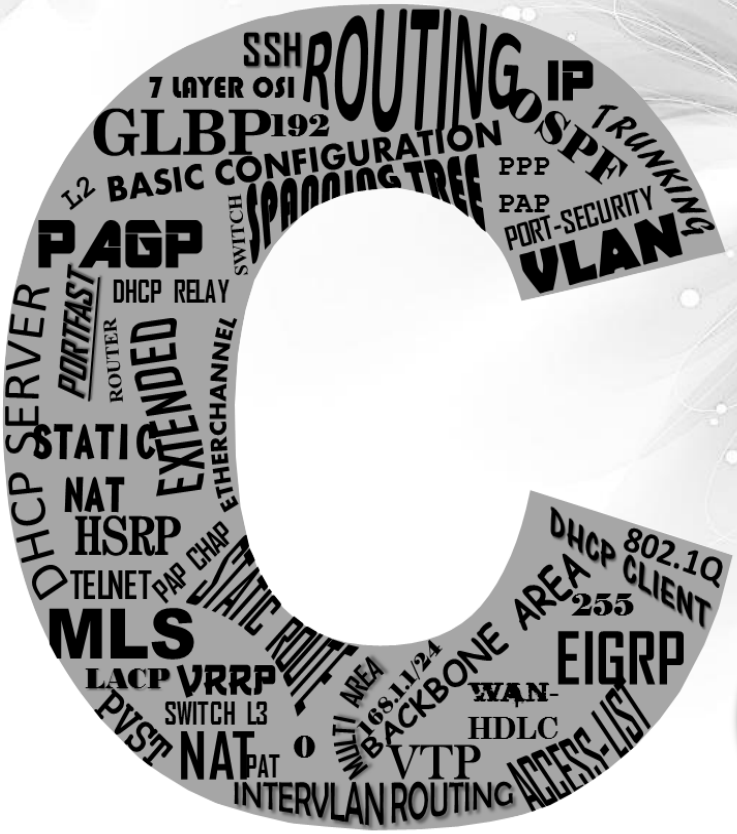
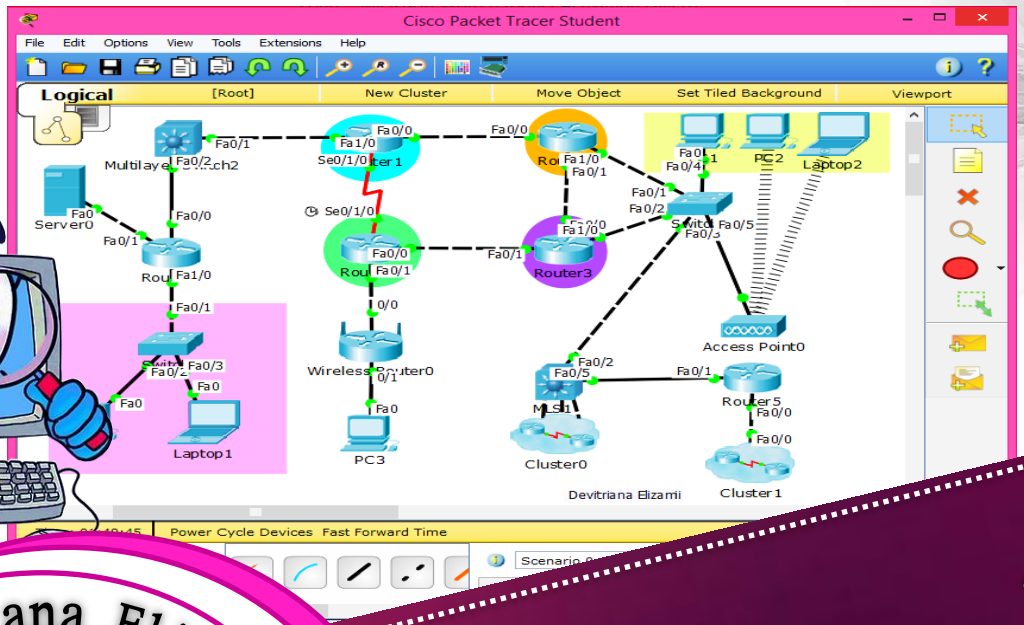
SemangArt Belajar Bersama

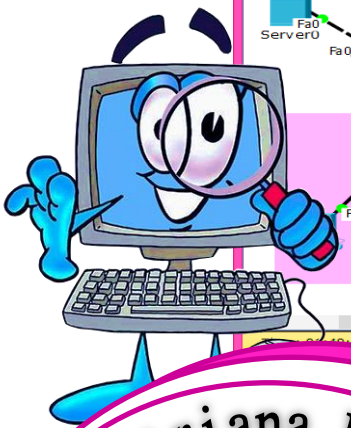
Expert



CCNA

Cisco Certified Network Associate





CISCO CERTIFIED CCNA ROUTING & SWITCHING

Devitriana Elizami

40 LAB Cisco

VLAN, Trunk, InterVLAN, MLS, DHCP Server, DHCP Client, Telnet, SSH, STP, PVST, Port-security, EtherChannel PaGP & LaCP, VTP, DTP, Static Routing, EIGRP, OSPF & Multi Areanya, Standard & Extended Access-List, Static NAT, Dynamic NAT, NAT PAT, WAN-HDLC, PPP, PPP PAP, PPP CHAP, DHCP Relay, Redistributing

KATA PENGANTAR

Assalamu'alaikum warrohmatullahi wabarokatu

Dengan menyebut nama Allah Subhanawata'ala yang Maha Pengasih lagi Maha penyayang. Puji syukur saya panjatkan kehadirat-Nya yang telah memberikan kesehatan jasmani dan rohani, sehingga saya dapat menyelesaikan buku ini. Sholawat serta salam saya haturkan kepada Nabi Besar Muhammad Shallallahu'alaihiwasallam, beserta keluarganya, sahabatnya dan para pengikutnya. Saya mengucapkan terimakasih kepada semua pihak yang telah membantu terselesaikannya buku "SemangArt Belajar Bersama CCNA", terutama untuk Orang Tua, Guru Pembimbing Kejuruan Teknik Komputer dan Jaringan di SMK Karya Guna Bhakti 2 Kota Bekasi, sahabat serta teman-teman seperjuangan.

Saya berharap buku ini dapat bermanfaat untuk semua orang terutama adik kelas yang akan mempelajari Cisco Packet Tracer dan GNS3. Saya sadar bahwa dalam menyusun buku ini masih banyak yang harus diperbaiki, maka dari itu saran dan kritik yang sifatnya membangun sangat saya harapkan agar dapat lebih baik lagi kedepannya.

Bekasi, Februari 2017

Devitriana Elizami

DAFTAR ISI

BAB I

Basic Information

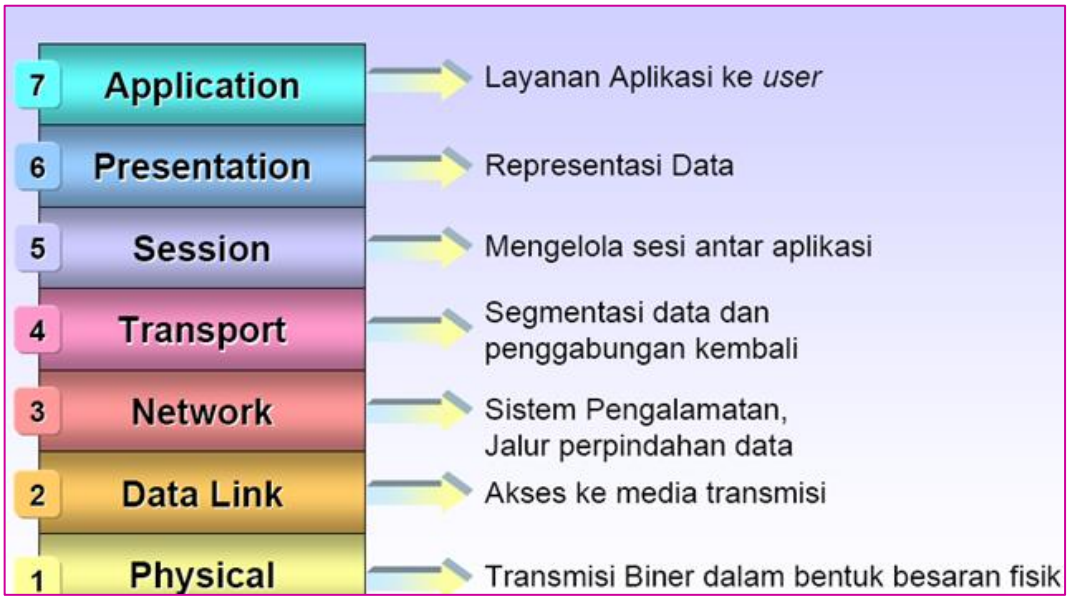
LAB 1 – 7 Layer OSI

Kenapa 7 layer OSI diciptakan?

Karena alat komunikasi yang diciptakan oleh IBM tidak dapat saling berkomunikasi dengan vendor lain atau jaringan yang berbeda. Sehingga oleh International Organization for Standardization (ISO) di Eropa pada tahun 1977 diciptakanlah standard OSI yang dapat saling berkomunikasi dengan vendor yang berbeda.

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protokol jaringan dan metode transmisi.

Ke 7 model layer OSI itu adalah :



Gambar 1.1 7 Layer OSI

7. Application Layer

Application Layer adalah lapisan yang menyediakan interface antara aplikasi yang digunakan untuk berkomunikasi dan jaringan yang mendasarinya, dimana pesan-pesan kesalahan akan dikirim. Protokol Application Layer digunakan untuk pertukaran data antara program yanng berjalan pada source dan host tujuan. Lapisan ke-7 ini menjelaskan spesifikasi untuk lingkup dimana aplikasi jaringan berkomunikasi dengan layanan jaringan.

Beberapa fungsi dari Application Layer adalah :

1. Sebagai alat pengumpul informasi dan data yang dikirimkan melalui jaringan
2. Sebagai user interface dalam menampilkan data dan informasi

Berikut adalah protokol yang berada dalam lapisan ini :

1. Web Server : HTTP (Hyper Text Transfer Protocol) dan HTTPS
2. Mail : SMTP (Simple Mail Transfer Protocol),
   POP3 (Post Office Protocol Version 3), dan
   IMAP (Internet Message Access Protocol)
3. FTP (File Transfer Protocol)
4. DHCP (Dynamic Host Configuration Protocol)
5. Telnet (Telecommunication Network)
6. DNS (Domain Name System)
7. SNMP (Simple Network Management Protocol)

6. Presentation

Berada pada layer ke 6 pada saat sebuah data akan diterima oleh user. Layer Presentation ini memiliki fungsi utama sebagai penerjemah. Yaitu menterjemahkan aplikasi menjadi bentuk data yang akan ditransmisikan ke layer-layer berikutnya atau sebaliknya (mentransmisikan/menterjemahkan data-data kedalam bentuk aplikasi).

Presentation Layer juga merupakan lapisan dimana data mulai disajikan dalam bentuk-bentuk tertentu (format), seperti .JPEG, .JPG, .DOC, dll.

Berikut adalah beberapa fungsi Presentation Layer :

1. Melakukan encrypsi (pengamanan) data atau pesan
2. Melakukan proses Kompresi dan Dekompresi
   - **Kompresi** adalah pemadatan atau pengecilan kapasitas data
   - **Dekompresi** adalah membuka dan memperjelas data yang akan diterima dan diteruskan ke Application Layer

5. Session

Adalah sebuah layer yang bertugas untuk mengendalikan dialog-dialog yang terjadi antar node dan untuk melakukan menagement dari sebuah koneksi serta mendefinisikan bagaimana sebuah koneksi dapat dibangun.

Session Layer mempunyai beberapa fungsi yaitu :

1. Melakukan komunikasi pada sebuah jaringan
2. Pembentukan hubungan
3. Pemindahan dan pertukaran data

Protokol pada Session Layer adalah :

1. NetBIOS (NetBIOS Extended User Interface)
2. PAP (Printer Access Protocol)\
3. NETBEUI
4. NFS (Network File System)
5. SQL (Structured Query Language)
6. RPC (Remote Procedure Call)
7. ASP (Apple Talk Session Protocol)

Contoh dari Session Layer adalah Gateway.

Network Component adalah Gateway.

3. Transport

Lapisan ini bertanggung jawab untuk menyediakan layanan yang dapat diandalkan kepada protocol yang terletak diatasnya.

Beberapa layanannya adalah :

1. Flow Control (Mengatur Alur), yaitu untuk menjamin bahwa perangkat yang mentransmisi data tidak mengirimkan lebih banyak data daripada yang dapat ditangani oleh perangkat yang menerimanya.
2. Packet Sequencing (Megurutkan Paket) untuk mengubah data yang hendak dikirimkan menjadi segmen-segmen data (proses segmentasi) dan tentunya memiliki fitur untuk menyusunnya kembali.
3. Fitur Acnowledgment untuk menjamin bahwa data dikirimkan dengan benar dan akan dikirimkan lagi jika data tidak sampai ke tujuan.

Fungsi dari Transport Layer adalah :

1. Menerima data dari Session Layer untujk diproses
2. Memecah data menjadi bagian-bagian yang lebih kecil untuk memudahkan proses transmisi data dan mempermudah data agar bisa melewati layer/lapisan selanjutnya dengan lebih baik, optimal dan efisien.
3. Meneruskan data ke Network Layer

4. Network

Layer ini digunakan untuk menghubungkan jaringan-jaringan yang berbeda agar dapat saling berinteraksi. Misalnya dalam perpindahan paket dari satu jaringan ke jaringan lain dapat menimbulkan masalah yang banyak. Cara pengalamatan yang digunakan oleh sebuah jaringan dapat berbeda dengan cara yang dipakai oleh jaringan lainnya. Suatu jarigan mungkin tidak adapat menerima paket sama sekali karena ukuran kapasitas paket data yang terlalu besar, protokolnya pun bisa berbeda pula. Oleh karena itu network ditugaskan untuk menyelesaikan persoalan tersebut.

Berikut adalah beberapa fungsi dari Network Layer :

1. Menentukan tujuan data pada sebuah jaringan
2. Mendefinisikan alamat IP
3. Membuat paket data terurut (header)
4. Melakukan prosess routing

Protokol pada Network Layer adalah IP, ARP, RARP, ICMP, RIP, OSPF, IGMP, IPX, NWLink, NetBEUI, OSI, DDP, DECnet, dll.

Network Component : Router, Brouter, Frame Relay Device, ATM Switch, advanced Cable Tester, dll.

5. Data Link

Dalam proses transmisi data yang terjadi, Data Lnk Layer merupakan layer ke 6 bagi transmitter (pengirim data) dan merupakan layer ke 2 bagi receiver (menerima data).

Data Link Layer memiliki tugas utama yaitu untuk menyediakan sebuah prosedur pengiriman data antar jaringan. Jadi, dengan adanya data link layer ini, setiap paket data akan ditransmisikan ataupun akan diterima oleh user, akan diproses, sehingga memungkinkan untuk dilanjutkan ke layer berikutnya, yaitu Network Layer ataupun Physical Layer.

Salah satu ciri yang terpenting pada Data Link Layer adalah bahwa lapisan ini secara fisik memiliki alamat tersendiri atau address yang sudah dikodekan secara langsung ke dalam sebuah network card atau kartu jaringan tersebut ketika pertama kali dibuat. Inilah yang dikenal dengan istilah **MAC Address**. Jadi, apabila kita mendengar nama MAC Address didalam jaringan komputer, maka hal ini sudah pasti mengacu pada lapisan atau Data Link layer.

Data Link Layer memiliki beberapa fungsi yaitu :

1. Melakukan proses Grouping secara logic (tidak terlihat)
   Grouping adalah proses penyusutan beberapa paket data menjadi satu kesatuan yang utuh. Perlu kita ketahui, ketika paket data mulai berjalan melewati lapisan OSI, maka paket data tersebut akan terpecah-pecah menjadi beberapa bagian kecil. Tugas dari data link layer inilah yang dapat melakukan proses grouping.
2. Menyediakan akses ke dalam media menggunakan MAC Address
3. Mendeteksi kesalahan pengiriman dan penerimaan paket data dan melakukan proses pengkoreksian
4. Menggabungkan paket data ke dalam byte dan menggabungkan byte ke dalam frame

1. Physical Layer

Merupakan lapisan ke 7 pada layer OSI ketika sebuah paket data mulai ditransmisikan oleh transmitter. Dimana dalam hal ini adalah sebuah server komputer dan merupkan lapisan yang pertama kali harus dilewati oleh paket data atau informasi ketika akan melakukan proses penerimaan oleh receiver.

Physical Layer merupakan layer yang memiliki koneksi dan juga definisi terdekat dengan perangkat keras jaringan, yang kemudian membantu sebuah transmisi jaringan dapat berjalan dengan lancar sesuai dengan apa yang diinginkan.

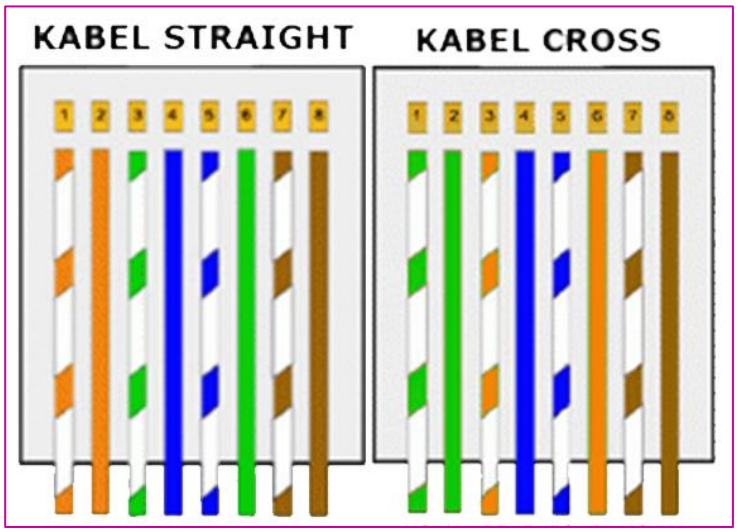
Berikut adalah proses penting yang dilakukan oleh Physical Layer adalah :

1. Physical Layer akan terhubung langsung dengan perangkat keras jaringan, seperti kabel, hub, switch, LAN Card, dll.
2. Melakukan proses sinkronisasi etrhadap bit data.
3. Physical Layer mampu berkomuniaksi secara langsung dengan berbagai jenis media transmisi
4. Physical Layer dapat menentukan kebutuhan listrik, prosedur dan juga fungsional dari sebuah jaringan komputer.
5. Dapat melakukan proses penonaktifan hubungan fisik antar sistem
6. Dapat melakukan proses pemindahan bit antar device atau alat

Karena merupakan layer yang berhubungan dengan bentuk fisik dari beberapa perangkat keras jaringan komputer, maka berikut adalah media fisik yang memanfaatkan lapisan Physical Layer :

1. Kabel : UTP, Coaxial, Fiber Optik, dll
2. NIC (Network Interface Card)
3. Hub
4. Switch

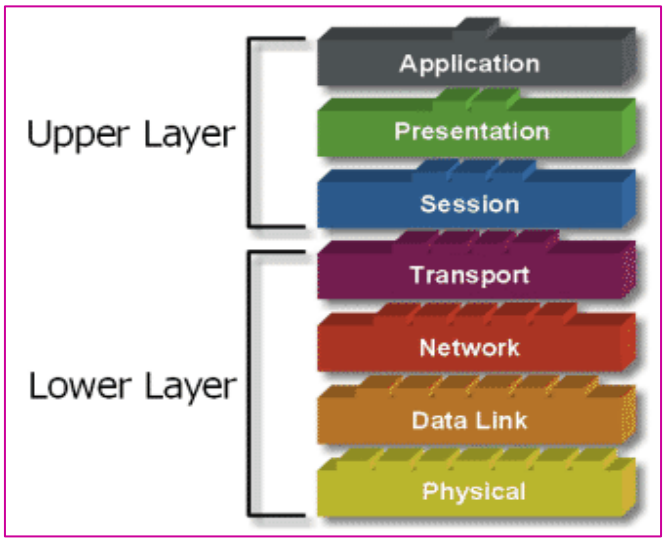
a. Berikut adalah urutan straight dan cross pada kabel UTP (Unshielded Twisted Pair) :



Gambar 1.2 Urutan Kabel Straight dan Cross

	1	2	3	4	5	6	7	8
Straight	Putih Orange	Orange	Putih Hijau	Biru	Putih Biru	Hijau	Putih Coklat	Coklat
Cross	Putih Hijau	Hijau	Putih Orange	Biru	Putih Biru	Orange	Putih Coklat	Coklat

b. Upper dan Lower Layer



Gambar 1.3 Upper dan Lower Layer pada model OSI

- **Upper Layer (Lapisan Atas)**

Layer ini fokus pada penanganan tampilan akhir kepada pengguna dan bagaimana file direpresentasikan pada komputer. Upper layer juga berhubungan dengan persoalan aplikasi dan pada umumnya diimplementasikan pada software aplikasi yang berisi sebuah komponen komunikasi.

- **Lower Layer (Lapisan Bawah)**

Adalah inti dari proses komunikasi didalam jaringan. Lower layer juga mengendalikan persoalan transportasi data yang diimplementasikan ke dalam hardware dan software pada media jaringan.

Kedua layer tersebut tidak dapat dipisahkan. Maka setiap layer harus bisa berkomunikasi dengan layer diatasnya maupun dibawahnya melalui serangkaian protokol dan standar.

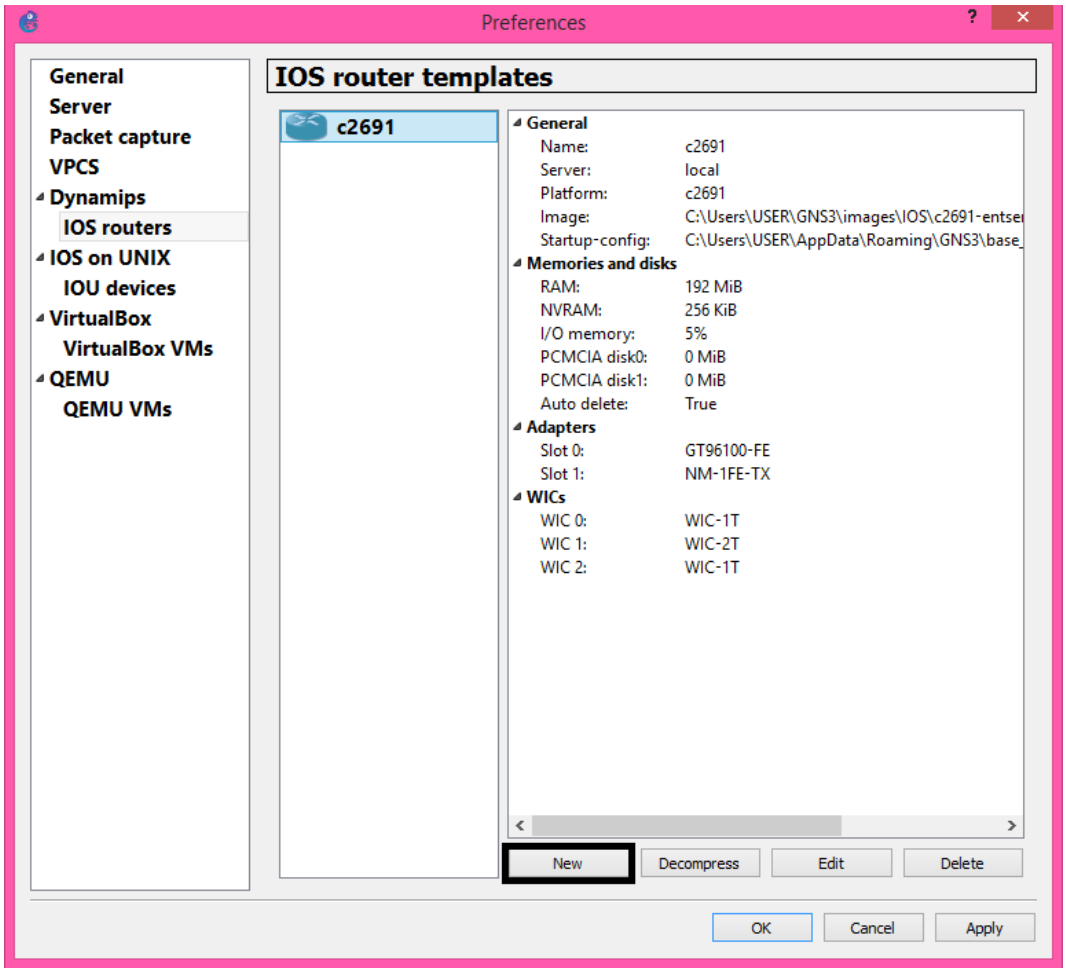
LAB 2 – Preparation Cisco (GNS3 (Graphical Network Simulator 3))

Untuk belajar cisco dapat menggunakan virtual yaitu GNS3 dan Cisco Packet Tracer. Prinsip kerja dari GNS3 adalah penggunaannya yang memakai Cisco IOS **asli** pada komputer, sehingga device yang ada di GNS3 seperti PC, Router, bahkan Switch dapat berfungsi sebagaimana perangkat aslinya dan nyata dalam mengkonfigurasi.

Yang harus disiapkan adalah :

Aplikasi GNS3 yang sudah harus diinstal terlebih dahulu di laptop atau pc yang kalian gunakan (bisa cek di web resminya https://www.gns3.com/) dan siapkan Cisco IOS nya yang akan digunakan nanti.

1. Jika GNS3 sudah diinstal, buka aplikasinya
2. Lalu tambahkan Cisco IOS



Gambar 2.1 GNS3 > preferences

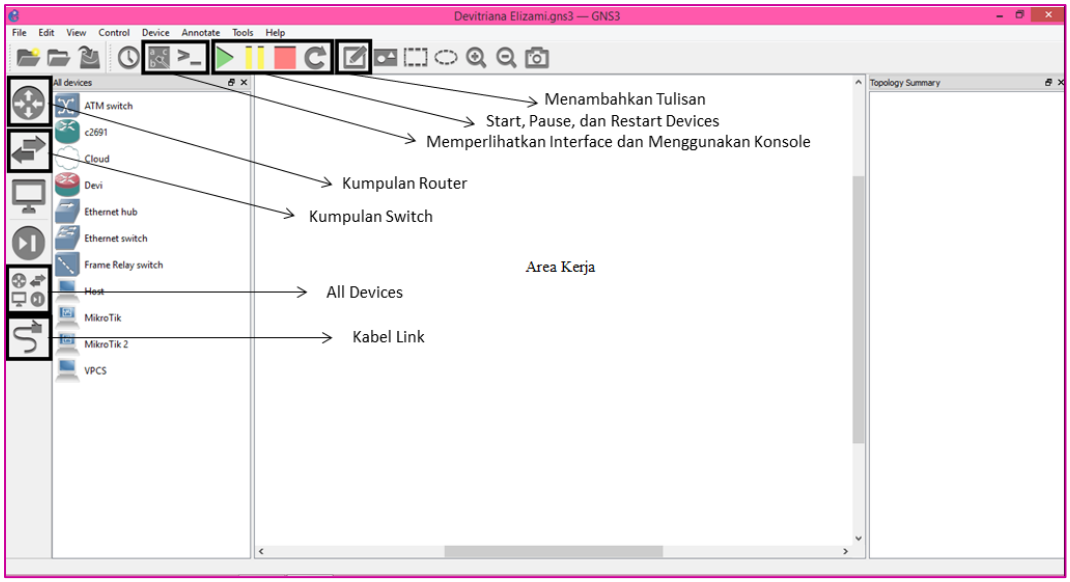
Cisco Router => buka tab "Edit" >> Preferences >> Dynamips >> IOS Routers >> New.

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 klik Next
3. Lalu masukkan alokasi untuk RAM (terserah berapa saja tergantung kemampuan laptop atau komputer kalian, semakin tinggi maka 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%, lalu klik Finish

Cisco Switch = buka tab "Edit" >> Preferences >> IOS on UNIX >> IOU Devices >> New

1. Ketika muncul tab baru isilah nama utuk Switchnya. Lalu pilih New Image, lalu pilih apakah Layer 2 atau Layer 3 dan masukkan IOU image jika tipe yang dipilih adalah Layer 2 maka IOU imagenya pun Layer2. Lalu klik Finish
2. Jika ingin menambahkan network pada router maupun switch klik Edit lalu klik slot untuk router. Klik network untuk switch
3. Nah sekarang kita sudah bisa menggunakan Cisco router dan Cisco Switch

Berikut adalah tampilan GNS3



Gambar 2.2 Area Kerja GNS3

Beberapa keterangan diatas adalah :

1. Kumpulan Router Device yang dapat kalian gunakan
2. Kumpulan Switch Device yang dapat kalian gunakan
3. Kumpulan Device yang kita masukkan IOS dan IOU nya
4. Kabel penghubung
5. Start (yang akan menyalakan semua device)

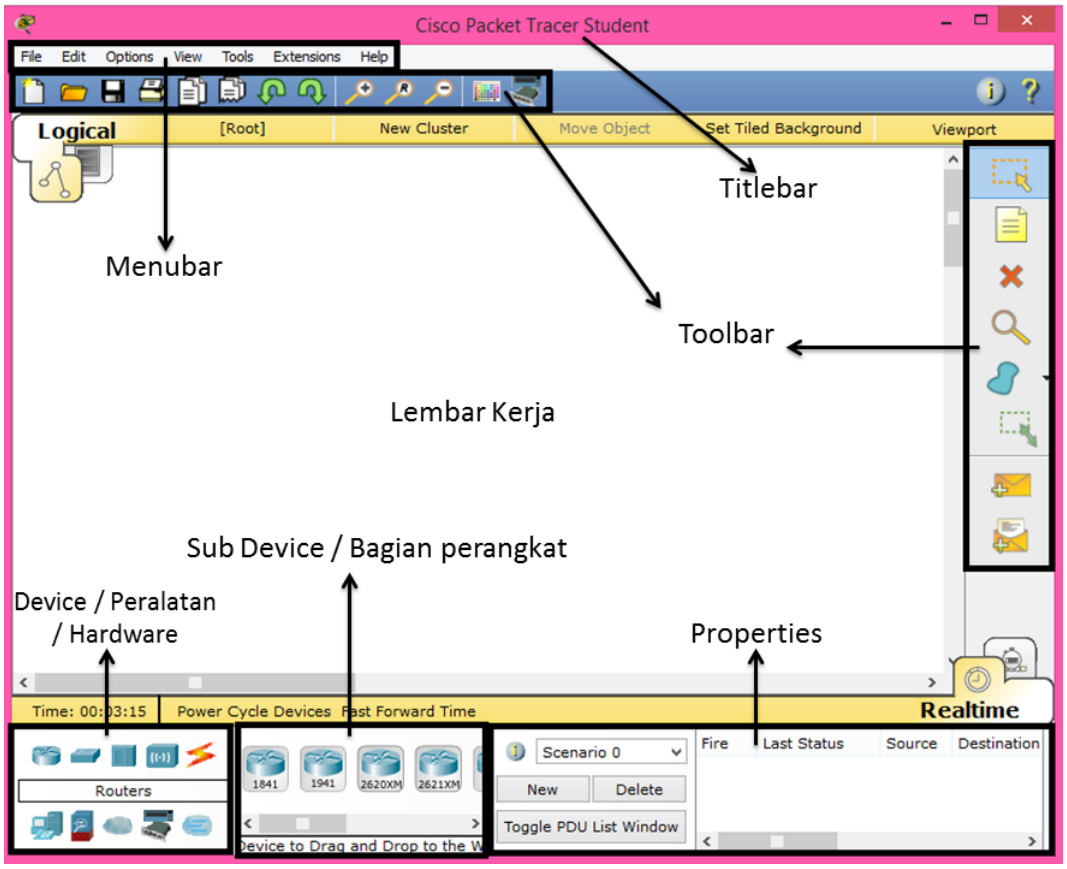
6. Console connect to all devices, untuk membuka terminal CLI yang akan kita gunakan untuk konfigurasi
7. Show/hide interface labels, akan memperlihatkan atau menyembunyikan interface yang digunakan pada setiap device
8. Untuk menambahkan device cukup **drag and drop** device ke area kerja, lalu sambungkan device dengan kabel
9. Dan konfigurasikan sesuai keinginan kalian

LAB 3 – Preparation Cisco Packet Tracer

Selain menggunakan GNS3 kita juga dapat menggunakan aplikasi Cisco Packet Tracer. Jika memakai GNS3 banyak memakan memori dan penggunaannya pun agak berat. Sedangkan, pada Cisco Packet Tracer tidak banyak memakan memori sehingga lebih ringan. Paket Tracer merupakan simulator alat jaringan Cisco yang sering digunakan sebagai medi pembelajaran, pelatihan dan penelitian.

Tujuan utama Packet Tracer adalah untuk menyediakan alat bagi siswa atau pengajar agar dapat memahami prinsip jaringan komputer dan juga memahami skill dibidang alat-alat jaringan.

Target Packet Tracer yaitu menyediakan simulasi jaringan yang real, namun terdapat batasan berupa penghilangan beberapa perintah yang digunakan pada alat aslinya yaitu pengurangan **command** pada Cisco IOS. Dan Packet Tracer tidak bisa digunakan untuk memodelkan jaringan produktif/aktif.



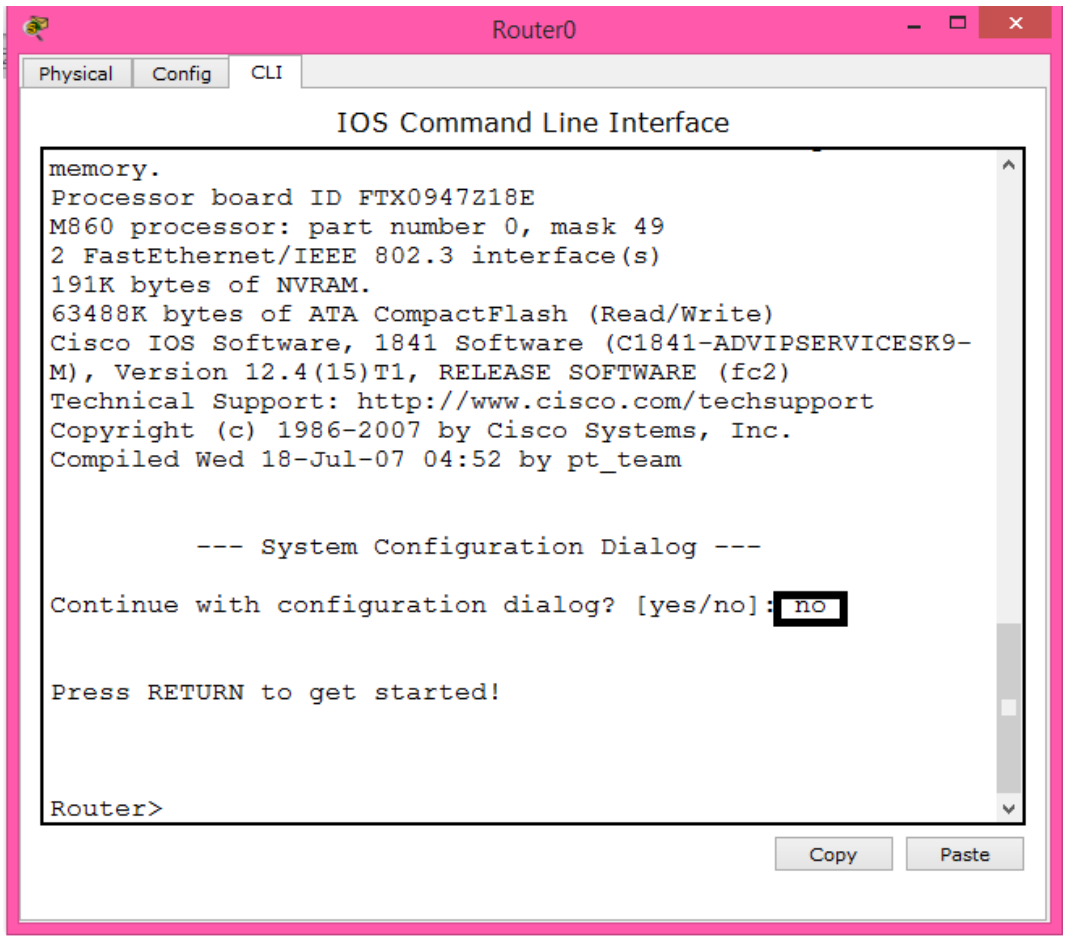
Gambar 3.1 Tampilan Cisco Packet Tracer

Terdapat beberapa device yang dapat kalian lihat pada kotak dibawah sebelah kiri. Hampir sama seperti GNS3, untuk menggunakannya tinggal di **drag and drop** saja ke area kerja. Klik pada devicenya lalu klik CLI untuk menggunakan konsole atau terminalnya.

Keterangan :

1. Menu Bar : Menyediakan File, Pilihan dan Menu Bantuan.
2. Toolbar : Menyediakan shortcut icon pada Menu File, mencangkup Aktivitas Wizard. Kalian juga dapat menemukan tombol informasi jaringan yang dapat kalian gunakan. Dan dapat memilih, memindahkan, menghapus, menambahkan, dll.
3. Area Kerja : Untuk menempatkan berbagai desain jaringan.
4. Title Bar : Judul desain Packet Tracer.
5. Device : Terdapat beberapa kategori perangkat yang dapat digunakan.
6. Sub Device : Memperlihatkan semua jenis dari kategori yang dipilih.
7. Properties : Menampilkan hasil ping perangkat.

Berikut adalah tampilan yang akan muncul



Gambar 3.2 Tampilan Terminal pada Router0

Jika kalian memilih **Yes** maka kalian akan mengkonfigurasinya secara otomatis tidak menggunakan perintah.

LAB 4 – User, Privileged dan Global Configuration Mode

Cisco memiliki beberapa mode :

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

1. User Mode

User mode tandanya adalah **"hostname>" atau ">"**. Sedikit konfigurasi yang bisa kalian lakukan dimode ini. Tidak bisa mengkonfigurasi router pada mode ini, kalian dapat menggunakan **?** (tanda tanya) jika tidak tahu 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

2. Privileged Mode

Tandanya adalah **"hostname#"** atau **"#"** untuk dapat masuk ke mode ini ketik perintah **enable**. Gunakan perintah **?** (tanda tanya) untuk melihat apa saja yang dapat dikonfigurasikan di mode ini. Dan pada mode ini juga kalian dapat melihat konfigurasi yang telah kalian konfigurasikan pada router.

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

Misalkan kita ingin melihat ip address

Router#**show ip int 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
clock	Display the system clock
controllers	Interface controllers status
crypto	Encryption module
debugging	State of each debugging option
dhcp	Dynamic Host Configuration Protocol status
dot11	IEEE 802.11 show information
ephone	Show all or one ephone status
file	Show filesystem information
flash	display information about flash: file system
flow	Flow information
frame-relay	Frame-Relay information
history	Display the session command history
hosts	IP domain-name, lookup style, nameservers, and host table
interfaces	Interface status and configuration
ip	IP information
ipv6	IPv6 information
line	TTY line information
logging	Show the contents of logging buffers

login	Display Secure Login Configurations and State
mac-address-table	MAC forwarding table
ntp	Network time protocol
parser	Show parser commands
policy-map	Show QoS Policy Map
privilege	Show current privilege level
processes	Active process statistics
protocols	Active network routing protocols
queue	Show queue contents
queueing	Show queueing configuration
running-config	Current operating configuration
secure	Show secure image and configuration archive
sessions	Information about Telnet connections
snmp	Snmp statistics
spanning-tree	Spanning tree topology
ssh	Status of SSH server connections
standby	Standby configuration
startup-config	Contents of startup configuration
storm-control	Show storm control configuration
tcp	Status of TCP connections
tech-support	Show system information for Tech-Support
terminal	Display terminal configuration parameters
users	Display information about terminal lines

3. Global Configuration Mode

Pada mode inilah kita mengkonfigurasi router dan switch. Tandanya adalah **"hostname(config)#"** untuk masuk ke mode ini menggunakan perintah **configure terminal.**

```
Router#configure terminal

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

Router(config)#
```

Pada cisco mudahnya kita dapat menyingkat perintah. Untuk menyelesaikan perintahnya tinggal tekan **TAB.** Perhatikan contoh berikut ini :

```
Router#conf t

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

Router(config)#^Z

Router#

%SYS-5-CONFIG_I: Configured from console by console
```

Dari mode ini, kita dapat kembali ke mode privileged menggunakan **CTRL + Z.**

LAB 5 – Konfigurasi Dasar

Pada saat perintah salah maka akan muncul :

```
Router>devi

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

Untuk mengatasinya kita dapat menekan CTRL + SHIFT + 6

Jika kita ingin melihat versi cisco kita dapat menggunakan 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 fa 0/0

Router(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router(config-if)#ip address 10.10.10.1 255.255.255.0
```

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

Untuk melihat IP Address yang sudah dikonfigurasi, lakukan dengan perintah **show ip interface brief** didalam **mode privileged** (#). Jika ingin melihat ip address didalam **mode global** tambahkan kata do, jadi **do show ip interface brief.**

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.10.10.1      YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
Router(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.10.10.1      YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Status port yang dapat ditemui adalah :

1. Administratively down down : Status port dalah keadaan mati
2. Down down : Masalah pada Layer 1
3. Up down : Masalah pada Layer 2
4. Up up : Layer 1 dan 2 sudah

Pada contoh diatas statusnya adalah **up** dan **down,** dikarenakan interface lawan belum dikonfigurasi.

Mengubah hostname **(nama)** dengan perintah **hostname *nama-perangkat***

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

Devitriana-R1(config)#
```

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

```
Devitriana-R1#show running-config

Building configuration...

Current configuration : 570 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Devitriana-R1

.....
```

Mengkonfigurasi password pada perangkat

```
Devitriana-R1(config)#enable password 123

atau

Devitriana-R1(config)#enable secret 123

Devitriana-R1>enable

Password: (123)

Devitriana-R1#
```

Jika menggunakan password maka bentuknya **plain-text** (terlihat) jika dilihat pada running-config (show run).

“enable password 123”

Jika menggunakan secret maka akan terenkripsi, seperti terlihat dibawah ini

“enable secret 5 1mERr$3HhIgMGBA/9qNmgzccuxv0”

Pada cisco, setiap konfigurasi akan tersimpan pada running-config. Maka pada saat kita **me-reboot** atau men-**shutdown** perangkat, konfigurasi akan hilang. Maka kita perlu menyimpannya ke **startup-config.** Dengan perintah **write.**

```
Devitriana-R1#write

Building configuration...

[OK]

Devitriana-R1#copy running-config startup-config

Destination filename [startup-config]? (enter)

Building configuration...

[OK]
```

Jika ingin menyimpannya ke **startup-config** didalam **mode global configuration**, maka harus menambahkan **do** didepan, jadi **do write.**

```
Devitriana-R1(config)#do write

Building configuration...

[OK]
```

Dan untuk mengembalikan ke konfigurasi awal, perintahnya adalah **write erase** (menghapus). Kemudian perlu di reboot terlebih dahulu dengan perintah **reload.**

```
Devitriana-R1#write erase

Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] (enter)

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram


Devitriana-R1#reload

Proceed with reload? [confirm] (enter)

System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized
```

Self decompressing the image :
[OK]
Restricted Rights Legend

BAB II

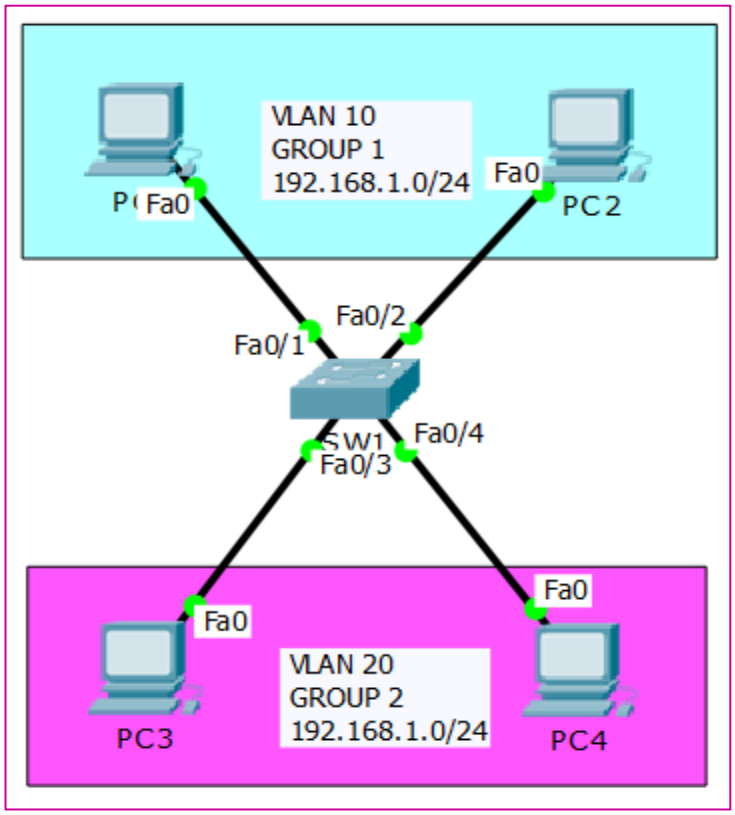
Switching

LAB 6 – 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.** VLAN dilakukan untuk mencegah banyaknya broadcast domain yang dapat memakan bandwidth yang besar dan dapat berpengaruh pada performa jaringan.

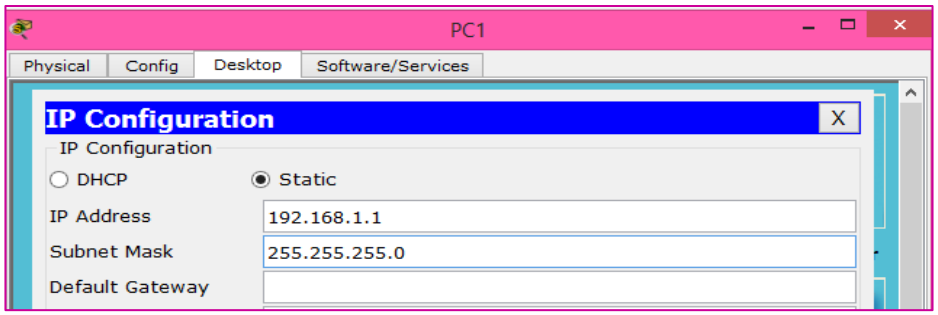
Perbedaan VLAN dengan LAN adalah jika pada **LAN** memerlukan administrasi fisik sebagai lokasi perubahan user, kebutuhan untuk recabling, mengatasi stasiun baru, konfigurasi ulang router dan switch, mobilisasi user dalam jaringan menghasilkan biaya yang lebih besar. Sedangkan jika user bergerak dalam **VLAN,** pekerjaan administrasi dapat dihilangkan karena tidak adanya kebutuhan untuk mengkonfigurasi ulang router. Selain itu, data yang disiarkan dalam VLAN lebih aman jika dibandingkan dengan LAN. Karena data sensitif hanya dapat diakses oleh user yang berada pada VLAN.

Dengan menggunakan VLAN kita dapat mengelompokkan user atau group pada satu switch. **Misalnya** VLAN 10 = GROUP-1 , VLAN 20 = GROUP-2. Maka berikut adalah topologi yang akan kita gunakan :



Gambar 6.1 Topologi jaringan

Konfigurasikan IP Address pada semua PC terlebih dahulu (menyesuaikan pada HOST ID atau nama PC). Klik pada PC, masuk ke Desktop > IP Configuration > isikan IP Address.



Gambar 6.2 Konfigurasi IP Address pada PC

Setelah IP Address dikonfigurasi semua, sekarang lakukan ping pada PC1 ke PC3. Karena dilihat dari networknya sama. Maka hasilnya akan replay. Buka PC > Desktop > Commant Prompt, lalu lakukan ping

```
Packet Tracer PC Command Line 1.0

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data :

Replay from 192.168.1.3: bytes=32   time=52ms   TTL=128

Replay 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-second:

    Minimum = 0ms, Maximum = 52ms, Average = 13ms
```

Sekarang kita konfigurasi VLAN agar PC di GROUP 1 dan PC di GROUP 2 berbeda network dan tidak bisa di ping atau saling berkomunikasi. Sebelumnya kita ganti hostname pada switch dahulu.

```
Switch>enable

Switch#configure terminal

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

Switch(config)#hostname SW1
```

Kemudian buat VLAN :

```
SW1(config)#vlan 10
SW1(config-vlan)#name GROUP-1
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name GROUP-2
```

Sekarang arahkan PC sesuai VLAN yang sudah dibuat

```
SW1(config)#interface fa 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit

SW1(config)#interface fa 0/2
SW1(config-if)#swichport mode access
SW1(config-if)#swichport access vlan 10
SW1(config-if)#exit
```

Selain mengarahkan satu persatu interface sesuai vlan, kita juga dapat mengarahkan interface sekaligus, tetapi secara berurutan.

```
SW1(config)#interface range fa 0/3-4
SW1(config-if-range)#swichport mode access
SW1(config-if-range)#switchport access vlan 20
```

Setelah itu kita check vlan yang sudah dibuat dengan perintah **show vlan brief** didalam mode privileged**.** Default VLAN adalah VLAN 1, maka dari itu kita tidak boleh memasukkan vlan 1, minimal vlan 10.

```
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
10	**GROUP-1**	**active**	**Fa0/1, Fa0/2**
20	**GROUP-2**	**active**	**Fa0/3, Fa0/4**
1002	fddi-default	active	

Sekarang lakukan ping lagi dari PC1 ke PC3

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data :

Request time out.

Request time out.

Ping statistics for 192.168.1.3 :

    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Hasilnya akan RTO karena berbeda VLAN, sekarang coba kita ping dari VLAN yang sama (1 GROUP), misalnya PC1 ke PC2

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data :

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

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

Ping statistics for 192.168.1.2 :

    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-second:

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

LAB 7 – Trunking

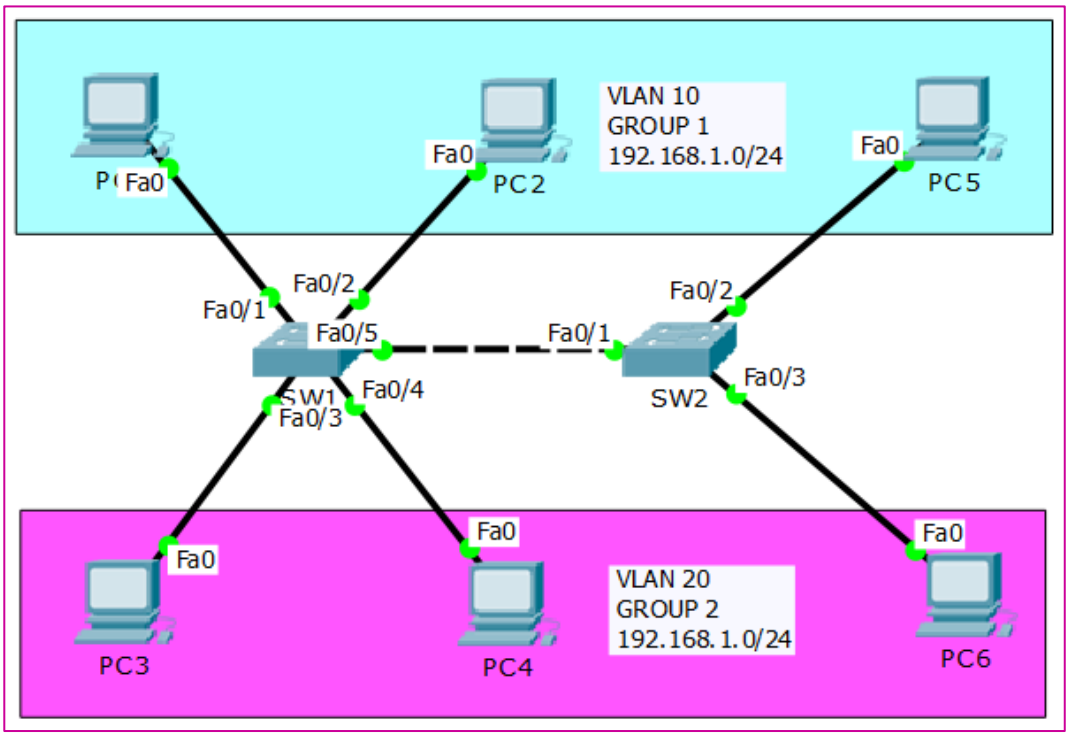
Trunking adalah sebuah konsep dimana sistem komunikasi dapat menyediakan akses jaringan untuk banyak client dengan satu set garis/frekuensi, dan tidak memebrikan secara individu.

Trunking digunakan untuk menghubungkan 2 switch yang menggunakan vlan dengan proses **encapsulation**. Jika kita memiliki beberapa switch dan menggunakan VLAN yang sama ataupun beda ditiap-tiap switchnya, maka kita harus mengkonfigurasi interface yang mengarah ke switch.

Dalam VLAN Trunking ada beberapa hal yang harus diperhatikan :

- Port Mode
  1. Mode Access : Port dengan mode ini hanya akan bisa membawa 1 VLAN, itulah mengapa biasanya mode ini di setting pada port switch yang terhubung ke **Endpoint** (PC, Server, Laptop, dll). Port mode access bisa saja digunakan untuk menghubungkan switch ke switch lain jika port tersebut memang benar-benar hany digunakan untuk membawa 1 VLAN.
  2. Mode Trunk : Pada mode ini bisa untuk membawa banyak VLAN. Port mode ini akan menajadi trunk jika pada switch lawan di setting ke mode trunk atau dynamic trunking protocol yang akan kita bahas di LAB berikutnya.

Berikut adalah topologi yang akan kita gunakan :



Gambar 7.1 Topologi Trunking

Kita akan melanjutkan dari konfigurasi dari lab yang sebelumnya. Karena tadi kita sudah mengkonfigurasi SW1 dan PC1-4, maka sekarang kita akan mengkonfigurasi SW2 dan PC5-6 saja.

Konfigurasikan IP address pada PC5 menggunakan 192.168.1.5/24 dan PC6 menggunakan 192.168.1.6/24

Dan coba kita lakukan ping dari PC5 ke PC6, maka hasilnya akan replay.

```
PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data :

Replay from 192.168.1.6: bytes=32  time=11ms  TTL=128

Replay from 192.168.1.6: bytes=32  time=16ms  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 = 1ms, Maximum = 15ms, Average = 0ms
```

Tetapi jika kita ping dari PC5 ke PC2 yang sudah di konfigurasi VLAN, maka hasilnya akan RTO (Request Time Out). Karena PC5 yang berada di SW2 menggunakan VLAN 1 (Default), sedangkan PC2 yang berada di SW1 menggunakan VLAN 20.

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data :

Request time out.

Request time out.

Ping Statistics for 192.168.1.2 :

    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C

^C
```

Sekarang kita konfigurasi PC5 agar menggunakan VLAN 10 dan PC6 VLAN 20.

```
Switch#conf t
Switch(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#name GROUP-1
SW2(config-vlan)#vlan 20
SW2(config-vlan)#name GROUP-2
SW2(config-vlan)#exit
SW2(config)#int fa 0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
SW2(config)#int fa 0/3
SW2(config-if)#sw mode acc
SW2(config-if)#sw acc vlan 20
SW2(config-if)#ex
```

Sekarang PC5 sudah menggunakan VLAN 20 sekarang coba test ping lagi ke PC2.

```
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data :
Request time out.
Request time out.
Ping Statistics for 192.168.1.2 :
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```

Hasilnya akan RTO karena kita menggunakan switch yang berbeda, maka interface yang terhubungnya harus di konfigurasi trunk.

```
SW1(config)#int fa 0/5

SW1(config-if)#switchport mode trunk



SW2(config)#int fa 0/1

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

Kita dapat mengkonfigurasi pada salah satu switch ataupun keduanya. Kita dapat mengecek konfigurasi trunk dengan perintah **show interface trunk**.

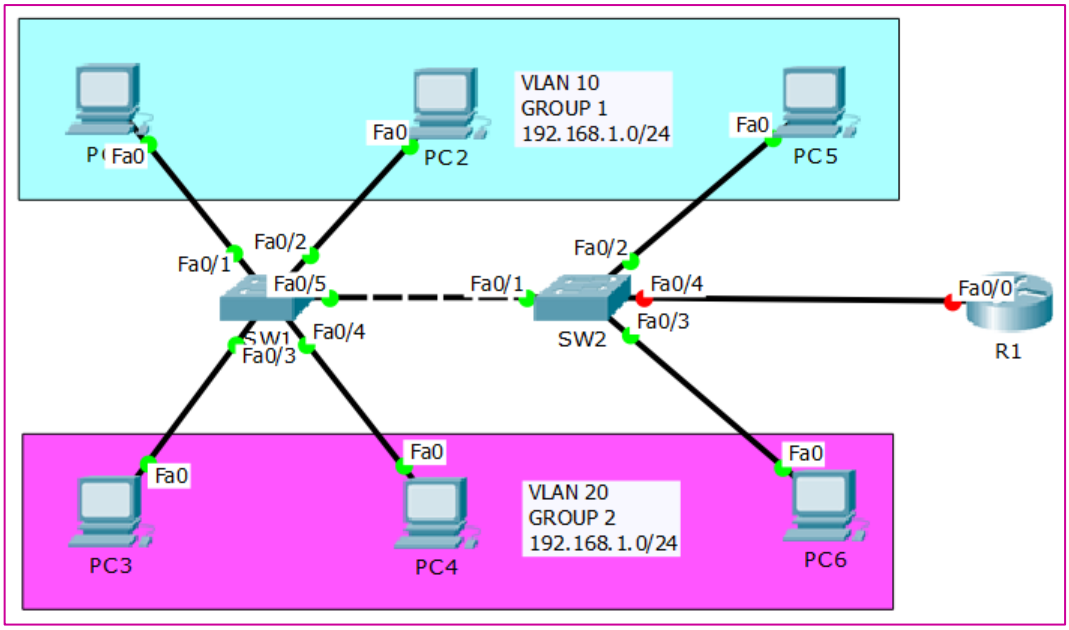
```
SW1#show int trunk
Port    Mode    Encapsulation    Status      Native vlan
Fa0/5   on      802.1q           trunking    1

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 PC2

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data :

Replay from 192.168.1.2: bytes=32  time=11ms  TTL=128

Replay from 192.168.1.2: bytes=32  time=16ms  TTL=128

Replay 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 = 16ms, Average = 0ms
```

LAB 8 – InterVLAN Routing (802.1Q)

InterVLAN routing digunakan untuk menghubungkan VLAN yanng berbeda Network menggunakan router. Router dapat kita konfigurasikan beberapa sub-interface yang sudah di encapsulation menjadi 802.1Q. Berikut adalah topologi jaringannya :



Gambar 8.1 Topologi InterVlan Routing

Kita akan melanjutkan konfigurasi dari lab sebelumnya. Penambahan router yang nantinya akan berfungsi sebagai gateway bagi semua PC. Interface antar R1 dan SW2 memang awalnya merah, karena pada R1 default interfacenya dalam keadaan shutdown.

Maka untuk menyalakannya/menghijaukan, tetapi sebelumnya kita beri hostname. Lakukanlah konfigurasi berikut :

Router>**en**

Router#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**hostname R1**

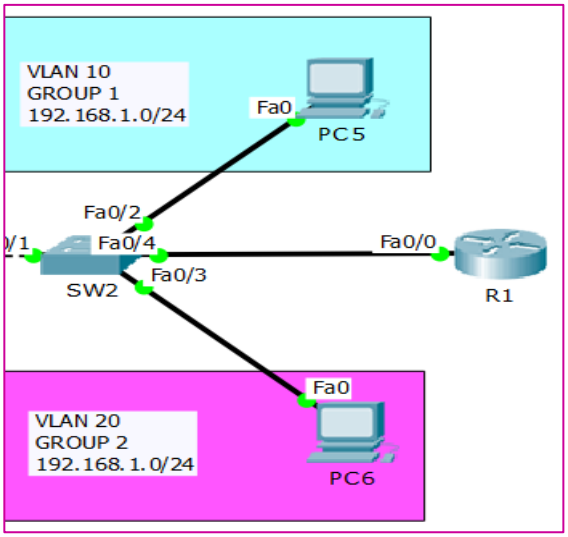
R1(config)#**int fa 0/0**

R1(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

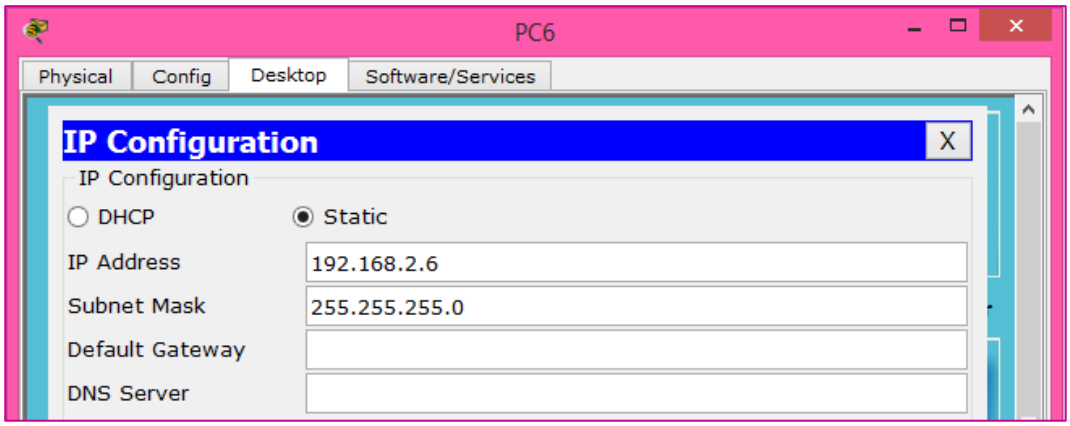
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Maka hasilnya seperti gambar berikut :



Gambar 8.2 Router telah di no shutdown

Sebelumnya ganti dulu IP Address pada VLAN 20 agar berbeda segmen



Gambar 8.3 Konfigurasi IP Address pada VLAN 20

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

R1(config)#**int fa 0/0.10**
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

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 fa 0/0.20**

```
R1(config-subif)#encapsulation dot1q 20

R1(config-subif)#ip address 192.168.2.254 255.255.255.0

R1(config-subif)#ex
```

Kemudian check Ip Address yang sudah kita buat tadi :

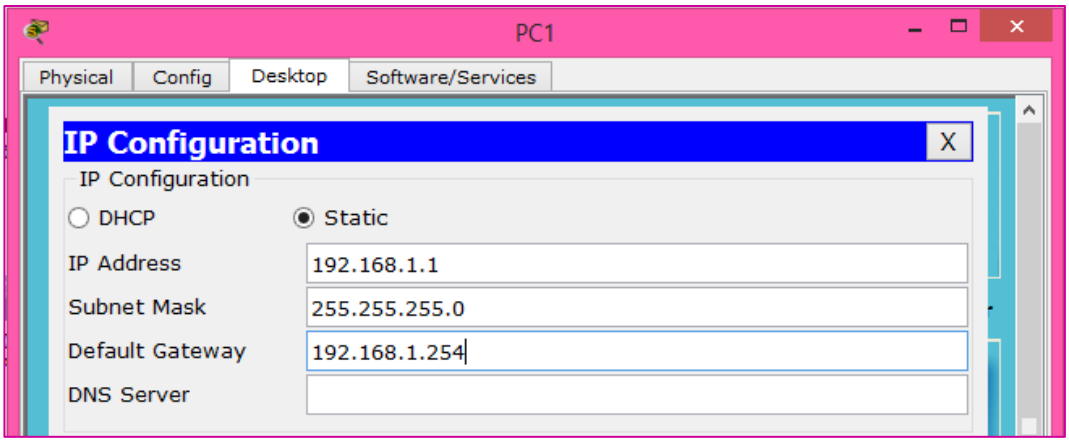
```
R1#show ip int br

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 yang mengarah ke-router.

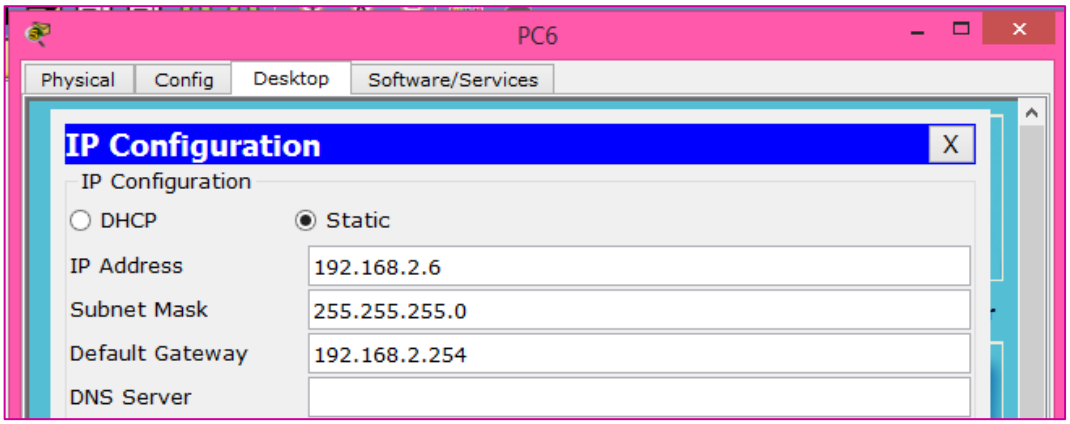
```
SW2(config)#int fa 0/4

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

Konfigurasikan 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 8.4 Konfigurasi IP Gateway pada VLAN 10



Gambar 8.5 Konfigurasi IP Gateway pada VLAN 20

Sekarang coba lakukan ping antara PC1 dan PC6

PC>**ping 192.168.2.6**

Pinging 192.168.2.6 with 32 bytes of data :

Request time out.

Replay from 192.168.2.6: bytes=32 time=1ms TTL=127

Replay from 192.168.2.6: bytes=32 time=15ms TTL=127

Replay from 192.168.2.6: bytes=32 time=13ms TTL=127

Ping Statistics for 192.168.2.6 :

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

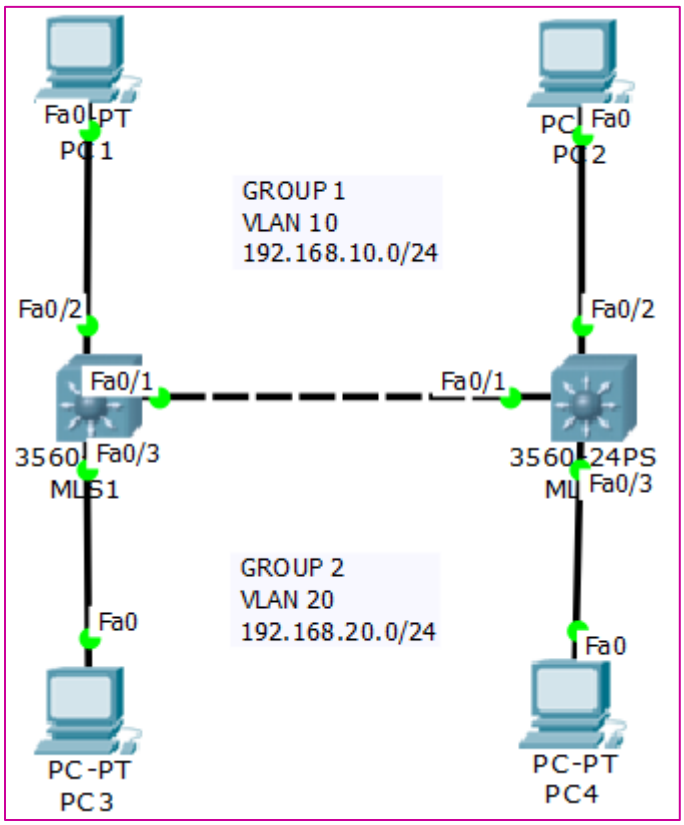
Minimum = 1ms, Maximum = 15ms, Average = 9ms

Maka hasilya akan replay ^_^

LAB 9 – Konfigurasi Trunk pada MLS (Switch L3)

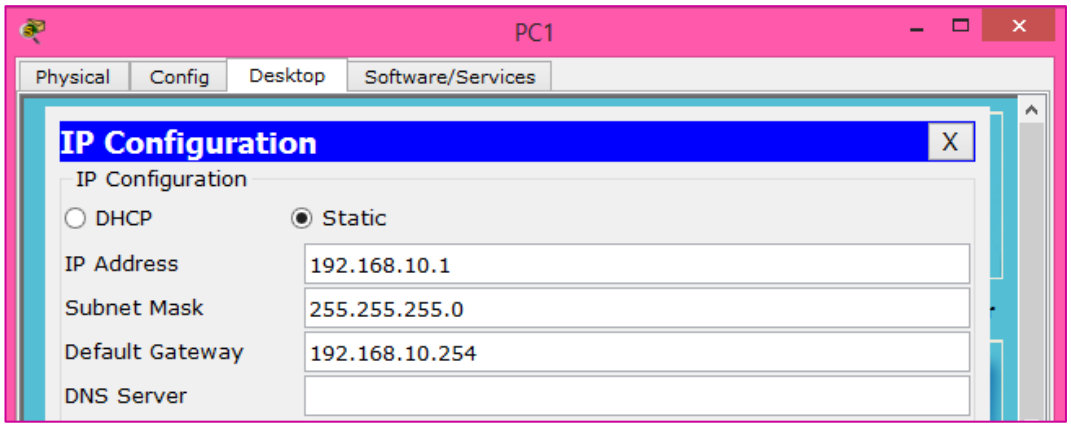
MLS (Multi Layer Switch) merupakan switch yang mensupport Layer 3 dan Layer 2. Jadi pada switch ini kita dapat mengkonfigurasi IP Address dan melakukan routing.

Untuk konfigurasi VLAN pada MLS sama seperti pada Switch Layer 2, tetapi jika mengkonfigurasi trunk sedikit berbeda.

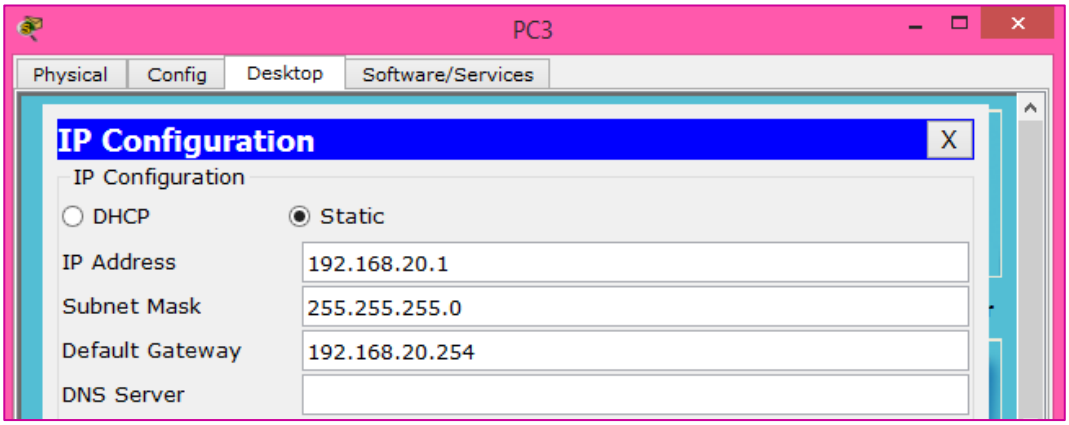


Gambar 9.1 Topologi Trunking MLS Switch

Konfigurasikan IP Address pada tiap-tiap PC. Dan untuk gatewaynya kita memakai IP host 254.



Gambar 9.2 Konfigurasi IP Address pada VLAN 10



Gambar 9.3 Konfigurasi IP Address pada VLAN 20

Kemudian kita konfigurasikan VLAN pada MLS1

```
Switch>en

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname MLS1

MLS1(config)#vlan 10

MLS1(config-vlan)#ex


MLS1(config-vlan)#name GROUP-1

MLS1(config)#vlan 20

MLS1(config-vlan)#name GROUP-2
```

Kemudian arahkan interface PC di MLS1 ke VLAN yang sudah dibuat tadi

```
MLS1(config)#int fa 0/2

MLS1(config-if)#sw mode acc

MLS1(config-if)#sw acc vlan 10

MLS1(config-if)#ex

MLS1(config)#int fa 0/3

MLS1(config-if)#sw mode acc

MLS1(config-if)#sw acc vlan 20
```

Dan Konfigurasi IP Address sebagai Gateway pada MLS1

```
MLS1(config)#int vlan 10
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

MLS1(config-if)#ip address 192.168.10.254 255.255.255.0

MLS1(config-if)#int vlan 20
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed
state to up

MLS1(config-if)#ip address 192.168.20.254 255.255.255.0

MLS1(config-if)#ex

MLS1(config)#ip routing
```

IP Routing digunakan untuk mengaktifkan fitur routing pada Switch Layer 3.

Dan pada interface **harus di encapsulation menjadi dot1q** terlebih dahulu sebelum di trunk. Lakukanlah konfigurasi berikut :

```
MLS1(config)#int fa 0/1

MLS1(config-if)#switchport trunk encapsulation dot1q

MLS1(config-if)#sw mode trunk
```

Selanjutnya kita konfigurasikan MLS2

```
Switch>en

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname MLS2

MLS2(config)#vlan 10

MLS2(config-vlan)#name GROUP-1

MLS2(config)#vlan 20

MLS2(config-vlan)#name GROUP-2

MLS2(config-vlan)#ex
```

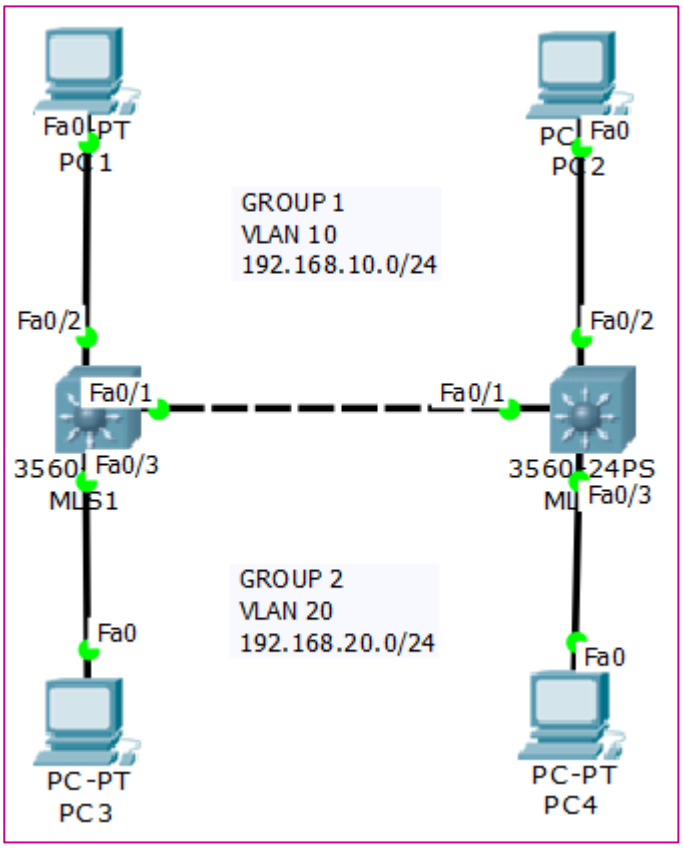
```
MLS2(config)#int fa 0/2
MLS2(config-if)#sw mode acc
MLS2(config-if)#sw acc vlan 10
MLS2(config-if)#ex
MLS2(config)#int fa 0/3
MLS2(config-if)#sw mode acc
MLS2(config-if)#sw acc vlan 20
MLS2(config)#int fa 0/1
MLS2(config-if)#sw trunk encapsulation dot1q
MLS2(config-if)#sw mode trunk
```

MLS2 hanya berfungsi sebagai switch biasa, oleh karena itu tidak di konfigurasi IP Routing dan IP Address. Sekarang lakukan ping dari PC1 ke PC3. Hasilnya akan replay karena kita sudah mengaktifkan fitur routing pada MLS.

```
PC>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data :
Request time out.
Replay from 192.168.20.1: bytes=32   time=16ms   TTL=127
Replay from 192.168.20.1: bytes=32   time=0ms    TTL=127
Replay from 192.168.20.1: bytes=32   time=0ms    TTL=127
Ping Statistics for 192.168.20.1 :
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 5ms
```

LAB 10 – Konfigurasi DHCP Server

Fungsi dari **DHCP Server** adalah memberikan pengalamatan IP Address secara otomatis pada client yang **mengaktifkan DHCP Client**. Untuk DHCP Server pada switch maupun router sama saja. Berikut adalah topologi yang akan kita gunakan :



Gambar 10.1 Topologi DHCP Server

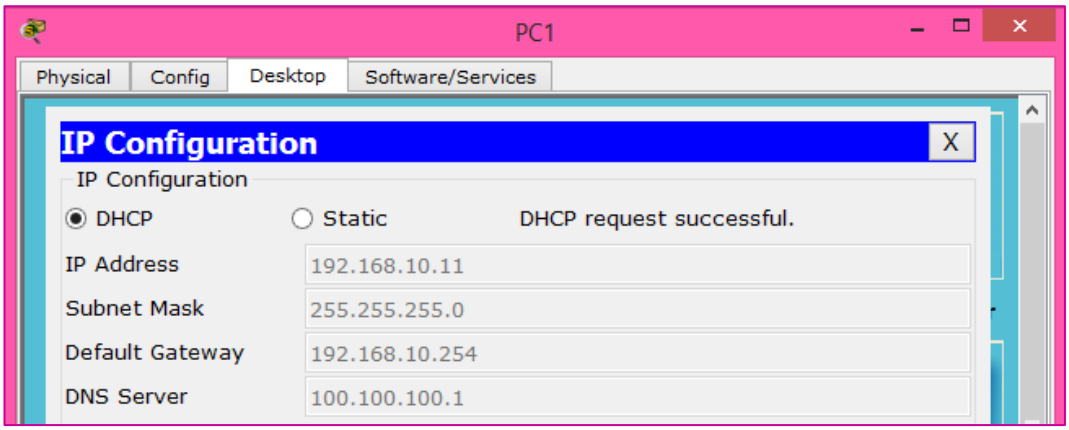
Kita melanjutnya konfigurasi dari lab sebelumnya. Hanya saja sekarang kita akan mengkonfigurasi DHCP Server dan DHCP Client pada PC1-4.

```
MLS1(config)#ip dhcp pool GROUP-1

MLS1(dhcp-config)#network 192.168.10.0 255.255.255.0

MLS1(dhcp-config)#dns-server 100.100.100.1

MLS1(dhcp-config)#default-router 192.168.10.254

MLS1(dhcp-config)#exit
```

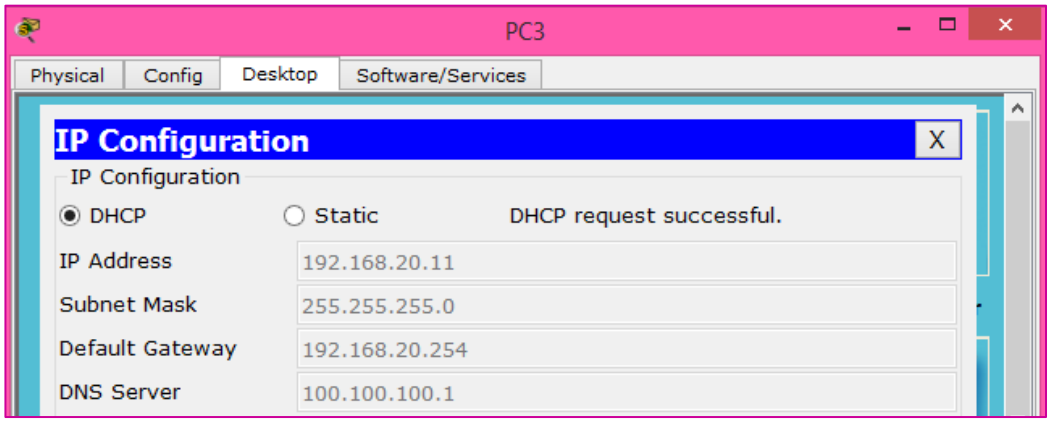
```
MLS1(config)#ip dhcp pool GROUP-2
MLS1(dhcp-config)#network 192.168.20.0 255.255.255.0
MLS1(dhcp-config)#dns-server 100.100.100.1
MLS1(dhcp-config)#default-router 192.168.20.254
MLS1(dhcp-config)#exit
MLS1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
MLS1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
```

GROUP-1 dan GROUP-2 hanya nama pool, dapat diberi dengan nama apa saja sesuka hati kalian. **Ip dhcp excluded-address** digunakan bilamana ada IP Address yang **tidak ingin kita bagikan kepada Client**. **Pada perintah diatas kita tidak akan membagikan ip host dari 1-10.**

Oleh karena itu client akan mendapatkan ip 11-253 karena memiliki prefix /24. Sekarang kita aktifkan DHCP Client pada PC.



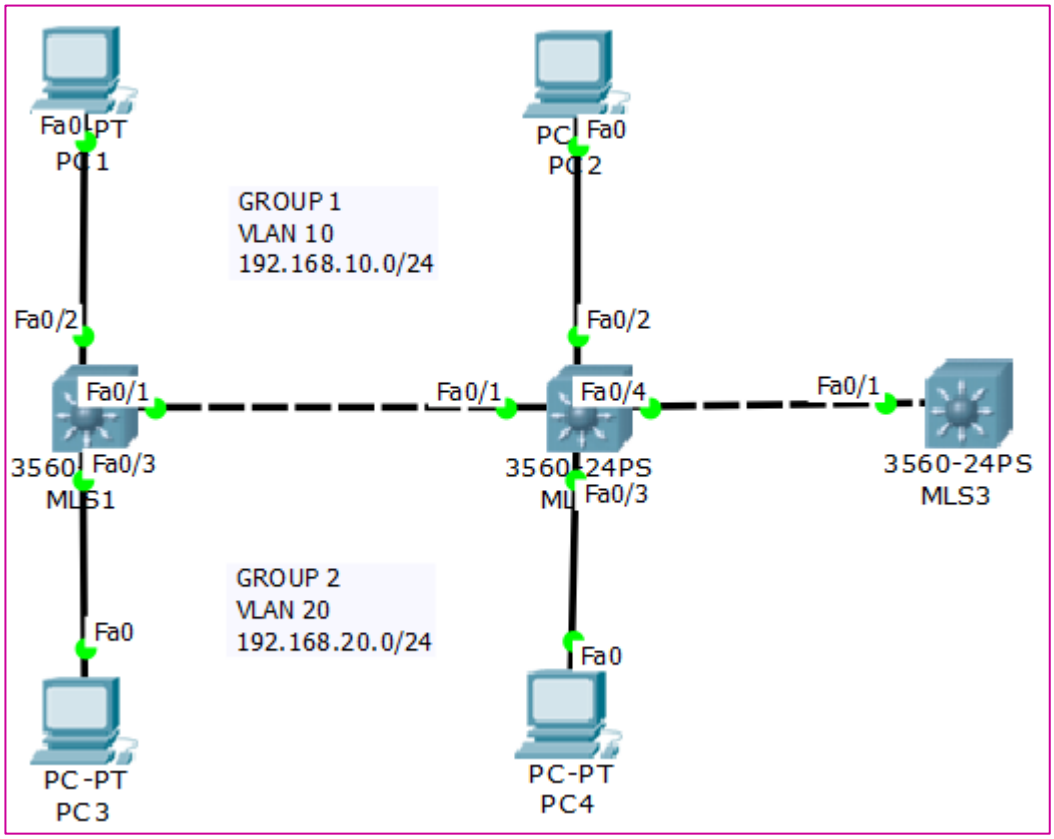
Gambar 10.2 DHCP Client pada PC1



Gambar 10.3 DHCP Client pada PC3

LAB 11 – Konfigurasi DHCP Client pada Switch atau Router

Misalkan ada DHCP Server yang dikonfigurasi pada jaringan dan kita ingin menggunkan DHCP Client pada switch ataupun router. Bisa dikatakan tujuan kita di lab ini adalah **memberikan ip client pada switch atau router**, jadi perangkat tersebut berfungsi selayaknya client. Karena ini tentang switching maka kita akan menggunakan Switch Layer 3 (MLS).



Gambar 11.1 Topologi DHCP Client

Kita udah terlebih dahulu interface fa 0/4 agar menggunakan VLAN 20

```
MLS2(config)#int fa 0/4

MLS2(config-if)#sw mode acc

MLS2(config-if)#sw acc vlan 20
```

Kemudian kita konfigurasikan DHCP Client pada MLS3

```
Switch(config)#hostname MLS3

MLS3(config)# int fa 0/1

MLS3(config-if)#no switchport

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

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

Switch(config-if)#ip address dhcp
```

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

Jika sudah mendapatkan IP Address maka akan mendapatkan log seperti berikut :

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

Dapat juga kita mengeceknya dengan perintah **show ip interface brief**

```
MLS3#sh 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
```

Sekarang coba kita lakukan ping dari MLS3 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 100 percent (5/5), round-trip min/avg/max = 0/6/12 ms
```

LAB 12 – Telnet pada Switch atau Router

Telnet (Telecommunications Network Protocol) merupakan remote login yang terjadi pada sebuah jaringan internet disebabkan karena adanya service dari protocol telnet yang memungkinkan penggunanya dapat login dan bekerja pada sistem jarak jauh. Dengan adanya telnet, pengguna dapat mengakses komputer lain secara remote melalui jaringan internet.

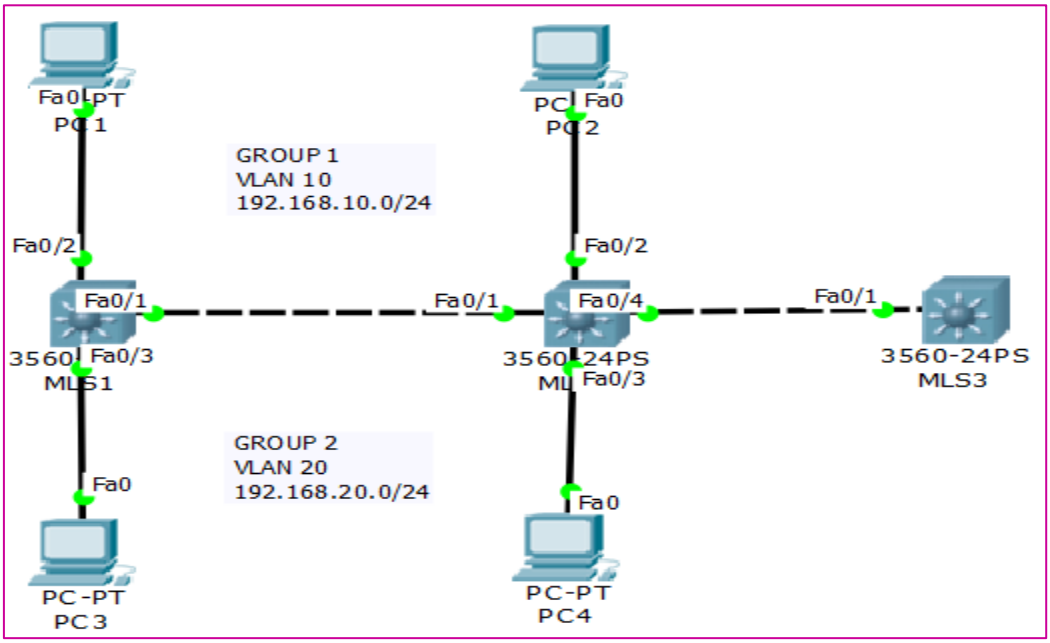
Berdasarkan penggunaannya, telnet memakai 2 program yaitu :

1. Client : Program pada client digunakan untuk meminta layanan pada server.
2. Server : Program yang terdapat pada server akan memberikan layanan yang diminta oleh client.

telnet mempunyai beberapa kelebihan dan kekurangan diantaranya :

1. **Kelebihan** : User interface yang cukup ramah. Maksudnya pengguna dapat memberikan perintah dari jarak jauh (remote) jadi seolah-olah penggunanya mengeksekusi perintah pada command line komputer.
2. **Kekurangan** : Dimana ada kelebihan selalu ada kekurangan. Adapun kekurangan dari telnet yaitu pengguna NTLM authentication tanpa adanya encrypsi, sehingga dapat memudahkan pencurian password yang dilakukan oleh sniffers.

Untuk konfigurasi telnet pada switch dan router sama saja. Hanya berbeda pada saat pemasangan IP Address. Jika di switch pada interface VLAN, sedangkan di router pada interface Physical. Berikut adalah topologi yang akan kita gunakan :



Gambar 12.1 Topologi Telnet

Kita akan melanjutkan konfigurasi pada lab sebelumnya. Kita akan mengkonfigurasi telnet pada (MLS yang terhubung ke MLS yang akan dibuat telnet) MLS2 dan membuat VLAN 30 sebagai remote-access.

```
MLS2(config)#vlan 30

MLS2(config-vlan)#name Remote-Access

MLS2(config-vlan)#ex


MLS2(config)#int vlan 30

MLS2(config-if)#ip address 30.30.30.10 255.255.255.0

MLS1(config)#enable secret 123

MLS1(config)#line vty 0 4

MLS1(config-line)#password devi
```

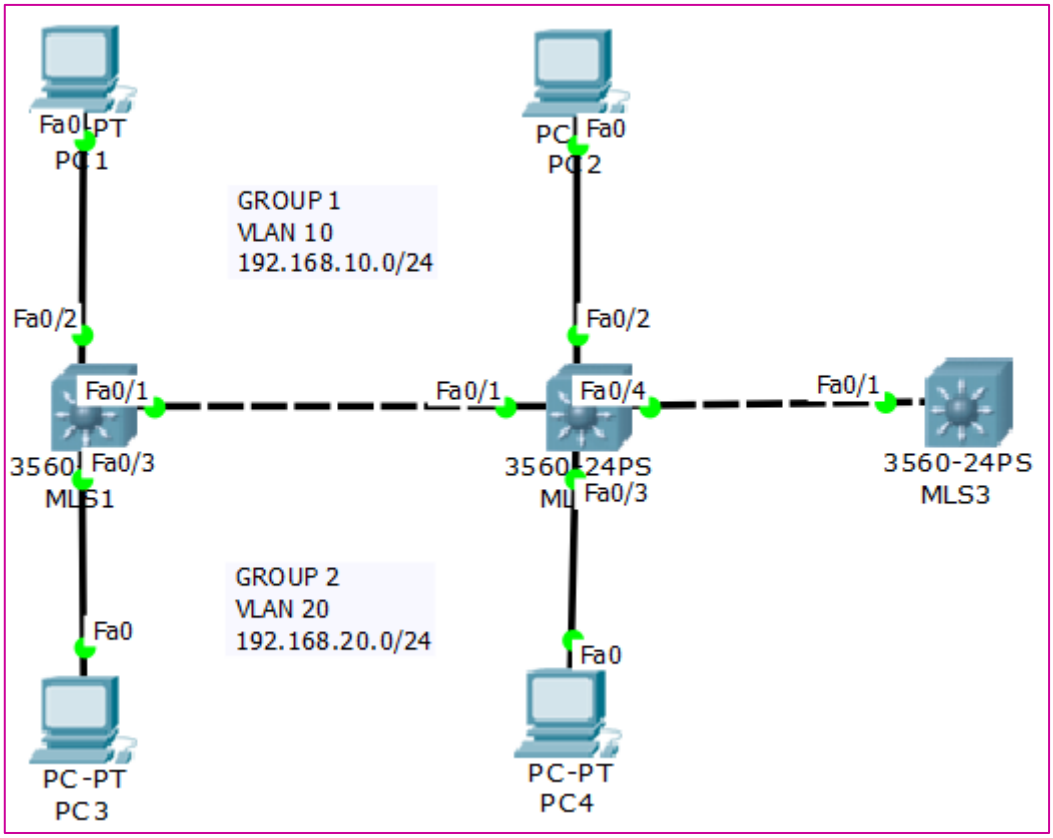
Enable secret untuk mengkonfigurasi password pada saat masuk ke mode privileged. **Line vty 0 4** akan membuat telnet dengan 5 user aktif sekaligus (0-4). **Password** untuk password telnetnya.

```
MLS2#telnet 30.30.30.10

Trying 30.30.30.10 ...Open

User Access Verification

Password: (123)

MLS2>en

Password:

MLS2#ping 30.30.30.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/19 ms

MLS2#sh 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 13 – SSH pada Switch atau Router

SSH (Secure Shell) adalah sebuah protocol jaringan yang terencrypsi untuk menjalankan Shell Session (terminal) dengan aman dan tidak bisa terbaca oleh orang lain karena terkoneksi melalui SSH Tunneling. Jadi website, account, dll yang kita input tidak akan tercatat pada log dirouter ataupun server.

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



Gambar 13.1 Topologi SSH

Kita akan menggunakan topologi sebelumnya. Selanjutnya tinggal kita atur SSH pada MLS2.

MLS2(config)#**username SSH password devi**

MLS2(config)#**ip domain name devi.kgb**

MLS2(config)#**crypto key generate rsa**

The name for the keys will be: MLS2.devi.kgb
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]

MLS2(config)#line vty 0 4

*Mar 1 0:41:45.233: RSA key size needs to be at least 768 bits for ssh version
2
*Mar 1 0:41:45.233: %SSH-5-ENABLED: SSH 1.5 has been enabled

MLS2(config-line)#transport input ssh

MLS2(config-line)#login local

MLS2(config-line)#ex
```

Buat terlebih dahulu loginnya (username dan password), kemudian ganti domainnya. **Transport input** akan mengubah yang awalnya telnet menjadi SSH

Test remote dari Client PC

```
PC>ssh -1 SSH 30.30.30.10
Open
Password : (devi)

MLS2>en

Password: (123)

MLS2#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
```

Dan jika kita menggunakan telnet, maka tidak akan bisa. Karena tadi kita sudah menggantinya dengan SSH.

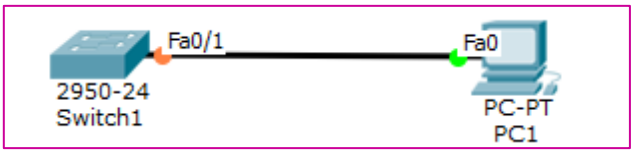
```
MLS2#telnet 30.30.30.10
Trying 30.30.30.10 ...Open

[Connection to 30.30.30.10 closed by foreign host]
```

LAB 14 – Spanning Tree Portfast

Pada saat kita mengoneksikan kabel ke switch maka warna awalnya adalah orange, kemudian berubah menjadi hijau. Ada proses yang memakan waktu 50 detik yaitu :

Bloking	➔	**Listening**	➔	**Learning**	➔	**Forwading**
	20 sec		15 sec		15 sec	

Berikut adalah topologi yang kita gunakan :



Gambar 14.1 Spanning Tree Portfast

Dan jika mengarak ke client tidak akan dibutuhkan. Kita dapat mempercepatnya dengan **portfast.**

```
Switch(config)#hostname Switch1

Switch1(config)#int fa 0/1

Switch1(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 has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.

Switch1(config-if)#ex
```

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

```
Switch1(config)#int ra fa 0/1-5

Switch1(config-if-range)#spanning-tree portfast

Switch1(config)#spanning-tree portfast default
```

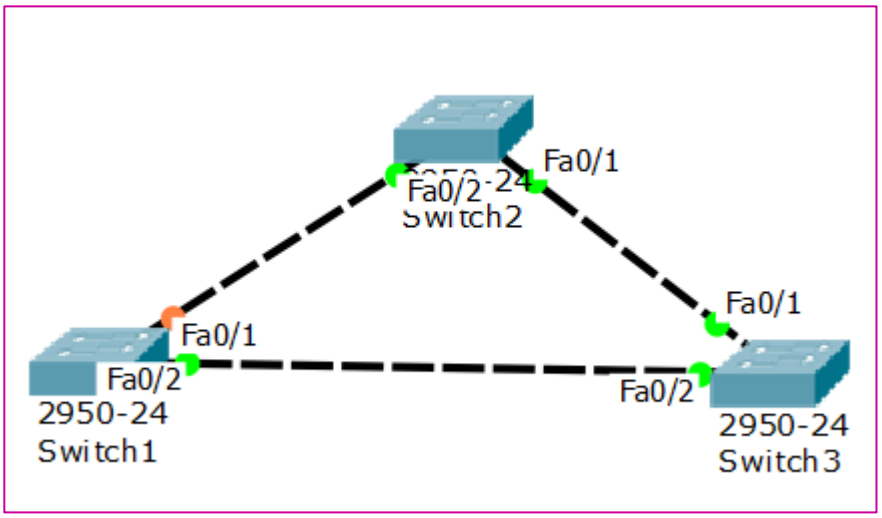
```
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%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.
```

Port-fast default akan mengaktifkan portfast pada semua port interfacenya.

Untuk pengujian coba lakukan penambahan device seperti PC, maka akan langsung hijau tanpa orange terlebih dahulu.

LAB 15 – Spanning Tree Protocol (PVST)

STP atau Spanning Tree Protocol adalah protocol yang digunakan untuk mencegah looping pada switch. Karena jika switch tidak mengetahui paket data yang dikirim maka akan melakukan broadcasting, ke semua interface kecuali pengirim. Berikut adalah topologi yang akan kita gunakan :



Gambar 15.1 Topologi STP

Misalnya ada paket data yang tidak diketahui oleh Switch1, maka Switch1 akan memberikan ke Switch3. Kemudian Switch3 bila tidak tahu akan memberikannya ke Switch2 (0/1). Dan bila Switch2 tidak tahu maka akan mengirimkan lagi ke Switch1. Inilah yang dinamakan looping. (muter-muter aja disitu)

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

1. Jika prioritynya yang paling terbesar maka akan diblock
2. Dilihat dari cost yang terbesar akan di block
3. Dilihat dari Prio. NBR nya yang paling terbesar
4. Dilihat dari Mac-addressnya yang terbesar

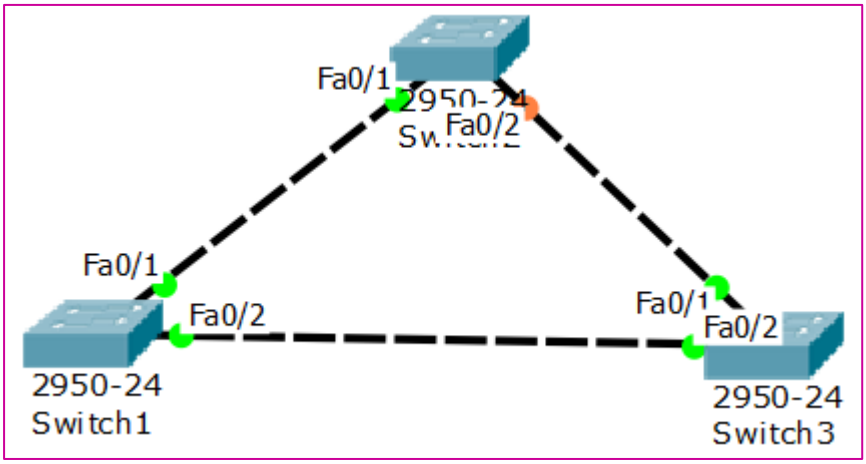
```
Switch1#show spanning-tree

VLAN0001
    Spanning tree enabled protocol ieee
    Root ID     Priority    32769
                Address     0001.C7A4.76B8
                Cost        19
                Port        2(FastEthernet0/2)
                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
     Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
                Address     00D0.D301.3D49
                Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
                Aging Time  20

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

Jika dilihat pada topologi, Switch1 lah yang diblock karena memiliki mac-address terbesar. Sekarang kita ganti prioritynya, maka nanti pada Switch1 tidak akan diblock. Kita pilih priority yang terkecil.

```
Switch1(config)#spanning-tree vlan 1 priority 409 (enter)

% 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

Switch1(config)#spanning-tree vlan 1 priority 4096
```

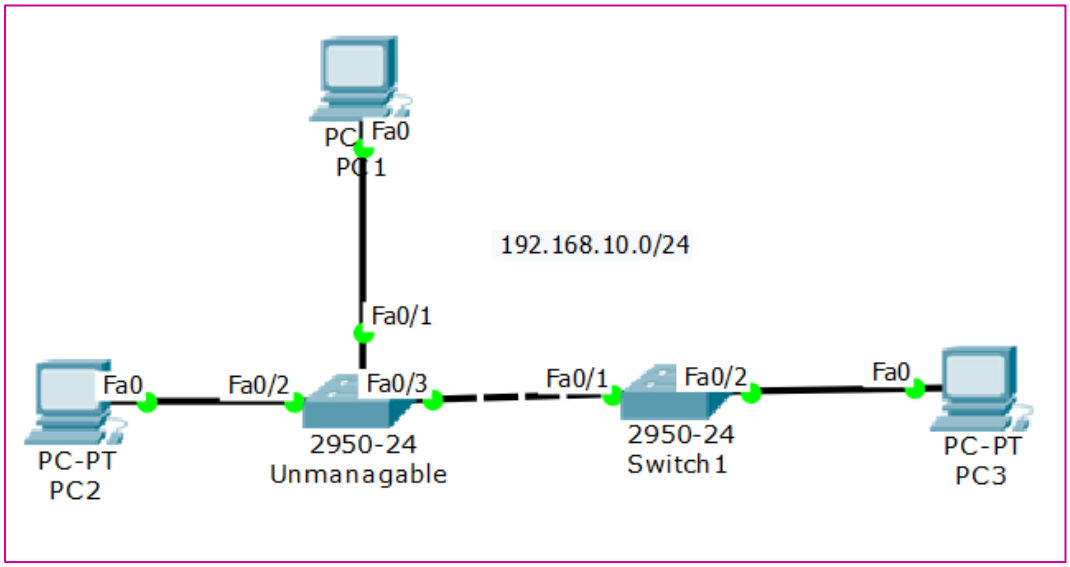
Maka yang diblock akan pindah ke priority yang besar, seperti gambar berikut :



Gambar 15.2 Topologi sesudah diganti priority

LAB 16 – Mengamankan Interface dengan Port-Security

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



Gambar 16.1 Topologi Port-Security

Port-security dapat digunakan untuk :

1. Membatasi jumlah mac-address pada suatu interface
2. Mengizinkan **hanya** mac-address tertentu yang dapat menggunakannya

Seperti topologi diatas, kita memiliki Unmanagable switch dan managable switch (switch1). Misalkan kita hanya mengijinkan PC2 saja yang boleh terkoneksi dengan PC3. Maka kita membatasi hanya dengan 1 mac-address saja yang boleh melewati PC3 yaitu PC2. Sebelumnya kita konfigurasi IP Address terlebih dahulu pada semua PC. Lalu coba lakukan test ping dari PC1 ke PC3.

PC>**ping 192.168.10.3**

Pinging 192.168.10.3 with 32 bytes of data :

Request time out.

Replay from 192.168.10.3: bytes=32 time=39ms TTL=128

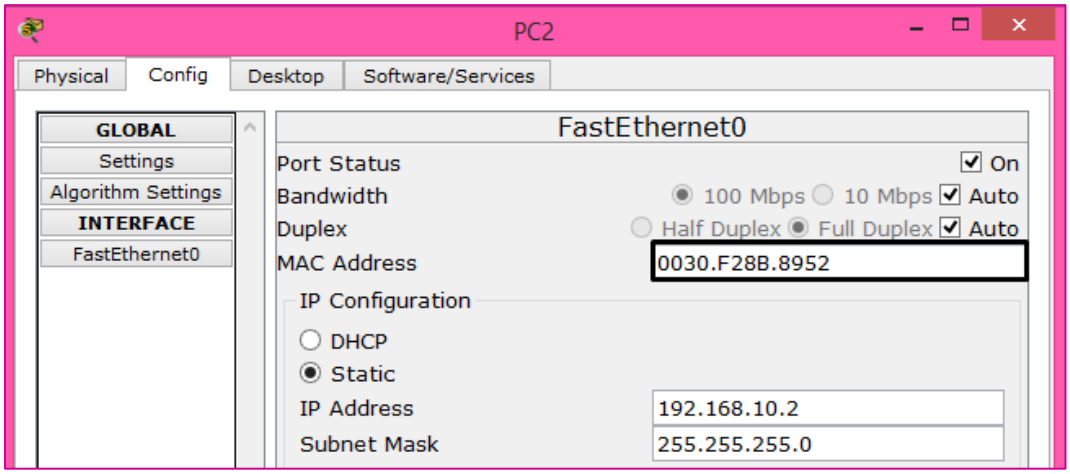
Replay from 192.168.10.3: bytes=32 time=18ms TTL=128

Ping Statistics for 192.168.10.3 :

```
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 39ms, Average = 19ms
```

Otomatis bisa ngeping karena itu menggunakan konfigurasi default.

Sekarang kita lihat terlebih dahulu Mac-address yang dimiliki PC2 yaitu 0030.F28B.8952 (jadi hanya PC2 yang diberi izin)

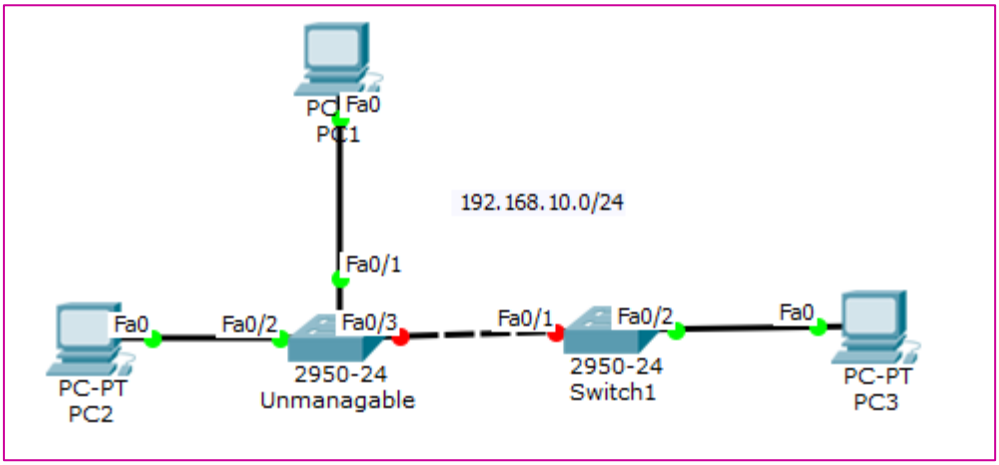


Gambar 16.2 Mac-address pada PC2

Kemudian konfigurasikan port-security pada Switch1

```
Switch1(config)#int fa 0/1

Switch1(config-if)#sw mode acc

Switch1(config-if)#sw port-security

Switch1(config-if)#sw port-security max 2

Switch1(config-if)#sw port-security mac-address 0030.F28B.8952

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
```

Maka interface nya akan **mati**, ini dikarenakan PC1 tidak diberi izin.



Gambar 16.3 Topologi ketika sudah dilakukan konfigurasi port-security

Untuk menyalakannya ketik perintah berikut :

```
Switch1(config)#int fa 0/1

Switch1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down

Switch1(config-if)#no shutdown
```

Ada 3 mode violation (yang akan terjadi jika ada yang melanggar) :

```
Switch1(config-if)#switchport port-security violation ?

    protect Security violation protect mode

    restrict Security violation restrict mode

    shutdown Security violation shutdown mode
```

1. **Protect : Memblock tetapi tidak mengirimkan message**
2. **Restrict : Memblock tetapi akan mengirimkan message**
3. **Shutdown : Akan *men*-shutdown interface**

Kita juga konfigurasi agar mac-addressnya secara otomatis

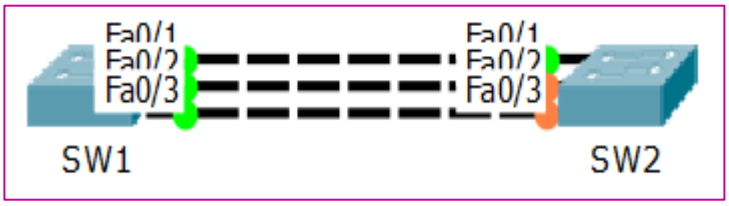
```
Switch1(config-if)#switchport port-security mac-address sticky
```

LAB 17 – EtherChannel LaCP

EtherChannel adalah teknik trunking dimana sebuah port pada device (switch) digabung menjadi satu jalur logika dalam sebuah grup. Berfungsi untuk meningkatkan kecepatan koneksi antar switch. Bisa mencegah looping karena mekanisme STP (Blocking Port). EtherChannel LaCP (Link Aggregation Control Protocol) yang merupakan Open Standard milik IEEE dan mengijinkan pengguna untuk mengabungkan beberapa port fisik menjadi sebuah channel logical tunggal.

Ada 3 type EtherChannel, yaitu :

1. L2 EtherChannel LaCP (Open Standard)
2. L2 EtherChannel PaGP (Cisco Proprietary atau protocol yang hanya digunakan untuk perangkat cisco)
3. L3 EtherChannel



Gambar 17.1 Topologi LaCP

Seperti yang terlihat pada gambar diatas metode STP akan hanya membolehkan satu interface saja yang aktif. Dengan metode EtherChannel, kita akan menggabungkan semua interfacenya menjadi satu.

Pada LaCP ada 2 mode yaitu :

1. Active
2. Passive

Satu switch harus menggunkan **mode active**, sedangkan yang satunya lagi dapat menggunakan **active/passive. Tidak bisa menggunakan passive-passive.** Karena nanti sama-sama diam/tidak ada jawaban.

Lakukan konfigurasi pada SW1 dan SW2 :

- SW1

```
SW1(config)#interface range fa 0/1-3

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

Creating a port-channel interface Port-channel 1

SW1(config-if-range)#channel-protocol lacp
```

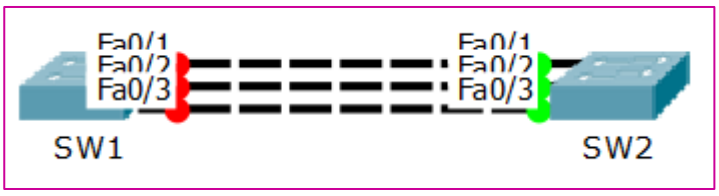
```
SW1(config-if-range)#ex

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

- SW2

```
SW2(config)#int range fa 0/1-3
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)#int port-channel 1
SW2(config-if)#switchport mode trunk
```

Setelah kita konfigurasi, akan terbuat **interface** baru yaitu **port-chennel 1** yang didapat dari **channel-group 1** *(terserah mau channel berapa)*. Interface inilah yang menjadi gabungan dari 3 interface diatas. **Mode trunk** digunakan supaya perangkat antar switch dapat berkomunikasi.

Sebelumnya 3 interface akan **merah**

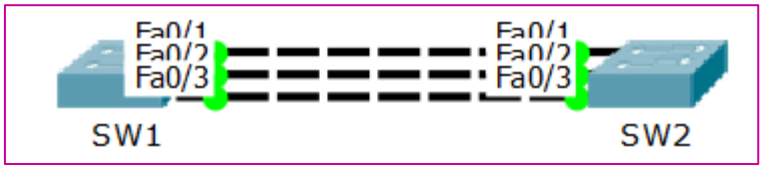


Gambar 17.2 Topologi setelah dikonfigurasi

Untuk menghijaukan kita lakukan konfigurasi berikut :

```
SW1(config-if-range)#shutdown

SW1(config-if-range)#no shutdown
```

Taraaaa sekarang kabel sudah hijau semua



Gambar 17.3 Kabel Topologi sudah hijau

Dapat kita cek 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)
```

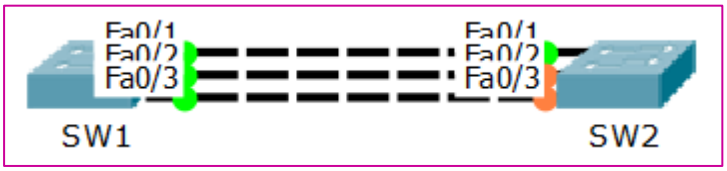
LAB 18 – EtherChennel PaGP

PaGP (Port Aggregation Protocol) merupakan Cisco Proprietary digunakan untuk membuat EtherChannel otomatis. Paket PaGP dikirim diantara port EtherChannel untuk negosiasi formasi dari channel

Ada 2 mode pada PaGP, yaitu :

1. Auto
2. Desirable

Kita menggunakan topologi pada lab sebelumnya



Gambar 18.1 Topologi PaGP

Kita hanya dapat menggunakan mode **Desirable-Desirable** atau **Desirable-Auto.**

Sekarang kita memakai mode Desirable-Desirable, lakukan konfigrasi seperti pada SW1 berikut :

```
SW1(config)#interface range fa 0/1-3

SW1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

SW1(config-if-range)#channel-protocol pagp

SW1(config-if-range)#ex


SW1(config)#interface port-channel 1

SW1(config-if)#switchport mode trunk
```

Setelah itu kita konfigurasi SW2

```
SW2(config)#int ra fa 0/1-3

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

Creating a port-channel interface Port-channel 1

SW2(config-if-range)#channel-protocol pagp
```

```
SW2(config-if-range)#ex

SW2(config)#interface port-channel 1

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

Sebelumnya 3 kabel interface akan merah, untuk menghijaukannya kita lakukan konfigurasi berikut :

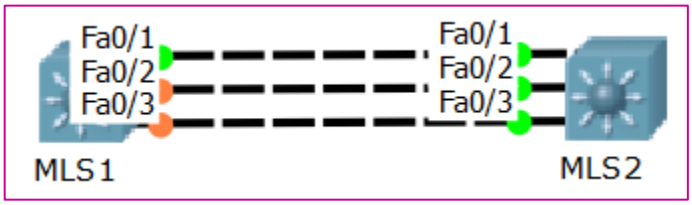
```
SW1(config-if-range)#shutdown

SW1(config-if-range)#no shutdown
```

Kita dapat mengecek dengan mengetikkan perintah berikut :

```
SW2(config)#do 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 19 – Static EtherChannel L3 (Layer 3)

Berikut adalah model topologi yang akan kita gunakan :



Gambar 19.1 Topologi Static EtherChannel L3

Untuk konfigurasi sama seperti pada Switch di layer 2, namun kali ini kita akan menggunakan static etherchannel. Static etherchannel pada setiap interface yang harus memiliki mode yang sama. Misalnya **access**, yaa access semua.

Terdapat beberapa mode di Ethercannel dapat dilihat dengan perintah :

```
SW1(config)#int ra fa 0/1-3

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
```

Kemudian kita konfigurasikan MLS1

```
MLS1(config)#int ra fa 0/1-3

MLS1(config-if-range)#no switchport

MLS1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1

MLS1(config-if-range)#ex

MLS1(config)#int port-channel 1

MLS1(config-if)#no switchport

MLS1(config-if)#ip address 12.12.12.1 255.255.255.0
```

Kemudian kita konfigurasikan pada MLS2

```
MLS2(config)#int ra fa 0/1-3

MLS2(config-if-range)#no switchport

MLS2(config-if-range)#channel-group 1 mode on

MLS2(config-if-range)#ex

MLS2(config)#int port-channel 1

MLS2(config-if)#no switchport

MLS2(config-if)#ip address 12.12.12.2 255.255.255.0
```

Kemudian kita bisa cek konfigurasinya dengan perintah

```
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 kita lakukan ping

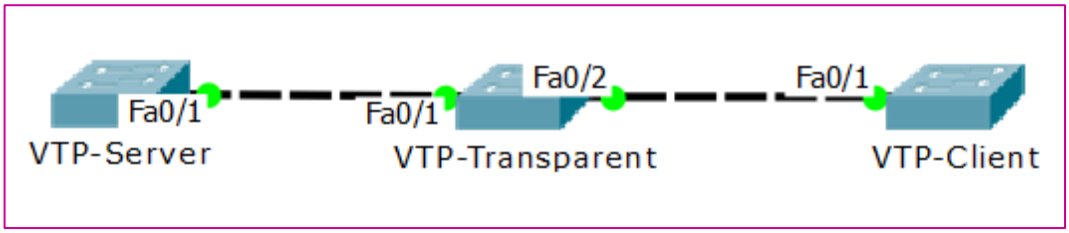
```
MLS1#ping 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/19/76 ms
```

LAB 20 – VTP (VLAN Trunking Protocol)

VTP digunakan ketika kita memiliki banyak switch dan memiliki VLAN yang sama. Kita hanya perlu mengkonfigurasi switch yang menjadi VTP Server maka switch yang menjadi VTP Client akan mengikuti VLAN yang di buat pada VTP Server, begitupun ketika ada perubahan di VTP Server. Sedangkan VTP Transparent hanya berfungsi sebagai penerus informasi yang sampai ke dirinya ke switch-switch yang lain.

Terdapat 3 mode pada VTP, yaitu :

1. Server
2. Transparent
3. Client



Berikut adalah topologi yang akan kita gunakan :

Gambar 20.1 Topologi VTP

Kemudian kita konfigurasikan trunk dan VTP pada switch

- VTP-Server

VTP-Server(config)#**int fa 0/1**

VTP-Server(config-if)#**switchport mode trunk**

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

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

VTP-Server(config-if)#**ex**

VTP-Server(config)#**vtp mode server**
Device mode already VTP SERVER.

VTP-Server(config)#**vtp domain devi.id**
Changing VTP domain name from NULL to devi.id

VTP-Server(config)#**vtp password 123**
Setting device VLAN database password to 123

- VTP-Transparent

```
VTP-Transparent(config)#int ra fa 0/1-2

VTP-Transparent(config-if-range)#sw mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

VTP-Transparent(config-if-range)#ex

VTP-Transparent(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.

VTP-Transparent(config)#vtp domain devi.id
Domain name already set to devi.id.

VTP-Transparent(config)#vtp password 123
Setting device VLAN database password to 123
```

- VTP-Client

```
VTP-Client(config)#int fa 0/1

VTP-Client(config-if)#sw mode trunk

VTP-Client(config-if)#ex

VTP-Client(config)#vtp mode client
Setting device to VTP CLIENT mode.

VTP-Client(config)#vtp domain devi.id
Domain name already set to devi.id.

VTP-Client(config)#vtp password 123
Setting device VLAN database password to 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
                                    1002 fddi-default active
                                    1003 token-ring-default active
                                    1004 fddinet-default active
                                    1005 trnet-default active
```

Belum ada VLAN yang terbentuk, jadi kita buat VLAN-nya

```
VTP-Server(config)#vlan 10

VTP-Server(config-vlan)#name Administrator
```

Coba kita lihat VLAN pada VTP-Client, apakah sudah terbentuk

```
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
10    Administrator                    active
```

Coba kita lihat VLAN pada switch VTP-Transparent

```
P-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
1002  fddi-default                     active
```

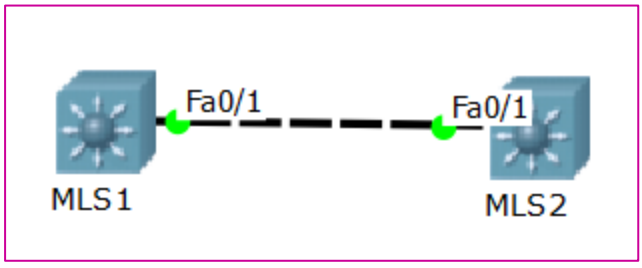
LAB 21 – DTP (Dynamic Trunking Protocol

DTP adalah pembuatan status pada switchport. Status switchport yang bagus ditentukan dari awal pembuatan, ingin dijadikan **Access** atau **Trunk.** namun jika belum menentukannya, kalian dapat menggunakan Dynamic Auto atau Dynamic Desirable. Dynamic Auto memiliki fungsi yang sama dengan mode Access yaitu membuat hubungan jaringan dengan mengatur IP komunikasi pada setiap port. Sedangkan Dynamic Desirable memiliki fungsi yang sama dengan mode Trunk yaitu membuat hubungan jaringan pada setiap port tanpa mengatur IP.

DTP mempunyai beberapa mode yaitu :

1. **Desirable** **:** Mode ini selalu ingin menjadi trunk apabila bertemu dengan mode auto, trunk dan desirable. Mode ini mengirim dan menerima pesan DTP.
2. **Auto** **:** Mode ini hanya bisa menerima pesan DTP yang datang. **Mode ini adalah mode default untuk kebanyakan switch**. Mode ini hanya menjadi trunk apabila bertemu dengan mode trunk dan desirable.
3. **Trunk** **:** Mode ini adalah mode default atau mode manual yang digunakan dalam membuat jalur trunking apabila bertemu dengan mode auto, desirable, dan trunk juga. **Mode ini kita pakai untuk yang mengarah ke Router/Switch lain.**
4. **Access** **:** Mode ini adalah jalur yang digunakan untuk 1 VLAN. Mode ini digunakan dalam 1 buah VLAN yang sama dan dalam 1 Switch (VLAN default pada switch cisco). **Mode ini kita pakai untuk mengarah ke Client.**
5. **No-Negotiate** **:** pada mode ini tidak mengaktifkan pesan DTP, sehingga tidak ada pengirim atau penerima DTP dari Switch lain.

Berikut adalah topologi yang akan kita gunakan :



Gambar 21.1 Topologi Dynamic Trunking Protocol

Kita check terlebih dahulu default apa saja yang sudah ada pada MLS, dengan perintah **"show interface fastethernet (0/1) switchport"**

MLS1#**sh int fa 0/1 switchport**

Name: **Fa0/1**

Switchport: **Enabled**

Administrative Mode: **dynamic auto**

Operational Mode: **static access**

Administrative Trunking Encapsulation: **dot1q**

Operational Trunking Encapsulation: **native**

Negotiation of Trunking: **On**

Access Mode VLAN: **1 (default)**

Trunking Native Mode VLAN: **1 (default)**

Terlihat bahwa Mode Dynamic Auto telah secara otomatis terkonfigurasi di 2 MLS. Maka hasilnya adalah Static Access. Sekarang coba kita ubah MLS1 dengan mode Dynamic Desirable.

MLS1(config)#**int fa 0/1**

MLS1(config-if)#**sw mode dynamic desirable**

Kemudian kita show lagi di MLS1, dan modenya pun berubah.

MLS1#**show int fa 0/1 sw**

Name: **Fa0/1**

Switchport: **Enabled**

Administrative Mode: **dynamic desirable**

Operational Mode: **trunk**

Coba kita show juga di MLS2

```
MLS2#show int fa 0/1 sw

Name: Fa0/1

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: trunk
```

Jika kita lihat, pada MLS1 modenya **Dynamic Desirable** dan MLS2 modenya **Dynamic Auto**. Maka hasilnya adalah **Trunk.**

Lalu bagaimana kalau kita ubah modenya menjadi Static dan Dynamic

- MLS1

```
MLS1(config)#int fa 0/1

MLS1(config-if)#sw mode trunk
```

Kemudian kita show lagi

```
MLS1#show int fa 0/1 sw

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk
```

Taraaa.. karena MLS1 adalah static dan MLS2 adalah dynamic auto maka hasilnya adalah **trunk.**

Untuk mempermudah, kalian dapat melihat tabel berikut ini :

	Static Trunk	Static Access	Dynamic Auto	Dynamic Desirable
Static Trunk	Trunk	Limited	Trunk	Trunk
Static Access	Limited	Access	Access	Access
Dynamic Auto	Trunk	Access	Access	Trunk
Dynamic Desirable	Trunk	Access	Trunk	Trunk

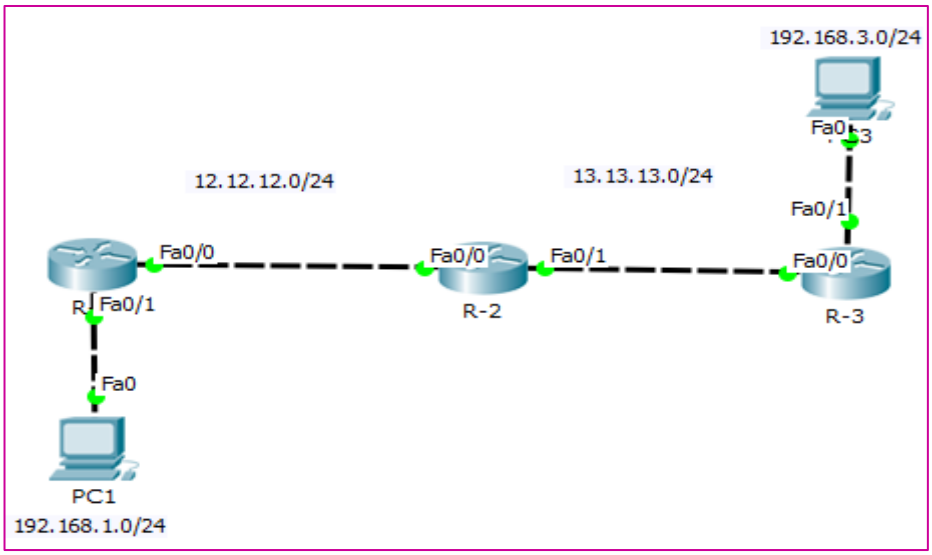
BAB III

Routing

LAB 22 – Static Routing

Static route adalah routing yang dilakukan secara manual ke routing tablenya. Bagaimana menentukan network tujuan, subnet mask, dan jalur router menuju networknya. Prinsip kerjanya adalah **kemana-lewat mana**.

Berikut adalah topologi yang kita gunakan :



Gambar 22.1 Topologi Static Route

Kita akan menggunakan loopback sebagai client nya. Sekarang kita konfigurasikan IP Address pada router.

- R-1

R-1(config)#**int fa 0/0**

Router(config-if)#**no shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

R-1(config-if)#i**p address 12.12.12.1 255.255.255.0**

R-1(config-if)#**ex**

R-1(config)#**int fa 0/1**

R-1(config-if)#**no shutdown**

R-1(config-if)#i**p address 192.168.1.1 255.255.255.0**

- R-2

R-2(config)#**int fa 0/0**

R-2(config-if)#**no shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R-2(config-if)#**ip address 12.12.12.2 255.255.255.0**

Ro-2(config-if)#**ex**

R-2r(config)#**int fa 0/1**

Router(config-if)#**no shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

R-2 (config-if)#**ip address 13.13.13.1 255.255.255.0**

R-2 (config-if)#**ex**

- R-3

R-3(config)#**int fa 0/1**

R-3 (config-if)#**no shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

R-3(config-if)#**ip address 192.168.3.1 255.255.255.0**

R-3(config-if)#**ex**

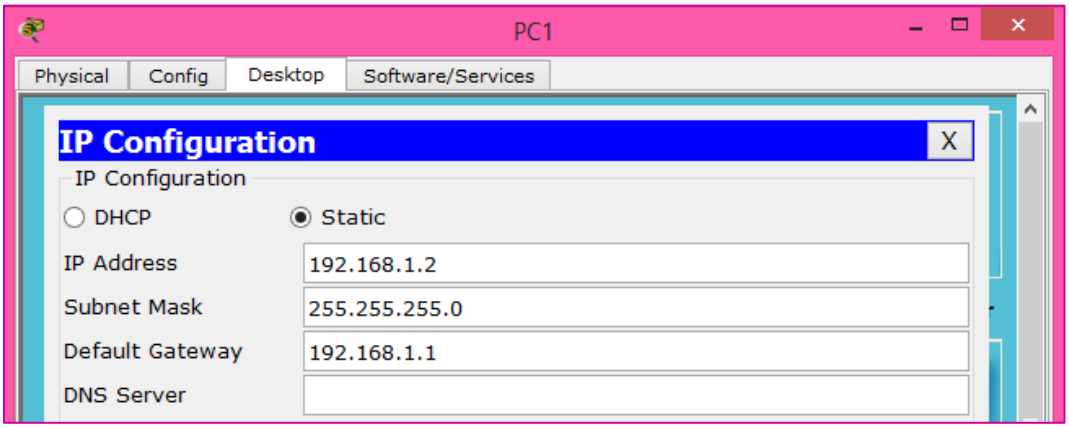
R-3(config)#**int fa 0/0**

R-3 (config-if)#**no shutdown**

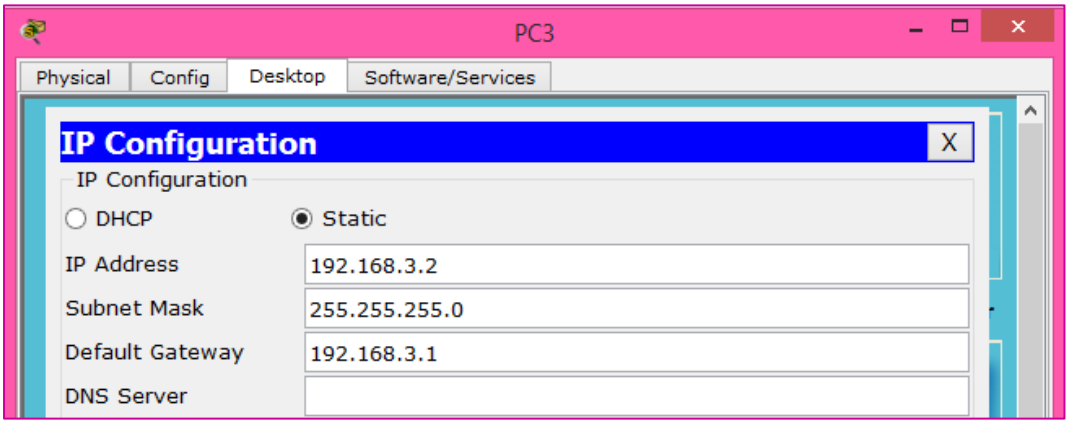
R-3(config-if)#**ip address 13.13.13.2 255.255.255.0**

R-3(config-if)#**ex**

Kemudian berikan IP Address beserta gateway yang tadi kita sudah buat pada PC1 dan PC3.



Gambar 22.2 Pemberian IP Address pada PC1



Gambar 22.3 Pemberian IP Address pada PC3

Sekarang coba kita lihat **Table Routing** pada R-1

Router#**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

R-1, R-2, dan R-3 hanya memiliki network yang directly connected saja. Dan tidak mengetahui network yang lain. Maka ketika **client R-1** ping ke **client R-3** tidak akan bisa.

```
PC>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data :
Replay from 192.168.1.1: Destination host unreachable.
Replay from 192.168.1.1: Destination host unreachable.
Replay from 192.168.1.1: Destination host unreachable.
Ping statistics for 192.168.3.2 :
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Kemudian kita konfigurasi **routing static** pada semua router, formatnya adalah

ip route (network tujuan) (netmask tujuan) (next-hop-address)

Next hop dapat menggunakan **ip address** atau **interface out-nya**

- R-1

```
Router(config)#ip route 13.13.13.0 255.255.255.0 12.12.12.2
Router(config)#ip route 192.168.3.0 255.255.255.0 13.13.13.2
```

- R-2

```
Router(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
Router(config)#ip route 192.168.3.0 255.255.255.0 13.13.13.2
```

- R-3

```
R-3(config)#ip route 12.12.12.0 255.255.255.0 13.13.13.1
R-3(config)#ip route 192.168.1.0 255.255.255.0 13.13.13.1
```

Static Route harus dikonfigurasi di masing-masing routernya. Sekarang kita akan melihat routing table lagi

```
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
     13.0.0.0/24 is subnetted, 1 subnets
S    13.13.13.0 [1/0] via 12.12.12.2
C    192.168.1.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 [1/0] via 13.13.13.2
```

Jika kita melakukan ping kembali dari PC1 ke PC3 sudah bisa, begitupun jika PC3 ping ke PC1

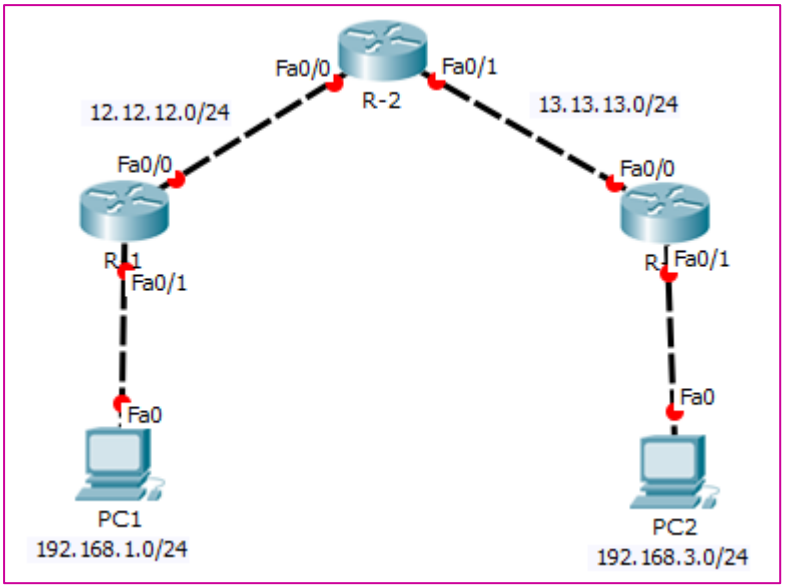
```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data :

Replay from 192.168.3.2: bytes=32   time=1ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=15ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=12ms   TTL=125


Ping statistics for 192.168.3.2 :

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

Approximate round trip times in milli-seconds :

    Mininum = 1ms, Maximum = 21ms, Everage = 12ms
```

LAB 23 – Basic Config EIGRP

Dynamic Routing Protocol akan memasukkan routing secara otomatis ke routing tabel. Salah satunya adalah EIGRP (Enhanced Interior Gateway Routing Protocol) yang merupakan protocol routing yang termasuk dalam Distance Vector dan merupakan Cisco Proprietary (hak milik).

- Kelebihan :
  1. Melakukan konvergensi secara tepat ketika menghindari loop
  2. Memerlukan lebih sedikit memori dan proses

- Kekurangan :
  1. Hanya untuk router cisco



Gambar 23.1 Topologi Routing EIGRP

Kita melanjutkan konfigurasi pada lab sebelumnya. Tetapi menggunakan topologi yang berbeda. Hapus terlebih dahulu konfigurasi static routing pada ketiga router.

- R-1

```
R-1(config)#no ip route 13.13.13.0 255.255.255.0 12.12.12.2

R-1(config)#no ip route 192.168.3.0 255.255.255.0 fa0/0
```

- R-2

```
R-2(config)#no ip route 192.168.1.0 255.255.255.0 12.12.12.1

R-2(config)#no ip route 192.168.3.0 255.255.255.0 13.13.13.2
```

- R-3

```
R-3(config)#no ip route 12.12.12.0 255.255.255.0 13.13.13.1

R-3(config)#no ip route 192.168.1.0 255.255.255.0 12.12.12.2
```

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

```
R-1#show ip route

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

Gateway of last resort is not set

     12.0.0.0/24 is subnetted, 1 subnets
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 diingat supaya bisa adjacency AS (nama router eigrp) harus sama.

- R-1

```
R-1(config)#router eigrp 123

R-1(config-router)#no auto-summary

R-1(config-router)#network 192.168.1.0 0.0.0.255

R-1(config-router)#network 12.12.12.0 0.0.0.255

R-1(config-router)#passive-interface fa 0/1

%DUAL-5-NBRCHANGE: IP-EIGRP 123: Neighbor 12.12.12.2
(FastEthernet0/0) is up: new adjacency
```

- R-2

```
R-2(config)#router eigrp 123

R-2(config-router)#no auto-summary

R-2(config-router)#network 12.12.12.0 0.0.0.255
%DUAL-5-NBRCHANGE: IP-EIGRP 123: Neighbor 12.12.12.1
(FastEthernet0/0) is up: new adjacency

R-2(config-router)#network 13.13.13.0 0.0.0.255
%DUAL-5-NBRCHANGE: IP-EIGRP 123: Neighbor 13.13.13.2
(FastEthernet0/1) is up: new adjacency
```

- R-3

```
R-3(config)#router eigrp 123

R-3(config-router)#no auto-summary

R-3(config-router)#network 192.168.3.0 0.0.0.255

R-3(config-router)#network 13.13.13.0 0.0.0.255
%DUAL-5-NBRCHANGE: IP-EIGRP 123: Neighbor 13.13.13.1
(FastEthernet0/0) is up: new adjacency

R-3(config-router)#passive-interface fa 0/1
```

Beberapa keterangan diatas artinya adalah :

1. **Router EIGRP 123** : Mengaktifkan routing EIGRP dengan AS-123 (boleh bebas)
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 (hello-packet digunakan untuk menemukan serta membentuk suatu hubungan tetangga antar router).
5. **Neighbor** : Tetangga

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

Setelah dikonfigurasi, sekarang lihat lagi routing tabelnya

```
R-1#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
     13.0.0.0/24 is subnetted, 1 subnets
D       13.13.13.0 [90/30720] via 12.12.12.2, 00:10:21, 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, 00:09:36, FastEthernet0/0
```

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

Sekang kita ping dari PC1 ke PC3

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data :

Replay from 192.168.3.2: bytes=32   time=11ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=12ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=0ms   TTL=125


Ping statistics for 192.168.3.2 :

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

Approximate round trip times in milli-seconds :

    Mininum = 0ms, Maximum = 17ms, Everage = 10ms
```

LAB 24 – Basic Config OSPF (Backbone Area)

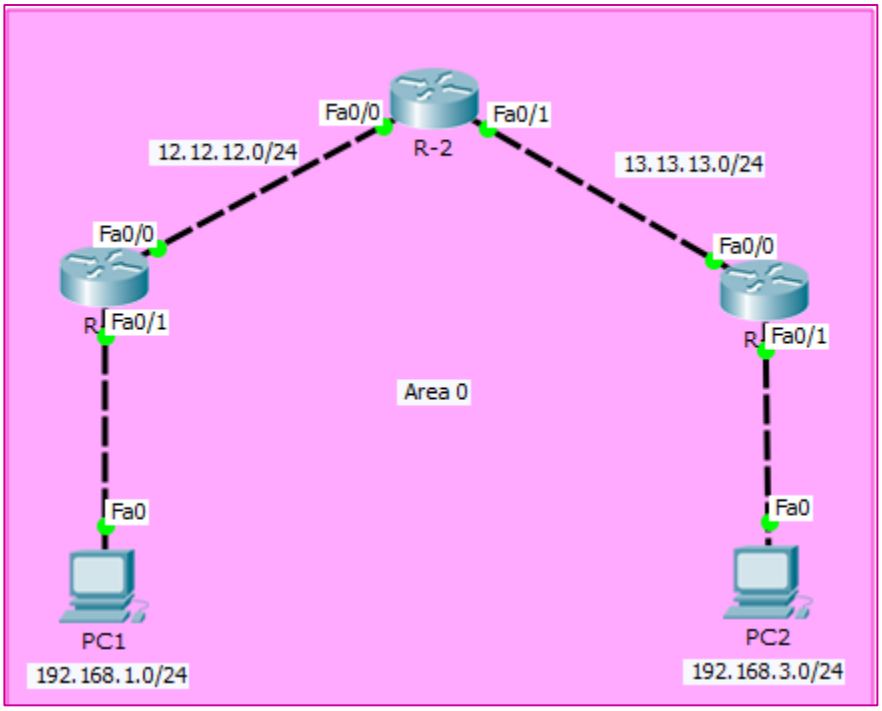
OSPF (Open Shortest Path First) merupakan Dynamic Routing juga, dan termasuk routing protokol berjenis IGRP (Interior Gateway Routing Protocol). Alasan mengapa mengkonfigurasi OSPF dalam sebuah topologi adalah untuk mengurangi overhead (waktu pemrosesan) routing, mempercepat convergance, serta membatasi ketidakstabilan network disebuah area dalam suatu network. OSPF menggunakan Cost sebagai metric atau penentuan best-path nya.

OSPF mempunyai beberapa kelebihan dan kekurangan yaitu :

- Kelebihan
  1. Tidak menghasilkan routing loop
  2. Mendukung penggunaan beberapa metrik sekaligus
  3. Dapat menghasilkan banyak jalur ke sebuah tujuan
  4. Membagi jaringan yang besar menjadi beberapa area
  5. Waktu yang diperlukan untuk konvergen lebih cepat

- Kekurangan
  1. Membutuhkan basis data yang besar
  2. Lebih rumit

Berikut adalah topologi yang akan kita gunakan :



Gambar 24.1 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 R-1, R-2 dan R-3.

- R-1

```
R-1(config)#no router eigrp 123
```

- R-2

```
R-2(config)#no router eigrp 123
```

- R-3

```
R-3(config)#no router eigrp 123
```

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

```
R-1(config)#do show ip route

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

Gateway of last resort is not set

     12.0.0.0/24 is subnetted, 1 subnets
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.

- R-1

```
R-1(config)#router ospf 1

R-1(config-router)#network 192.168.1.0 0.0.0.255 area 0

R-1(config-router)#network 12.12.12.0 0.0.0.255 area 0

00:19:06: %OSPF-5-ADJCHG: Process 1, Nbr 13.13.13.1 on FastEthernet0/0
from LOADING to FULL, Loading Done
```

- R-2

```
R-2(config)#router ospf 2

R-2(config-router)#network 12.12.12.0 0.0.0.255 area 0

R-2(config-router)#network 13.13.13.0 0.0.0.255 area 0

00:20:21: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.1 on
FastEthernet0/1 from LOADING to FULL, Loading Done
```

- R-3

```
R-3(config)#router ospf 3

R-3(config-router)#network 192.168.3.0 0.0.0.255 area 0

R-3(config-router)#network 13.13.13.0 0.0.0.255 area 0

00:20:21: %OSPF-5-ADJCHG: Process 3, Nbr 13.13.13.1 on FastEthernet0/0
from LOADING to FULL, Loading Done
```

Beberapa keterangan diatas adalah :

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

Kenapa 0.0.0.255 karena :

```
255.255.255.255
255.255.255.0
0 . 0 . 0 . 255
```

Bisa kita lihat neighbornya dengan perintah

```
R-1#show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time  Address     Interface
13.13.13.1   1    FULL/BDR   00:00:30   12.12.12.2  FastEthernet0/0
```

Sudah adjacency sekarang kita lihat lagi routing tabelnya.

```
R-1#show ip route

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

Gateway of last resort is not set

     12.0.0.0/24 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, FastEthernet0/0
     13.0.0.0/24 is subnetted, 1 subnets
O       13.13.13.0 [110/2] via 12.12.12.2, 00:14:01, 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, 00:12:56, FastEthernet0/0
```

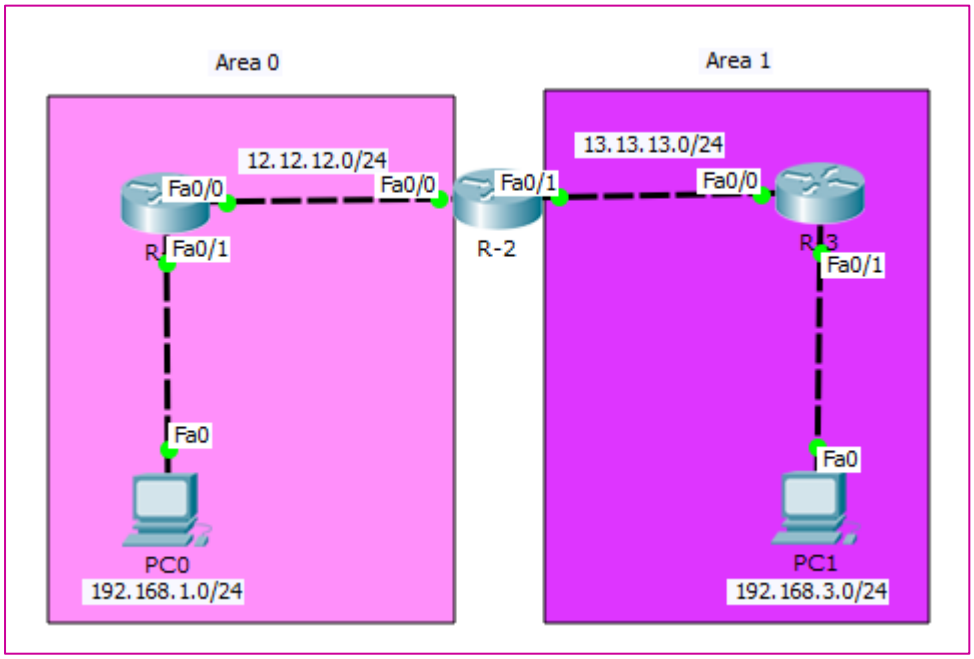
Sudah ada tanda **O** itu meenandakan OSPF 110 merupakan AD dari OSPF 2 dan 3 merupakan metric atau cost yang digunakan.

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data :

Replay from 192.168.3.2: bytes=32   time=17ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=15ms   TTL=125

Ping statistics for 192.168.3.2 :

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

LAB 25 – Multi Area OSPF

Jika dilab sebelumnya kita hanya mengkonfigurasi satu area saja. Sekarang akan mengkonfigurasi dengan dua area yang berbeda. Multi area OSPF digunakan sebagai pengendali informasi routing pada setiap network, karena ditiap-tiap area OSPF memiliki sistem managemen tersendiri agar informasi yang ada tidak keluar ataupun masuk ke area lain begitu saja.

Berikut adalah topologi yang akan kita gunakan :



Gambar 25.1 Topologi Multi Area OSPF

Keta akan membuat dua Area yaitu Area 0 dan Area 1. Area 0 harus ada karena merupakan backbone area. Hapus konfigurasi OSPF Area 0 pada R-2 dan R-3

- R-2

```
R-2(config)#router ospf 2

R-2(config-router)#no network 13.13.13.0 0.0.0.255 area 0
```

- R-3

```
R-3(config)#no router ospf 3
```

Lalu kita konfigurasi agar R-2 dan R-3 menggunakan Area 1

- R-2

```
R-2(config)#router ospf 2

R-2(config-router)#network 13.13.13.0 0.0.0.255 area 1
```

- R-3

```
R-3(config)#router ospf 3

R-3(config-router)#network 13.13.13.0 0.0.0.255 area 1

R-3(config-router)#network 192.168.3.0 0.0.0.255 area 1
```

Maka jika kita lihat routing tabel pada R-1

```
R-1#show ip route

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

Gateway of last resort is not set

     12.0.0.0/24 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, FastEthernet0/0
     13.0.0.0/24 is subnetted, 1 subnets
O IA    13.13.13.0 [110/2] via 12.12.12.2, 00:06:14, 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, 00:05:16, FastEthernet0/0
```

Tanda **IA** (Inter Area) yang merupakan route yang di dapat dari area yang berbeda. R-1 menggunakan Area 0 maka network 13.13.13.0 dan 192.168.3.0 menggunakan Area 1.

Sedangkan jika kita lihat pada R-2

```
R-2#sh 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
     13.0.0.0/24 is subnetted, 1 subnets
C       13.13.13.0 is directly connected, FastEthernet0/1
O    192.168.1.0/24 [110/2] via 12.12.12.1, 00:18:17, FastEthernet0/0
O    192.168.3.0/24 [110/2] via 13.13.13.2, 00:09:02, FastEthernet0/1
```

Coba kita ping dari PC1 ke PC3

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data :

Replay from 192.168.3.2: bytes=32   time=11ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=12ms   TTL=125

Replay from 192.168.3.2: bytes=32   time=0ms   TTL=125


Ping statistics for 192.168.3.2 :

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

Approximate round trip times in milli-seconds :

    Mininum = 0ms, Maximum = 11ms, Everage = 3ms
```

Note : Kalaupun nantinya kalian ingin ada **Area 2**, maka **Area 0** tetap harus berada ditengah. Karena Area 0 adalah area backbone.

LAB 26 – Basic Config RIP

RIP (Router Information Protocol) adalah routing protocol yang menggunakan algoritma distance vector, yaitu algoritma Bellman-Ford. Pertama kali dikenalkan pada tahun 1969 dan merupakan algoritma routing yang pertama di ARPANET. Versi awal dari routing protocol ini dibuat oleh XeroX Parc"s PARC Universal Packet Internetworking dengan nama Gateway Internet Protocol. Kemudian diganti nama menjadi Router Information Protocol yang merupakan bagian dari Xerox Network Services.

RIP merupakan routing protocol dengan algoritma distance vector, yang menghitung jumlah hop (count hop) sebagai routing metric. Jumlah maksimum dari hop yang diperbolehkan adalah 15 hop. Tiap RIP router saling tukar informasi routing tiap 30 detik.

RIP memiliki 3 versi yaitu :

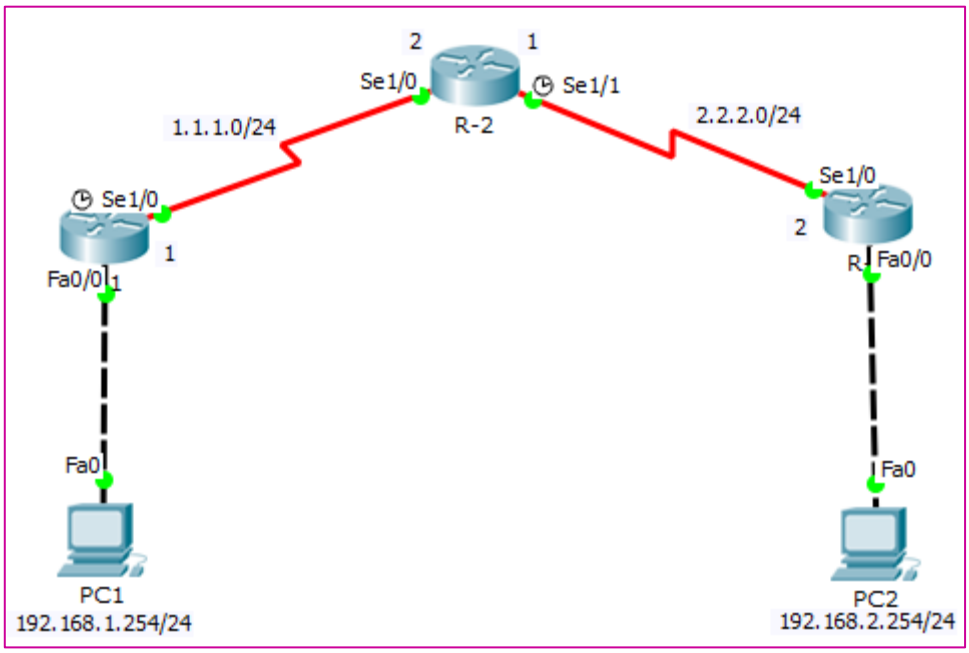
1. **RIPv1** merupakan bagian dari distance vector yang mencari hop terpendek atau router terbaik, RIP versi 1 juga merupakan classful dan tidak mengenal subnet mask
2. **RIPv2** sama seperti RIPv1, tetapi RIPv2 merupakan class list routing dan mengenal subnet mask
3. **RIPng** (RIP Next Generation/ RIP Generasi berikutnya) untuk mendukung Ipv6

Berikut adalah kelebihan dan kekurangan RIP :

- **Kelebihan :**
  1. RIP memiliki timer kapan router harus kembali memberikan informasi routing.
  2. Jika terjadi perubahan pada jaringan, sementara timer belum habis, router harus tetap mengirimkan informasi routing karena dipicu oleh perubahan tersebut.
  3. Pengaturannya tidak rumit, dan jarang terjadi kegagalan link jaringan.

- **Kekurangan :**
  1. Jumlah host terbatas
  2. RIP tidak memiliki informasi tentang subnets setiap route
  3. Ketika pertama kali dijalankan hanya mengetahui cara routing ke dirinya sendiri (informasi lokal) dan tidak mengetahui topologi jaringan tempatnya berada.

Berikut adalah topologi yang akan kita gunakan :



Gambar 26.1 Topologi Router RIP

Berikan hostname beserta IP Address terlebih dahulu pada setiap routernya

- R-1

Router(config)#**hostname R-1**

R-1(config)#**int fa 0/0**

R-1(config-if)#**no sh**
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R-1(config-if)#**ip add 192.168.1.254 255.255.255.0**

R-1(config-if)#**ex**

R-1(config)#**int se 1/0**

R-1(config-if)#**no sh**
%LINK-5-CHANGED: Interface Serial1/0, changed state to down

R-1(config-if)#**ip add 1.1.1.1 255.255.255.0**

R-1(config-if)#**clock rate 64000**

R-1(config-if)#**ex**

- R-2

Router(config)#**hostname R-2**

R-2(config)#**int se 1/0**

R-2(config-if)#**no sh**
%LINK-5-CHANGED: Interface Serial1/0, changed state to up

R-2(config-if)#**ip add 1.1.1.2 255.255.255.0**

R-2(config-if)#**ex**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R-2(config)#**int se 1/1**

R-2(config-if)#**no sh**
%LINK-5-CHANGED: Interface Serial1/1, changed state to down

R-2(config-if)#**ip add 2.2.2.1 255.255.255.0**

R-2(config-if)#**clock rate 64000**

R-2(config-if)#**ex**
%LINK-5-CHANGED: Interface Serial1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up

- R-3

Router(config)#**hostname R-3**

R-3(config)#**int se 1/0**

R-3(config-if)#**no sh**

R-3(config-if)#**ip add 2.2.2.2 255.255.255.0**

R-3(config-if)#**ex**

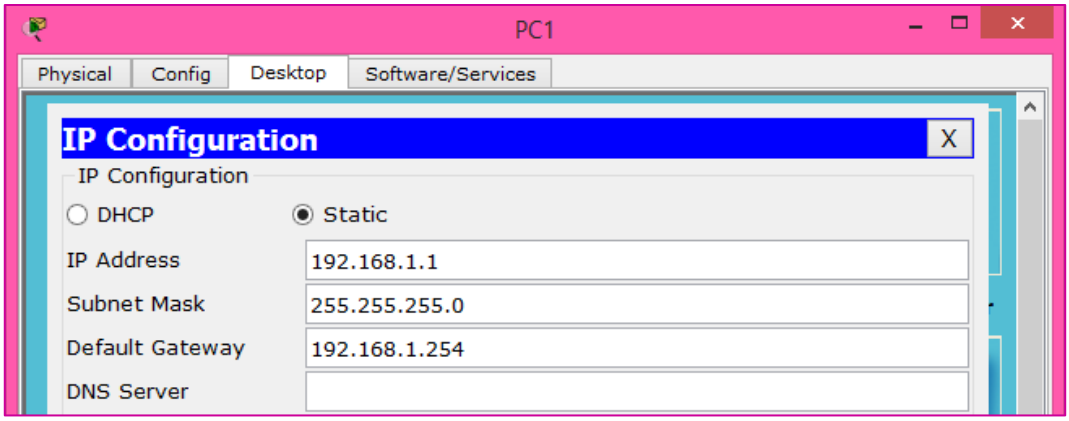
R-3(config)#**int fa 0/0**

R-3(config-if)#**no sh**

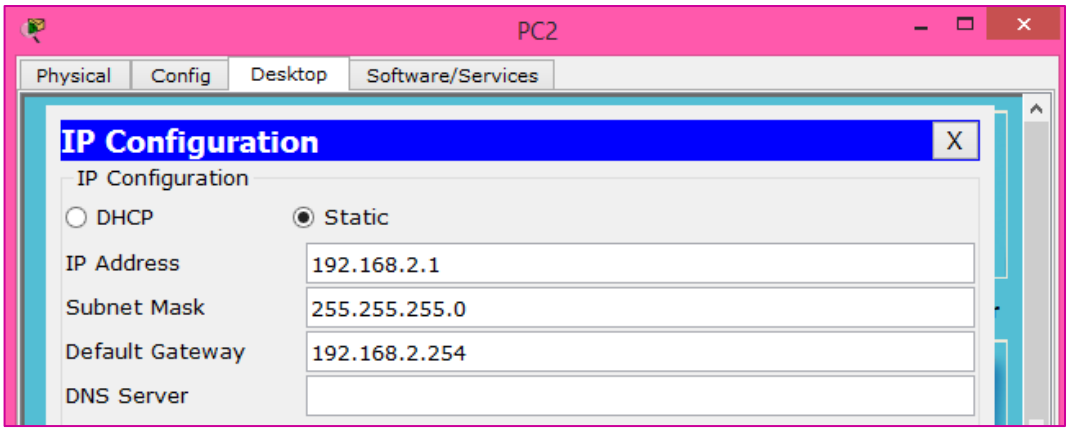
R-3(config-if)#**ip add 192.168.2.254 255.255.255.0**

R-3(config-if)#**ex**

Beri IP Address pada PC1 dan PC2 :



Gambar 26.2 Pemberian IP Address pada PC1



Gambar 26.3 Pemberian IP Addres spada PC2

Coba kita lakukan ping antar PC

PC>**ping 192.168.2.1**

Pinging 192.168.2.1 with 32 bytes of data :

Replay from 192.168.1.1: Destination host unreachable.

Replay from 192.168.1.1: Destination host unreachable.

Replay from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.1 :

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

Terlihat bahwa PC1 dan PC2 belum terhubung, kemudian kita konfigurasikan router RIP supaya antar PC bisa ngeping.

- R-1

```
R-1(config)#router rip
R-1(config-router)#network 192.168.1.0
R-1(config-router)#network 1.1.1.0
R-1(config-router)#ex
```

- R-2

```
R-2(config)#router rip
R-2(config-router)#network 1.1.1.0
R-2(config-router)#network 2.2.2.0
R-2(config-router)#ex
```

- R-3

```
R-3(config)#router rip
R-3(config-router)#network 192.168.2.0
R-3(config-router)#network 2.2.2.0
R-3(config-router)#ex
```

Untuk pengujian lakukan ping

```
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data :
Replay from 192.168.2.1: bytes=32   time=3ms   TTL=125
Replay from 192.168.2.1: bytes=32   time=4ms   TTL=125

Ping statistics for 192.168.2.1:
      Packets: Sent = 4, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds :
     Mininum = 2ms, Maximum =4ms, Everage = 3ms
```

LAB 27 – Redistribute

Apa itu **redistribute** ???

Redistribute adalah suatu konfigurasi untuk menyebarkan network dengan routing protocol yang berbeda atau cara untuk meredistribusikan kembali routing table yang dibentuk oleh suatu routing protocol untuk diteruskan ke routing protocol lain. Dengan redistribute kita bisa membentuk routing table yang lengkap dari suatu topologi walaupun menggunakan routing protocol yang berbeda.

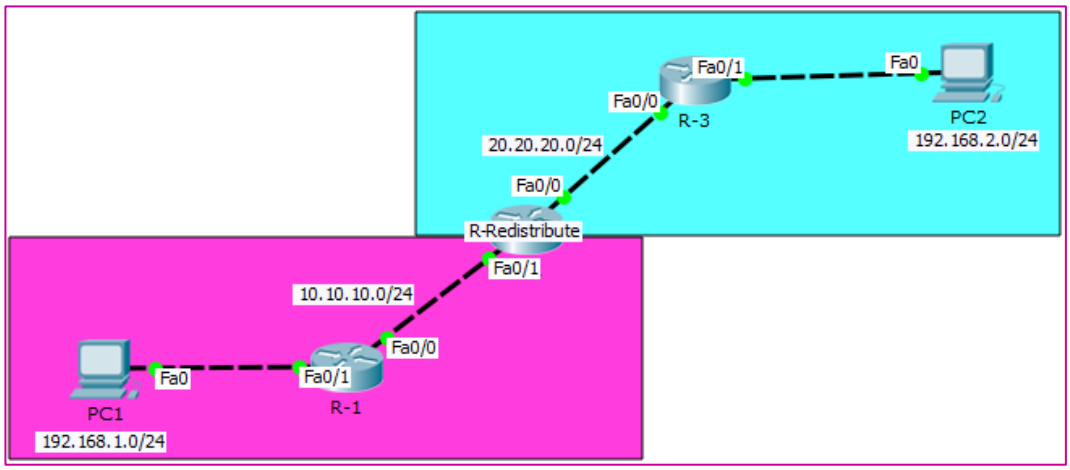
Redistribute ada beberapa macam diantaranya redistribute EIGRP, redistribute OSPF, redistribute RIP, redistribute Static, dan redistribute connected.

1. **Redistribute EIGRP** : Proses ketika routing sebuah router mengambil informasi dan mendistribusikan ke protocol yang berbeda. Menggunakan dua tipe routing protocol yang berbeda yaitu Distance Vector dan LinkState.
2. **Redistribute OSPF** : Suatu proses ketika routing sebuah router mengambil informasi dan mendistribusikan ke protocol yang lain. Dimana jalur yang terbaik adalah jalur yang mempunyai *cumulatif cost* yang paling rendah.
3. **Redistribute RIP** : Suatu proses ketika routing sebuah router mengambil informasi yang telah ditemukan dalam satu routing protocol dan mendistribusikan ke protocol routing yang berbeda dalam local area dan wide area network dengan menggunakan routing vector jarak algoritma.

- Cara kerjanya :

Yaitu router yang menjadi penghubung antara network dengan routing protocol yang berbeda akan menggunakan routing protocol sesuai dengan routing protocol yang dipergunakan oleh kedua network tersebut, misal interface F0/0 pada router tersebut berhubungan dengan network yang menggunakan RIP maka router tersebut harus menggunakan RIP dan pada F0/1 menggunakan OSPF maka router tersebut juga harus menggunakan OSPF sesuai dengan network tempat interface tersebut terhubung.
Untuk membuat agar routing tabel yang dibentuk oleh RIP bisa diteruskan menuju ke OSPF maka dipergunakan redistribute RIP, dan sebaliknya agar routing tabel yang terbentuk pada OSPF bisa diteruskan menuju RIP maka dipergunakanlah redistribute OSPF.

Berikut adalah topologi yang akan kita gunakan :



Gambar 27.1 Topologi Redistribute

Berikan IP Address pada setiap perangkat

- R-1

Router(config)#**hostname R-1**

R-1(config)#**interface FastEthernet0/0**

R-1(config-if)#**no shutdown**

R-1(config-if)#**ip address 10.10.10.1 255.255.255.0**

R-1(config-if)#**exit**

R-1(config)#**interface FastEthernet0/1**

R-1(config-if)#**no shutdown**

R-1(config-if)#**ip address 192.168.1.254 255.255.255.0**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

- R-2

Router(config)#**hostname R-2**

R-2(config)#**interface FastEthernet0/0**

R-2(config-if)#**no shutdown**

R-2(config-if)#**ip address 20.20.20.1 255.255.255.0**

R-2(config-if)#**exit**

R-2(config)#**interface FastEthernet0/1**

R-2(config-if)#**no shutdown**

R-2(config-if)#**ip address 10.10.10.2 255.255.255.0**
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R-2(config-if)#**exit**

- R-3

Router(config)#**hostname R-3**

R-3(config)#**interface FastEthernet0/0**

R-3(config-if)#**no shutdown**

R-3(config-if)#**ip address 20.20.20.2 255.255.255.0**

R-3(config-if)#**exit**

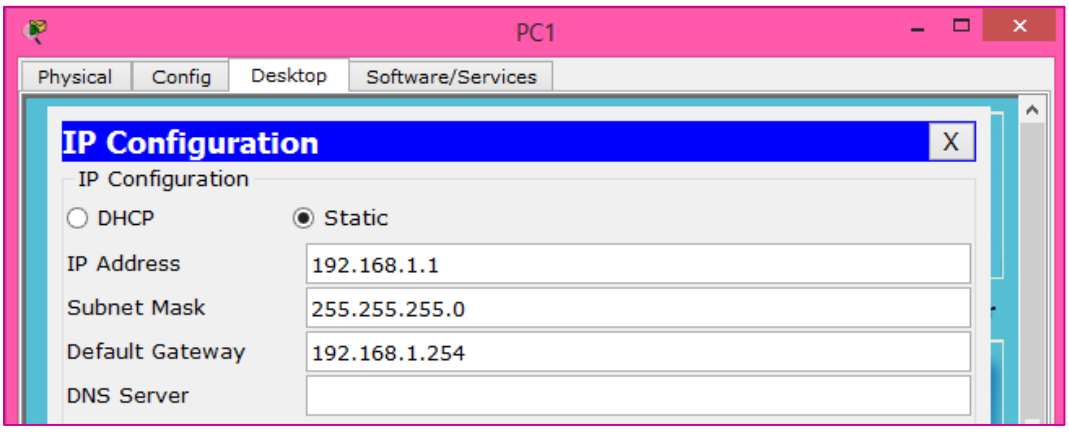
R-2(config)#**interface FastEthernet0/1**

R-2(config-if)#**no shutdown**

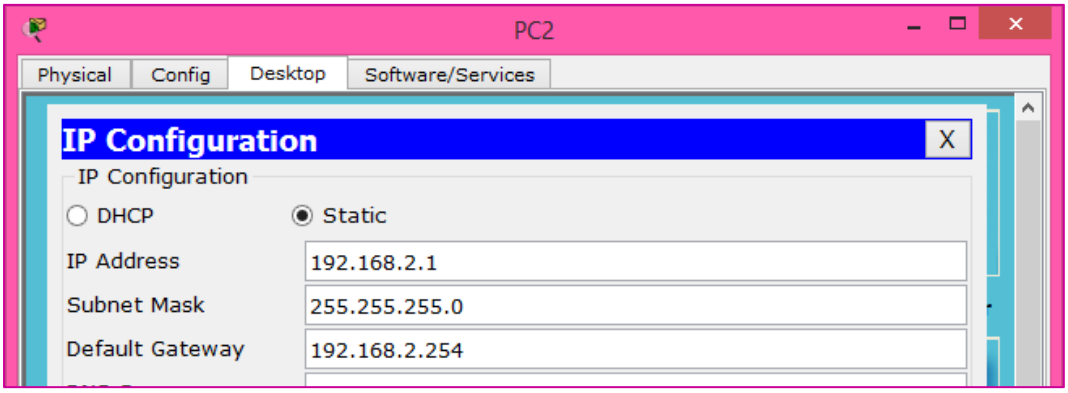
R-2(config-if)#**ip address 192.168.2.254 255.255.255.0**
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R-2(config-if)#**exit**

Masukkan IP Address pada PC1 dan PC2 :



Gambar 27.2 Pemberian IP Address pada PC1



Gambar 27.3 Pemberian IP Address pada PC2

1. Redistribute OSPF dan EIGRP

konfigurasikan router OSPF pada R-1 :

```
R-1(config)#router ospf 1
R-1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R-1(config-router)#network 10.10.10.0 0.0.0.255 area 0
R-1(config-router)#ex
```

kemudian konfigurasikan router EIGRP pada R-3

```
R-3(config)#router eigrp 1
R-3(config-router)#network 192.168.2.0 0.0.0.255
R-3(config-router)#network 20.20.20.0 0.0.0.255
R-3(config-router)#no auto-summary
R-3(config-router)#ex
```

Baru deh konfigurasi router OSPF beserta EIGRP di R-2 (Router Redistribute) :

```
R-2(config)#router ospf 1
R-2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R-2(config-router)#ex
R-2(config)#router eigrp 1
R-2(config-router)#network 20.20.20.0 0.0.0.255
```

Coba kita lakukan test ping dari R-1 ke R-3 dan PC1 ke PC2

```
R-1#ping 20.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data :

Replay from 192.168.2.1 : Destination host unreachable.

Replay from 192.168.2.1 : Destination host unreachable.

Pinging statistics for 192.168.2.1:

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

Terlihat bahwa perangkat belum bisa ping. Oleh sebab itu kita harus mengkonfigurasikan Redistribut di R-2 :

```
R-2(config)#router ospf 1

R-2(config-router)#redistribute eigrp 1 subnets

R-2(config-router)#ex
```

Sebelum melakukan redistribute pada router EIGRP, lakukan show interface untuk mengetahui MTU, Bandwidth, Delay, dan Reliability.

```
R-2#show interface

FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is 0004.9a08.4401 (bia 0004.9a08.4401)
Internet address is 20.20.20.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
...
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Lance, address is 0004.9a08.4402 (bia 0004.9a08.4402)
Internet address is 10.10.10.2/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
...
```

Barulah kita konfigurasikan router EIGRP

```
R-2(config)#router eigrp 1

R-2(config-router)#redistribute ospf 1 metric ?
<1-4294967295> Bandwidth metric in Kbits per second

R-2(config-router)#redistribute ospf 1 metric 100000 ?
<0-4294967295> EIGRP delay metric, in 10 microsecond units

R-2(config-router)#redistribute ospf 1 metric 100000 1000 ?
<0-255> EIGRP reliability metric where 255 is 100% reliable

R-2(config-router)#redistribute ospf 1 metric 100000 1000 10 ?
<1-255> EIGRP Effective bandwidth metric (Loading) where 255 is 100%
loaded

R-2(config-router)#redistribute ospf 1 metric 100000 1000 10 255 ?
<1-65535> EIGRP MTU of the path
R-2(config-router)#redistribute ospf 1 metric 100000 1000 10 255 1500 ?
match Redistribution of OSPF routes
<cr>

R-2(config-router)#redistribute ospf 1 metric 100000 1000 10 255 1500

R-2(config-router)#ex
```

Lakukan ping dari R-1 ke R-3

```
R-1#ping 20.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/16 ms
```

```
R-3#ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Kemudian lakukan ping antara PC1 dan PC2 :

```
PC>ping 192.168.2.1

Pinging 192.168.2.1with 32 bytes of data :

Replay from 192.168.2.1: bytes=32 time=14ms TTL=128

Replay from 192.168.2.1: bytes=32 time=17ms TTL=128

Ping statistics for 192.168.2.1:

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

Approximate round trip times in milli-second:

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

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data :

Replay from 192.168.1.1: bytes=32 time=10ms TTL=128

Replay from 192.168.1.1: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.1.1 :

    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-second:

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

2. Redistribute RIP to OSPF

kita akan memakai topologi yang sebelumnya. Hapus terlebih dahulu konfigurasi EIGRP di R-3, yang akan kita ganti dengan RIP. Serta hapus konfigurasi redistribut pada R-2 :

```
R-3(config)#no router eigrp 1
```

```
R-2(config)#no router eigrp 1


R-2(config)#router ospf 1

R-2(config-router)#no redistribute eigrp 1 subnets
```

Kemudian konfigurasikan router RIP :

- R-3

```
R-3(config)#router rip
R-3(config-router)#network 192.168.2.0
R-3(config-router)#network 20.20.20.0
R-3(config-router)#ex
```

- R-2

```
R-2(config)#router rip
R-2(config-router)#network 20.20.20.0
R-2(config-router)#ex
```

Kemudian konfigurasikan Redistribute pada R-2 :

```
R-2(config)#router rip
R-2(config-router)#redistribute ospf 1 metric 0
R-2(config-router)#ex

R-2(config)#router ospf 1
R-2(config-router)#redistribute rip subnets
R-2(config-router)#ex
```

Kita lakukan ping dari R-1 ke R-3 atau sebaliknya, apakah success??

```
R-3#ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/11 ms
```

```
R-1#ping 20.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Sudah **success!!!** Sekarang kita lakukan ping dari PC1 ke PC2

```
PC>ping 192.168.2.1

Pinging 192.168.2.1with 32 bytes of data :

Replay from 192.168.2.1: bytes=32 time=18ms TTL=128

Replay from 192.168.2.1: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.2.1:

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

Approximate round trip times in milli-second:

    Minimum = 13ms, Maximum = 18ms, Average = 15ms
```

```
PC>ping 192.168.1.1

Pinging 192.168.1.1with 32 bytes of data :

Replay from 192.168.1.1: bytes=32 time=14ms TTL=128

Replay from 192.168.1.1: bytes=32 time=17ms TTL=128

Ping statistics for 192.168.1.1:

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

Approximate round trip times in milli-second:

    Minimum = 10ms, Maximum = 11ms, Average = 0ms
```

Untuk lebih jelasnya lihatlah pada tabel berikut :

1.	Router EIGRP	✓ Redistribute RIP metric ...
		✓ Redistribute OSPF (ID) metric ...
2.	Router OSPF	✓ Redistribute RIP subnets
		✓ Redistribute EIGRP (ID) subnets
3.	Router RIP	✓ Redistribute OSPF (ID) metric ...
		✓ Redistribute EIGRP (ID) metric ..

LAB 28 – HSRP (Fail-Over)

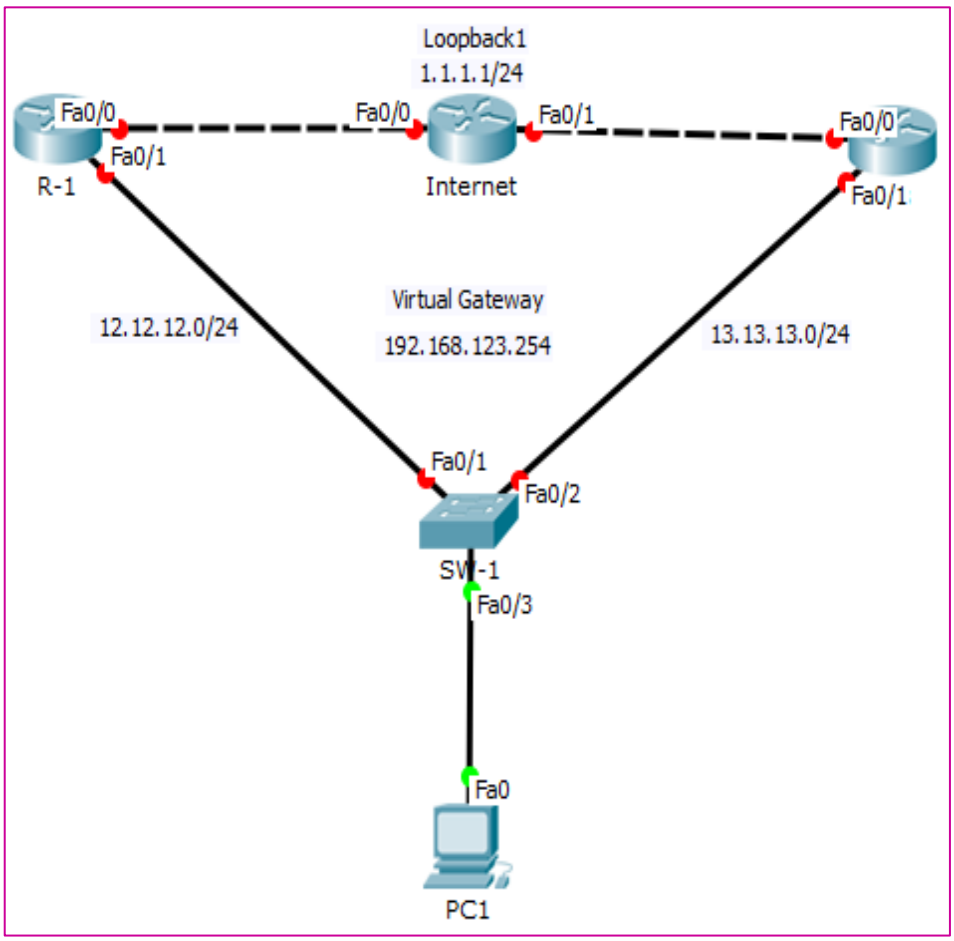
HSRP (Cisco Proprietary/hak milik) adalah sebuah protocol redudancy standar cisco yang menetapkan sebuah router yang secara otomatis mengambil alih jika router yang lain gagal. Pada koneksi ke internet kita harus memiliki backup link. Karena jika tidak, maka pada saat kabel utama terputus, semua jaringan akan terputus. Ini dinamakan dengan high availlability (HSRP akan memakai satu link dan bila gagal akan digantikan dengan backup link (Fail-Over)). HSRP menerapkan mekanisme failover transparent pada end device didalam jaringan.

Didalam HSRP mendefinisikan 2 status router yaitu Router Aktif dan Router Standby. Router standby digunakan sebagai redudancy dari router aktif jika router aktif gagal merouting.

Ada 3 metode yang dapat digunakan pada high availlability :

1. HSRP (Hot Standby Router Protocol)
2. VRRP (Virtual Router Redudancy Protocol)
3. GLBP (Gateway Load Balancing Protocol)

Berikut adalah topologi yang akan kita gunakan :



Gambar 28.1 Topologi HSRP

Cara kerjanya adalah kedua router akan membuat IP virtual-gateway terlebih dahulu yang akan digunakan untuk client. Pemilihan jalur yang digunakan aadalah dari IP Address terkecilnya. Konfigurasi IP Adddress dan routing IGP (OSPF atau EIGRP). Kali ini kita akan menggunakan EIGRP dengan AS-123.

- R-1

```
R-1(config)#int fa 0/0

R-1(config-if)#no sh

R-1(config-if)#ip address 192.168.123.254 255.255.255.0

R-1(config-if)#ex



R-1(config)#int fa 0/1

R-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

R-1(config-if)#ip address 12.12.12.1 255.255.255.0
R-1(config-if)#ex



R-1(config)#router eigrp 123

R-1(config-router)#no auto-summary

R-1(config-router)#network 192.168.123.0

R-1(config-router)#network 12.12.12.0
```

- R-2

```
R-2(config)#int fa 0/0

R-2(config-if)#no shutdown

R-2(config-if)#ip address 192.168.123.2 255.255.255.0

R-2(config-if)#ex
```

R-2(config)#**int fa 0/1**

R-2(config-if)#**ip address 13.13.13.2 255.255.255.0**

R-2(config-if)#**no sh**

R-2(config)#**router eigrp 123**

R-2(config-router)#**no auto-summary**

R-2(config-router)#**network 13.13.13.0**

R-2(config-router)#**network 192.168.123.0**

- Internet

Internet(config)#**int fa 0/0**

Internet(config-if)#**no sh**
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Internet(config-if)#**ip address 12.12.12.3 255.255.255.0**

Internet(config-if)#**ex**

Internet(config)#**int fa 0/1**

Internet(config-if)#**no sh**

Internet(config-if)#**ip address 13.13.13.3 255.255.255.0**

Internet(config-if)#**int lo1**

Internet(config-if)#**ip address 1.1.1.1 255.255.255.0**

Internet(config-if)#**ex**

Internet(config)#**router eigrp 123**

Internet(config-router)#**no auto-summary**

Internet(config-router)#**network 0.0.0.0**

Setelah mengkonfigurasi IP Address dan EIGRP. Sekarang kita konfigurasi HSRP

- R-1

```
R-1(config)#int fa 0/0

R-1(config-if)#standby 1 ip 192.168.123.254

R-1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

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

- R-2

```
R-2(config)#int fa0/0

R-2(config-if)#standby 1 ip 192.168.123.254

R-2(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

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

Yang active adalah R-1 sedangkan jalur R-2 digunakan untuk backup link. Kalian bisa mencek konfigurasi dengan perintah **show standby brief**.

```
R-1#show standby br
                     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 ping **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  192.168.123.254
2   1 ms  1 ms  0 ms  1.1.1.1

Trace Complete
```

Misalnya kita ingin ubah agar jalur menggunakan R-2. Ubah prioritynya menjadi lebih besar. Defaultnya adalah 100

- R-1

```
R-1(config)#int fa 0/0

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

- R-2

```
R-2(config)#int fa 0/0

R-2(config-if)#standby 1 priority 110

R-2(config-if)#standby 1 preempt
```

Perintah **preempt** digunakan agar memepercepat process pemindahan link.

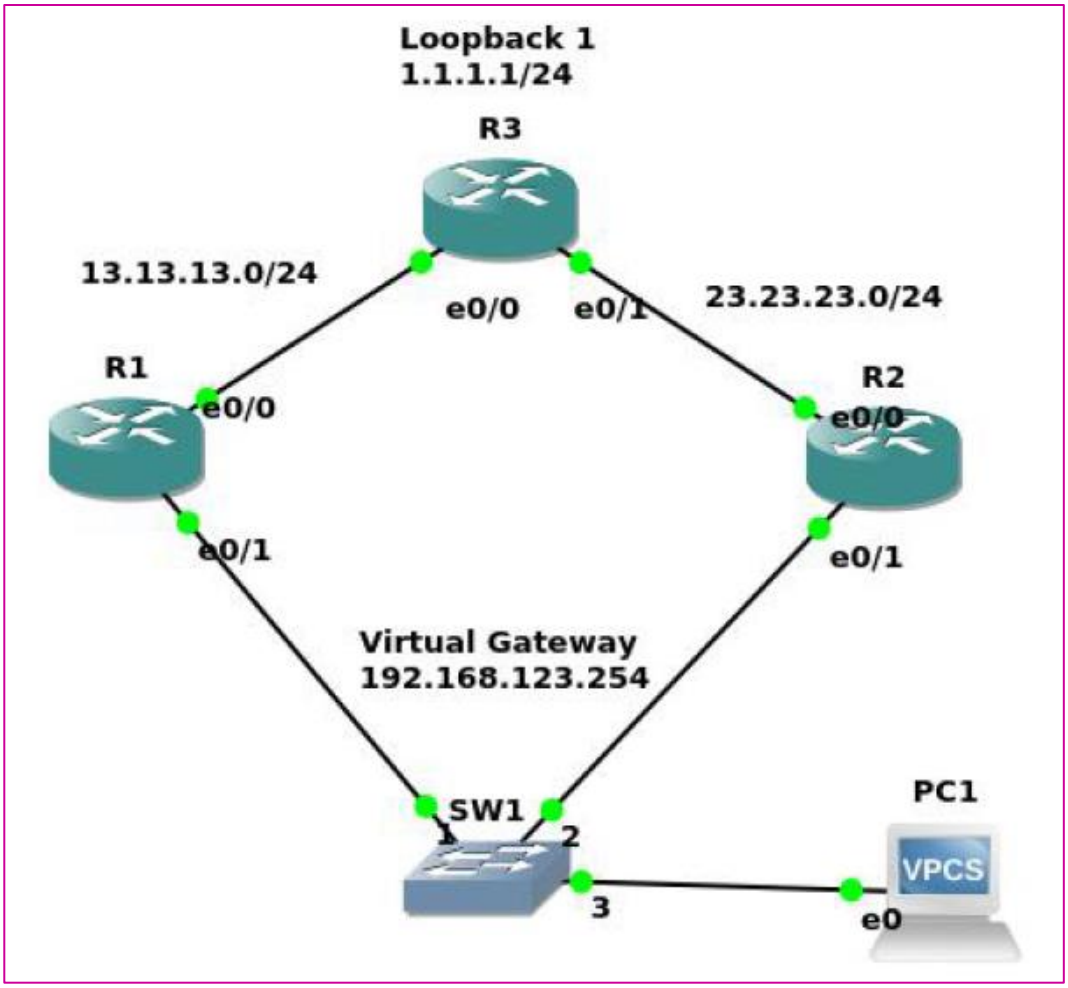
Test lagi dengan menggunakan tracert.

```
PC>tracert 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops :

1     1 ms  0 ms  13 ms  192.168.123.254
2     1 ms  11 ms  0 ms  1.1.1.1

Trace Complete
```

LAB 29 – VRRP (Fail-Over)

VRRP konsepnya sama saja seperi HSRP bedanya hanya saja VRRP merupakan open standart sedangkan HSRP cisco proprietary. VRRP adalah sebuah interface (virtual) dari Router OS MikroTik yang memungkinkan kita untuk membuat beberapa router sebagai gateway dari jaringan lokal yang satu segment. Komunikasi antar router akan menggunakan Virtual Router ID dan pada interface VRRP dimasing-masing router akan dipasang sebuah single IP Address yang nantinya akan digunakan sebagai gateway dari jaringan lokal tersebut. Karena ada beberapa router yang menjadi gateway dari satu jaringan lokal, maka kita bisa melakukan sebuah "Prioritas". Yang artinya ada satu router yang bisa dijadikan sebagai gateway utama dan yang lain akan menjadi backup. Seperti mekanisme "Fail Over", jika jalur dari gateway utama terputus maka bisa memakai jalur yang lain.

Karena pada **Cisco Packet Tracer** tidak mendukung fitur VRRP, maka kali ini kita akan menggunakan GNS3. Berikut adalah topologi yang akan kita gunakan :



Gambar 29.1 Topologi VRRP (Fail-Over)

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

```
PC> 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 persis dengan HSRP, hanya berbeda protocol yang digunakan. Berikut adalah konfigurasinya

- R-1

```
R-1(config-if)#vrrp 1 ip 192.168.123.254

R-1(config-if)#
*Jan  21  10:03:31.323 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state Init-> Backup
R-1(config-if)#
*Jan  21  10:04:34.939 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state Backup-> Master
R-1(config-if)#
*Jan  21  10:05:58.289 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state Master-> Backup
```

- R-2

```
R-1(config-if)#vrrp 1 ip 192.168.123.254

R-1(config-if)#
*Jan  21  10:10:51.323 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state Init-> Backup
R-1(config-if)#
*Jan 21  10:13:52.939 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state Backup-> Master
```

Dari konfigurasi diatas kita bisa melihat log nya. R-2 menjadi Master sedangkan R-1 menjadi backup. Seme seperti HSRP tinggal kita ubah saja prioritynya.

- R-1

```
R-1(config-if)#vrrp 1 ip 192.168.123.254

R-1(config-if)#vrrp 1 preemt
```

- R-2

```
R-2(config-if)#vrrp 1 preemt
```

Verifikasi dengan melihat VRRP briefnya

- R-1

```
R-1#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
```

- R-2

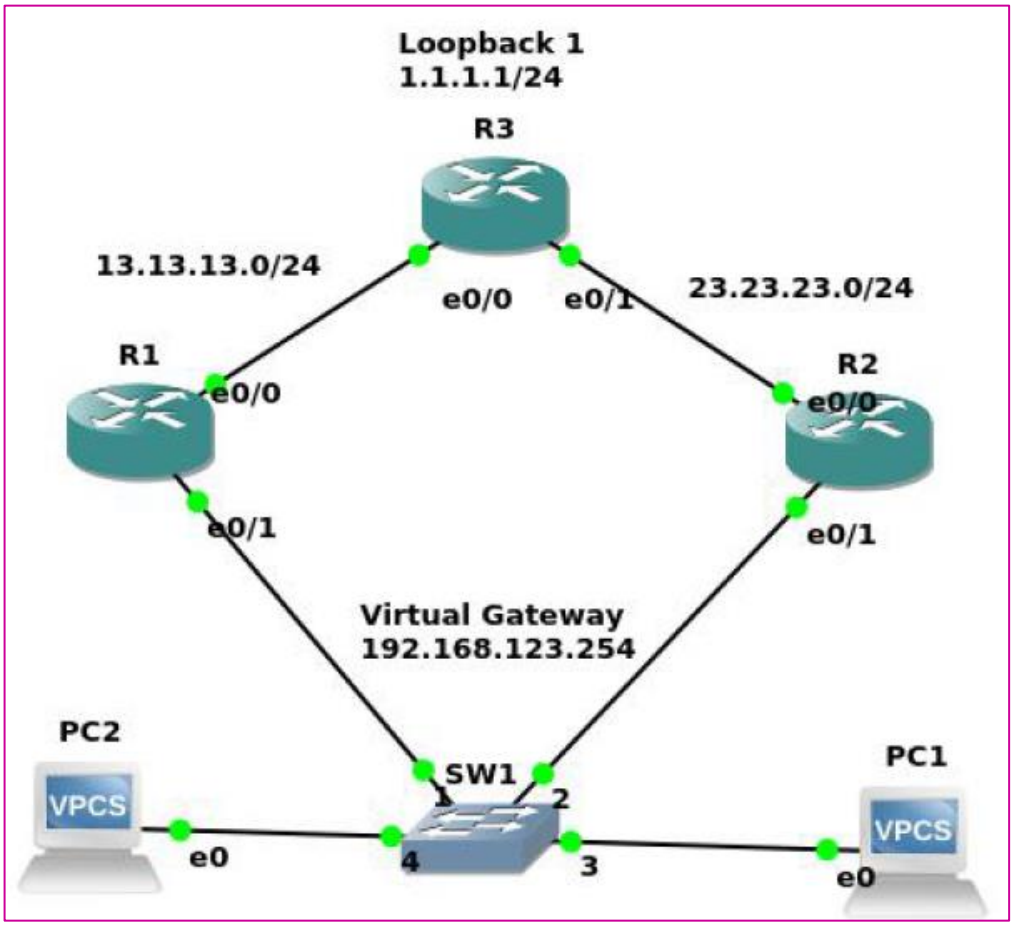
```
R-1#show vrrp brief

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 R-1. Kita dapat verifikasi dengan perintah trace

```
PC>tracert 1.1.1.1

Tracing route 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 30 – GLBP (Load-Balancing)

Pada lab sebelumnya yaitu HSRP dab VRRP merupakan Fail-Over yaitu 1 link menjadi link utama sisanya akan menjadi backup saja. Pada GLBP kita akan melakukan Load Balancing yang merupakan sebuah konsep yang gunanya untuk menyeimbangkan beban. Intinya adalah membagi kerja router yang besarnya sama/seimbang/balance. GLBP tidak disupport juga di Cisco Packet Tracer jadi kita akan menggunakan GNS3. Kita menggunakan konfigurasi dan topologi pada lab sebelumnya. Hanya ada tambahan 1 client.



Ganbar 30.1 Topologi GLBP

Hapus terlebih dahulu konfigurasi VRRP pada R-1 dan R-2

```
R-1(config)#int eth0/1

R-1(config-if)#no vrrp 1
```

```
R-2(config)#int eth0/1

R-2(config-if)#no vrrp 1
```

Setelah itu kita konfigurasi GLBP pada R-1 dan R-2

- R-1

```
R-1(config-if)#glbp 1 ip 192.168.123.254

R-1(config-if)#glbp 1 priority 110

R-1(config-if)#glbp 1 preempt

R-1(config-if)#
*Jan  21  10:20:51.363 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 state speak-> Active
R-1(config-if)#
*Jan  21  10:21:02.939 : %VRRP-6-STATECHANGE : Et0/1 Grp 1 Fwd 1 state Listen-> Active
```

- R-2

```
R-2(config-if)#glbp 1 ip 192.168.123.254

R-2(config-if)#glbp 1 preempt

R-2(config-if)#
*Jan  21  10:50:51.393 : %SYS-2-NOBLOCK : may_suspent with blocking disabled. - Process= "IP Input", IP1=  0, pid= 76, Traceback= 0x816F13Bz 0xA728AD3z 0x9430615z 0x9430532z
R-2(config-if)#
*Jan  21  11.03.22.654 : %GLBP-6-FWDSTATECHANGE : Eth0/1 Grp 1 FWD 2 state Listen-> Active
```

Kita akan mengkonfigurasi agar R-1 yang menjadi pemberi AVG (ARP ke Client)

Verifikasi dengan meggunakan GLBP brief

- R-1

```
R-1#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   -
```

- R-2

```
R-1#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 melalui R-1 dan PC2 melalui R-2

- R-1

```
PC>tracert 1.1.1.1

Tracing route to 1.1.1.1, 8 hops max, press Ctrl+C to stop

1    192.168.123.1  0.660  ms  0.551  ms  0.648  ms
2    *13.13.13.3  0.815  ms (ICMP type:3, code:3, Destinatiom port unreachable
```

- R-2

```
PC>tracert 1.1.1.1

Tracing route to 1.1.1.1, 8 hops max, press Ctrl+C to stop

1    192.168.123.2  0.334  ms  0.554  ms  0.648  ms
2    *23.23.23.3  0.815  ms (ICMP type:3, code:3, Destinatiom port unreachable
```

Hasilnya adalah PC1 melalui R-1 dan PC2 melalui R-2

Note : Fungsi Tracert adalah memberitahukan kita ip mana yang dilewati dan jumlah hop untuk mencpai alamat tujuan yang kita trace. Jumlah hop tergantung pada jumlah server yang diantaranya. Setelah memulai tracing, misalnya trace ke devitriana.sch.id. kapanpun kita membuka http://www.devitriana.sch.id dalam web browser, request kita selalu melalui ISP dulu (untuk mendapatkan ip dari http://www.devitriana.sch.id dari daftar nama domainnya), kemudian server lain dalam jalur tersebut, dan terakhir baru ke http://www.devitriana.sch.id.

LAB 31 – Standart Access-list (1-99)

Access-list adalah pengelompokkan paket berdasarkan kategori. Access-list sama seperti firewall yaitu digunakan untuk memfilter/menyaring paket. Bisa juga digunakan untuk menandai paket lalu dilanjutkan dengan mengkonfigurasi fitur yang lain seperti NAT, EIGRP, dll.

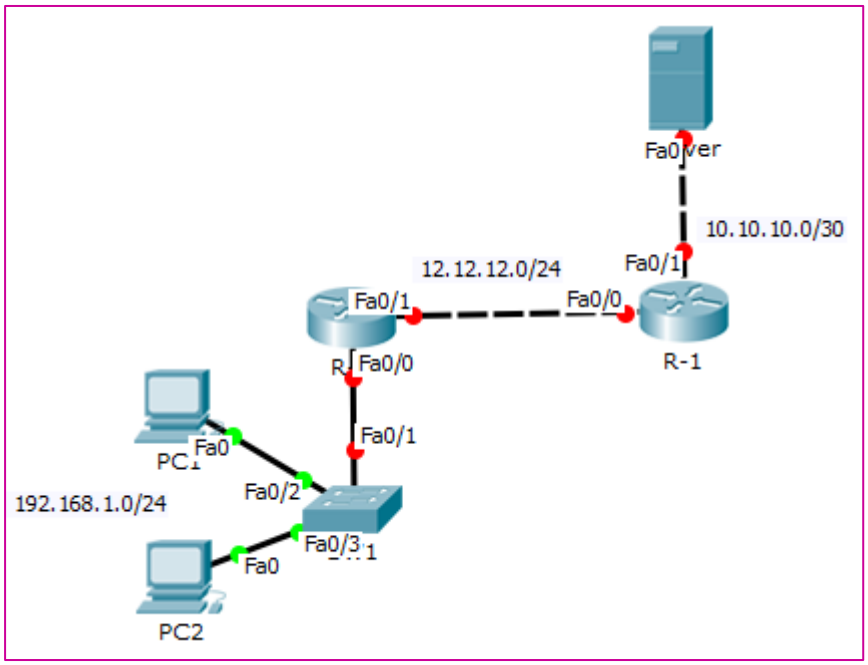
Terdapat 3 aturan yang berlaku bagi sebuah paket, jika access list diterapkan pada router :

1. Setiap paket akan dibandingkan secara berurut (dari atas ke bawah) dengan rules yang berlaku.
2. Jika menemukan kondisi yang sesuai, maka paket tersebut akan mengikuti aturan (rules) yang ada didalam Access List.
3. Apabila paket tersebut tidak menemukan aturan yang sesuai, maka paket tersebut tidak diperbolehkan lewat atau mengakses jaringan.

Access-list dibagi menjadi 2 yaitu :

1. Standard Access-list (1-99) : Yang akan melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.
2. Extended Access-list (100-199) : Yang akan menyeleksi sebuah paket yang berdasarkan alamat IP pengirim (Source) dan penerima (Destination), protokol, dan jenis paket port yang dikirim.

Berikut adalah topologi yang akan kita gunakan :



Gambar 31.1 Topologi Standar Access-list

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

Kita konfiugrasikan terlebih dahulu IP Address dan EIGRP AS 100 pada semua device agar bisa terhubung

- R-1

R-1(config)#**int fa 0/0**

R-1(config-if)#**no shu**

R-1(config-if)#**ip address 12.12.12.1 255.255.255.0**

R-1(config-if)#**ex**

R-1(config)#**int fa 0/1**

R-1(config-if)#**no sh**

R-1(config-if)#**ip address 10.10.10.1 255.255.255.252**

R-1(config-if)#**ex**

R-1(config)#**router eigrp 1**

R-1(config-router)#**no auto-summary**

R-1(config-router)#**network 12.12.12.0**

R-1(config-router)#**network 10.10.10.0**
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 1: **Neighbor 12.12.12.2** *(FastEthernet0/0) is up: new adjacency*

- R-2

R-2(config)#**int fa 0/1**

R-2(config-if)#**no sh**

R-2(config-if)#**ip address 12.12.12.2 255.255.255.0**

R-2(config-if)#**ex**

R-2(config)#**int fa 0/0**

R-2(config-if**)#no sh**

R-2(config-if)#**ip address 192.168.1.254 255.255.255.0**

R-2(config-if)#**ex**

R-2(config)#**router eigrp 1**

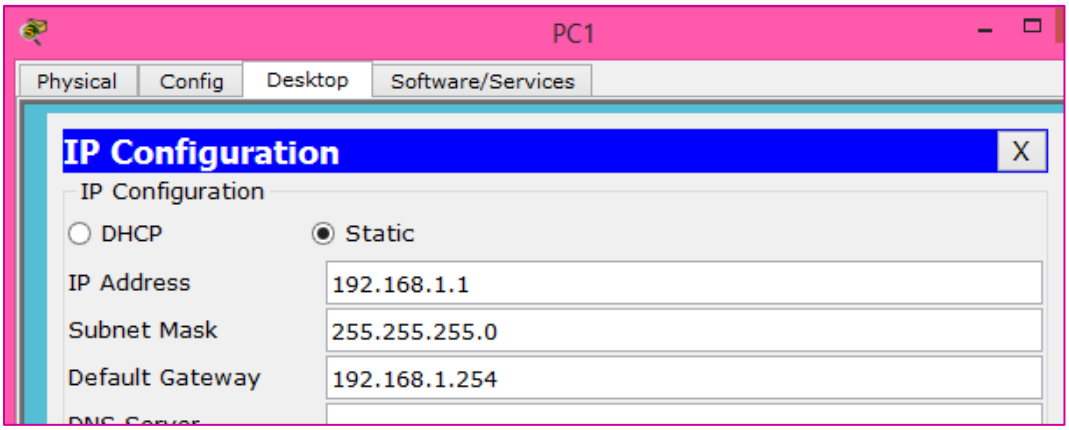
R-2(config-router)#**no auto-summary**

R-2(config-router)#network 12.12.12.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: **Neighbor 12.12.12.1** *(FastEthernet0/1) is up: new adjacency*

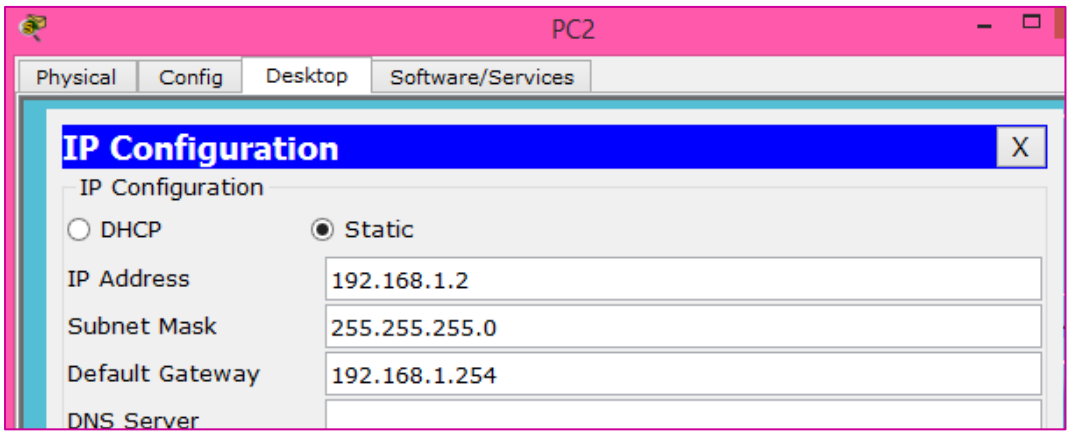
R-2(config-router)#**network 192.168.1.0**

Note : router eigrp **1 : angkanya boleh bebas, tetapi harus disamakan**

Kita beri IP Address pada PC1 dan PC2 beserta gatewaynya :



Gambar 31.2 Pemberian IP Address pada PC1



Gambar 31.3 Pemberian IP Address pada PC2

Selanjutnya kita ping dari PC2 ke PC1 dari PC2 ke Server

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data :

Replay from 192.168.1.1: bytes=32   time=16ms   TTL=128

Replay from 192.168.1.1: bytes=32   time=12ms   TTL=128


Ping statistics for 192.168.1.1 :

      Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds :

     Mininum = 1ms, Maximum = 16ms, Everage = 8ms
```

Dan ping dari PC2 ke Server

```
PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data :

Replay from 10.10.10.1: bytes=32   time=13ms   TTL=254

Replay from 10.10.10.1: bytes=32   time=16ms   TTL=254

Ping statistics for 10.10.10.1 :

      Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds :

     Mininum = 13ms, Maximum = 16ms, Everage = 14ms
```

Sekarang kita sudah bisa ping, yang artinya sudah terhubung. Kita konfigurasikan **Standard Access-list agar PC2 tidak bisa terhubung ke jaringan luar namun masih bisa terhubung ke PC1**.

```
R-2(config)#access-list 1 deny host 192.168.1.2

R-2(config)#access-list 1 permit any

R-2(config)#int fa 0/1

R-2(config-if)#ip access-group 1 out
```

Note : **Out** digunakan agar access-list digunakan pada saat keluar interface **fa0/1**

Sekarang coba lakukan ping lagi dari PC2 ke PC1 dan dari PC2 ke Server

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data :

Replay from 192.168.1.1: bytes=32   time=1ms   TTL=128

Replay from 192.168.1.1: bytes=32   time=0ms   TTL=128


Ping statistics for 192.168.1.1 :

      Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds :

     Mininum = 0ms, Maximum = 1ms, Everage = 8ms


PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data :

Replay from 192.168.1.254: Destination host unreacable.

Replay from 192.168.1.254: Destination host unreacable.

Ping statistics for 10.10.10.1 :

      Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```

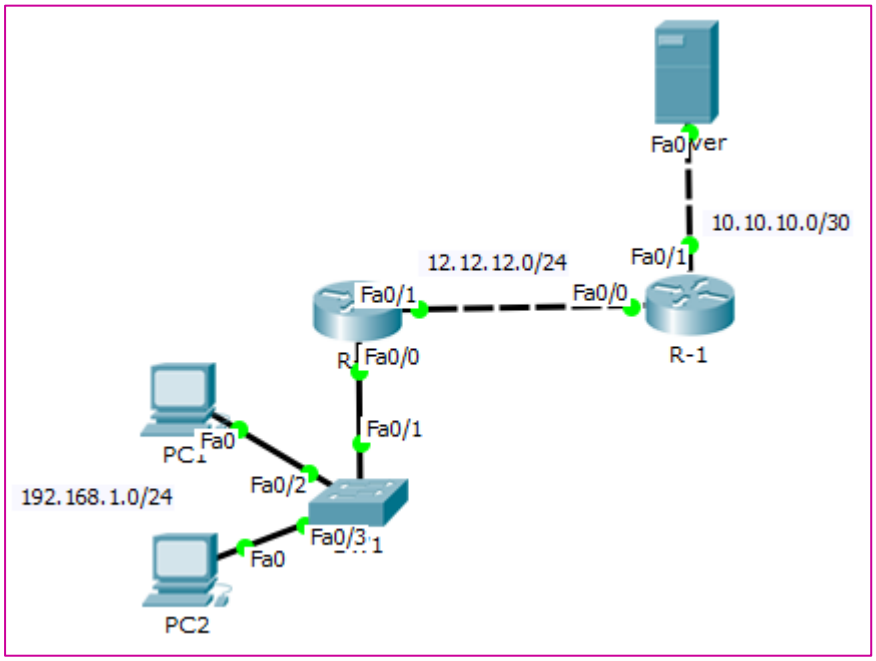
Ping dari PC2 ke PC1 tidak bisa, tetapi jika ngeping ke Server tidak akan bisa.
Mari kita lihat access-listnya dengan perintah :

```
R-2#show access-lists
Standard IP access list 1
        10 deny host 192.168.1.2 (3 match(es))
        20 permit any
```

Terlihat bahwa ada 4 paket yang terblock (3 paket icmp)

LAB 32 – Extended Access-list

Jika menggunakan Standard kita memblock maka semua service akan terblock. Jika menggunakan Extended kita dapat memblock service tertentu saja. Sedangkan yang lain dapat digunakan. Angka yang digunakan adalah 100-199.



Gambar 32.1 Topologi Extended Access-list

Kita melanjutkan konfigurasi dari LAB sebelumya. Hapus terlebih dahulu konfigurasi Standart Access-List pada R2

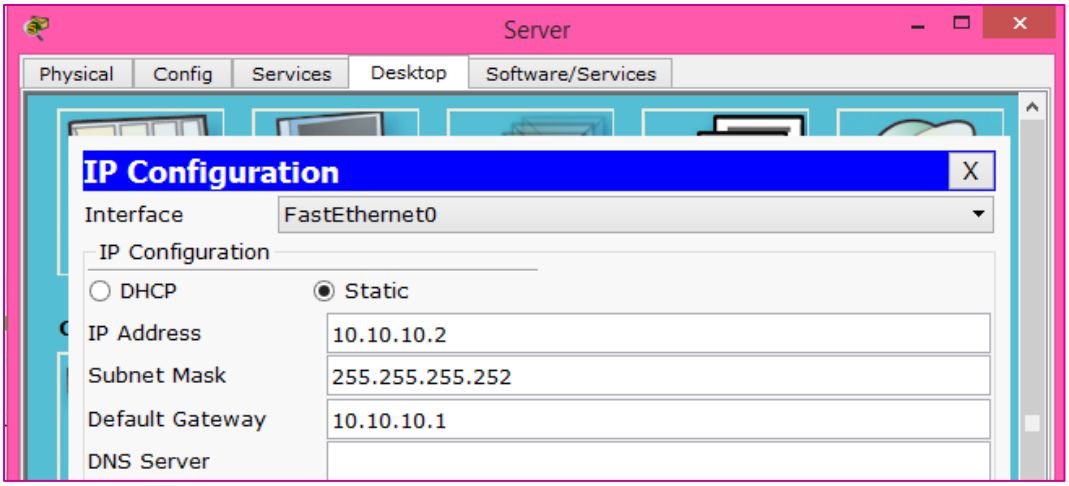
```
R-2(config)#no access-list 1
```

Tujuan kita di LAB ini adalah :

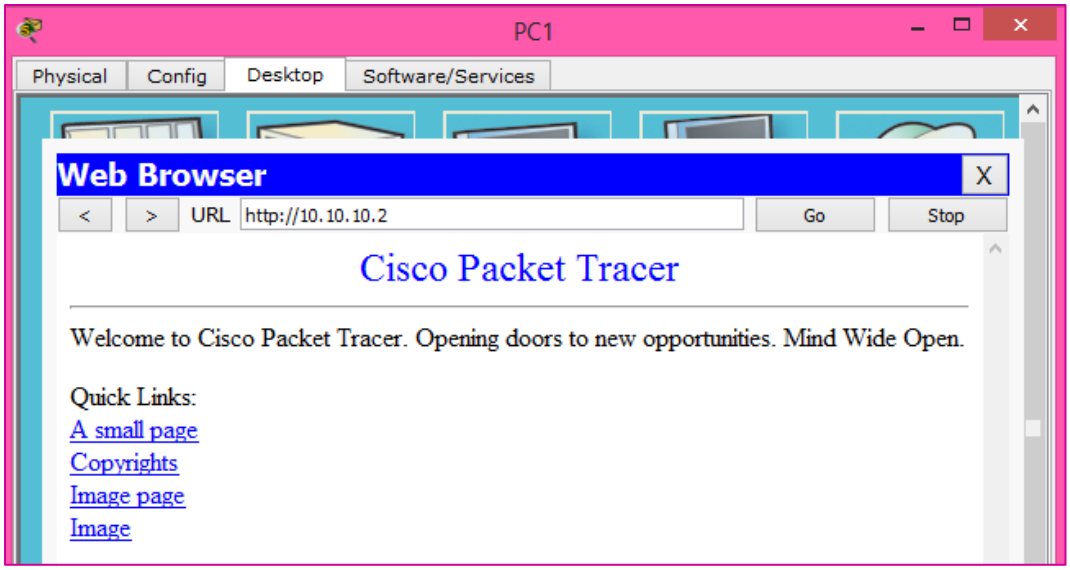
1. PC1 tidak bisa ping namun bisa membuka http server
2. PC2 bisa ping namun tidak bisa membuka http server

Server **pada defaultnya** sudah mengaktifkan http, cek pada web browser di client. **Desktop > Web Server**

Tetapi sebelum melakukan cek, berikan IP Address terlebih dahulu pada Server



Gambar 32.2 Pemberian IP Address pada Server



Gambar 32.3 Tampilan Web Server

Sekarang konfigurasi Extended Access-list. Namun sekarang kita menggunakan metode **nama**.

```
R-2(config)#ip access-list extended BLOCK

R-2(config-ext-nacl)#deny icmp host 192.168.1.1 host 10.10.10.2

R-2(config-ext-nacl)#deny tcp host 192.168.1.2 host 10.10.10.2 eq www

R-2(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

R-2(config-ext-nacl)#permit ip any any
```

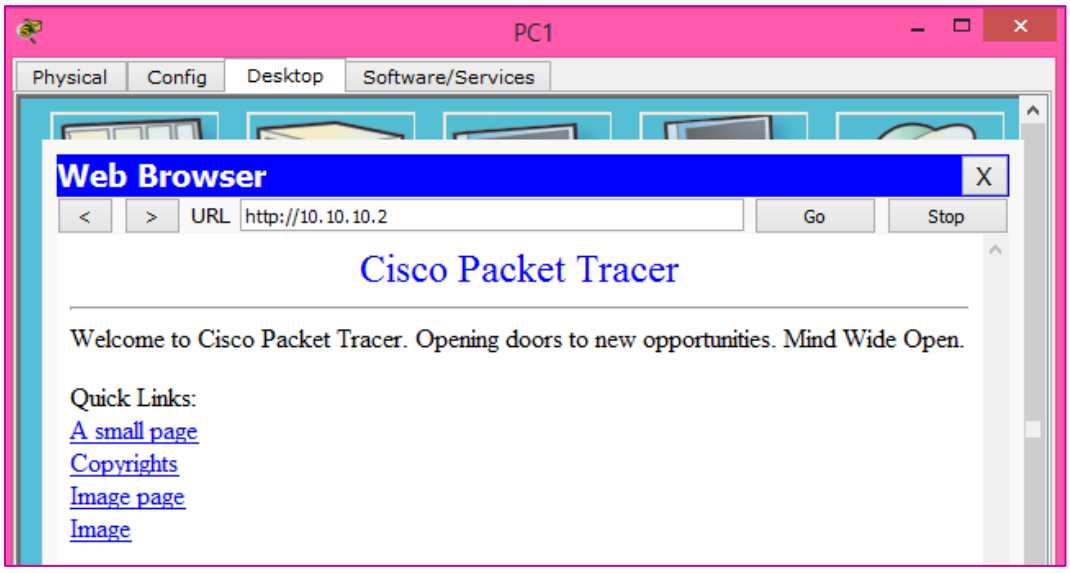
Lalu aktifkan pada interface bisa menggunakan **out** berarti pada interface **fa0/1.** Jika **in** berarti pada interface **fa 0/0.** Kita aktifkan pada interface **fa 0/0 berarti in.**

```
R-2(config)#int fa 0/0

R-2(config-if)#ip access-group BLOCK in
```

- Kita verifikasi pada PC1 terlebih dahulu

```
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Replay from 192.168.1.254: Destination host unreacable.

Replay from 192.168.1.254: Destination host unreacable.

Ping statistics for 10.10.10.2 :

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

Dan kita masih bisa mnegakses **web server**



Gambar 32.4 Tampilan Web Server pada PC1

- Kemudian kita verifikasi pada PC2

PC>**ping 10.10.10.2**

Pinging 10.10.10.2 with 32 bytes of data :

Replay from 10.10.10.2: bytes=32 time=1ms TTL=126

Replay from 10.10.1.2: bytes=32 time=11ms TTL=126

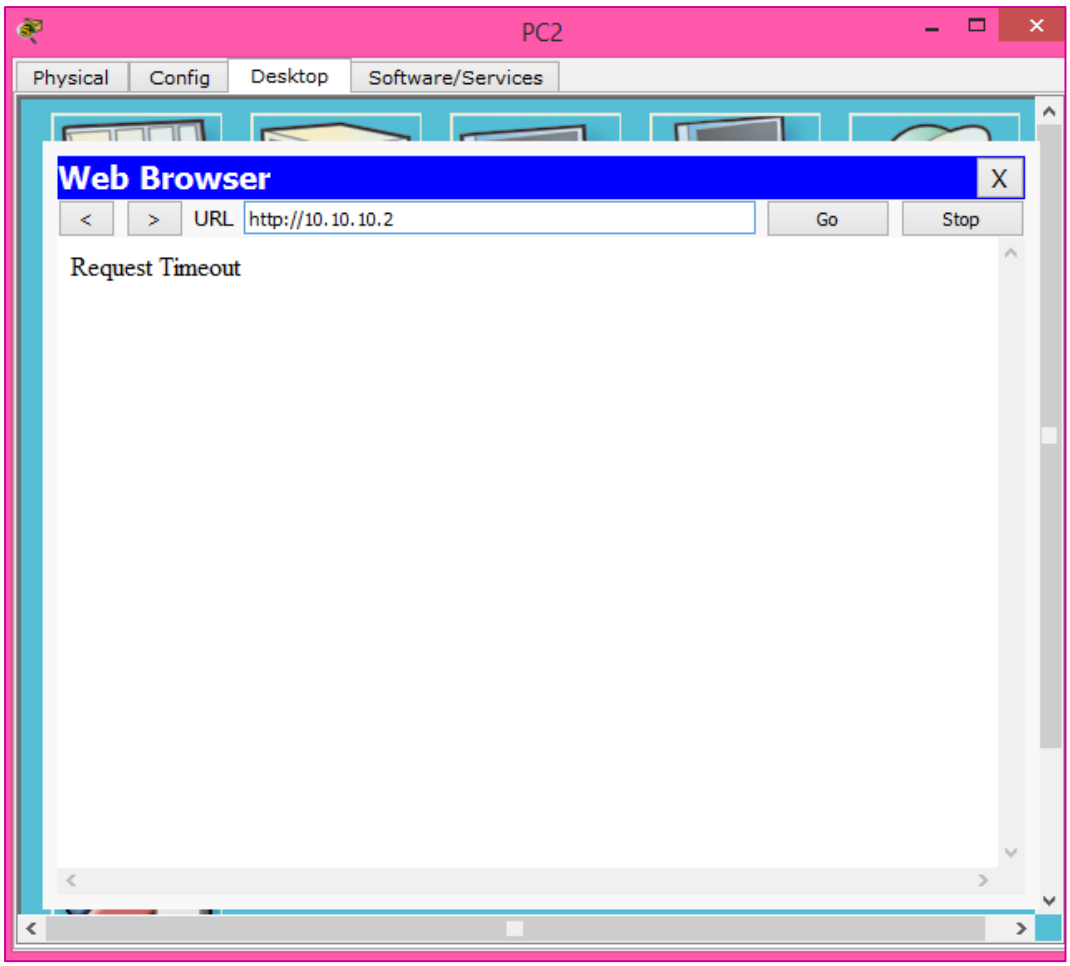
Ping statistics for 10.10.10.2 :

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

Approximate round trip times in milli-seconds :

Mininum = 0ms, Maximum = 11ms, Everage = 3ms

Buka browser pada PC2



Gambar 32.5 Tampilan Web Server PC2

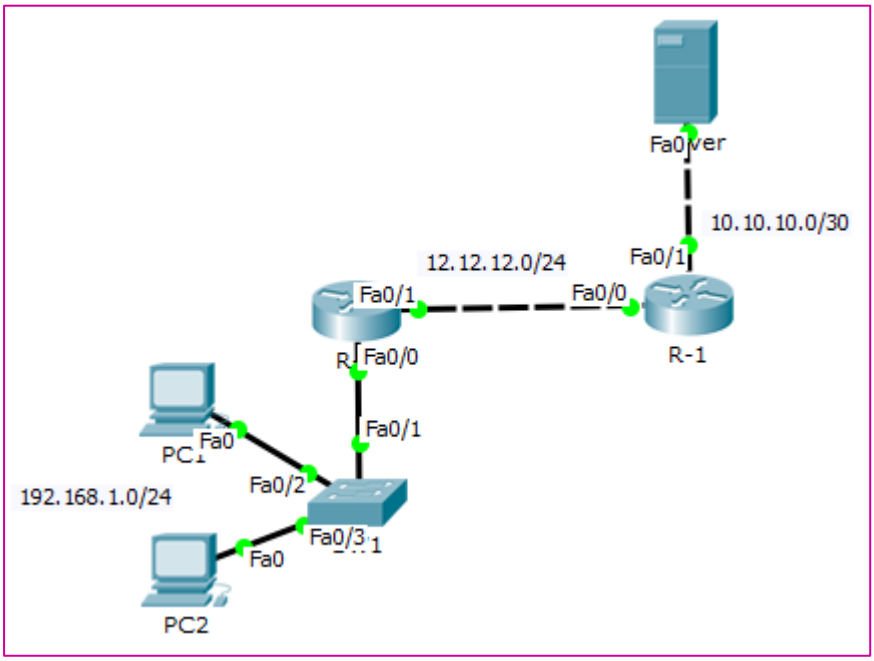
LAB 33 – Static NAT

NAT (Network Address Translation) digunakan untuk mengubah alamat IP Private menjadi IP Public. Ini dikarenakan **pada internet tidak dikenal IP Private.** Dengan static NAT kita akan menguah IP private menjadi IP Public secara manual.

- Kelebihan :
  1. Mengurangi adanya duplikasi IP Address pada jaringan atau biasa dikenal dengan conflict IP Address.
  2. Adanya NAT akan menghindari pengalamatan ulang pada saat jaringan tersebut berubah.
  3. Dapat menghemat IP Legal yang diberikan oleh ISP (Internet Service Provider).
  4. Dapat meningkatkan fleksibilitas untuk koneksi jaringan internet.

- Kelemahan :
  1. NAT dapat menyebabkan keterlambatan proses, ini disebabkan karena data yang dikirim harus melalui perangkat NAT terlebih dahulu.
  2. NAT dapat menyebabkan beberapa aplikasi tidak berjalan dengan normal
  3. NAT dapat menghilangkan kemampuan untuk melacak data, karena data tersebut akan melewati firewall.

Berikut adalah topologi yang kita pakai :



Gambar 33.1 Topologi Static NAT

Kita melanjutkan konfigurasi pada lab sebelumnya. Anggap **R1 dan Server adalah internet**. Maka dari itu kita hapus konfigurasi EIGRP dan Access-list.

Lalu tambahkan default-router ke internet.

```
R-2(config)#no router eigrp 1

R-2(config)#no ip access-list extended BLOCK

R-2(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.1
```

Kemudian test ping dari R2 ke Server

```
R-2#ping 10.10.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/18/84 ms
```

Terlihat bahwa dari router **R2 sudah bisa namun dari client belum bisa**

```
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Request time out.

Request time out.



Ping statistics for 10.10.10.2 :

    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Sekarang kita konfigurasi static NAT yang akan mengubah IP Address 192.168.1.1 menjadi 12.12.12.50 dan IP Address 192.168.1.2 menjadi 12.12.12.100.

Aktifkan NAT pada interface :

- ✓ Lokal = Inside
- ✓ Internet = Outside

```
R-2(config)#ip nat inside source static 192.168.1.2 12.12.12.100

R-2(config)#ip nat inside source static 192.168.1.1 12.12.12.50

R-2(config)#int fa 0/0

R-2(config-if)#ip nat inside

R-2(config-if)#ex

R-2(config)#int fa 0/1

R-2(config-if)#ip nat outside

R-2(config-if)#ex
```

Sekarang coba kita test ping dari client

```
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Request time out.

Replay from 10.10.1.2: bytes=32   time=11ms   TTL=126

Replay from 10.10.1.2: bytes=32   time=13ms   TTL=126

Ping statistics for 10.10.10.2 :

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

Approximate round trip times in milli-seconds :

     Mininum = 12ms, Maximum = 12ms, Everage = 13ms
```

Kemudian kita show ip nat nya dengan perintah **ip nat translations**

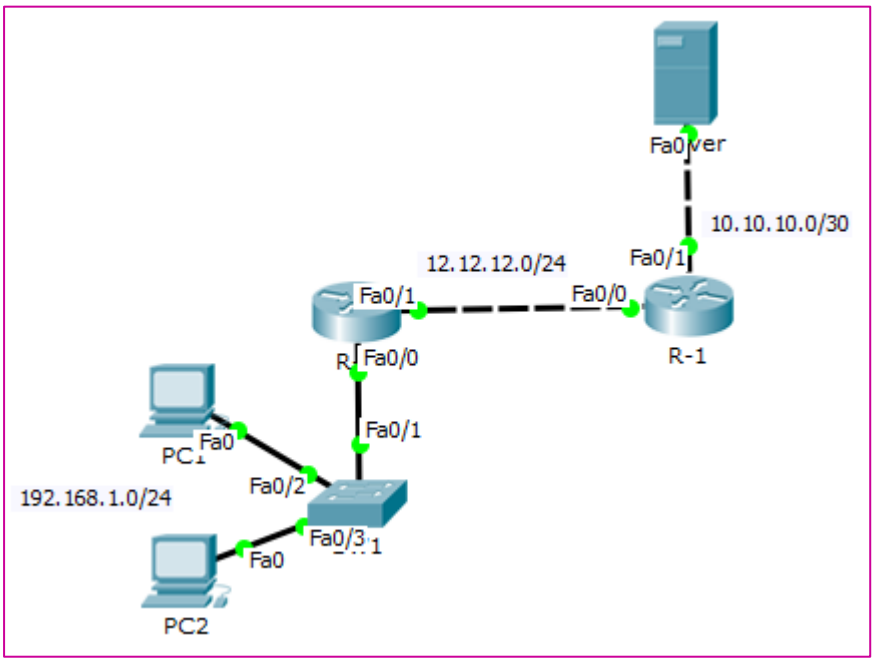
```
R-2#show ip nat translations

Pro    Inside global      Inside local       Outside local      Outside global
icmp 12.12.12.100:37  192.168.1.2:37     10.10.10.2:37      10.10.10.2:37
icmp 12.12.12.100:38  192.168.1.2:38     10.10.10.2:38      10.10.10.2:38
icmp 12.12.12.100:39  192.168.1.2:39     10.10.10.2:39      10.10.10.2:39
icmp 12.12.12.50:40   192.168.1.2:40     10.10.10.2:40      10.10.10.2:40
icmp 12.12.12.50:41   192.168.1.2:41     10.10.10.2:41      10.10.10.2:41
---    12.12.12.100       192.168.1.2        ---                ---
---    12.12.12.50        192.168.1.1        ---                ---
```

Terlihat bahwa IP Addressnya berubah.

LAB 34 – Dynamic NAT

Jika pada Static NAT kita mengubah IP Addressnya secara manual. Sedangkan pada Dynamic NAT kita akan membuat pool yang dapat digunakan untuk client.

Berikut adalah topologi yang akan kita gunakan :



Gambar 34.1 Topologi Dynamic NAT

Sebelumnya kita hapus konfigurasi Static NAT pada lab sebelumnya.

```
R-2(config)#no ip nat inside source static 192.168.1.2 12.12.12.100

R-2(config)#no ip nat inside source static 192.168.1.1 12.12.12.50
```

Setelah itu, buat pool pada Access-list yang digunakan nanti untuk **NAT.**

Note : POOL1 adalah nama pool boleh bebas

```
R-2(config)#access-list 1 permit 192.168.1.0 0.0.0.255

R-2(config)#ip nat pool POOL! 12.12.12.50 12.12.12.100 netmask
255.255.255.0
```

Lalu konfigurasi Dynamic NAT dan aktifkan pada interfacenya.

```
R-2(config)#ip nat inside source list 1 pool POOL1

R-2(config)#int fa 0/0

R-2(config-if)#ip nat inside

R-2(config-if)#ex

R-2(config)#int fa 0/1

R-2(config-if)#ip nat outside

R-2(config-if)#ex
```

Coba kita test ping lagi dari client

```
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Replay from 10.10.10.2: bytes=32   time=1ms   TTL=126

Replay from 10.10.1.2: bytes=32   time=11ms   TTL=126


Ping statistics for 10.10.10.2 :

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

Approximate round trip times in milli-seconds :

     Mininum = 0ms, Maximum = 11ms, Everage = 3ms
```

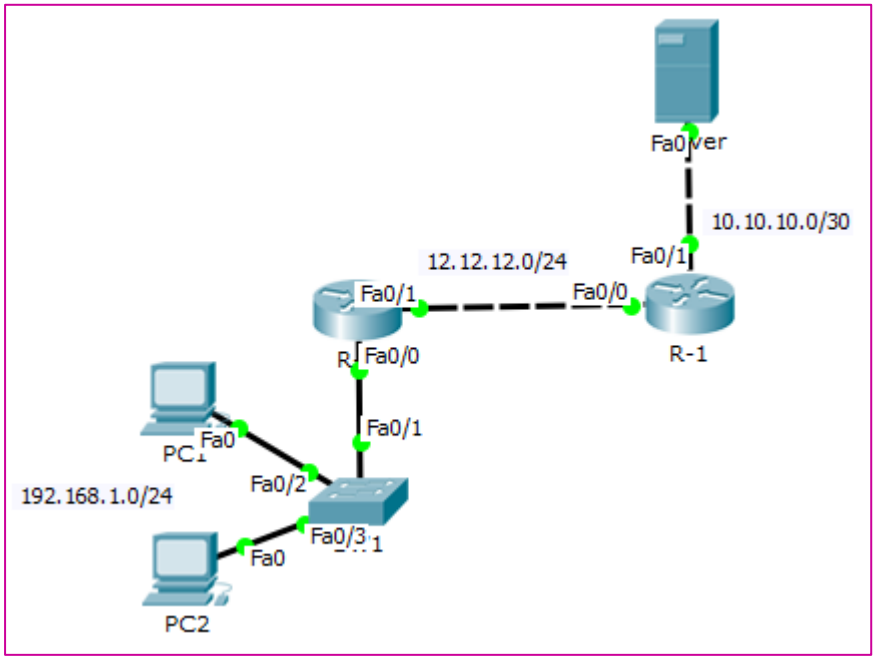
Kemudian kita cek pada R2 dengan perintah **show ip nat translations**

```
R-2#show ip nat translations

Pro    Inside global     Inside local       Outside local      Outside global
icmp 12.12.12.52:32    192.168.1.1:32     10.10.10.2:32      10.10.10.2:32
icmp 12.12.12.52:33    192.168.1.1:33     10.10.10.2:33      10.10.10.2:33
icmp 12.12.12.52:34    192.168.1.1:34     10.10.10.2:34      10.10.10.2:34
```

LAB 35 – NAT PAT

Jika dengan menggunakan Static NAT dan Dynamic NAT maka 1 private address diubah menjadi IP Public. Bagaimana jika kita hanya mempunyai 1 IP Public saja??

Maka gunakan NAT karena dengan PAT maka bukan IP yang diubah namun protocolnya. Berikut adalah topolohi yang akan kita gunakan :



Gambar 35.1 Topologi NAT PAT

Kita melanjutkan konfigurasi pada lab sebelumnya. PAT juga menggunakan pool jadi kita tidak perlu menghapusnya. Hapus konfigurasi Dynamic NAT nya saja.

```
R-2(config)#no ip nat inside source list 1 pool POOL1
```

Setelah dihapus, otomatis client tidak bisa ping ke Server

```
PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Request time out.

Request time out.

Ping statistics for 10.10.10.2 :

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

Tambahkan konfigurasi NAT PAT

```
R-2(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 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data :

Replay from 10.10.10.2: bytes=32   time=0ms   TTL=126

Replay from 10.10.1.2: bytes=32   time=0ms   TTL=126


Ping statistics for 10.10.10.2 :

      Packets: Sent = 4, Received = 4, Lost = 1 (0% loss),

Approximate round trip times in milli-seconds :

     Mininum = 0ms, Maximum = 0ms, Everage = 0ms
```

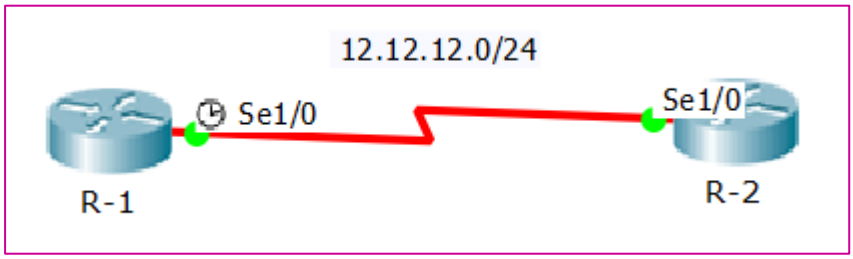
Lalu verifikasi pada R2

```
R-2#show ip nat translations

Pro    Inside global     Inside local      Outside local     Outside global
icmp  12.12.12.52:49    192.168.1.1:49    10.10.10.2:49     10.10.10.2:49
icmp  12.12.12.52:50    192.168.1.1:50    10.10.10.2:50     10.10.10.2:50
icmp  12.12.12.52:51    192.168.1.1:51    10.10.10.2:51     10.10.10.2:51
```

LAB 36 – WAN-HDLC

WAN technologi merupakan technologi yang digunakan untuk menghubunglan router yang jauh/tidak bisa dicapai oleh kabel **FastEthernet.** WAN menggunakan kabel Serial dan sifatnya adalah point-to-point.

Berikut adalah topologi yang akan kita gunakan :



Gambar 36.1 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 cek **encapsulation** HDLC nya.

```
R-1#show int se1/0

Serial2/0 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
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 1 interface resets
```

Dalam menggunakan kabel serial ada dua pengguna yaitu DTE dan DCE. DCE biasanya dipegang oleh ISP dan sebagai penentu **clock rate.**Clock rate harus di atur jika tidak mka kan berjalan.pada cisco packet tracer tandanya ada gambar

clock di atas router.Jika menggunakan terminal bisa di check dengan perintah berikut.

- R-1

```
R-1#sho 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:
...
```

- R-2

```
R-2#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 ratenya.

- R-1

```
R-1(config-if)#clock rate 56000

R-1(config-if)#ip address 12.12.12.1 255.255.255.0

R-1(config-if)#no shutdown
```

- R-2

```
R-2(config)#int se 1/0

R-2(config-if)#ip address 12.12.12.2 255.255.255.0

R-2(config-if)#no shutdown
```

Verifikasi pada R1 bahwa clock rate nya sudah kiita ubah.

```
R-1#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:
```

Kemudian kita test ping antar router

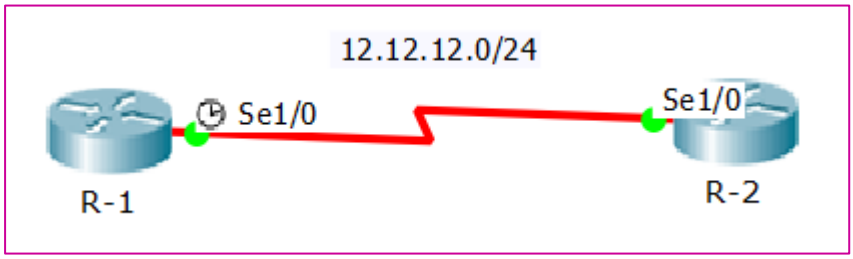
```
R-1#ping 12.12.12.2

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 = 1/1/5 ms
```

Note :

- ✓ Clock Rate : Dalam pengetahuan komputer, istilah clock rate biasanya digunakan untuk menyebut kecepatan kerja procesor yang diukur dalam satuan herz. Sebenarnya clock rate menyatakan banyaknya siklus per detik (cycles per second) . Siklus yang dimaksud adalah siklus transfer data dari satu register procesor ke lainnya. Misalnya dalam 1 detik terjadi 100 siklus pengiriman data, maka dapat dikatakan clock ratenya adalah 100 herz. Dengan demikian jika clock rate suatu procesor 800 Mhz, maka procesor tersebut mampu mengerjakan 800 juta siklus pengiriman data per detik. Clock rate disebut juga dengan frekuensi.

LAB 37 – PPP (Point-to-Point) Protocol

PPP merupakan Open Standard. Kita harus mengkonfigurasi terlebih dahulu untuk bisa menggunakannya.



Gambar 37.1 Topologi PPP

Melanjutkan konfigurasi dari lab sebelumnya. Kita hanya perlu mengubah encryption yang dipakai oleh kedua router.

- R-1

```
R-1(config)#int se 1/0

R-1(config-if)#encapsulation ppp
```

Setelah kita konfigurasi maka Serial akan down. Ini dikarenakan kedua router menggunakan encryption yang berbeda. Kemudian kita atur juga pada router sebelahnya.

- R-2

```
R-2(config)#int se 1/0

R-2(config-if)#encapsulation ppp
```

Verifikasi encapsulation

```
R-1#show int se1/0

Serial2/0 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)
```

Kemudian lakukan test ping antar router

```
R-1#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 = 1/26/125 ms
```

LAB 38 – PPP PAP

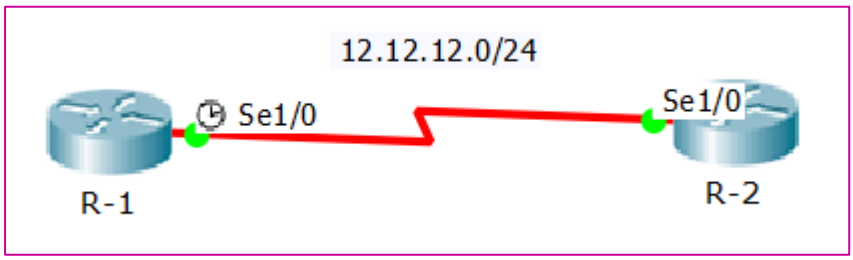
Pada PAP kita dapat menggunakan authentikasi. PAP (Password Authentication Protocol) yaitu prosedur authentikasi dengan 2 langkah :

- User yang ingin mengakses sistem mengirimkan authentikasi identitas biasanya user dan password.
- Sistem mengecek validitas identifikasi dan password dengan cara menerima atau menolak koneksi.

Ada 2 jenis authentikasi yaitu :

1. **PAP (Password Authentication Protocol) merupakan Plain Text**
2. **CHAP (Challenge Handshake Authentication Protocol) merupakan Encryption**

Kita menggunakan topologi dari lab sebelumnya



Gambar 38.1 Topologi PPP PAP

Kita buat terlebih dahulu **username dan password.**

- R-1

```
R-1(config)#username AKUN password 123
```

- R-2

```
R-2(config)#username USER password 456
```

Lalu konfigurasikan authentikasi pada router R1 dan R2

- R-1

```
R-1(config)#int se1/0
R-1(config-if)#ppp authentication pap
R-1(config-if)#ppp pap sent-username USER password 456
```

- R-2

R-2(config)#**int se1/0**

R-2(config-if)#**ppp authentication pap**

R-2(config-if)#**ppp pap sent-username AKUN password 123**

Note : format perintahnya adalah **PPP PAP sent-username** *user-lawan* **password** *password-lawan*

Kita bisa liat authentikasinya dengan menggunakan perintah debug lalu mematikan dan menyalakan interface

R-1#**debug ppp negotiation**
PPP protocol negotiation debugging is on

R-1 (config)#**int se 1/0**

R-1 (config-if)#**shutdown**
%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

R-1 (config-if)#**no shutdown**
%LINK-5-CHANGED: Interface Serial1/0, changed state to up

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

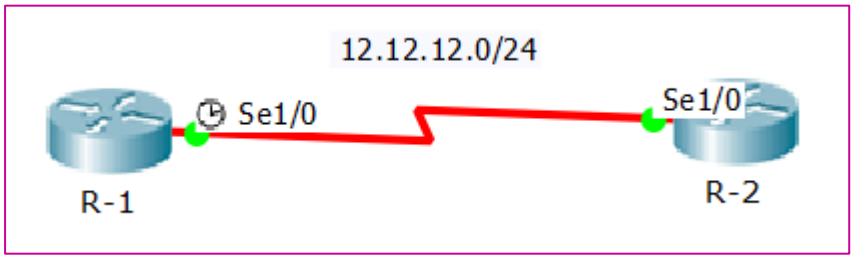
Coba test ping antar router

```
R-1#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 = 1/26/125 ms
```

LAB 39 – PPP CHAP

Sebelumnya kita sudah menggunakan PAP, sekarang kita menggunakan CHAP (Challenge Handshake Aunthentication Protocol) adalah protocol authentikasi three-way-handshaking yang memberikan keamanan lebih tinggi dari PAP, dalam mode ini password akan disimpan secara aman dan tidak pernah dikirimkan secara online. CHAP akan mengencrypsi hanya authentikasinya saja, tidak mengencrypsi seluruh data.

Berikut adalah topologi yang akan kita gunakan :



Gambar 39.1 PPP CHAP

Jika pada lab sebelumnya kita membuat username dan password **bebas.** Sekarang kita harus membuatnya dengan format berikut :

Note : **username** *hostname-lawan* **password** *harus-sama*

Kita buat terlebih dahulu username dan passwordnya pada tiap router

- R-1

```
R-1(config)#username R-2 password 123
```

- R-2

```
R-2(config)#username R-1 password 456
```

Lalu aktifkan pada interface

- R-1

```
R-1(config)#int se1/0
R-1(config-if)#ppp authentication chap
```

- R-2

```
R-2(config)#int se1/0
R-2(config-if)#ppp authentication chap
```

Perintah debug akan melihatkan authentikasinya

```
R-1#debug ppp negotiation
PPP protocol negotiation debugging is on

R-1(config)#int se1/0

R-1(config-if)#shutdown

R-1(config-if)#no shutdown

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: I CONFREQ [Closed] id 1 len 10

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

Serial1/0 PPP: Phase is FORWARDING, Attempting Forward

Serial1/0 Phase is ESTABLISHING, Finish LCP

Serial1/0 Phase is up
```

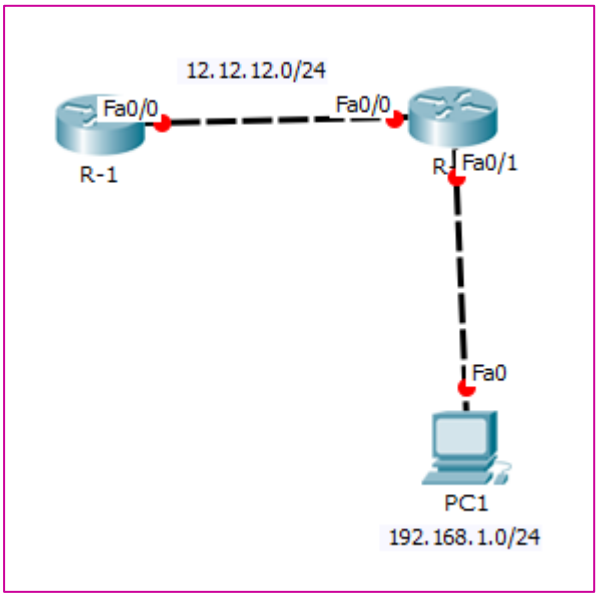
Coba kita test ping antar router

```
R-1#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 = 1/26/125 ms
```

LAB 40 – PPP Relay

DHCP Relay sudah masuk kedalam materi CCNAv3. DHCP Relay akan meneruskan IP Address yang diberikan oleh server ke client yang memintanya. Jadi biasanya kita mendapatkan IP Address dengan gateway yang satu segment. Jika dengan DHCP Relay maka IP Address dan gateway nya berbeda.

Berikut adalah topologi yang akan kita gunakan :



Gambar 40.1 Topologi DHCP Relay

Konfigurasi IP Address dan buat DHCP Server pada R-1 beserta routingnya

```
R-1(config)#int fa0/0

R-1(config-if)#ip add 12.12.12.1 255.255.255.0

R-1(config-if)#no shutdown

R-1(config-if)#ip dhcp pool DEVI

R-1(dhcp-config)#network 192.168.1.0 255.255.255.0

R-1(dhcp-config)#default-router 192.168.1.254

R-1(dhcp-config)#dns-server 100.100.100.100

R-1(dhcp-config)#ex

R-1(config)#ip dhcp excluded-address 192.168.1.250 192.168.1.254

R-1(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.2
```

Note : - **DEVI** merupakan nama poolnya saja (bebas).

- **Default-router** merupakan gateway yang akan diberikan ke client.

- **DNS-Server** merupakan IP DNS Server

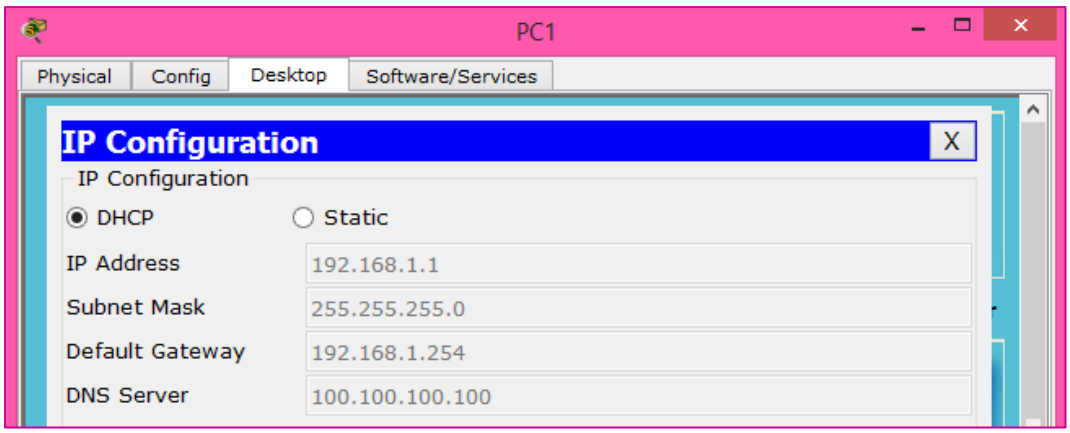
- **IP DHCP Excluded-Address** perintah ini digunakan jika ada IP Address yang tidak ingin dibagikan. **Yaitu dari 192.168.1.250-192.168.1.254**

Perlu ditambahkan routing agar R-1 dapat mengetahui network yang dibagikannya

Setelah itu konfigurasi IP Address dan DHCP Relay pada R-2

```
R-2(config)#int fa 0/1

R-2(config-if)#ip add 192.168.1.254 255.255.255.0

R-2(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

R-2(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 lihat pada client apakah sudah mendapatkan IP Address atau belum.



Gambar 40.2 DHCP Client pada PC1

PROFILE PENULIS

Assalamu'alaikum wr.wb

Saya adalah seorang gadis yang lahir delapan belas tahun lalu di Bekasi, tepatnya pada 23 Desember 1998. Nama lengkap saya Devitriana Elizami. Saya lahir dikeluarga yang serba berkecukupan, tetapi alhamdulillah dengan selalu syukur, hidup kami insyaallah selalu bahagia. Saya anak ke dua dari tiga bersaudara, dan saya anak perempuan satu-satunya.

Saya mempunyai hobi menggambar, dan saya bercita-cita menjadi seorang pelukis profesional. Sejak umur 14 tahun saya sudah mulai bekerja sebagai tukang gambar sambil bersekolah hingga duduk dibangku SMK. Penghasilan saya tidak bisa ditetapkan setiap bulannya, karena tergantung seberapa banyak saya mendapatkan pesanan dan seberapa sanggup saya mengerjakan pesanan tersebut.

Alhamdulillah saya selalu mendapatkan peringkat 5 besar di pendidikan formal dan sering mendapatkan beasiswa. Sedangkan dipendidikan non-formal saya pernah mendapat 2 piala beserta sertifikat yaitu juara 3 Lomba Menggambar Pahlawan dalam rangka Hari Pahlawan dan Bulan Bahasa, dan juara 2 Lomba Mading dalam rangka Memperingati Hari Kartini. Selain itu banyak lomba dan sertifikat yang saya menangkan di event online berbagai grup seni. Semua karya saya, saya share lewat account Facebook dengan nama DevitrianArt, dan Instagram saya DevitrianArt.

Saat ini saya duduk dibangku SMK kelas 12 berjurusan Teknik Komputer dan Jaringan di SMK Karya Guna Bhakti 2 Kota Bekasi. Saya baru saja menyelesaikan training networking MTCNA, MTCRE, dan CCNA untuk mendapatkan sertifikat internasional dengan mengikuti examinationnya. Saat ini saya sedang menyelesaikan 3 buku yaitu CCNA, MTCNA, dan MTCRE. Dan website aktif saya yaitu https://www.curhatanseorangit.wordpress.com .

Pasti banyak yang bertanya-tanya, kenapa saya mengambil 2 arah yang berbeda (Seni dan Komputer), saya senang dan merasa tertantang jika menguasai 2 hal yang bersamaan. Kalau bisa saya ingin jadi Multitalent ☺

Lambat laun cita-cita sebagai pelukis profesional itu mulai bercabang. Perkembangan zaman yang semakin hari semakin canggih, dan persaingan di dunia kerja pun makin ketat. Membuat saya berfikir harus memanfaatkan dan mengembangkan potensi diri. Masalah "**cita-cita**" sebenarnya hanya patokan, yang pasti maksimalkanlah apa yang akan dihadapi, dengan doa dan ikhtiar insyaallah hasilnya akan lebih baik.

Demikian profile saya, jika ada kesalahan kata mohon dimaafkan. Terimasih.
Wassalamu'alaikum wr.wb