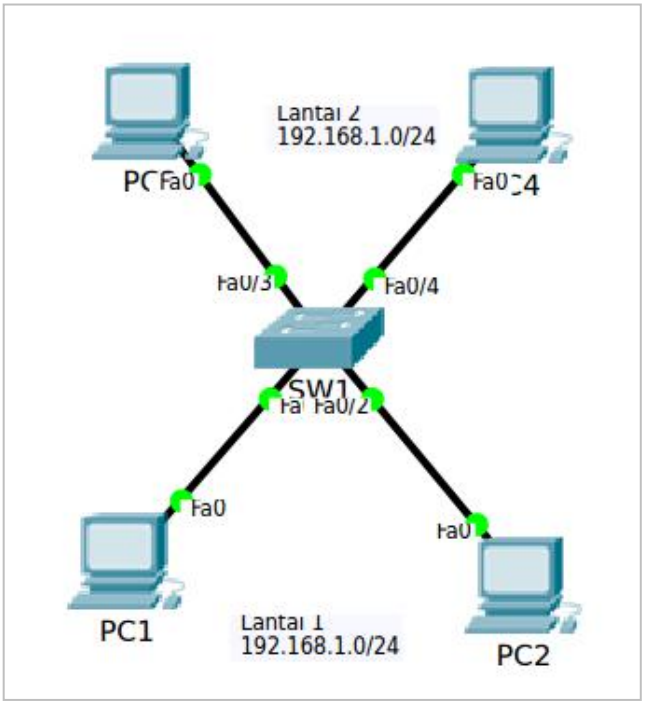
The Alchemy of SWITCHING

LAB 5 - VLAN (Virtual LAN)

Pada switch unmanagable maka semua interface nya akan menjadi satu network. Sedangkan pada switch managable kita dapat mengkonfigurasi agar masing-masing interface memiliki network-network yang berbeda. Ini dinamakan dengan segmentasi jaringan pada switch yaitu **VLAN.**

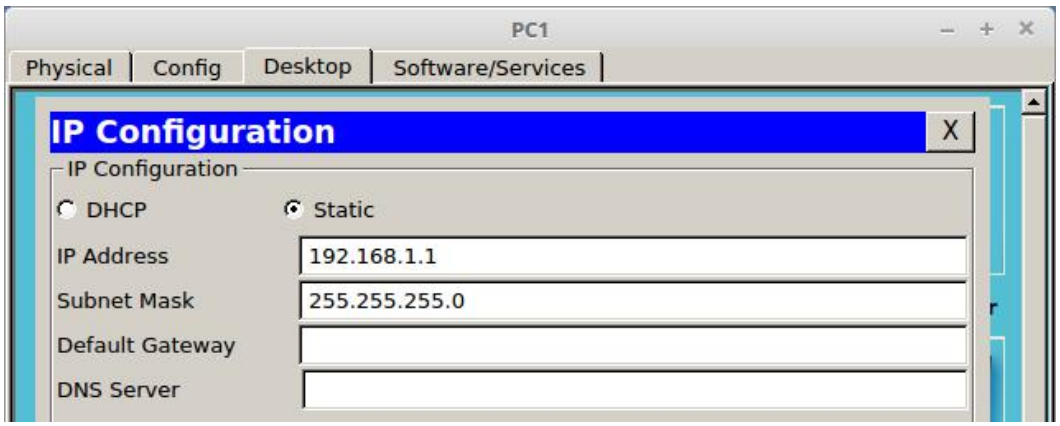
Dengan menggunakan VLAN kita dapat mengelompokkan user atau group pada switch. Misal VLAN 10 = Guru, VLAN 20 = Siswa dan VLAN 30 = TU.

Buat topologi jaringan seperti berikut.



Gambar 5.1 Topologi Jaringan

Konfigurasi IP Address pada semua PC terlebih dahulu. Klik 2x pada PC lalu masuk pada desktop > IP Configuration. Isi kan IP Addressnya.



Gambar 5.2 Konfigurasi IP Address pada PC

Konfigurasi IP Address pada semua PC. Host ID menyesuaikan nama dari PC tersebut. PC1 berarti IP Addressnya adalah 192.168.1.1

Setelah IP Address dikonfigurasi semua, sekarang lakukan ping dari PC1 ke PC3, Karena di lihat dari networknya sama, maka seharusnya hasilnya reply. Buka PC > Desktop > Command Prompt, lalu lakukan ping.

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:


Reply from 192.168.1.3: bytes=32 time=33ms TTL=128

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.1.3:

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

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 33ms, Average = 8ms
```

Sekarang kita akan konfigurasi VLAN agar PC di Lantai 1 dan PC di Lantai berbeda network.

```
Switch>enable

Switch#conf ter

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname SW1
```

Uban nama switchnya menjadi SW1. Sekarang buat VLAN nya

```
SW1(config)#vlan 10

SW1(config-vlan)#name Lantai-1


SW1(config-vlan)#vlan 20

SW1(config-vlan)#name Lantai-2
```

Kita membuat VLAN 10 dengan nama Lantai-1 dan VLAN 20 dengan nama Lantai-2

Ubah mode interface menjadi access, lalu masukkan ke VLAN 10 untuk Lantai-1

```
SW1(config)#int fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10


SW1(config-if)#int fa0/2
SW1(config-if)#switch mode acc
SW1(config-if)#switch acc vlan 10
```

Selain memasukkan satu-satu interfacenya kita bisa menggunakan perintah **range** jika memasukkan interface sekaligus.

```
SW1(config)#interface range fa0/3-4
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switch acc vlan 20
```

Setelah itu kita check VLAN yang sudah terbuat, dengan perintah **show vlan brief.** Default VLAN adalah **VLAN 1**

```
SW1#show vlan brief


VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Lantai-1                          active    Fa0/1, Fa0/2
20   Lantai-2                          active    Fa0/3, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
```

Sudah terlihat VLAN yang kita buat beserta dengan interfacenya. Sekarang lakukan ping lagi antara PC1 ke PC3

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:


Request timed out.

Request timed out.

Request timed out.

Request timed out.


Ping statistics for 192.168.1.3:

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

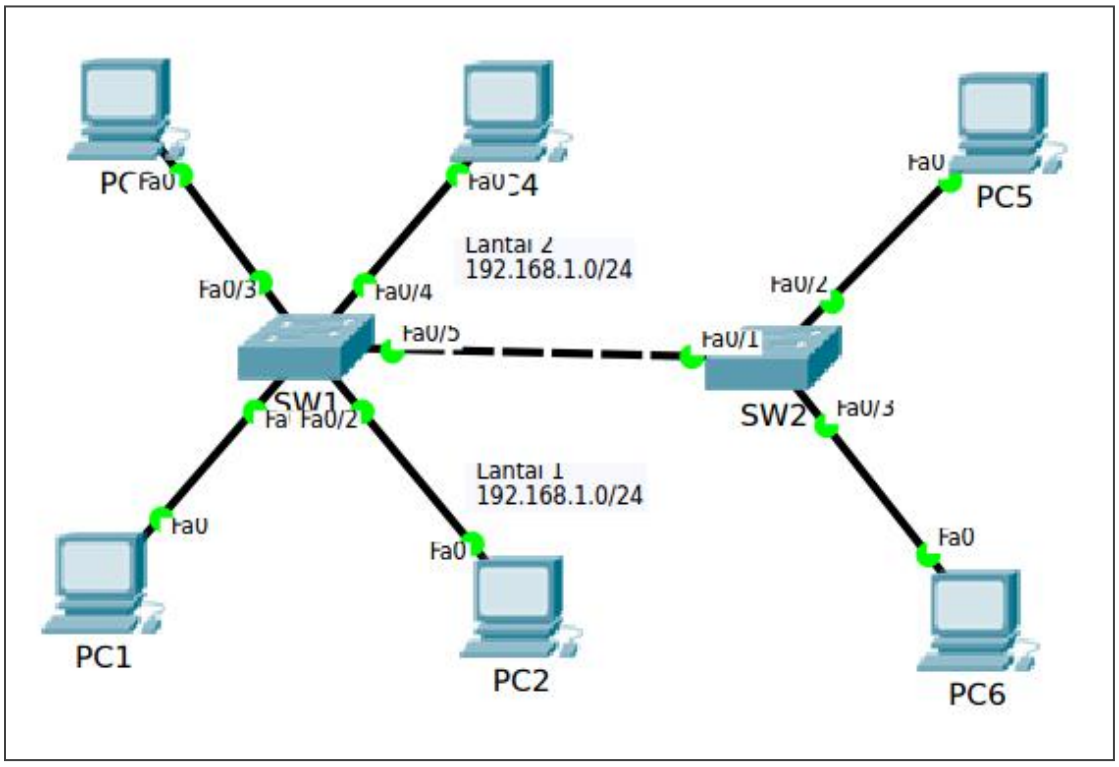
Hasilnya akan RTO karena berbeda VLAN. Sekarang coba kita jika sesama VLAN (Sesama-lantai).

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:


Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Reply from 192.168.1.2: bytes=32 time=3ms TTL=128

Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Reply from 192.168.1.2: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.1.2:

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

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Dari PC1 ke PC2.

LAB 6 - Trunking

Trunking digunakan untuk menghubungkan dua switch yang menggunakan VLAN dengan proses **encapsulation**. Jika kita memiliki beberapa switch dan menggunakan VLAN di tiap switch maka kita harus mengkonfigurasi Trunking di interface yang mengarah ke switch, karena jika tidak maka tidak akan berhasil. Topologi yang akan digunakan seperti berikut



Gambar 6.1 Topologi Trunking

Kita akan melanjutkan dari Topologi sebelumnya. Karena sebelumnya kita sudah mengkonfigurasi SW1 dan PC1-4. Maka kita konfigurasi Sw2 dan PC5-6 saja.

Konfigurasi IP Address pada PC5 menggunakan 192.168.1.5/24 dan PC6 menggunakan 192.168.1.6/24.

Dan coba kita lakukan test ping.

```
PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
```

```
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.1.6:

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

Approximate round trip times in milli-seconds:

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

Sekarang masih terhubung dan test ping lagi mengarah PC yang berada pada SW1 yang sudah di konfigurasi VLAN. Maka hasilnya akan RTO, karena PC5 menggunakan VLAN1 (Default) dan PC4 menggunakan VLAN20.

Sekarang kita atur PC5 agar menggunakan VLAN20 dan PC6 VLAN10. Konfigurasi VLAN terlebih dahulu

```
Switch>en

Switch#conf ter

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname SW2


SW2(config)#vlan 10

SW2(config-vlan)#name Lantai-1

SW2(config-vlan)#vlan 20


SW2(config-vlan)#name Lantai-2

SW2(config-vlan)#exit


SW2(config)#interface fa0/2

SW2(config-if)#switchport mode acces

SW2(config-if)#switch acc vlan 20


SW2(config-if)#int fa0/3

SW2(config-if)#swi mode acc

SW2(config-if)#switch acc vlan 10
```

Sekarang PC5 sudah menggunakan VLAN20 sekarang coba test ping lagi ke PC4.

```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:


Request timed out.

Request timed out.

Request timed out.

Request timed out.


Ping statistics for 192.168.1.4:

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

Hasilnya masih RTO karena kita menggunakan switch yang berbeda, maka link penghubungnya harus di konfigurasi Trunk.

```
SW1(config)#int fa0/5

SW1(config-if)#switchport mode trunk


SW2(config)#inter fa0/1

SW2(config-if)#switchport mode trunk
```

Kita bisa mengkonfigurasi pada salah satu switch atau kedua-duanya.

Bisa kita check menggunakan perintah

```
SW1#show int trunk

Port        Mode         Encapsulation  Status        Native vlan

Fa0/5       on           802.1q         trunking      1


Port        Vlans allowed on trunk

Fa0/5       1-1005


Port        Vlans allowed and active in management domain

Fa0/5       1,10,20
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       1,10,20
```

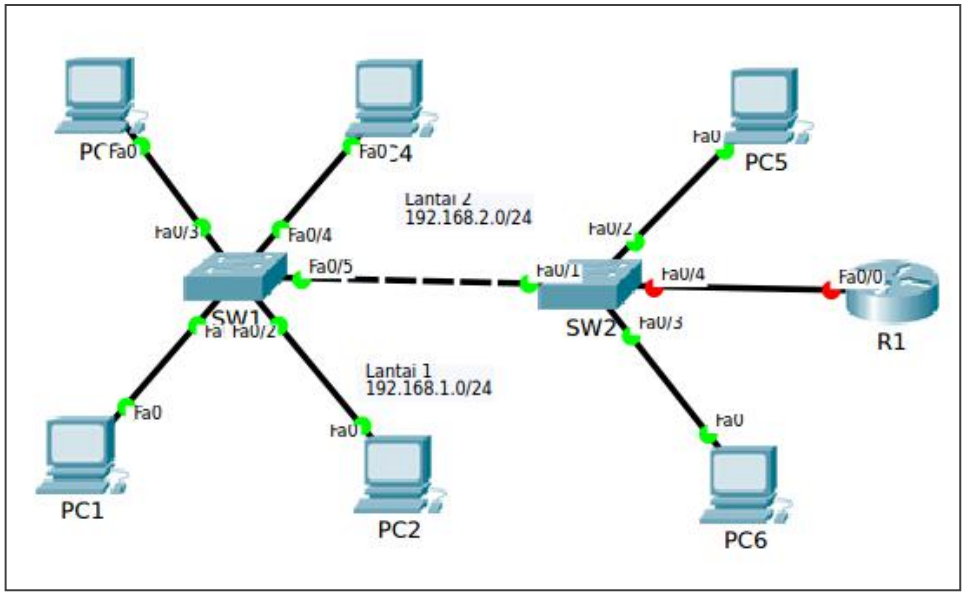
Sekarang lakukan test ping lagi dari PC5 ke PC4.

```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=13ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

LAB 7 - InterVLAN Routing (802.1Q)

InterVLAN routing digunakan untuk menghubungkan VLAN yang berbeda network menggunakan router. Di router dapat dikonfigurasi beberapa sub-interface yang sudah di encapsulation menjadi 802.1Q.

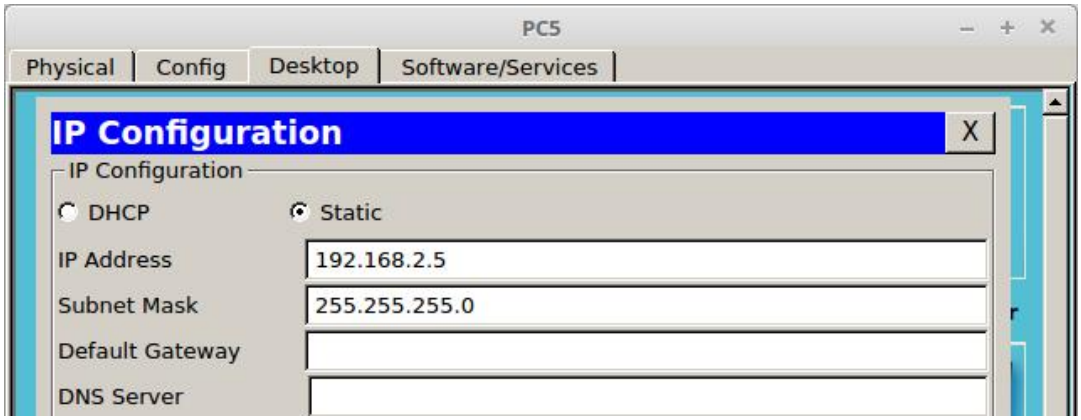
Topologi jaringannya seperti berikut



Gambar 7.1 InterVLAN Routing

Mengikuti konfigurasi pada LAB Sebelumnya. Kita menambahkan router yang berfungsi sebagai gateway bagi PC-PC. Link antar R1 dan SW2 memang awalnya merah karena pada R1 default interfacenya dalam keadaan shutdown.

Sebelumnya ganti dulu IP address pada VLAN 20



Gambar 7.2 Konfigurasi IP Address pada PC5

Konfigurasi hostname dan nyalakan interface fa0/0 R1

```
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int fa0/0
R1(config-if)#no shutdown
```

Sekarang kita buat **Sub-interface** yang digunakan sebagai gateway bagi VLAN 10 dan VLAN 20.

```
R1(config)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.1.254 255.255.255.0
R1(config-subif)#ex

R1(config)#int fa0/0.20
R1(config-subif)#encapsu dot1 20
R1(config-subif)#ip add 192.168.2.254 255.255.255.0
```

Check IP Address yang sudah kita buat tadi

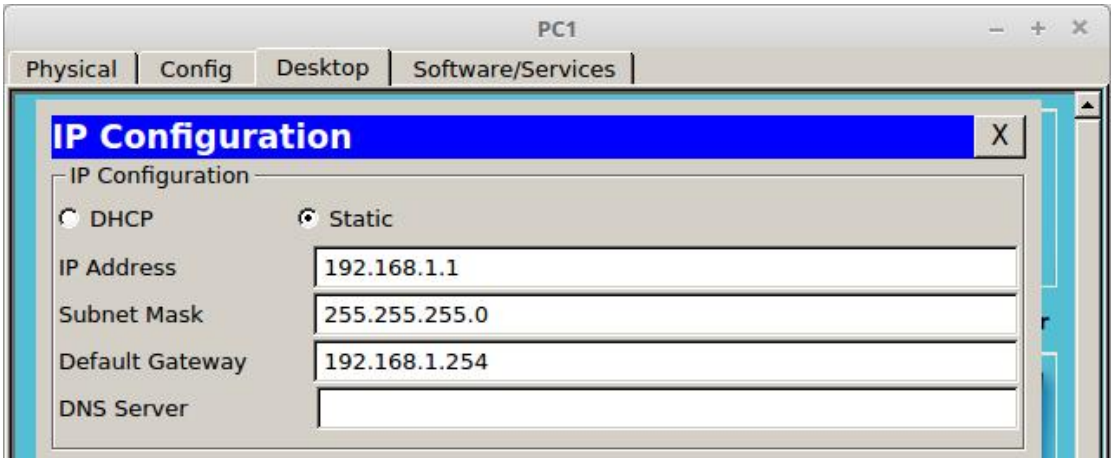
```
R1#show ip int br
Interface                  IP-Address      OK? Method  Status
Protocol

FastEthernet0/0        unassigned      YES unset  up                    up

FastEthernet0/0.10     192.168.1.254   YES manual up                    up

FastEthernet0/0.20     192.168.2.254   YES manual up                    up

FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
```

Statusnya sudah UP sekarang kita perlu mengkonfigurasi Trunking pada interface mengaraha ke Router

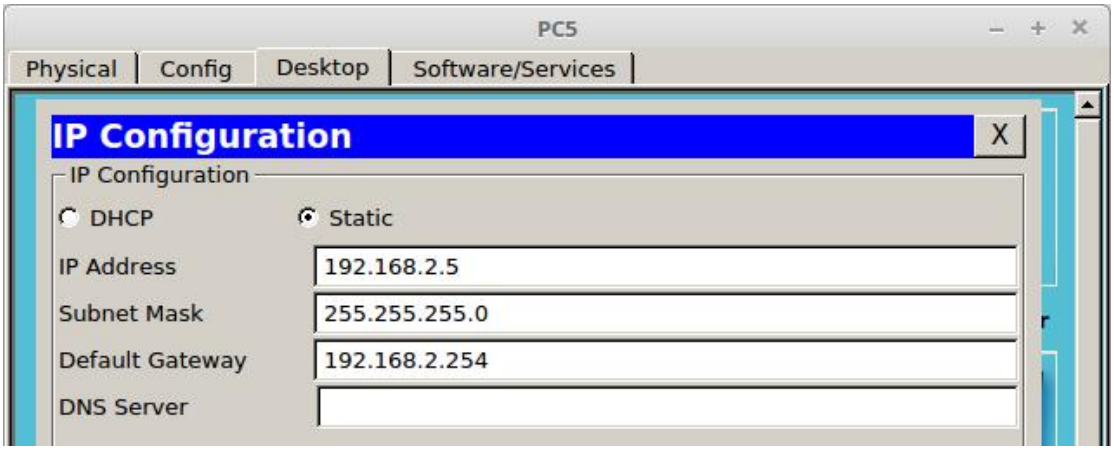
```
SW2(config)#int fa0/4
SW2(config-if)#swit mode tru
```

Konfigurasi IP Gateway pada setiap PC. **Gateway** digunakan sebagai pintu masuk untuk menuju network yang lainnya.

1. VLAN 10 : 192.168.1.254
2. VLAN 20 : 192.168.2.254



Gambar 7.3 Konfigurasi IP Gateway pada VLAN 10



Gambar 7.4 Konfigurasi IP Gateway pada 20

Sekarang coba lakukan ping antara PC1 dan PC5

```
PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:
```

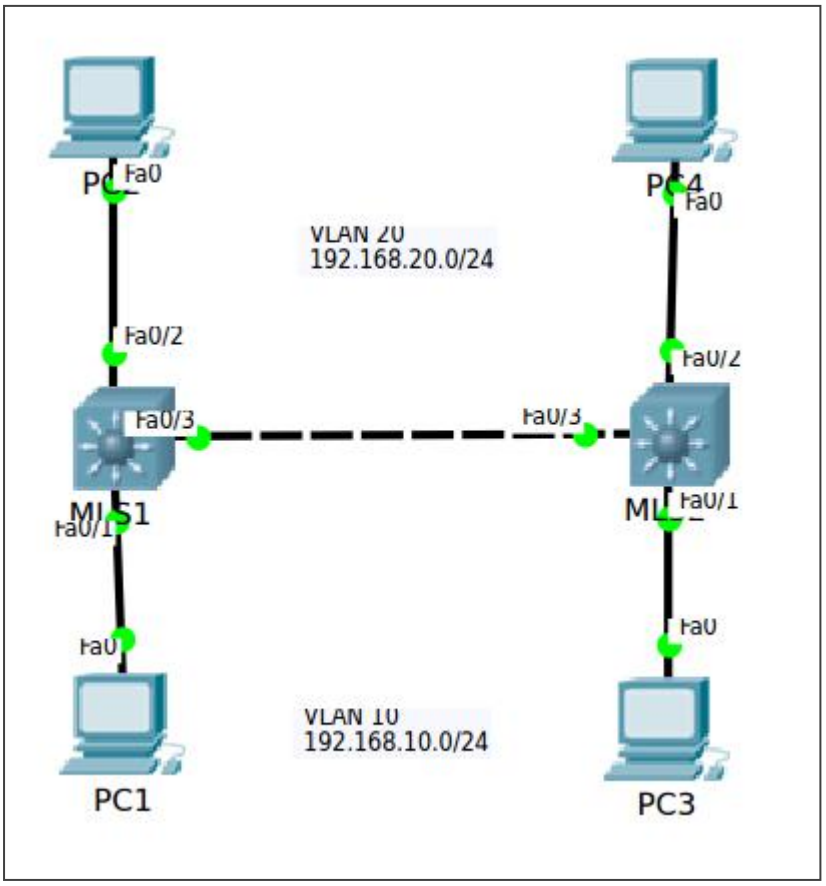
```
Request timed out.
Reply from 192.168.2.5: bytes=32 time=0ms TTL=127
Reply from 192.168.2.5: bytes=32 time=0ms TTL=127
Reply from 192.168.2.5: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.5:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Maka hasilnya akan reply

LAB 8 - Konfigurasi Trunk pada MLS (Switch L3)

Multi Layer Swtich merupakan switch yang mensupoort Layer 3 dan Layer 2. Jadi pada switch ini kita dapat mengkonfigurasi IP Address dan melakukan routing.

Untuk konfigurasi VLAN pada MLS sama seperti pada Switch Layer 2. Untuk konfigurasi Trunk agak berbeda.



Gambar 8.1 Topologi Trunking MLS Switch

Konfigurasi IP Address pada semua PC. Dan untuk gatewaynya memakai IP host 254. Konfigurasi VLAN pada MSL1

```
Switch(config)#hostname MSL1


MSL1(config)#vlan 10
MSL1(config-vlan)#name Lantai-Bawah
```

```
MSL1(config-vlan)#vlan 20
MSL1(config-vlan)#name Lantai-Atas
MSL1(config-vlan)#exi

MSL1(config)#int fa0/1
MSL1(config-if)#switchport mode access
MSL1(config-if)#switch access vlan 10

MSL1(config-if)#int fa0/2
MSL1(config-if)#swit mode acc
MSL1(config-if)#swit acc vlan 20
```

Dan juga konfigurasi IP Address sebagai gateway pada MLS1 dan Trunk

```
MSL1(config)#int vlan 10
MSL1(config-if)#ip address 192.168.10.254 255.255.255.0

MSL1(config-if)#int vlan 20
MSL1(config-if)#ip add 192.168.20.254 255.255.255.0
MSL1(config-if)#exit

MSL1(config)#ip routing

MSL1(config)#int fa0/3
MSL1(config-if)#switchport trunk encapsulation dot1q
MSL1(config-if)#switch mode trunk
```

Perintah **ip routing** digunakan untuk mengaktifkan fitur routing pada Switch layer 3. Dan pada interface harus di encapsulasi menjadi dot1q terlebih dahulu sebelum menggunakan trunk. Konfigurasi pada MLS2

```
Switch(config)#hostname MLS2

MLS2(config)#vlan 10
MLS2(config-vlan)#name Lantai-Bawah
```

```
MLS2(config-vlan)#vlan 20
MLS2(config-vlan)#name Lantai-Atas
MLS2(config-vlan)#ex

MLS2(config)#int fa0/1
MLS2(config-if)#switch mode acc
MLS2(config-if)#switch acc vlan 10

MLS2(config-if)#int fa0/2
MLS2(config-if)#swi mode acc
MLS2(config-if)#swi acc vlan 20

MLS2(config)#interface fa0/3
MLS2(config-if)#swi trunk encapsu dot1q
MLS2(config-if)#swi mode trunk
```

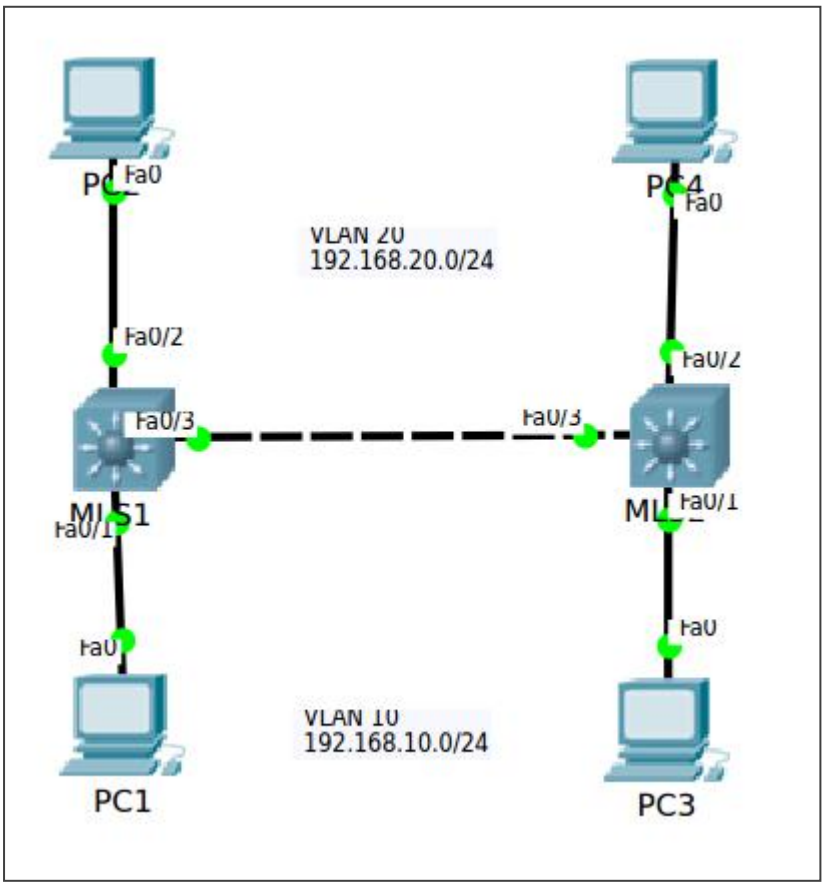
MLS2 hanya berfungsi sebagai switch biasa oleh karena itu tidak di konfigurasi IP routing dan IP Address. Sekarang lakukan Ping dari PC1 ke PC4.

```
PC>ping 192.168.20.4
Pinging 192.168.20.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.4: bytes=32 time=0ms TTL=127
Reply from 192.168.20.4: bytes=32 time=0ms TTL=127
Reply from 192.168.20.4: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Hasilnya reply karena kita sudah mengaktifkan fitur routing pada MLS

LAB 9 - Konfigurasi DHCP Server

Untuk konfigurasi DHCP Server pada switch maupun router sama saja. Fungsi dari DHCP Server adalah memberikan pengalamatan IP Address secara otomatis ke Client yang mengaktifkan DHCP Client.



Gambar 9.1 Topologi DHCP Server

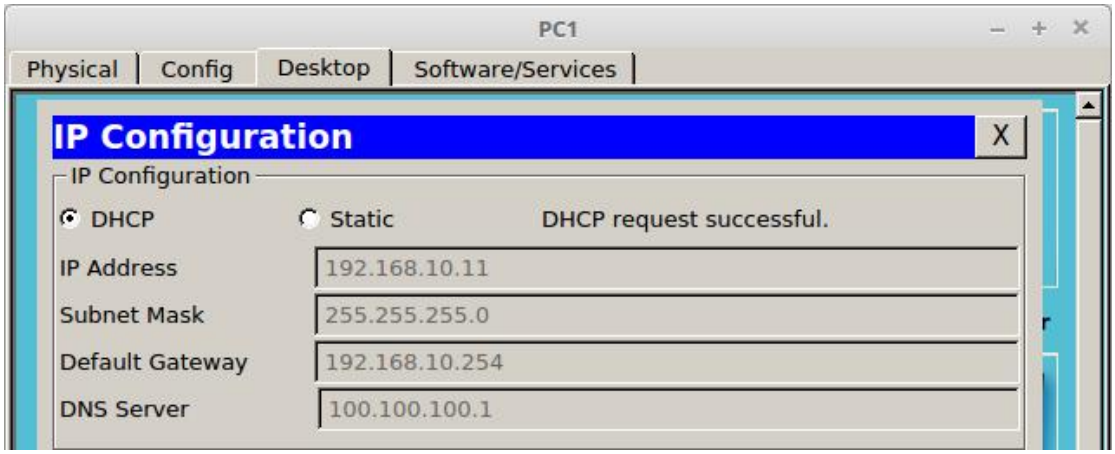
Melanjutkan konfigurasi pada lab sebelumnya. Hanya saja sekarang kita akan mengkonfigurasi DHCP Server dan DHCP Client pada PC1-4.

```
MSL1(config)#ip dhcp pool VLAN10
MSL1(dhcp-config)#network 192.168.10.0 255.255.255.0
MSL1(dhcp-config)#dns-server 100.100.100.1
MSL1(dhcp-config)#default-router 192.168.10.254
MSL1(dhcp-config)#exit


MSL1(config)#ip dhcp pool VLAN20
MSL1(dhcp-config)#network 192.168.20.0 255.255.255.0
```

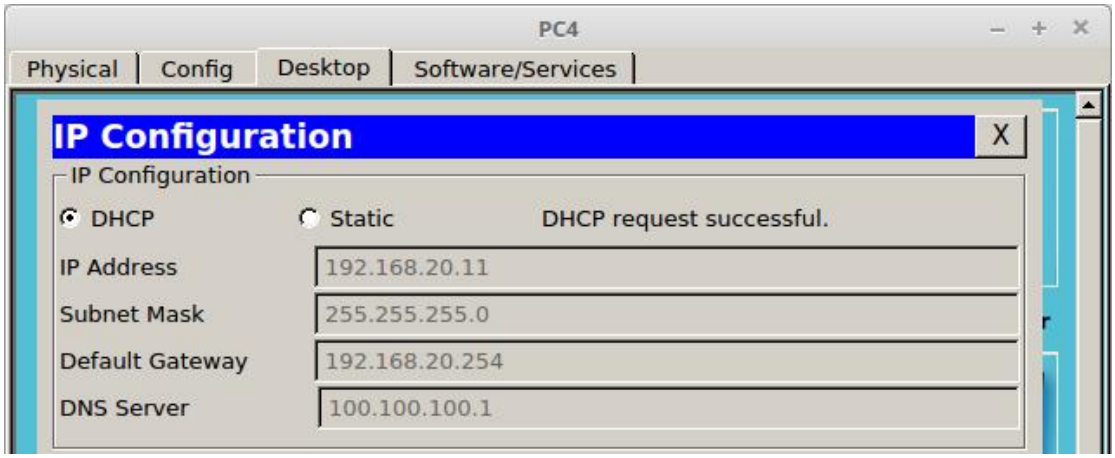
```
MSL1(dhcp-config)#dns-server 100.100.100.1
MSL1(dhcp-config)#default-router 192.168.20.254
MSL1(dhcp-config)#ex


MSL1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
MSL1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
```

VLAN10 dan VLAN20 hanya nama pool, bisa diberi nama apa saja. **Ip dhcp excuded-address** digunakan bilamana ada IP Address yang tidak ingin kita bagikan kepada Client. Pada perintah di atas tidak akan membagikan IP host dari 1 - 10.

Aktifkan DHCP Client pada Client



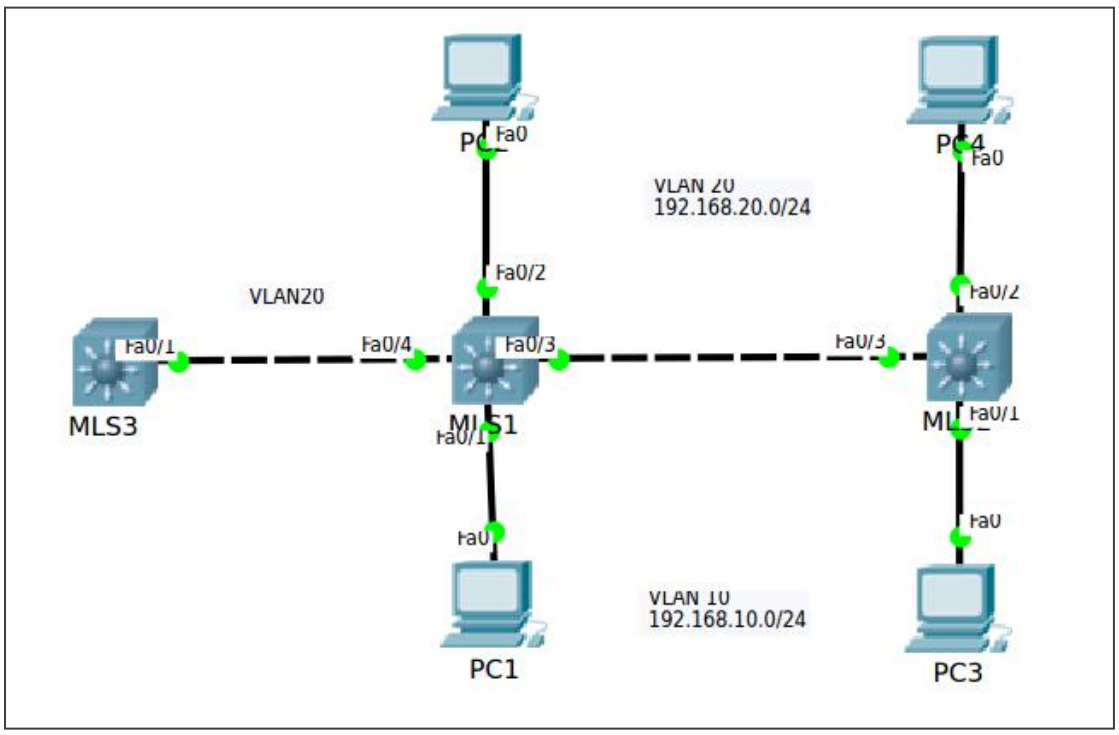
Gambar 9.2 DHCP Client pada PC1



Gambar 9.3 DHCP Client pada PC4

LAB 10 - Konfigurasi DHCP Client pada Switch atau Router

Misalkan ada DHCP Server yang dikonfigurasi pada jaringan dan kita ingin menggunakan DHCP Client pada switch ataupun router. Karena ini tentang switching, kita akan memakai Switch L3.



Gambar 10.1 Topologi DHCP Client

Ubah dulu interface fa0/4 agar menggunakan VLAN-20

```
MSL1(config)#int fa0/4
MSL1(config-if)#switchport mode acc
MSL1(config-if)#switch acc vlan 20
```

Konfigurasi DHCP Client pada MLS3

```
MLS3(config)#interface fa0/1
MLS3(config-if)#no switchport
MLS3(config-if)#ip address dhcp
```

No switchport digunakan untuk mengaktifkan fitur L3 agar bisa menggunakan IP Address

Dan jika sudah mendapat IP Address akan ada log seperti berikut

```
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned DHCP address 192.168.20.12, mask 255.255.255.0, hostname MLS3
```

Dan bisa juga check dengan perintah **show ip interface brief**

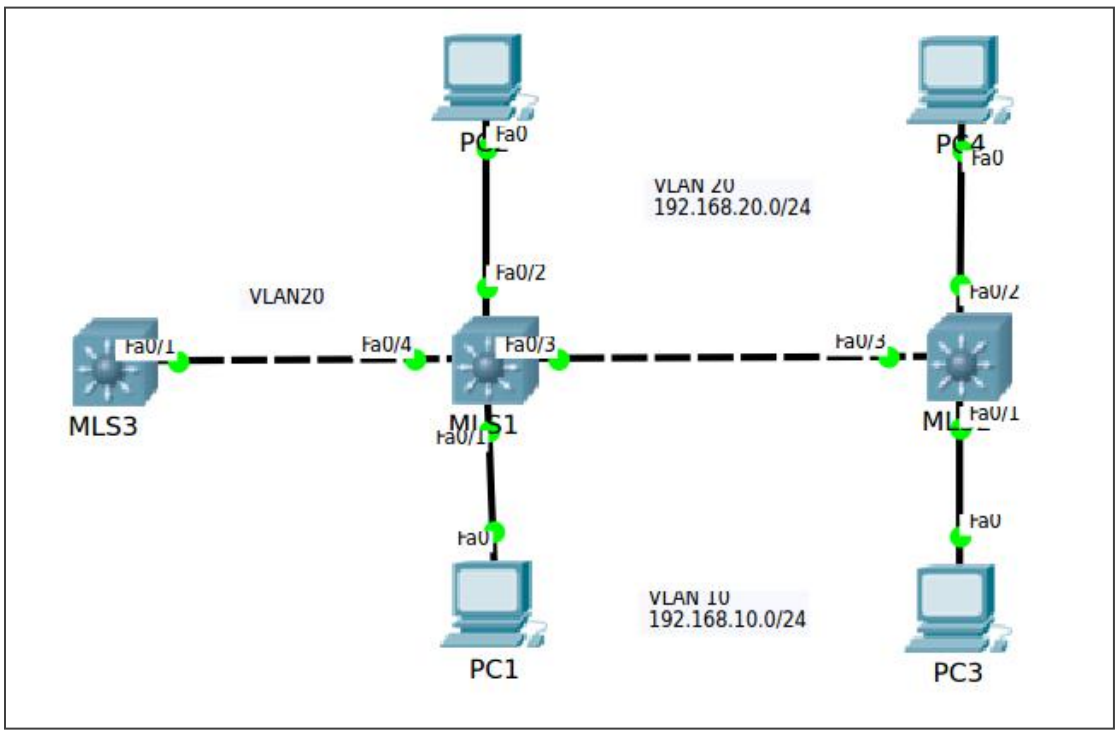
```
MLS3#show ip int br
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 192.168.20.12 YES DHCP up up
FastEthernet0/2 unassigned YES unset down down
```

Bisa lakukan test ping ke PC1

```
MLS3#ping 192.168.10.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

LAB 11 - Telnet pada Switch atau Router.

Untuk konfigurasi telnet pada switch dan router sama saja. Hanya berbeda pada pemasangan IP Address saja. Jika di switch pada Interface VLAN sedangkan di router pada interface Physical.



Gambar 11.1 Topologi Telnet

Melanjutkan konfigurasi pada lab sebelumnya. Kita akan konfigurasi Telnet pada MLS1 dan membuat VLAN30 sebagai remote-accessnya

```
MSL1(config)#vlan 30
MSL1(config-vlan)#name Remote-Access
MSL1(config-vlan)#ex


MSL1(config)#int vlan 30
MSL1(config-if)#ip add 30.30.30.30 255.255.255.0
MSL1(config-if)#ex


MSL1(config)#enable secret 123
```

```
MSL1(config)#line vty 0 4
MSL1(config-line)#password feri
```

Enable secret untuk mengkonfigurasi password pada saat masuk ke mode privileged. **Line vty 0 4** akan membuat telnet dengan 5 user aktif sekaligus (0-4) **password** untuk password telnetnya.

Test ping

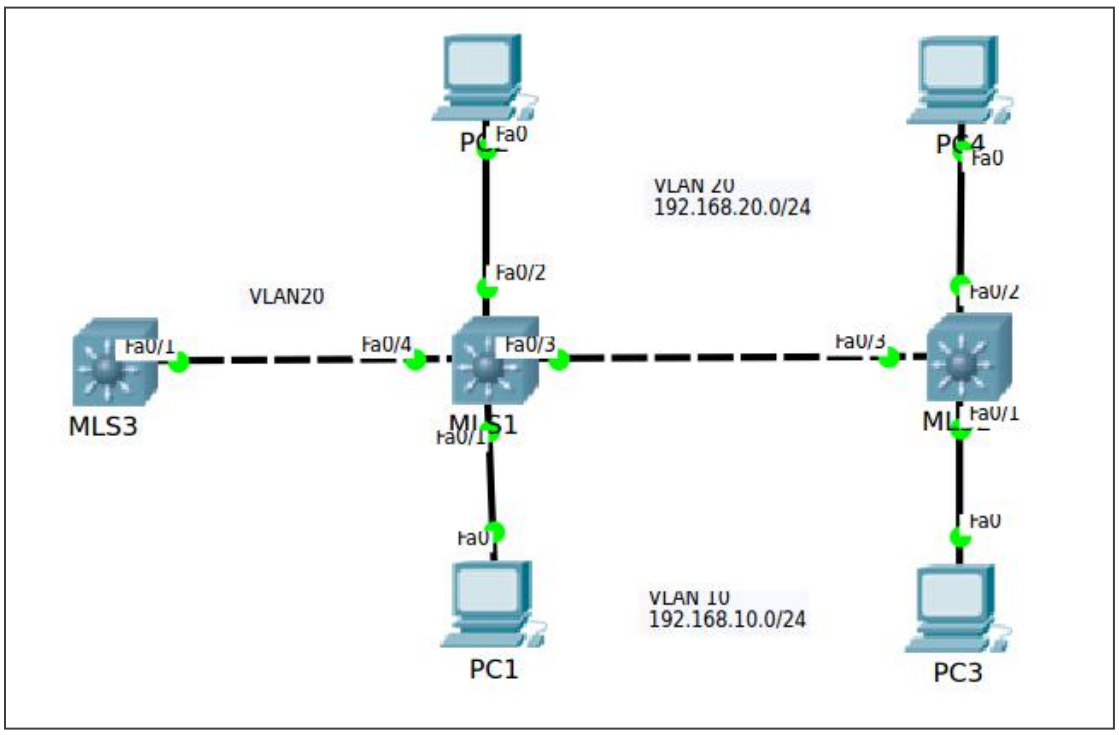
```
PC>ping 30.30.30.30
Pinging 30.30.30.30 with 32 bytes of data:

Reply from 30.30.30.30: bytes=32 time=1ms TTL=255
Reply from 30.30.30.30: bytes=32 time=0ms TTL=255
Reply from 30.30.30.30: bytes=32 time=0ms TTL=255
Reply from 30.30.30.30: bytes=32 time=0ms TTL=255

Ping statistics for 30.30.30.30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Jika terhubung, Lakukan telnet ke 30.30.30.30

```
PC>telnet 30.30.30.30
Trying 30.30.30.30 ...Open
User Access Verification
Password: (feri)
MSL1>enable
Password: (123)
MSL1#show ip int br
Interface                  IP-Address      OK? Method  Status
Protocol
FastEthernet0/1       unassigned      YES unset  up                    up

FastEthernet0/2       unassigned      YES unset  up                    up
```

LAB 12 - SSH pada Switch atau Router

Telnet dan SSH digunakan untuk meremote device dengan menggunakan IP Address. Hanya saja bedanya SSH di encrypsi maka paket data yang berjalan tidak dapat dibaca.



Gambar 12.1 Topologi SSH

Menggunakan topologi sebelumnya. Kita atur SSH pada MLS1.

```
MSL1(config)#username SSH password feri
MSL1(config)#ip domain name feri.idn
MSL1(config)#crypto key generate rsa


The name for the keys will be: MSL1.feri.idn
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
```

```
How many bits in the modulus [512]: 512

% Generating 512 bit RSA keys, keys will be non-exportable...[OK]


MSL1(config)#line vty 0 4

*Mar 1 2:55:4.502:  RSA key size needs to be at least 768 bits for ssh version
2

*Mar 1 2:55:4.502:  %SSH-5-ENABLED: SSH 1.5 has been enabled


MSL1(config-line)#transport input ssh

MSL1(config-line)#login local
```

Buat terlebih dahulu login dan passwordnya. Lalu harus mengganti domainnya. **Transport input** akan mengubah yang awalnya telnet menjadi SSH

Test remote dari CLient PC

PC>**ssh -l SSH 30.30.30.30**

Open

Password: (*feri)*

MSL1>**en**

Password: (*123*)

MSL1#**show ip int br**

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

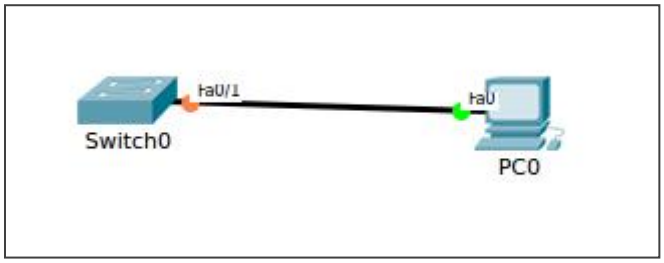
ssh -l *user ip-address server*

Dan jika kita menggunakan telnet, maka tidak akan bisa. Karena sudah diganti oleh SSH.

```
MSL1#telnet 30.30.30.30
Trying 30.30.30.30 ...Open


[Connection to 30.30.30.30 closed by foreign host]
```

LAB 13 - Spanning Tree Portfast

Pada saat mengkoneksikan kabel ke switch maka warnanya akan orange. Dari orange ke hijau ada proses yang memakan 50 detik, yaitu



Gambar 13.1 Spanning Tree Portfast

Blocking	---------->	Listening	---------->	Learning	--------->	Forwading
	20 sec		15 sec		15 sec	

Dan Ini digunakan proses antar switch. Dan jika mengarah ke Client tidak akan dibutuhkan, maka kita bisa percepat dengan portfast

```
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 5 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
```

Kita harus mengkonfigurasinya pada non-trunking mode saja. Jangan sampai mengkonfigurasinya pada mode trunk. Atau bisa menggunakan range

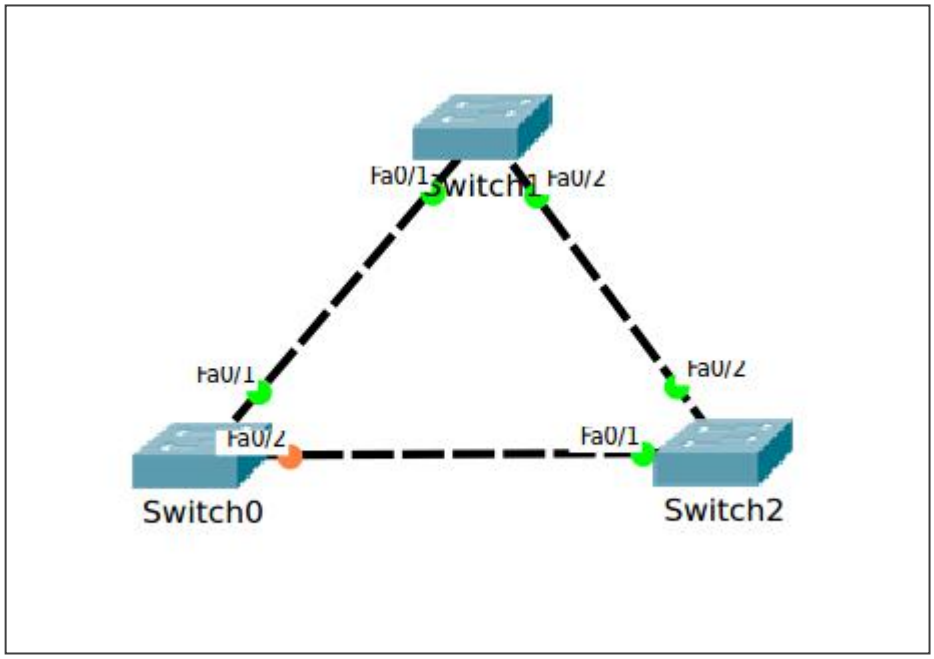
```
Switch(config)#interface range fa0/1-5
Switch(config-if-range)#spanning-tree portfast
```

```
Switch(config)#spanning-tree portfast default
```

port-fast default akan mengaktifkan portfast pada semua port interface

LAB 14 - Spanning Tree Protocol (PVST)

STP atau spanning tree protocol adalah protocol yang digunakan untuk mencegah looping pada switch. Karena switch jika tidak mengetahui paket data dikirim maka akan melakukan broadcasting, ke semua interface kecuali pengirim. Misal pada topologi di bawah ini



Gambar 14.1 Topologi STP

Misal ada paket data yang tidak diketahui oleh Switch 0, maka dia akan memberikannya ke Switch 1 misal, Lalu swtich satu bila tidak tahu akan memberikannya ke Switch 2 (fa0/2) dan bila switch2 tidak tau maka akan mengirimkan lagi ke Switch0, ini yang dinamakan looping.

Dengan mekanisme STP maka salah satu port akan di block. Tanpa kita konfigurasi juga, switch sudah menggunakan sistem ini. Bagaimana penentuan block ?

1. Pertama akan dilihat dari prioritynya yang terbesar akan di block
2. Dilihat dari Costnya yang terbesar akan di block
3. DIlihat dari Prio. NBR nya yang terbesar akan di block
4. Dilihat dari Mac-addressnya yang terbesar akan di block

```
Sw0#show spanning-tree

VLAN0001
```

```
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E5C.59DD
             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     00E0.B046.5B37
             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
```

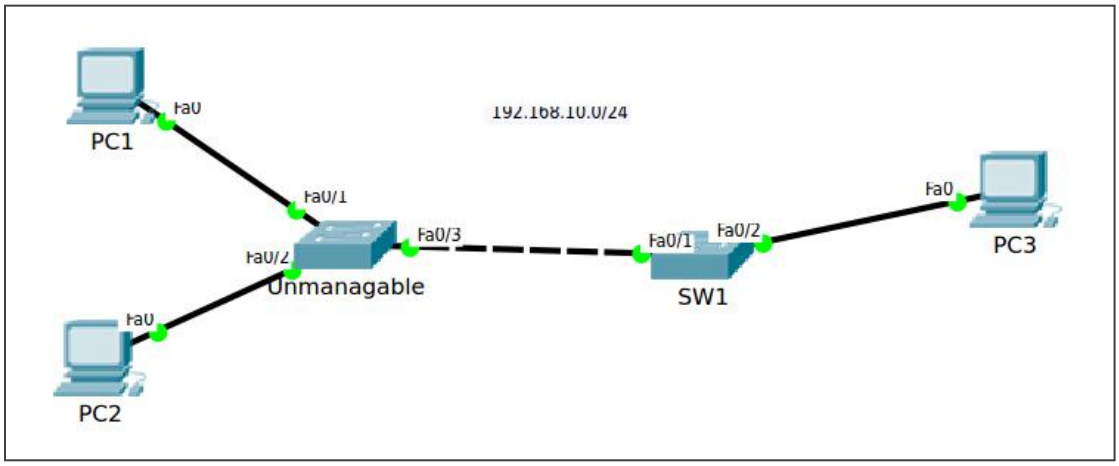
Jika dilihat pada topologi Sw0 lah yang di block karena memiliki Mac-address terbesar. Sekarang kita ganti prioritynya agar pada Sw0 tidak di block.

```
Sw0(config)#spanning-tree vlan 1 priority 409
% Bridge Priority must be in increments of 4096.
% Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440


Sw0(config)#spanning-tree vlan 1 priority 4096
```

Dan penentuan priority juga sudah ada standarnya. Sekarang liat lagi interface fa0/1 pada SW0 apakah mati atau tidak.

LAB 15 - Mengamankan Interface dengan port-security

Pada defaultnya switch tidak akan membatasi jumlah mac-address yang dipelajarin dalam suatu interface. Maka kita dapat mengkonfigurasi port-security untuk alasan keamanan



Gambar 15.1 Topologi Port-security

Port-security bisa digunakan untuk :

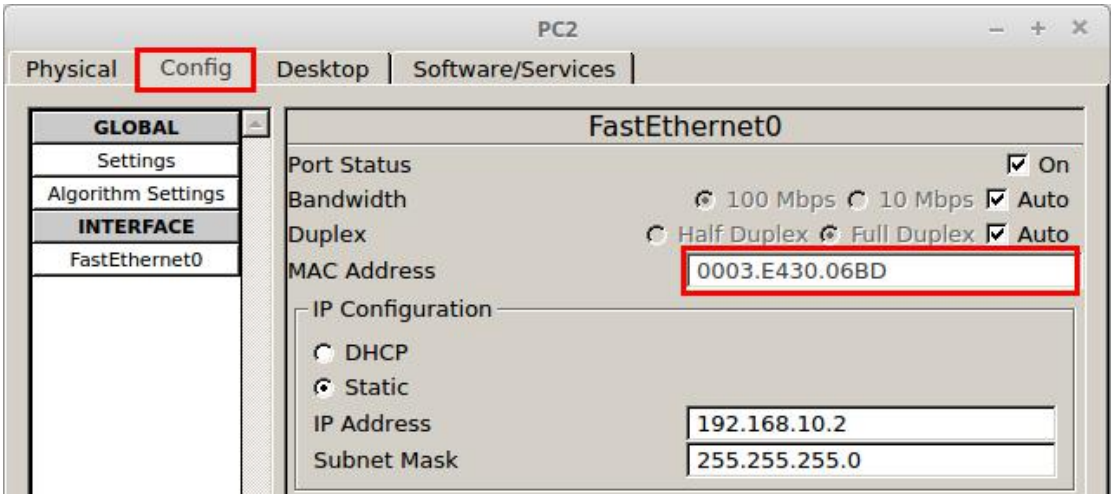
1. Membatasi Jumlah mac-address pada satu interface
2. Mengijinkan hanya Mac-address tertentu yang dapat menggunakan Tersebut.

Seperti topologi di atas. Kita memiliki unmanagable switch dan Managable switch (SW1). Misalkan kita hanya mengijinkan PC2 saja yang boleh terkoneksi dengan PC3. Maka kita akan membatasi hanya satu mac-address saja yang boleh melewati yaitu PC2. Sebelumnya konfigurasi IP Address pada semua PC. Lalu test ping dari PC1 ke PC3

```
PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=36ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128
```

```
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.10.3:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

Kita lihat terlebih dahulu Mac-address yang dimiliki PC2. Yaitu 0003.E430.06BD



Gambar 15.2 Mac-address pada PC2

Lalu konfigurasi port-security pada SW1

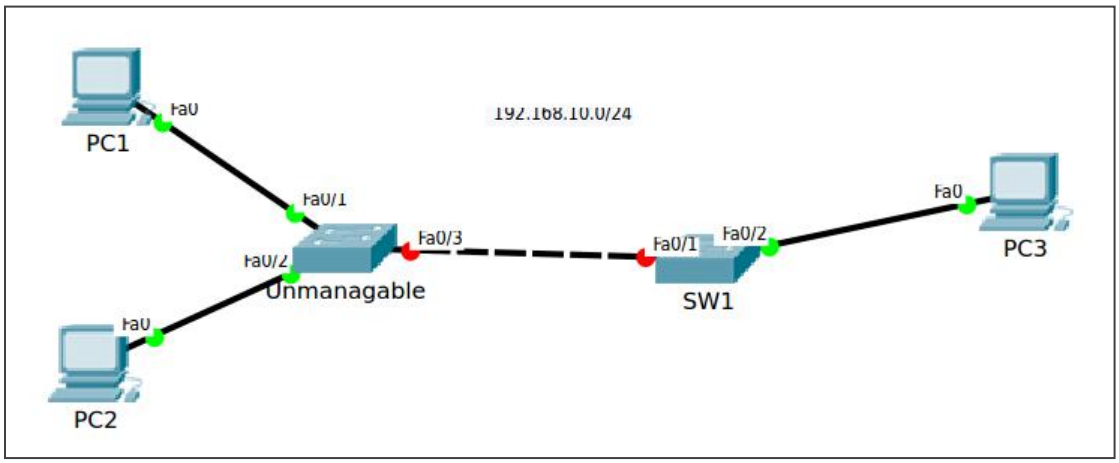
```
SW1(config)#int fa0/1

SW1(config-if)#swi mode acc

SW1(config-if)#switchport port-security

SW1(config-if)#swi port-secu max 2

SW1(config-if)#swi port-securi mac-address 0003.E430.06BD
```

Kita harus ubah terlebih dahulu ke mode accesss. Perintah **switchport port-security** digunakan untuk mengaktifkan fitur ini. Kita set max 2 mac-address yaitu **unmanagable** dan **PC2**. Dan Mac-addressnya PC2

Maka pada saat PC1 ping ke PC3 yang terjadi adalah

```
PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
```

```
Request timed out.

Request timed out.

Request timed out.


Ping statistics for 192.168.10.3:

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



Gambar 15.3 Interface fa0/1 dalam keadaan shutdown

Maka interfacenya mati, ini dikarenakan PC1 tidak diberi izin. Ada 3 mode violation (yang akan terjadi jika ada yang melanggar) :

```
SW1(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

1. Protect = Memblock tapi tidak mengirimkan messages
2. Restirce = Memblock tapi akan mengirimkan Messages
3. Shutdown = Akan men-*shutdown* interface.

Untuk menyalakannya ketik perintah

```
SW1(config)#int fa0/1
SW1(config-if)#shutdown
SW1(config-if)#no shutdown
```

Dan kita juga menkonfigurasi agar mac-addressnya secara otomatis

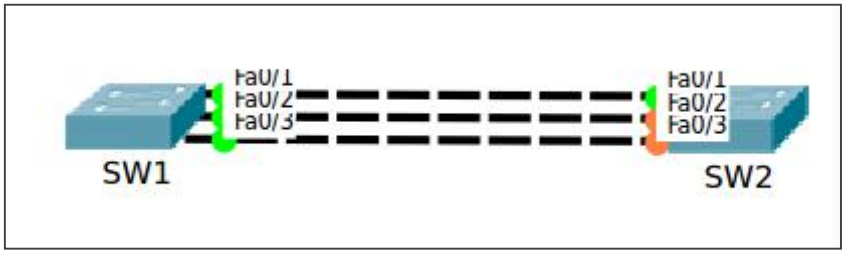
```
SW1(config-if)#switchport port-security mac-address sticky
```

LAB 16 - EtherChannel LaCP

Pada switch kita tidak dapat menggunakan beberapa kabel, karena mekanisme STP untuk mencegah looping. Kita bisa menggunakan Etherchannel. LaCP merupakan Open Standard

Ada 3 tipe etherchannel, yaitu :

1. L2 Etherchannel LaCP (Open Standard)
2. L2 Etherchannel PaGP (Cisco Proprietary)
3. L3 Etherchannel



Gambar 16.1 Topologi LACP

Seperti yang terlihat di atas metode STP akan hanya membolehkan satu interface saja yang aktif. Dengan metode Etherchannel, kita akan menggabungkan semua interfacenya menjadi satu.

Pada LACP modenya yaitu :

1. Active
2. Passive

Untuk konfigurasinya adalah

```
SW1(config)#interface range fa0/1-3
SW1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
SW1(config-if-range)#channel-protocol lacp
SW1(config-if-range)#exit


SW1(config)#interface port-channel 1
SW1(config-if)#switchport mode trunk
```

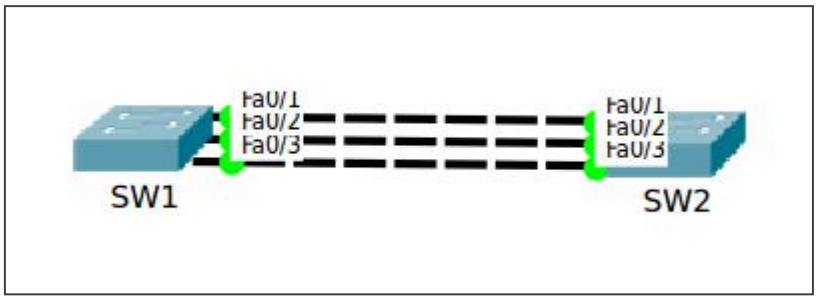
Pada SW2

```
SW2(config)#interface range fa0/1-3
```

```
SW2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
SW2(config-if-range)#channel-protocol lacp
SW2(config-if-range)#ex


SW2(config)#interface port-channel 1
SW2(config-if)#switchport mode trunk
```

Satu switch dengan mode **active** dan satunya lagi menggunakan **passive/active.** Tidak bisa menggunakan **passive-passive**

Setelah kita konfigurasi, nanti akan terbuat interface baru yaitu **port-channel 1** yang didapat dari **channel-group 1.** Interface inilah yang menjadi gabungan dari 3 interface di atas. Sekarang kabel sudah hijau semua.



Gambar 16.2 Setelah di konfigurasi LACP

Bisa juga mengcheck dengan perintah

```
SW1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

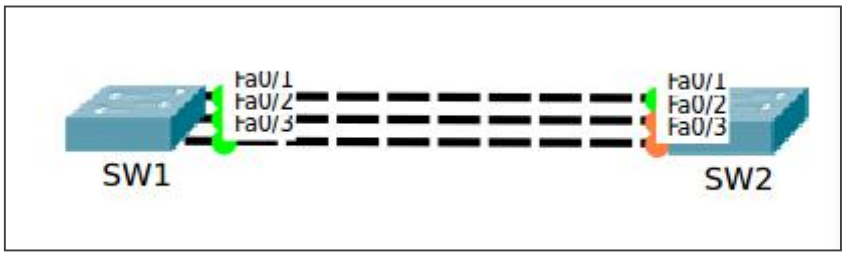
```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
----

1      Po1(SU)          LACP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

LAB 17 - Etherchannel PaGP

PaGP merupakan Cisco Proprietary. Dan pada PaGP menggunakan dua mode yaitu :

1. Auto
2. Desirable

Topologinya sama seperti sebelumnya.



Gambar 17.1 Topologi Etherchannel PaGP

```
SW1(config)#interface range fa0/1-3
SW1(config-if-range)#channel-group 1 mode desirable
SW1(config-if-range)#channel-protocol pagp
SW1(config-if-range)#ex

SW1(config)#int port-channel 1
SW1(config-if)#swi mode trunk
```

Pada SW2

```
SW2(config)#int range fa0/1-3
SW2(config-if-range)#channel-group 1 mode desirable
SW2(config-if-range)#channel-protocol pagp
SW2(config-if-range)#exit

SW2(config)#interface port-channel 1
SW2(config-if)#switc mode tru
```

Bisa menggunakan mode **Desirable-Desirable** atau **Desirable-auto**

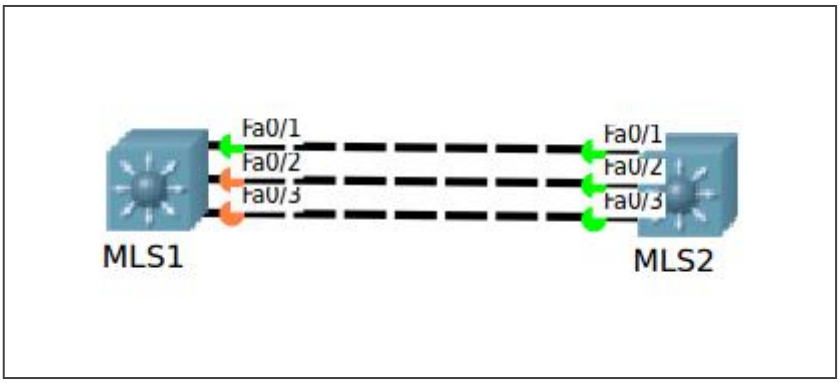
```
SW2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port



Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
----

1      Po1(SU)          PAgP   Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

LAB 18 - Static Etherchannel L3

Untuk konfigurasinya sama saja seperti pada Switch Layer 2, namun kali ini ktia akan menggunakan static etherchannel. Static etherchannel pada setiap interface harus memiliki mode yang sama. Misal, access maka access semua. Beberapa mode di Etherchannel

```
SW1(config-if-range)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
```

Topologi yang digunakan sama seperti sebelumnya



Gambar 18.1 Static Etherchannel

Konfigurasi nya pada MLS1

```
MLS1(config)#inter range fa0/1-3
MLS1(config-if-range)#no switchport
MLS1(config-if-range)#channel-group 1 mode on
MLS1(config-if-range)#ex

MLS1(config)#interface port-channel 1
MLS1(config-if)#no switchport
MLS1(config-if)#ip add 112.112.112.1 255.255.255.0
```

Konfigurasi pada MLS2

```
MLS1(config)#int range fa0/1-3
MLS1(config-if-range)#no switchport
MLS1(config-if-range)#channel-group 1 mode on
MLS1(config-if-range)#ex

MLS1(config)#interface port-channel 1
MLS1(config-if)#no switchport
MLS1(config-if)#ip add 112.112.112.2 255.255.255.0
```

Check Konfigurasinya

```
MLS1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port



Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
----

1      Po1(RU)          -      Fa0/1(P) Fa0/2(P) Fa0/3(P)
```

Coba lakukan ping

```
MLS1#ping 112.112.112.2


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 112.112.112.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

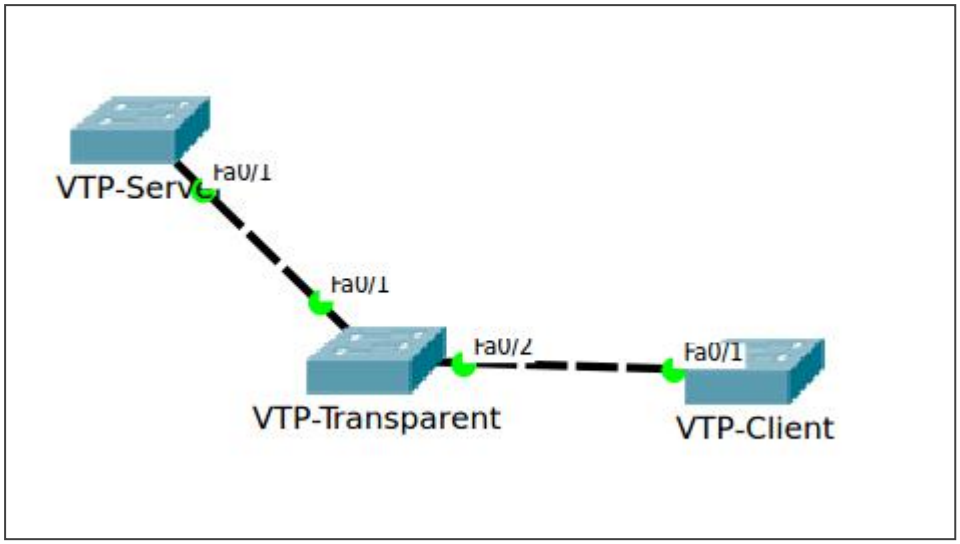
LAB 19 - VTP (VLAN Trunking Protocol)

VTP digunakan ketika kita memiliki banyak switch dan memilik VLAN yang sama. Kita hanya perlu mengkonfigurasi switch yang menjadi VTP Server maka switch client akan mengikuti VLANnya.

VTP ada 3 mode :

1. Server
2. Transparent
3. Client

Topologi yang akan digunakan seperti berikut



Gambar 19.1 Topologi VTP

Konfigurasi pada tiap tiap Switch

```
VTP-Server(config)#int fa0/1
VTP-Server(config-if)#swi mode trunk
VTP-Server(config-if)#ex

VTP-Server(config)#vtp mode server
VTP-Server(config)#vtp domain idn.id
VTP-Server(config)#vtp password 123
```

VTP-Transparent

```
VTP-Transparent(config)#interface range fa0/1-2
VTP-Transparent(config-if-range)#switch mode trunk
VTP-Transparent(config-if-range)#exit

VTP-Transparent(config)#vtp mode transparent
VTP-Transparent(config)#vtp domain idn.id
VTP-Transparent(config)#vtp password 123
```

VTP-Client

```
VTP-Client(config)#int fa0/1
VTP-Client(config-if)#switch mode trunk
VTP-Client(config-if)#exit

VTP-Client(config)#vtp mode client
VTP-Client(config)#vtp domain idn.id
VTP-Client(config)#vtp password 123
```

Lihat terlebih dahulu VLAN yang berada di VTP-Client

```
VTP-Client#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                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
1002 fddi-default                     active
1003 token-ring-default               active
```

Belum ada Vlan apapun, sekarang kita tambahkan VLAN pada VTP-Server

```
VTP-Server(config)#vlan 10
VTP-Server(config-vlan)#name IT-Consultan
```

Coba kita lihat lagi VLAN pada VTP-Client

```
VTP-Client#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                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   IT-Consultan                     active
```

Dan jika di lihat pada VTP-Transparent.

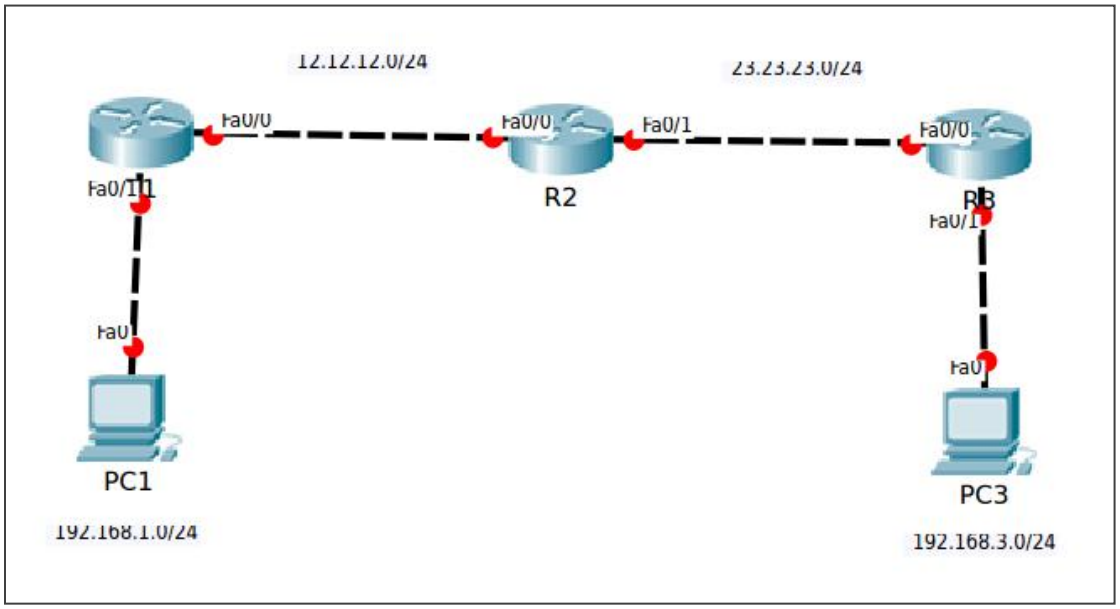
```
VTP-Transparent#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
```

The Alchemy of ROUTING

LAB 20 - Static Routing

Dalam mengirim paket data, melihat dari routing tabelnya. Dengan mengkonfigurasi static route. Kita akan menambahkan secara manual ke routing tabelnya.

Static route adalah routing yang di tentukan secara manual oleh Network Administrator ke dalam router. Menentukan network tujuan dan bagaimana jalur menuju network tersebut. Prinsip nya adalah **Mau Kemana Lewat Mana**



Gambar 20.1 Topologi Static Route

Kita akan menggunakan Loopback sebagai Clientnya. Konfigurasi IP Address

```
R1(config)#int fa0/0
R1(config-if)#no shut
R1(config-if)#ip add 12.12.12.1 255.255.255.0


R1(config)#int fa0/1
R1(config-if)#no sh
R1(config-if)#ip add 192.168.1.254 255.255.255.0
```

R2

```
R2(config)#int fa0/0
R2(config-if)#no sh
```

```
R2(config-if)#ip add 12.12.12.2 255.255.255.0


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

R3

```
R3(config)#int fa0/0
R3(config-if)#no sh
R3(config-if)#ip add 23.23.23.3 255.255.255.0


R3(config)#int fa0/1
R3(config-if)#no sh
R3(config-if)#ip add 192.168.3.254 255.255.255.0
```

Sekarang coba kita lihat routing tabel pada Router R1.

```
R1#show ip route
Gateway of last resort is not set


     12.0.0.0/24 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
```

Router R1, R2 dan R3 hanya memiliki network yang directly connected saja. Dan tidak mengetahui network yang lainnya. Maka ketika Client R1 ping ke Client R3 tidak akan bisa.

```
PC>ping 192.168.3.3


Pinging 192.168.3.3 with 32 bytes of data:


Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Request timed out.
```

```
Reply from 192.168.1.254: Destination host unreachable.
```

Lalu kita konfigurasi routing static pada semua router. Formatnya adalah

Ip route *network-tujuan netmask-tujuan next-hop-address*

Next-hop bisa menggunakan IP address atau interface out-nya

R1

```
R1(config)#ip route 23.23.23.0 255.255.255.0 12.12.12.2
R1(config)#ip route 192.168.3.0 255.255.255.0 fa0/0
```

R2

```
R2(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
R2(config)#ip route 192.168.3.0 255.255.255.0 23.23.23.3
```

R3

```
R3(config)#ip route 12.12.12.0 255.255.255.0 23.23.23.2
R3(config)#ip route 192.168.1.0 255.255.255.0 23.23.23.2
```

Static route harus di konfigurasi pada semua router. Sekarang kita akan melihat routing tabel kembali.

```
R1#show ip route
Gateway of last resort is not set

     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
S       23.23.23.0 [1/0] via 12.12.12.2
C    192.168.1.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Sekarang network dari client R3 sudah ada coba lakukan test ping lagi

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
```

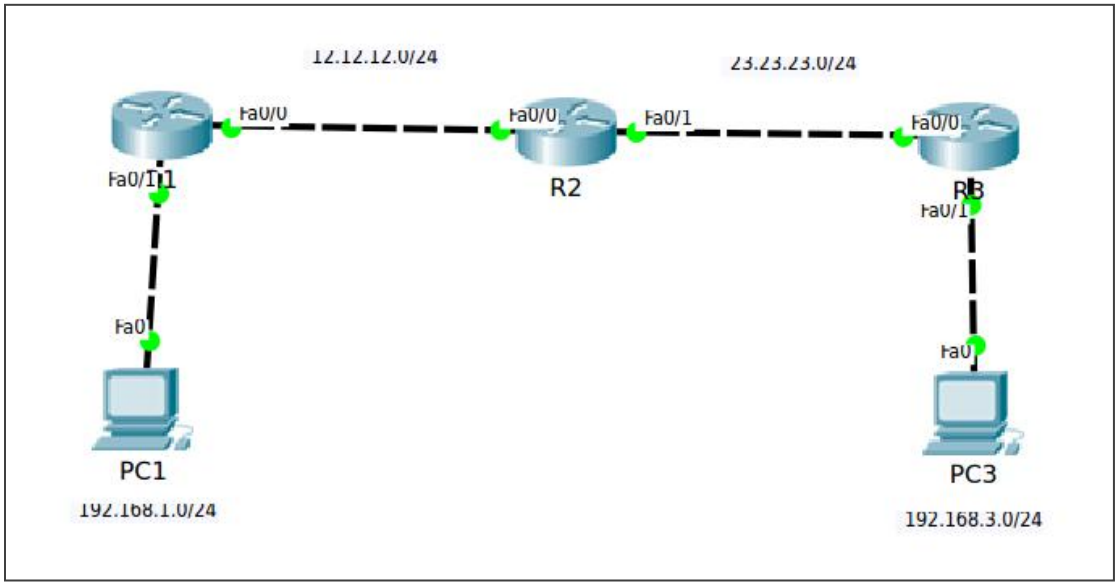
```
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Reply from 192.168.3.3: bytes=32 time=1ms TTL=125

Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Reply from 192.168.3.3: bytes=32 time=0ms TTL=125


Ping statistics for 192.168.3.3:

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

Approximate round trip times in milli-seconds:

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

Begitu juga pada PC3 sudah dapat terhubung ke PC1

```
PC>ping 192.168.1.1


Pinging 192.168.1.1 with 32 bytes of data:


Reply from 192.168.1.1: bytes=32 time=1ms TTL=125

Reply from 192.168.1.1: bytes=32 time=0ms TTL=125

Reply from 192.168.1.1: bytes=32 time=0ms TTL=125

Reply from 192.168.1.1: bytes=32 time=0ms TTL=125


Ping statistics for 192.168.1.1:

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

Approximate round trip times in milli-seconds:

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

LAB 21 - Basic Config EIGRP

Dynamic Routing protocol, akan memasukkan secara otomasi routing ke routing tabel. Salah satunya adalah EIGRP. EIGRP merupakan protocol routing yang termasuk dalam Distance Vector dan merupakan Cisco Proprietary.



Gambar 21.1 Topologi Routing EIGRP

Melanjutkan konfigurasi pada lab sebelumnya. Hapus terlebih dahulu konfigurasi static routing pada ketiga router.

R1

```
R1(config)#no ip route 23.23.23.0 255.255.255.0 12.12.12.2
R1(config)#no ip route 192.168.3.0 255.255.255.0 fa0/0
```

R2

```
R2(config)#no ip route 192.168.1.0 255.255.255.0 12.12.12.1
R2(config)#no ip route 192.168.3.0 255.255.255.0 23.23.23.3
```

R3

```
R3(config)#no ip route 12.12.12.0 255.255.255.0 23.23.23.2
R3(config)#no ip route 192.168.1.0 255.255.255.0 23.23.23.2
```

Kita lihat routing tabel pada R1, sekarang tinggal direclty connected saja.

```
R1#show ip route


Gateway of last resort is not set


     12.0.0.0/24 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
```

Sekarang konfigurasi **router eigrp** dengan **AS 123**. Dan perlu di ingat Biar bisa adjacency AS harus sama.

R1

```
R1(config)#router eigrp 123
R1(config-router)#no auto-summary


R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 12.12.12.0 0.0.0.255
R1(config-router)#passive-interface fa0/1
```

R2

```
R2(config)#router eigrp 123
R2(config-router)#no auto-summary


R2(config-router)#network 12.12.12.0 0.0.0.255
R2(config-router)#network 23.23.23.0 0.0.0.255
```

R3

```
R3(config)#router eigrp 123
R3(config-router)#no auto-summary


R3(config-router)#network 192.168.3.0 0.0.0.255
R3(config-router)#network 23.23.23.0 0.0.0.255
R3(config-router)#passive-interface fa0/1
```

Beberapa keterangan di atas :

1. **Router eigrp 123** : Mengaktifkan routing eigrp dengan AS-123
2. **No auto-summary** : Menonaktifkan fitur auto-summary
3. **Network** : Menadvertise network. 0.0.0.255 (Merupakan wild-card mask
4. **Passive-interface** : Tidak mengirimkan hello packet ke interface

Passive-interface ini digunakan ketika kita menadvertise network client, sedangkan client tidak membutuhkan hello packet.

Setelah di konfigurasi, sekarang lihat lagi routing tabelnya

```
R1#show ip route


Gateway of last resort is not set


     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
D       23.23.23.0 [90/30720] via 12.12.12.2, 00:09:45, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
D    192.168.3.0/24 [90/33280] via 12.12.12.2, 00:08:50, FastEthernet0/0
```

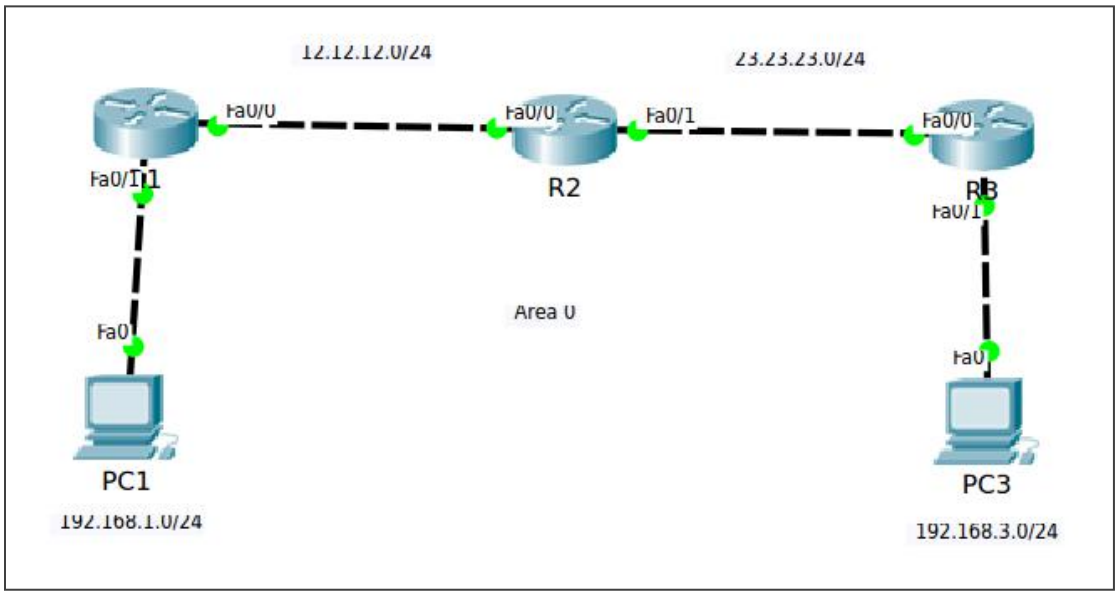
Tanda D menandakan Dual (EIGRP). **90** Merupakan **AD**(Administrative Distance). Sedangkan **30720** merupakan metric pada EIGRP.

Sekarang kita ping ke PC3

```
PC>ping 192.168.3.3


Pinging 192.168.3.3 with 32 bytes of data:


Reply from 192.168.3.3: bytes=32 time=1ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
```

LAB 22 - Basic Config OSPF - Backbone Area

OSPF merupakan Dynamic Routing juga, dan termasuk ke dalam Link State Protocol. OSPF menggunakan Cost sebagai metric atau penentuan best-path nya.



Gambar 22.1 Topologi Backbone Area

Pada OSPF jika kita hanya menggunakan satu area, maka area yang harus ada adalah Area 0. Area 0 ini di kenal juga dengan Backbone Area.

Melanjutkan konfigurasi pada lab sebelumnya. Hapus terlebih dahulu konfigurasi EIGRP pada Router R1,R2 dan R3

```
R1(config)#no router eigrp 123


R2(config)#no router eigrp 123


R3(config)#no router eigrp 123
```

Setelah itu kita lihat routing tabel nya, maka hanya tinggal directly connected saja.

```
R1#show ip route
```

```
Gateway of last resort is not set


     12.0.0.0/24 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
```

Sekarang kita konfigurasi OSPF dengan menggunakan Area 0 pada semua router

R1

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

R2

```
R2(config)#router ospf 2
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
```

R3

```
R3(config)#router ospf 3
R3(config-router)#network 23.23.23.0 0.0.0.255 area 0
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

Beberapa keterangan di atas :

1. Router ospf 1 : Mengaktifkan fitur OSPF dengan proccess-id 1
2. Process-id : Boleh berbeda pada masing-masing router.
3. Network : Menadvetise network dengan wild-card mask
4. Area : Menentukan network tersebut ikut dengan area berapa

Bisa kita lihat neighbornya dengan perintah

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
23.23.23.2      1   FULL/BDR        00:00:37    12.12.12.2      FastEthernet0/0
```

Sudah adjacency sekarang kita lihat lagi routing tabelnya.

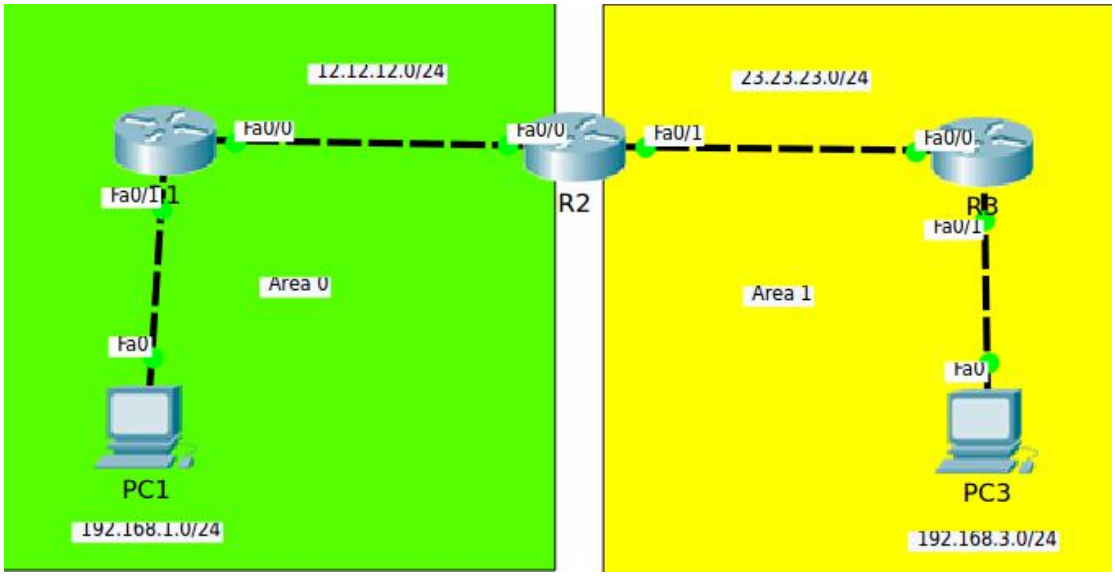
```
R1#show ip route

Gateway of last resort is not set

     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
O       23.23.23.0 [110/2] via 12.12.12.2, 00:15:58, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
O    192.168.3.0/24 [110/3] via 12.12.12.2, 00:14:02, FastEthernet0/0
```

Sudah ada dengan tanda **O** yang berarti OSPF. 110 merupakan AD dari OSPF. 2 atau 3 merupakan metric atau cost yang digunakan.

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=1ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

LAB 23 - Multi Area OSPF

Jika pada sebelumnya kita hanya mengkonfigurasi satu area saja. Sekarang kita akan mengkonfigurasi dengan dua area yang berbeda. Topologinya seperti berikut



Gambar 23.1 Topologi Multi Area OSPF

Kita akan membuat dua Area yaitu Area 0 dan Area 1. Area 0 harus ada karena merupakan backbone area. Hapus konfigurasi OSPF area 0 pada R3 dan R2.

R2

```
R2(config)#router ospf 2
R2(config-router)#no network 23.23.23.0 0.0.0.255 area 0
```

R3

```
R3(config)#no router ospf 3
```

Lalu kita konfigurasi lagi agar menggunakan Area 1

R2

```
R2(config)#router ospf 2
R2(config-router)#network 23.23.23.0 0.0.0.255 area 1
```

R3

```
R3(config)#router ospf 3
```

```
R3(config-router)#network 23.23.23.0 0.0.0.255 area 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 1
```

Maka jika kita lihat routing tabel pada R1

```
R1#show ip route
Gateway of last resort is not set
     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
O IA    23.23.23.0 [110/2] via 12.12.12.2, 00:13:06, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
O IA 192.168.3.0/24 [110/3] via 12.12.12.2, 00:01:09, FastEthernet0/0
```

Tanda **IA** berarti Inter Area, ini merupakan route yang di dapat dari area yang berbeda. R1 menggunakan Area 0 maka network 23.23.23.0 dan 192.168.3.0 menggunakan Area 1.

Sedangkan jika kita lihat pada R2

```
R2#show ip route
Gateway of last resort is not set
     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
C       23.23.23.0 is directly connected, FastEthernet0/1
O    192.168.1.0/24 [110/2] via 12.12.12.1, 02:12:11, FastEthernet0/0
O    192.168.3.0/24 [110/2] via 23.23.23.3, 00:13:08, FastEthernet0/1
```

Coba lakukan test ping ke PC3

```
PC>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
```

```
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
```

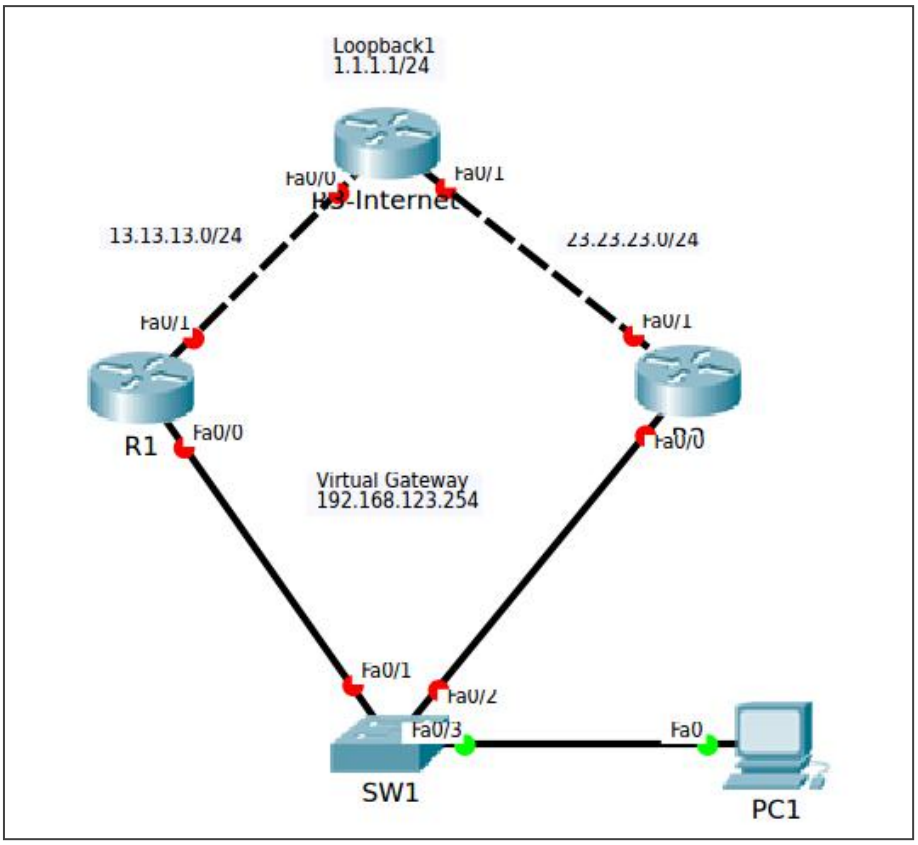
LAB 24 - HSRP (Fail-Over)

Pada koneksi ke internet kita harus memiliki backup link. Karena jika tidak, maka pada saat kabel utama putus, semua jaringan akan terputus. Ini dinamakan dengan high availlability.

Ada 3 metode yang dapat di gunakan pada high availability :

1. HSRP
2. VRRP
3. GLBP

HSRP singakatan dari Hot Standby Router Protocol. HSRP merupakan cisco proprietary. HSRP akan memakai satu link dan bila gagal akan digantikan dengan backup link (Fail-Over) Buat topologi seperti berikut.



Gambar 24.1 Topologi HSRP

Cara kerjanya adalah kedua router akan membuat IP virtual-gateway terlebih dahulu yang akan digunakan untuk Client. Pemilihan jalur yang digunakan adalah dilihat dari IP address terkeclinya. Konfigurasi IP Address

dan routing IGP (OSPF atau EIGRP). Kali ini kita akan menggunakan EIGRP dengan AS-123

```
R1(config)#int fa0/0
R1(config-if)#no sh
R1(config-if)#ip add 192.168.123.1 255.255.255.0

R1(config-if)#int fa0/1
R1(config-if)#no sh
R1(config-if)#ip add 13.13.13.1 255.255.255.0

R1(config)#router eigrp 123
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.123.0
R1(config-router)#network 13.13.13.0
```

R2

```
R2(config)#int fa0/0
R2(config-if)#no sh
R2(config-if)#ip add 192.168.123.2 255.255.255.0

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

R2(config)#router eigrp 123
R2(config-router)#no auto-summary
R2(config-router)#network 23.23.23.0
R2(config-router)#network 192.168.123.0
```

R3

```
R3-Internet(config)#int fa0/0
R3-Internet(config-if)#no sh
```

```
R3-Internet(config-if)#ip add 13.13.13.3 255.255.255.0


R3-Internet(config-if)#int fa0/1
R3-Internet(config-if)#no sh
R3-Internet(config-if)#ip add 23.23.23.3 255.255.255.0


R3-Internet(config-if)#int lo1
R3-Internet(config-if)#ip add 1.1.1.1 255.255.255.0
R3-Internet(config-if)#ex


R3-Internet(config)#router eigrp 123
R3-Internet(config-router)#no auto-summary
R3-Internet(config-router)#network 0.0.0.0
```

Setelah mengkonfigurasi IP Address dan EIGRP. Sekarang kita akan konfigurasi HSRP.

R1

```
R1(config)#int fa0/0
R1(config-if)#standby 1 ip 192.168.123.254
R1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby


%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
```

R2

```
R2(config)#int fa0/0
R2(config-if)#standby 1 ip 192.168.123.254
R2(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
```

Yang active adalah R1 sedangkan jalur R2 digunakan untuk backup link. Check konfigurasi

```
R1#show standby brief
```

```
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State    Active    Standby         Virtual IP
Fa0/0       1    100   Active   local     192.168.123.2   192.168.123.254
```

Coba kita test tracert pada Client

```
PC>tracert 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops:


1 1 ms 0 ms 0 ms 192.168.123.1

2 0 ms 0 ms 1 ms 1.1.1.1


Trace complete.
```

Misal kita ingin ubah agar jalur menggunakan R2. Ubah prioritynya menjadi lebih besar. Defaultnya adalah 100

```
R1(config)#int fa0/0

R1(config-if)#standby 1 preempt
```

R2

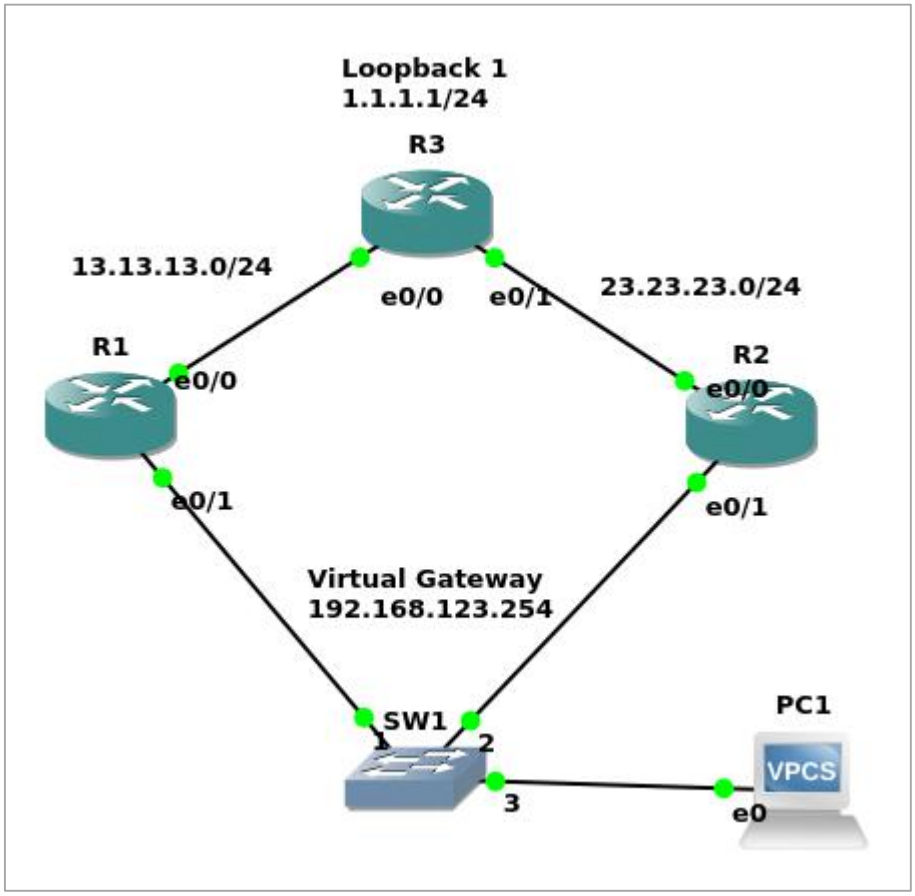
```
R2(config)#int fa0/0

R2(config-if)#standby 1 priority 110

R2(config-if)#standby 1 preempt
```

Perintah preempt digunakan agar mempercepat proses pemindahan link. Test lagi dengan menggunakan trace

```
PC>tracert 1.1.1.1


Tracing route to 1.1.1.1 over a maximum of 30 hops:


1 1 ms 0 ms 0 ms 192.168.123.2

2 0 ms 0 ms 0 ms 1.1.1.1


Trace complete.
```

LAB 25 - VRRP (Fail-Over)

VRRP konsepnya sama saja seperti HSRP bedanya hanya saja VRRP merupakan open standart sedangkan HSRP cisco proprietary. Karena pada **Cisco Packet Tracer** tidak mendukung fitur VRRP, maka kali ini kita akan menggunakan GNS3. Topologi yang akan digunakan



Gambar 25.1 Topologi VRRP

Konfigurasi IP Address dan EIGRP pada semua router dengan menyamakan konfigurasi pada lab sebelumnya. Namun pada VPCS, konfigurasi IP Addressnya seperti berikut

```
PC1> ip 192.168.123.10/24 192.168.123.254
Checking for duplicate address...
PC1 : 192.168.123.10 255.255.255.0 gateway 192.168.123.254
```

Konfigurasi VRRP sama HSRP sama persis hanya beda protocol saja. Konfigurasinya seperti berikut

R1

```
R1(config-if)#vrrp 1 ip 192.168.123.254
R1(config-if)#
*Dec  3 17:43:31.323: %VRRP-6-STATECHANGE: Et0/1 Grp 1 state Init -> Backup
R1(config-if)#
*Dec  3 17:43:34.939: %VRRP-6-STATECHANGE: Et0/1 Grp 1 state Backup -> Master
R1(config-if)#
*Dec  3 17:43:58.279: %VRRP-6-STATECHANGE: Et0/1 Grp 1 state Master -> Backup
```

R2

```
R2(config-if)#vrrp 1 ip 192.168.123.254
R2(config-if)#
*Dec  3 17:43:53.479: %VRRP-6-STATECHANGE: Et0/1 Grp 1 state Init -> Backup
R2(config-if)#
*Dec  3 17:43:57.095: %VRRP-6-STATECHANGE: Et0/1 Grp 1 state Backup -> Master
```

Dari konfigurasi di atas kita bisa melihat log nya. R2 menjadi Master sedangkan R1 menjadi Backup. Sama seperti HSRP tinggal kita ubah saja prioritynya

R1

```
R1(config-if)#vrrp 1 priority 110
R1(config-if)#vrrp 1 preempt
```

R2

```
R2(config-if)#vrrp 1 preempt
```

Verifikasi dengan melihat vrrp briefnya

R1

```
R1#show vrrp brief
Interface      Grp Pri Time  Own Pre State   Master addr     Group addr
Et0/1           1   110 3570      Y  Master  192.168.123.1   192.168.123.254
```

R2

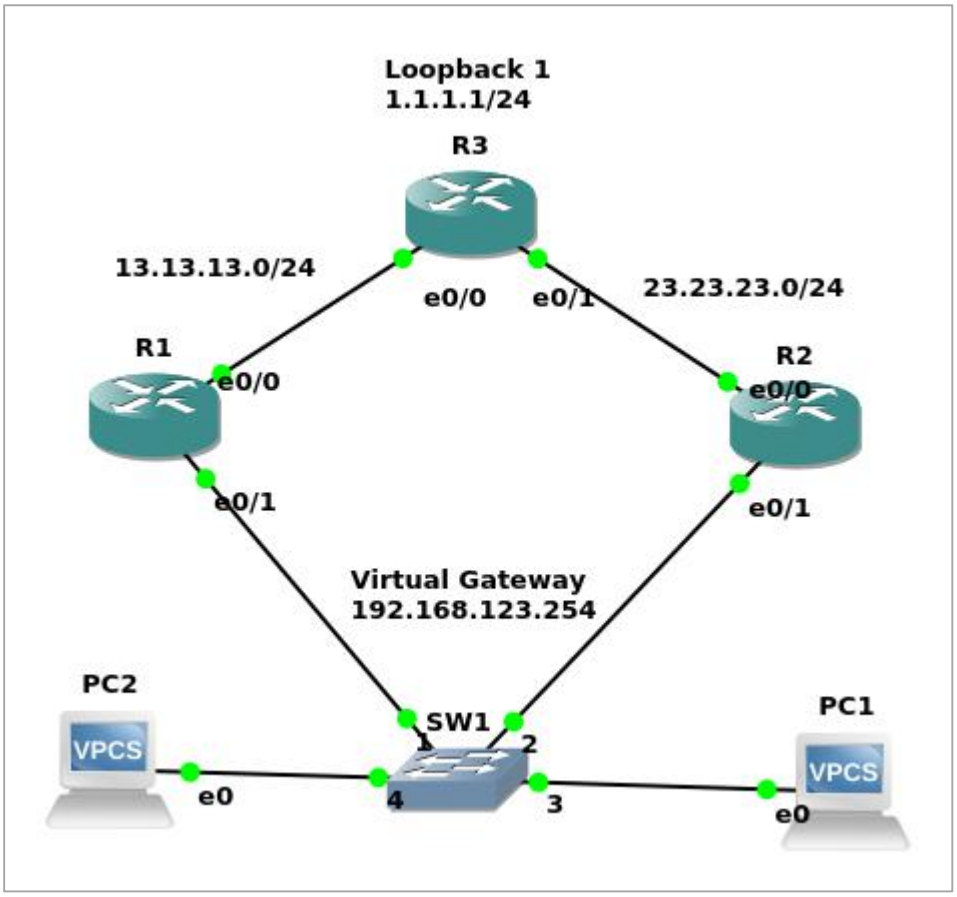
```
R2#show vrrp brief
Interface     Grp Pri Time  Own Pre State   Master addr     Group addr
Et0/1          1   100 3609      Y  Backup  192.168.123.1   192.168.123.254
```

Sekarang yang menjadi master adalah R1. Kita dapat verifikasi dengan perintah trace

```
PC1> trace 1.1.1.1

trace to 1.1.1.1, 8 hops max, press Ctrl+C to stop

 1   192.168.123.1   75.962 ms  0.323 ms  0.238 ms

 2   1.1.1.1   30.776 ms  38.444 ms  3.078 ms
```

LAB 26 - GLBP (Load-Balancing)

Pada lab sebelumnya yaitu HSRP dan VRRP merupakan Fail-Over yaitu 1 link menjadi link utama sisanya akan menjadi backup saja. Pada GLBP kita akan melakukan Load Balancing. GLBP tidak di support juga di Cisco Packet Tracer jadi kita akan menggunakan GNS3. Topologinya menggunakan lab sebelumnya. Hanya ada tambahan 1 Client



Gambar 26.1 Topologi GLBP

Hapus terlebih dahulu konfigurasi VRRP pada R1 dan R2.

```
R1(config)#int eth0/1
R1(config-if)#no vrrp 1
```

```
R2(config)#int eth0/1
R2(config-if)#no vrrp 1
```

Setelah itu kita konfigurasi GLBP pada R1 dan R2

R1

```
R1(config-if)#glbp 1 ip 192.168.123.254
R1(config-if)#glbp 1 priority 110
R1(config-if)#glbp 1 preempt
R1(config-if)#
*Dec  3 18:06:27.443: %GLBP-6-STATECHANGE: Ethernet0/1 Grp 1 state Speak -> Active
R1(config-if)#
*Dec  3 18:06:38.015: %GLBP-6-FWDSTATECHANGE: Ethernet0/1 Grp 1 Fwd 1 state Listen -> Active
```

R2

```
R2(config-if)#glbp 1 ip 192.168.123.254
R2(config-if)#glbp 1 preempt
R2(config-if)#
*Dec   3 18:06:38.019: %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "IP I
nput", ipl= 0, pid= 76,   -Traceback= 0x816F13Bz 0xA728AD3z 0x9430615z 0x9430532z
R2(config-if)#
*Dec  3 18:06:51.667: %GLBP-6-FWDSTATECHANGE: Ethernet0/1 Grp 1 Fwd 2 state Listen -> Act
ive
```

Kita akan mengkonfigurasi agar R1 yang menjadi pemberi AVG (ARP ke Client).

Verifikasi dengan menggunakan GLBP brief

R1

```
R1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Et0/1       1    -   110 Active   192.168.123.254 local           192.168.123.2
Et0/1       1    1   -   Active   0007.b400.0101  local           -
Et0/1       1    2   -   Listen   0007.b400.0102  192.168.123.2   -
```

R2

```
R2#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby
router
Et0/1       1    -   100 Standby  192.168.123.254 192.168.123.1   local
Et0/1       1    1   -   Listen   0007.b400.0101  192.168.123.1   -
Et0/1       1    2   -   Active   0007.b400.0102  local           -
```

Sekarang kita trace dari kedua client secara bersamaan. Maka hasilnya adalah

PC1

```
PC1> trace 1.1.1.1
trace to 1.1.1.1, 8 hops max, press Ctrl+C to stop
 1   192.168.123.1   0.660 ms  0.551 ms  0.586 ms
 2   *13.13.13.3   1.036 ms (ICMP type:3, code:3, Destination port unreachable)
```

PC2

```
PC2> trace 1.1.1.1
trace to 1.1.1.1, 8 hops max, press Ctrl+C to stop
 1   192.168.123.2   0.344 ms  0.554 ms  0.648 ms
 2   *23.23.23.3   0.815 ms (ICMP type:3, code:3, Destination port unreachable)
```

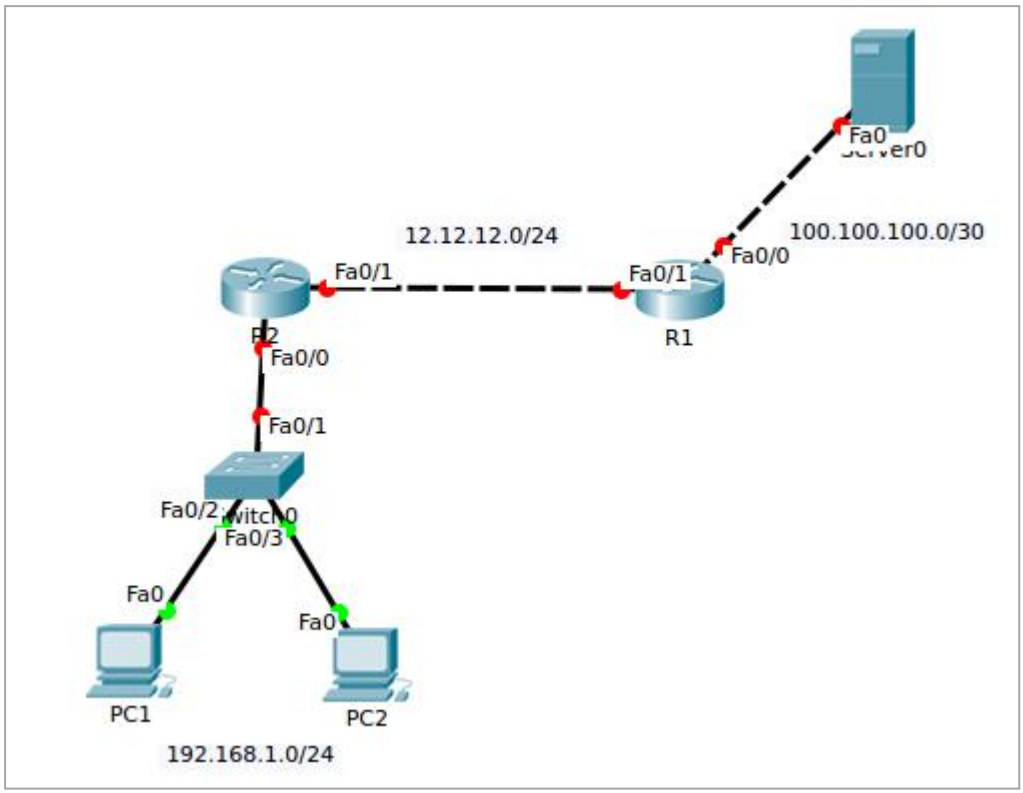
Hasilnya adalaha PC1 melalui R1 dan PC2 melalui R2

LAB 27 - Standard Access-list (1-99)

Access-list sama seperti firewall yaitu digunakan untuk memfilter paket. Bisa juga digunakan untuk menandai paket lalu di lanjutkan dengan mengkonfigurasi fitur yang lain seperti NAT, EIGRP dll. Access-list ada dua yaitu

1. Standard Access-list (1-99)
2. Extended Access-list (100-199)

Topologi yang akan digunakan



Gambar 27.1 Topologi Standar Access-list

Tujuan utama kita adalah PC2 akan di block jadi tidak bisa terhubung ke jaringan luar namun masih bisa terhubung ke jaringan lokal (PC1).

Konfigurasi terlebih dahulu IP Address dan EIGRP AS 100 pada semua device agar bisa terhubung.

R1

```
R1(config)#int fa0/0
R1(config-if)#no sh
```

```
R1(config-if)#ip add 100.100.100.1 255.255.255.252


R1(config)#int fa0/1
R1(config-if)#no sh
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#ex


R1(config)#router eigrp 1
R1(config-router)#no auto
R1(config-router)#network 12.12.12.0
R1(config-router)#network 100.100.100.0
```

R2

```
R2(config)#int fa0/0
R2(config-if)#no sh
R2(config-if)#ip add 192.168.1.254 255.255.255.0
R2(config-if)#int fa0/1
R2(config-if)#no sh
R2(config-if)#ip add 12.12.12.2 255.255.255.0


R2(config)#router eigrp 1
R2(config-router)#no auto
R2(config-router)#network 12.12.12.0
R2(config-router)#network 192.168.1.0
```

Kita test terlebih dahulu ping dari PC2 ke PC1 dan PC2 ke Server

```
PC>ping 192.168.1.1


Pinging 192.168.1.1 with 32 bytes of data:


Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms


PC>ping 100.100.100.2


Pinging 100.100.100.2 with 32 bytes of data:


Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126


Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Sekarang sudah bisa ping. Kita konfigurasi Standard Access-list agar PC2 tidak bisa terhubung ke jaringan luar namun masih bisa terhubung ke PC1

```
R2(config)#access-list 1 deny host 192.168.1.2
R2(config)#access-list 1 permit any
R2(config)#int fa0/1
R2(config-if)#ip access-group 1 out
```

Out digunakan agar access-list digunakan pada saat keluar interface fa0/1.

Sekarang test ping lagi

```
PC>ping 192.168.1.1


Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

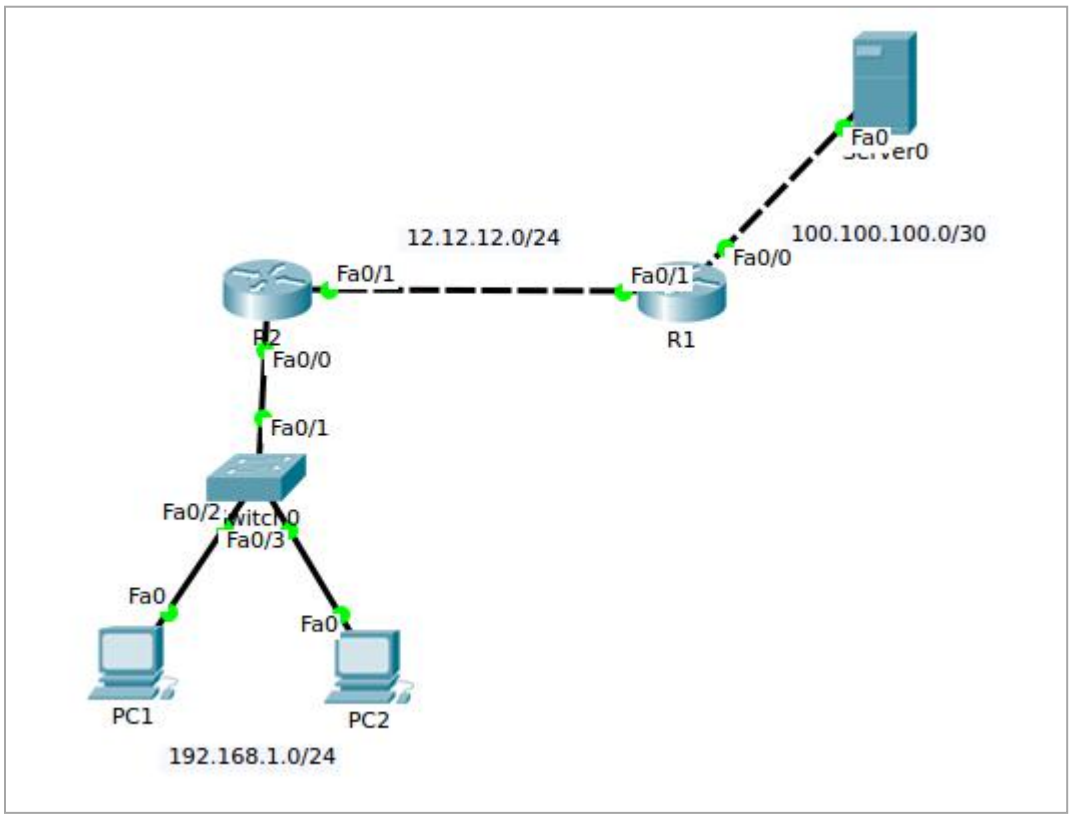
Ping ke PC1 bisa tapi ping ke Server tidak bisa. Lihat pada access-listnya

```
R2#show access-lists
Standard IP access list 1
    10 deny host 192.168.1.2 (4 match(es))
    20 permit any
```

Ada 4 paket yang terblock (4 paket icmp)

LAB 28 - Extended Access-list

Jika menggunakan standard kita memblock maka semua service akan terblock. Jika menggunakan Extended kita dapat memblock service tertentu saja, yang lain dapat digunakan. Angka yang digunakan adalah 100-199. Melanjutkan topologi sebelumnya.



Gambar 28.1 Topologi Extended Access-list

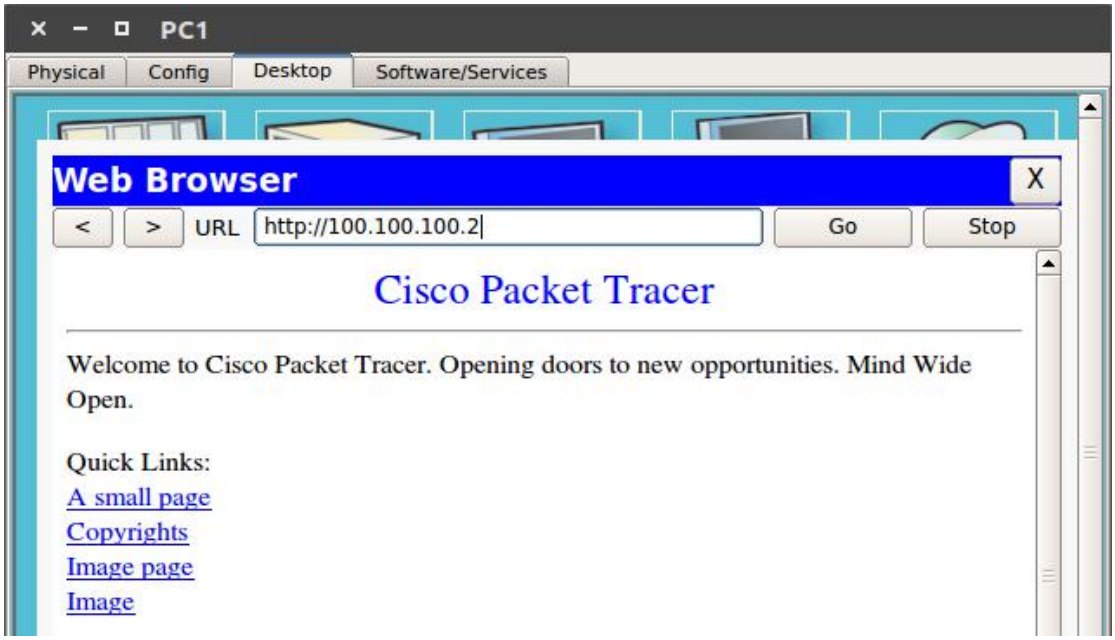
Melanjutkan topologi sebelumnya. Hapus terlebih dahulu konfigurasi standard access-list pada R2.

```
R2(config)#no access-list 1
```

Sekarang tujuan kita adalah :

1. PC1 tidak bisa ping namun bisa membuka http Server
2. PC2 bisa ping namun tidak bisa membuka http Server

Server0 pada defaultnya sudah mengaktifkan http, check pada web browser di Client. **Desktop > Web Browser.**



Gambar 28.2 Tampilan web server

Sekarang konfigurasi extended access-list. Namun sekarang kita menggunakan metode **nama**.

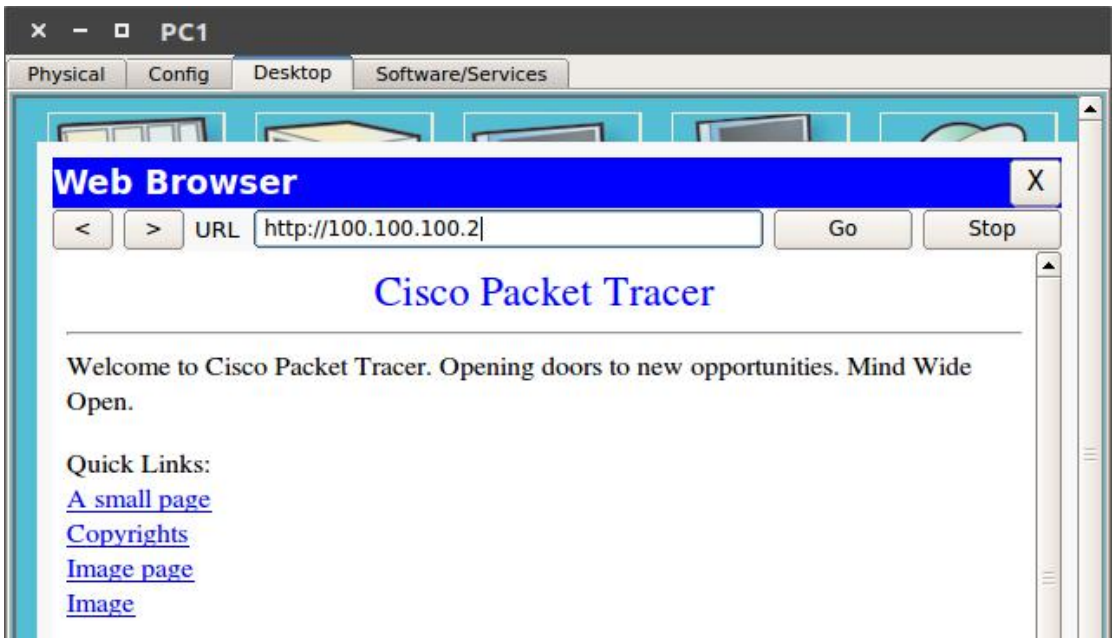
```
R2(config)#ip access-list extended BLOCK
R2(config-ext-nacl)#deny icmp host 192.168.1.1 host 100.100.100.2
R2(config-ext-nacl)#deny tcp host 192.168.1.2 host 100.100.100.2 eq www
R2(config-ext-nacl)#permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
R2(config-ext-nacl)#permit ip any any
```

Lalu aktifkan pada interface bisa menggunakan **out** berarti pada interface **fa0/1.** Jika **in** berarti pada interface **fa0/0.** Kita aktifkan pada interface fa0/0 berarti in

```
R2(config)#interface fa0/0
R2(config-if)#ip access-group BLOCK in
```

Verifikasi pada PC1 terlebih dahulu.

```
PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:


Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



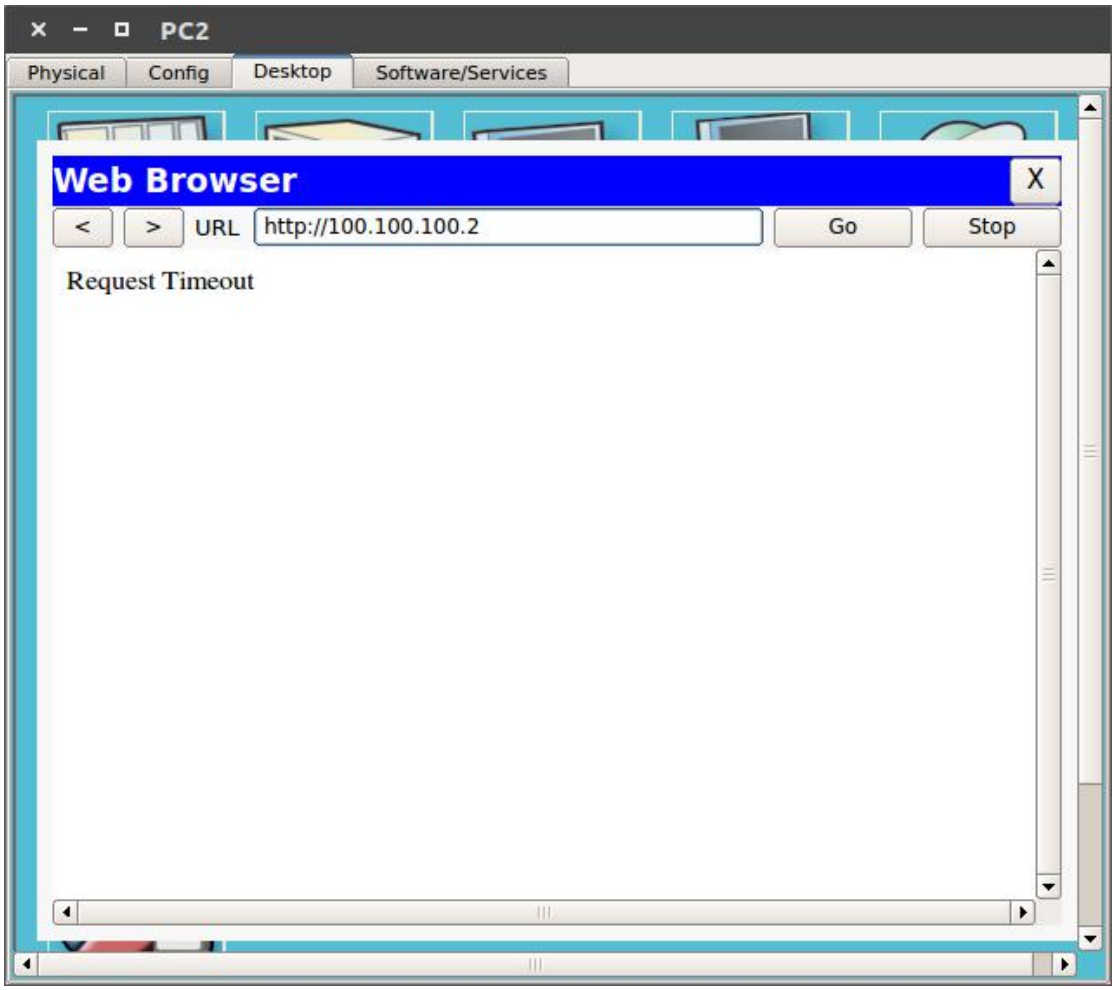
Gambar 28.3 Tampilan web server PC1

Verifikasi pada PC2

```
PC>ping 100.100.100.2


Pinging 100.100.100.2 with 32 bytes of data:
```

```
Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=11ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

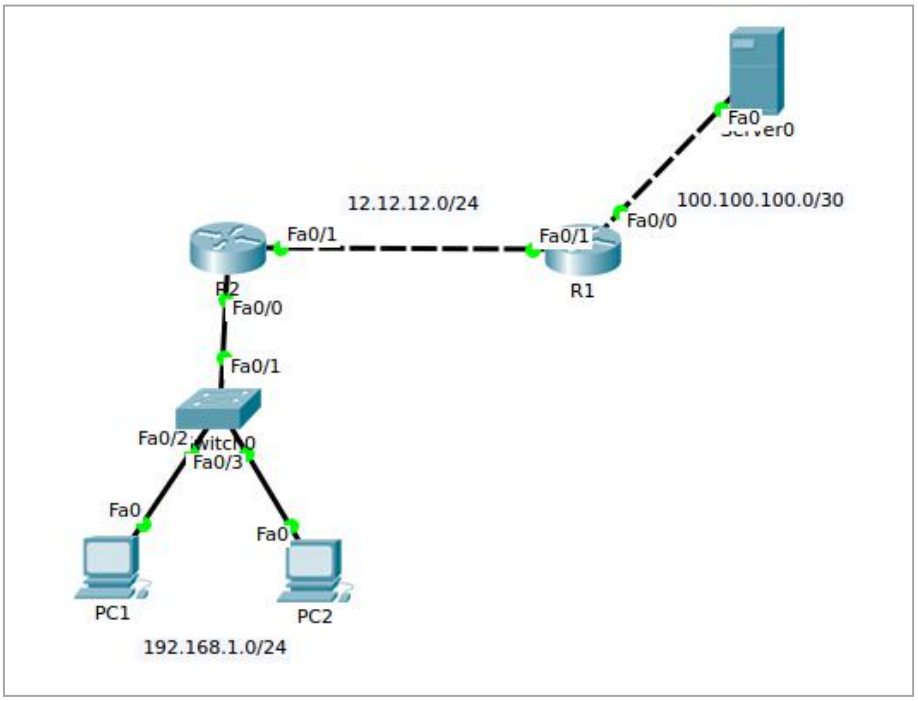
Buka browsernya



Gambar 28.4 Tampilan web server PC2

LAB 29 - Static NAT

NAT digunakan untuk mengubah alamat IP Private menjadi IP Public. Ini dikarenakan pada Internet tidak dikenal IP Private. Dengan static NAT kita akan mengubah IP Private menjadi IP Public secara manual.



Gambar 29.1 Topologi Static NAT

Melanjutkan konfigurasi pada lab sebelumnya. Anggap saja R1 dan Server0 adalah internet. Maka dari itu kita hapus konfigurasi EIGRP dan Access-list. Lalu tambahkan default-route ke internet.

```
R2(config)#no router eigrp 1
R2(config)#no ip access-list exten BLOCK
R2(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.1
```

Test ping ke Server0 dari R2

```
R2#ping 100.100.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Dari Router R2 sudah bisa namun dari client belum bisa

```
PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:


Request timed out.

Request timed out.

Request timed out.

Request timed out.


Ping statistics for 100.100.100.2:

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

Sekarang kita konfigurasi Static NAT yang akan mengubah IP address 192.168.1.1 menjadi 12.12.12.50 dan IP 192.168.1.2 menjadi 12.12.12.100.

Aktifkan NAT pada interface. Lokal = inside, Internet = outside

```
R2(config)#ip nat inside source static 192.168.1.2 12.12.12.100

R2(config)#ip nat inside source static 192.168.1.1 12.12.12.50

R2(config)#int fa0/0

R2(config-if)#ip nat inside

R2(config-if)#int fa0/1

R2(config-if)#ip nat outside
```

Sekarang coba test ping dari client

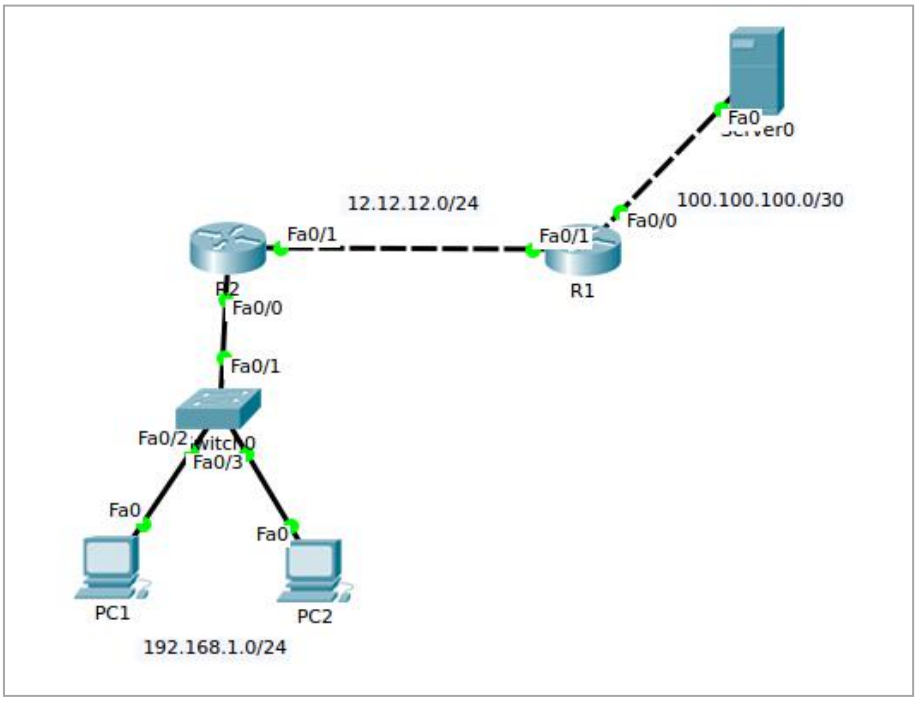
```
PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

Request timed out.

Reply from 100.100.100.2: bytes=32 time=0ms TTL=126

Reply from 100.100.100.2: bytes=32 time=0ms TTL=126

Reply from 100.100.100.2: bytes=32 time=0ms TTL=126


Ping statistics for 100.100.100.2:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:
```

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 12.12.12.100:37   192.168.1.2:37     100.100.100.2:37   100.100.100.2:37
icmp 12.12.12.100:38   192.168.1.2:38     100.100.100.2:38   100.100.100.2:38
icmp 12.12.12.100:39   192.168.1.2:39     100.100.100.2:39   100.100.100.2:39
icmp 12.12.12.100:40   192.168.1.2:40     100.100.100.2:40   100.100.100.2:40
icmp 12.12.12.50:24    192.168.1.1:24     100.100.100.2:24   100.100.100.2:24
icmp 12.12.12.50:25    192.168.1.1:25     100.100.100.2:25   100.100.100.2:25
icmp 12.12.12.50:26    192.168.1.1:26     100.100.100.2:26   100.100.100.2:26
icmp 12.12.12.50:27    192.168.1.1:27     100.100.100.2:27   100.100.100.2:27
---  12.12.12.100      192.168.1.2        ---                ---
---  12.12.12.50       192.168.1.1        ---                ---
```

Sekarang sudah terubah IP addressnya.

LAB 30 - Dynamic NAT

Jika pada Static NAT kita mengubah secara manual IP address nya. Jika Dynamic NAT akan membuat pool yang dapat digunakan untuk Client. Topologinya seperti lab sebelumnya



Gambar 30.1 Topologi Dynamic NAT

Hapus konfigurasi Static NAT pada lab sebelumnya.

```
R2(config)#no ip nat inside source static 192.168.1.2 12.12.12.100
R2(config)#no ip nat inside source static 192.168.1.1 12.12.12.50
```

Setelah itu, buat pool dan access-list yang digunakan untuk NAT nanti.

```
R2(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R2(config)#ip nat pool POOL1 12.12.12.50 12.12.12.100 netmask 255.255.255.0
```

Lalu konfigurasi Dynamic NAT dan aktifkan pada interface

```
R2(config)#ip nat inside source list 1 pool POOL1
R2(config)#int fa0/0
R2(config-if)#ip nat inside
R2(config-if)#int fa0/1
R2(config-if)#ip nat outside
```

Lalu test ping lagi dari Client.

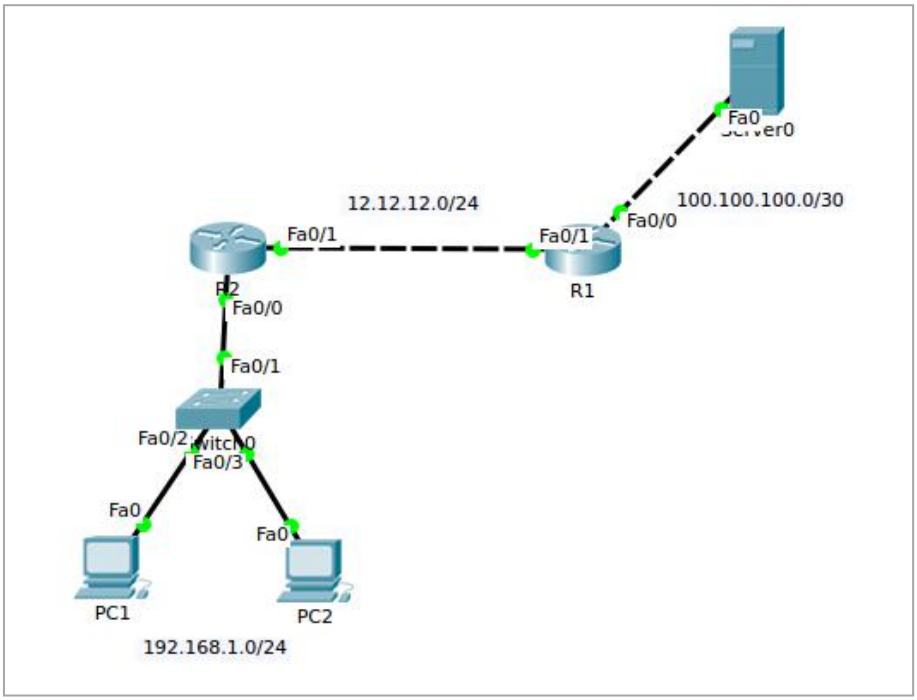
```
PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

Request timed out.
Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Check pada R2

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 12.12.12.52:32    192.168.1.1:32     100.100.100.2:32   100.100.100.2:32
icmp 12.12.12.52:33    192.168.1.1:33     100.100.100.2:33   100.100.100.2:33
icmp 12.12.12.52:34    192.168.1.1:34     100.100.100.2:34   100.100.100.2:34
icmp 12.12.12.52:35    192.168.1.1:35     100.100.100.2:35   100.100.100.2:35
```

LAB 31 - NAT PAT

Jika dengan menggunakan Static NAT dan Dynamic NAT maka 1 private address diubah menjadi 1 IP public. Bagaimana jika kita hanya punya 1 IP public saja ? Maka gunakan PAT karena dengan PAT maka bukan IP yang diubah namun protocolnya. Topologi menggunakan topologi sebelumnya



Gambar 23.1 Topologi NAT PAT

Melanjutkan konfigurasi pada lab sebelumnya. PAT juga menggunakan pool jadi kita tidak perlu menghapus nya. Hapus konfigurasi Dynamic NAT nya saja.

```
R2(config)#no ip nat inside source list 1 pool POOL1
```

Setelah di hapus otomatis client tidak bisa ping ke Server0

```
PC>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

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

```
Request timed out.


Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Tambahkan konfigurasi NAT PAT.

```
R2(config)#ip nat inside source list 1 pool POOL1 overload
```

Yang membedakan Dynamic NAT dengan NAT PAT hanya konfigurasi **overload** saja.

Test ping dari client ke server

```
PC>ping 100.100.100.2


Pinging 100.100.100.2 with 32 bytes of data:


Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126
Reply from 100.100.100.2: bytes=32 time=0ms TTL=126


Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Lalu verifikasi pada R2

```
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 12.12.12.52:49 192.168.1.2:49 100.100.100.2:49 100.100.100.2:49
icmp 12.12.12.52:50 192.168.1.2:50 100.100.100.2:50 100.100.100.2:50
icmp 12.12.12.52:51 192.168.1.2:51 100.100.100.2:51 100.100.100.2:51
icmp 12.12.12.52:52 192.168.1.2:52 100.100.100.2:52 100.100.100.2:52
```

LAB 31 - WAN - HDLC

WAN technologi merupakan technologi yang digunakan untuk menghubungkan router yang jauh yang tidak bisa di capai oleh kabel **fastEthernet**. WAN menggunakan kabel **Serial** dan sifatnya adalah point-to-point. Buat topologi sederhana seperti berikut.

Gambar 31.1 Topologi WAN-HDLC

HDLC merupakan cisco proprietary maka dari itu jika kedua sisi bukan cisco device maka tidak bisa menggunakan HDLC. Konfigurasinya sudah default ketika kita menggunakan kabel serial. Gunakan perintah ini untuk men-*check* ***encapsulation*** HDLC nya.

```
R1#show int se1/0
Serial1/0 is administratively down, line protocol is down (disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
```

Dalam menggunakan kabel serial ada dua pengguna yaitu DTE dan DCE. DCE biasanya di pegang oleh ISP dan sebagai penentu **clock rate.** Clock rate harus di atur jika tidak maka tidak akan berjalan. Pada cisco packet tracer tandanya ada gambar **clock** diatas router.

Jika menggunakan terminal bisa di check dengan perintah berikut.

R1

```
R1#show controllers se1/0
Interface Serial1/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
...
```

R2

```
R2#show controllers se1/0
Interface Serial1/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
...
```

Pada DTE clocknya akan menyesuaikan dari DCE. Sekarang kita konfigurasi agar interface hidup dan kita juga akan ganti clock rate nya.

R1

```
R1(config)#int se1/0
R1(config-if)#clock rate 56000
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown
```

R2

```
R2(config)#int se1/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no shutdown
```

Verifikasi pada R1 bahwa clock rate nya sudah kita rubah

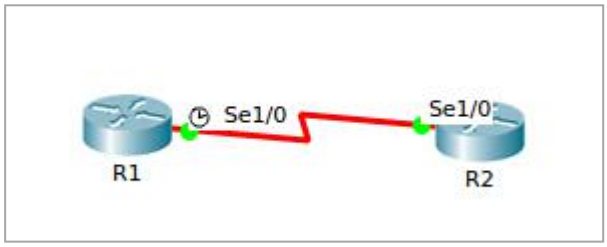
```
R1#show controllers se1/0
Interface Serial1/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 56000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
```

Test ping antar router

```
R1#ping 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/12 ms
```

LAB 32 - PPP (Point-to-Point) Protocol

PPP merupakan open standard. Kita harus konfigurasi terlebih dahulu untuk bisa menggunakannya.



Gambar 32.1 Topologi PPP

Melanjutkan konfigurasi sebelumnya. Kita hanya perlu mengubah encryprion yang dipakai oleh kedua router. Perintahnya

R1

```
R1(config)#int se1/0
R1(config-if)#encapsulation ppp
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
```

Setelah di konfigurasi maka Serial akan down ini di karenakan kedua router menggunakan encapsulation yang berbeda. Atur pada router sebelahnya

R2

```
R2(config)#int se1/0
R2(config-if)#encapsulation ppp
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
```

Verifikasi encapsulationnya.

```
R1#show int se1/0
Serial1/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 12.12.12.1/24
```

```
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
```

Lakukan test ping antar router

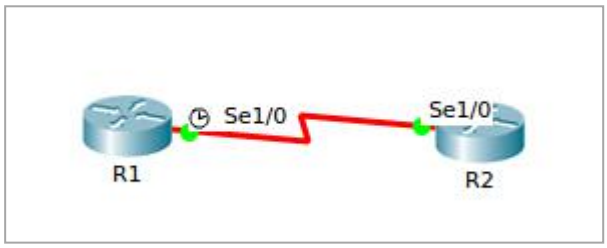
```
R1#ping 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/11 ms
```

LAB 33 - PPP PAP

Jika menggunakan PPP kita dapat menggunakan authentikasi. Ada dua jenis authentikasi :

1. PAP : Plain text
2. CHAP : Encryption

Topologinya masih menggunakan yang sebelumnya



Gambar 33.1 Topologi PPP

Untuk konfigurasinya. Buat terlebih dahulu username dan password.

R1

```
R1(config)#username AKUN password 123
```

R2

```
R2(config)#username USER password INIPASS
```

Lalu konfigurasi authentikasi pada router R1 dan R2

R1

```
R1(config)#int se1/0
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username USER password INIPASS
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
```

R2

```
R2(config)#int se1/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username AKUN password 123
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
```

Format perintah nya adalah

Ppp pap sent-username *User-Lawan* **password** *password-lawan*

Kita bisa lihat autentikasinya dengan menggunakan perintah **debug** lalu mematikan dan menyalakan interface

```
R1#debug ppp negotiation


R1(config)#int se1/0
R1(config-if)#sh
R1(config-if)#no sh


R1(config-if)#
%LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down


Serial1/0 PPP: Phase is TERMINATING
Serial1/0 LCP: State is Closed
Serial1/0 PPP: Phase is DOWN


%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down


Serial1/0 PAP: I AUTH-REQ id 17 len 15


Serial1/0 PAP: Authenticating peer


Serial1/0 PAP: Phase is FORWARDING, Attempting Forward




Serial1/0 PPP: Using default call direction
Serial1/0 PPP: Treating connection as a dedicated line
Serial1/0 PPP: Phase is ESTABLISHING, Active Open


Serial1/0 LCP: State is Open
```

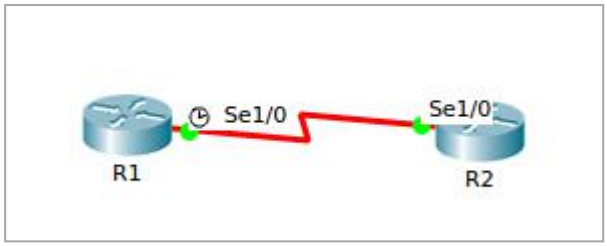
```
Serial1/0 PPP: Phase is AUTHENTICATING

Serial1/0 Using hostname from interface PAP

Serial1/0 Using password from interface PAP

Serial1/0 PAP: O AUTH-REQ id 17 len 15

Serial1/0 PAP: Phase is FORWARDING, Attempting Forward

Serial1/0 PAP: I AUTH-REQ id 17 len 15

Serial1/0 PAP: Authenticating peer

Serial1/0 PAP: Phase is FORWARDING, Attempting Forward

Serial1/0 PPP: Phase is FORWARDING, Attempting Forward
Serial1/0 Phase is ESTABLISHING, Finish LCP
Serial1/0 Phase is UP
```

Coba test ping antar router

```
R1#ping 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/17/65 ms
```

LAB 34 - PPP CHAP

Sebelumnya kita menggunakan pap kali ini menggunakan chap. Chap akan mengenkripsi hanya authentikasinya saja tidak mengenkripsi seluruh data. Topologi yang digunakan masih sama seperti sebelumnya.



Gambar 34.1 Topologi CHAP

Jika pada sebelumnya kita membuat user dan password yang bebas. Sekarang kita harus buat dengan format berikut

Username *hostname-lawan* **password** *harus-sama*

Kita buat dulu username dan passwordnya pada tiap router

R1

```
R1(config)#username R2 password PASS123
```

R2

```
R2(config)#username R1 password PASS123
```

Lalu aktifkan pada interface

R1

```
R1(config)#int se1/0
R1(config-if)#ppp authentication chap
```

R2

```
R2(config)#int se1/0
R2(config-if)#ppp authentication chap
```

Perintah debug akan melihat kan authentikasinya

```
R1#debug ppp negotiation


PPP protocol negotiation debugging is on
```

```
R1(config)#int se1/0
R1(config-if)#sh
R1(config-if)#no sh

Serial1/0 LCP: State is Open

Serial1/0 PPP: Phase is AUTHENTICATING

Serial1/0 IPCP: O CONFREQ [Closed] id 1 len 10
t
Serial1/0 IPCP: I CONFACK [Closed] id 1 len 10

Serial1/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial1/0 IPCP: I CONFACK [REQsent] id 1 len 10
er
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int
Serial1/0 IPCP: I CONFREQ [Closed] id 1 len 10

Serial1/0 IPCP: O CONFACK [Closed] id 1 len 10

Serial1/0 IPCP: I CONFREQ [REQsent] id 1 len 10

Serial1/0 IPCP: O CONFACK [REQsent] id 1 len
Serial1/0 LCP: State is Open

Serial1/0 PPP: Phase is AUTHENTICATING

Serial1/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial1/0 IPCP: I CONFACK [Closed] id 1 len 10
```

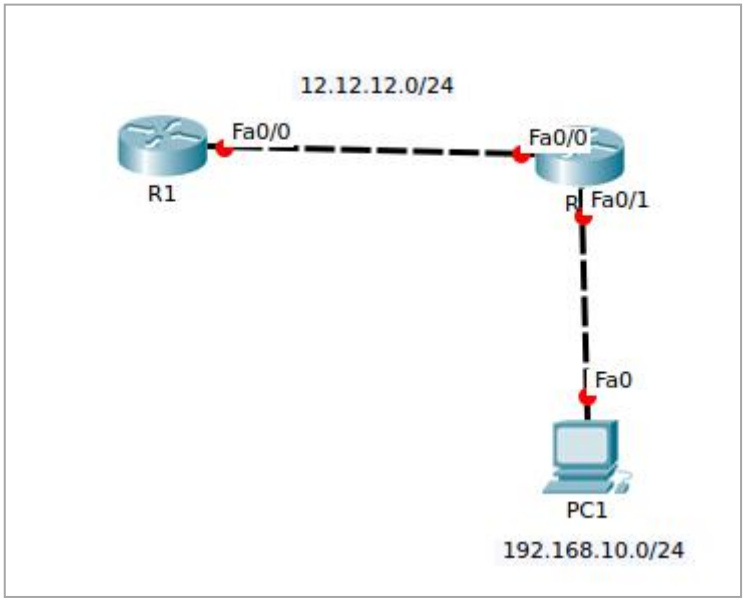
```
Serial1/0 IPCP: O CONFREQ [Closed] id 1 len 10

Serial1/0 IPCP: I CONFACK [REQsent] id 1 len 10

Serial1/0 PPP: Phase is FORWARDING, Attempting Forward
Serial1/0 Phase is ESTABLISHING, Finish LCP
Serial1/0 Phase is UP
```

Coba test ping antar router

```
R1#ping 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms
```

LAB 35 - DHCP Relay

DHCP Relay sudah masuk dalam materi CCNAv3. DHCP Relay akan meneruskan IP Address yang diberi Server ke clien yang memintanya. Jadi biasanya kita mendapatkan IP address dengan gateway yang satu segment. Jika dengan DHCP Relay maka IP Address dan gatewaynya berbeda.



Gambar 35.1 Topologi DHCP Relay

Konfigurasi IP Address dan buat DHCP Server pada R1.

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


R1(config)#ip dhcp pool IDN-Pool
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.254
R1(dhcp-config)#dns-server 100.100.100.100
R1(dhcp-config)#exit


R1(config)#ip dhcp excluded-address 192.168.1.250 192.168.1.254
R1(config)#ip route 192.168.10.0 255.255.255.0 12.12.12.2
```

IDN-Pool merupakan nama pool nya saja. Bisa di isi nama apa aja. **Default-router** merupakan IP Gateway yang akan diberikan ke client. **DNS-Server** merupakan IP dns server jika ada.

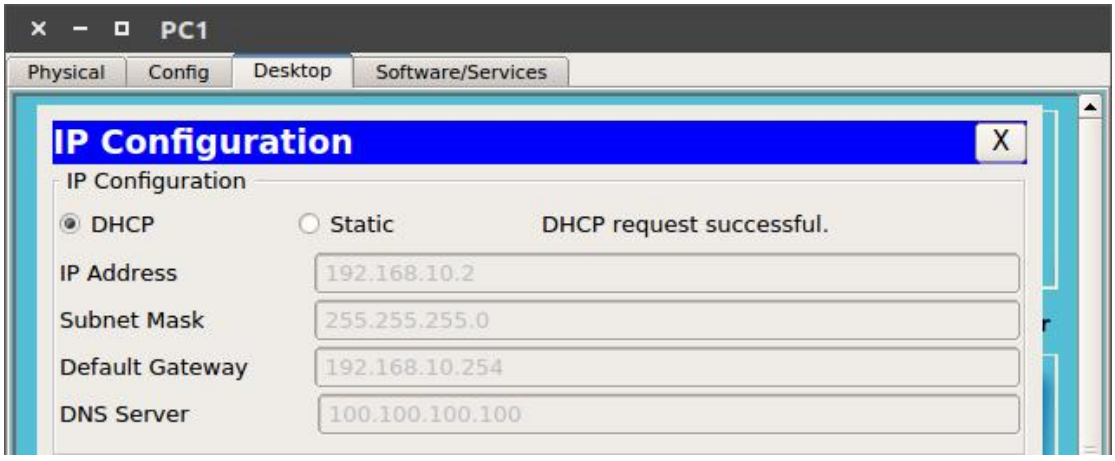
ip dhcp excluded-address perintah ini digunakan jika ada ip address yang tidak ingin dibagikan. Yaitu dari 192.168.1.250 - 192.168.1.254.

Perlu ditambah routing agar R1 dapat mengetahui network yang dibagikannya.

Setelah itu konfigurasi IP Address dan DHCP Relay pada R2

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


R2(config-if)#int fa0/1
R2(config-if)#ip add 192.168.1.254 255.255.255.0
R2(config-if)#no sh
R2(config-if)#ip helper-address 12.12.12.1
```

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



Gambar 35.2 DHCP Client pada PC1