



# Computer Network

## Hands on Lab



Januari 2018

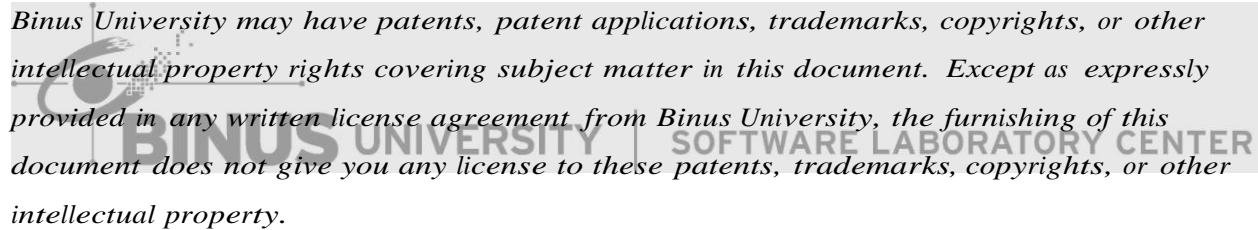
For the latest information, please see [bluejack.binus.ac.id](http://bluejack.binus.ac.id)



*Information in this document, including URL and other Internet Web site references, is subject to change without notice. This document supports a preliminary release of software that may be changed substantially prior to final commercial release, and is the proprietary information of Binus University.*

*This document is for informational purposes only. BINUS UNIVERSITY MAKES NO WARRANTIES, EITHER EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*The entire risk of the use or the results from the use of this document remains with the user. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Binus University.*

Binus University may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Binus University, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

*Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.*

© 2017 Binus University. All rights reserved.

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## ***Table of Content***

OVERVIEW .....	iii
Chapter01 - Introduction to Networking.....	1
Chapter02 - Crimping .....	13
Chapter03 - Introduction to TCP/IP and Subnetting.....	21
Chapter04 - Router Configuration .....	41
Chapter05 - Routing.....	53
Chapter06 - Access List .....	64
Chapter07 - VLAN.....	74
Chapter08 - Wi Fi .....	84
REFERENCES .....	92

# OVERVIEW

## Chapter 01

- Introduction to Networking

Membahas konsep jaringan komputer, topologi jaringan, perangkat jaringan, dan pengenalan 7 Layer OSI.

## Chapter 02

- Crimping

Membahas cara crimping kabel UTP dengan memperhatikan urutan dan fungsi dari tiap jenis kabel UTP CAT-5.

## Chapter 03

- Introduction to TCP/IP and Subnetting

Membahas konsep TCP/IP meliputi pengalaman IP pada layer 3 OSI dan aplikasi subnetting. Selain itu, juga membahas MAC address, frame dan paket, dan IPv6.

## Chapter 04

- Router Configuration

Membahas konfigurasi ip address pada interface router baik dilakukan pada packet tracer maupun MikroTik.

## Chapter 05

- Routing

Membahas konsep routing pada router, mekanisme static dan dynamic routing.

## Chapter 06

- Access List

Membahas konsep access list, pembuatan access list dan penerapannya.

## Chapter 07

- VLAN

Membahas konsep VLAN, pembuatan VLAN dan penerapannya.

## **Chapter 01**

### **Introduction to Networking**



## 1.1. Pengenalan Jaringan Komputer

Jaringan komputer adalah suatu sistem yang terdiri dari komputer dan perangkat jaringan lain yang terhubung melalui suatu media untuk saling berkomunikasi dengan bertukar data.

Tujuan dari jaringan komputer antara lain sebagai berikut:

- Komunikasi: contohnya email, chatting, telepon (VOIP).
- Akses informasi: contohnya web browsing.
- Membagi sumber daya. Contohnya berbagi pemakaian printer, CPU, memori, harddisk, software dan data.

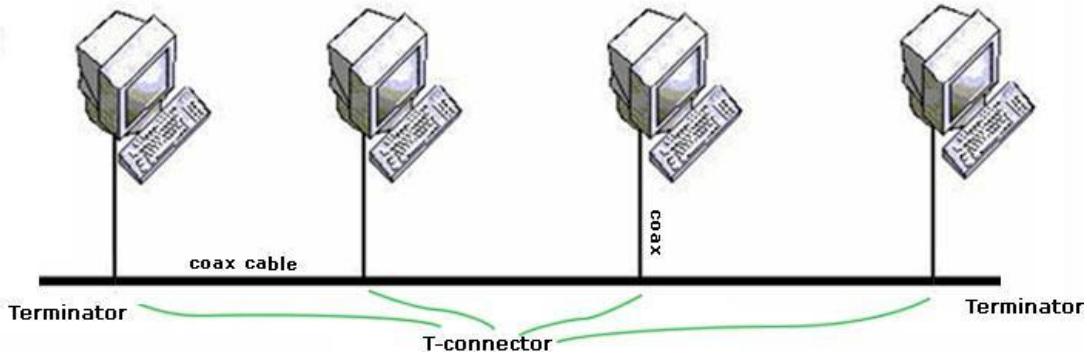
## 1.2. Topologi jaringan

Topologi jaringan adalah bentuk atau pola yang digunakan dalam menghubungkan antar node pada jaringan.

Berdasarkan topologi jaringan, jaringan komputer dapat dibedakan menjadi beberapa bagian, antara lain:

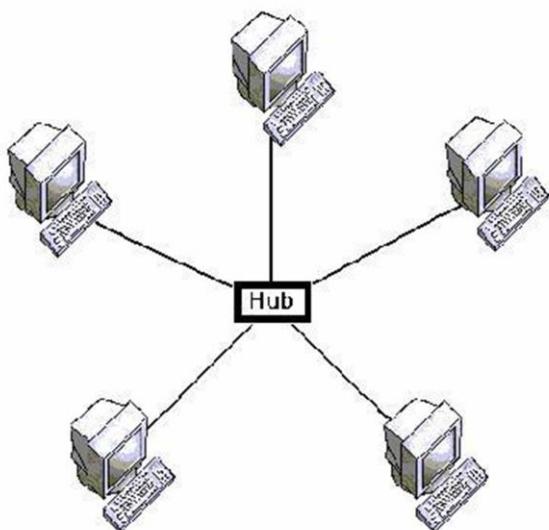
### • Topologi bus

Topologi bus menggunakan “*single backbone segment*” sebagai penghubung semua komputer yang ada pada jaringan. Semua komputer langsung terhubung ke komputer tersebut.



- Topologi bintang (*Star*)

Topologi bintang menghubungkan semua workstation ke satu buah titik pusat. Titik pusat ini biasanya berupa hub atau switch sehingga seolah-olah komputer yang terhubung berbentuk seperti bintang.



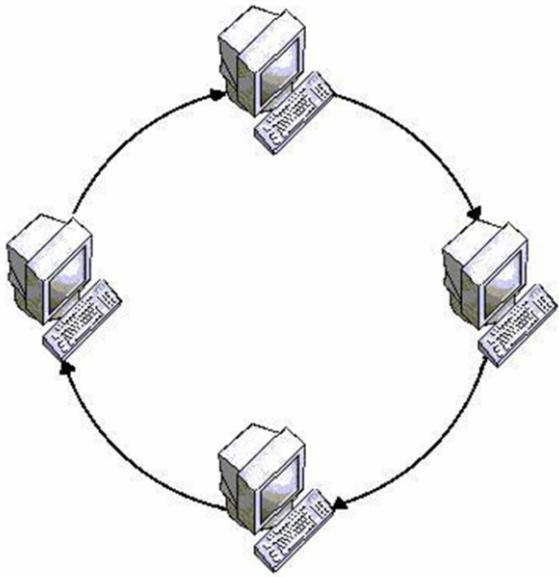
- Topologi *extended star*

Topologi *extended star* menggabungkan beberapa topologi *star* menjadi satu.



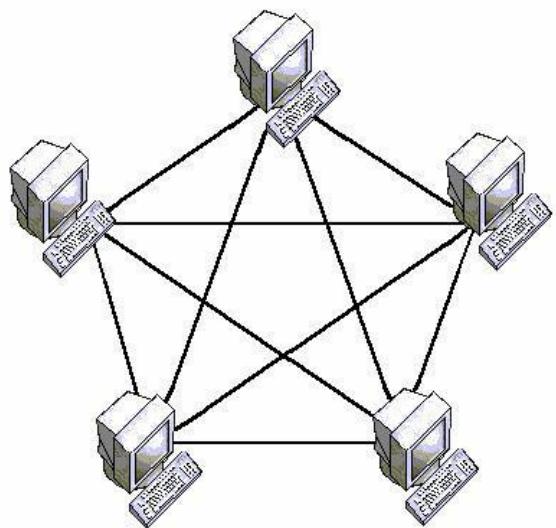
- Topologi cincin (Ring)

Topologi cincin berbentuk rangkaian workstation yang masing-masing terhubung ke dua workstation lainnya, sedemikian sehingga membentuk jalur melingkar membentuk cincin. Pada topologi cincin, komunikasi data dapat terganggu jika satu titik mengalami gangguan.



- Topologi *mesh*

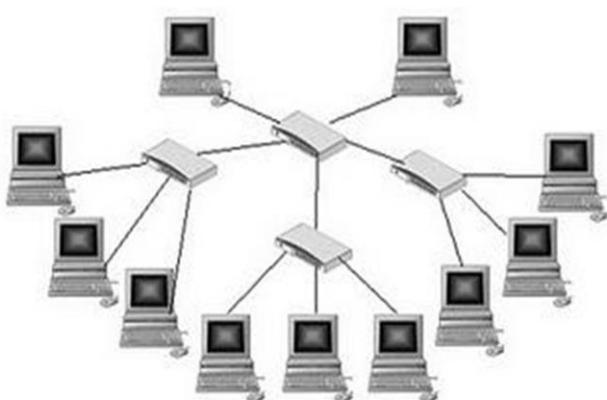
Topologi *mesh* adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam jaringan. Akibatnya, dalam topologi mesh setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (*dedicated links*). Topologi mesh biasanya digunakan di jaringan yang memerlukan ketersediaan jaringan (uptime) tinggi seperti pada jaringan datacenter.



- Topologi pohon (*tree*)

Topologi jaringan ini disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hierarki yang berbeda.

Untuk hierarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin keatas mempunyai hierarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer



### 1.3. Media dalam Jaringan Komputer

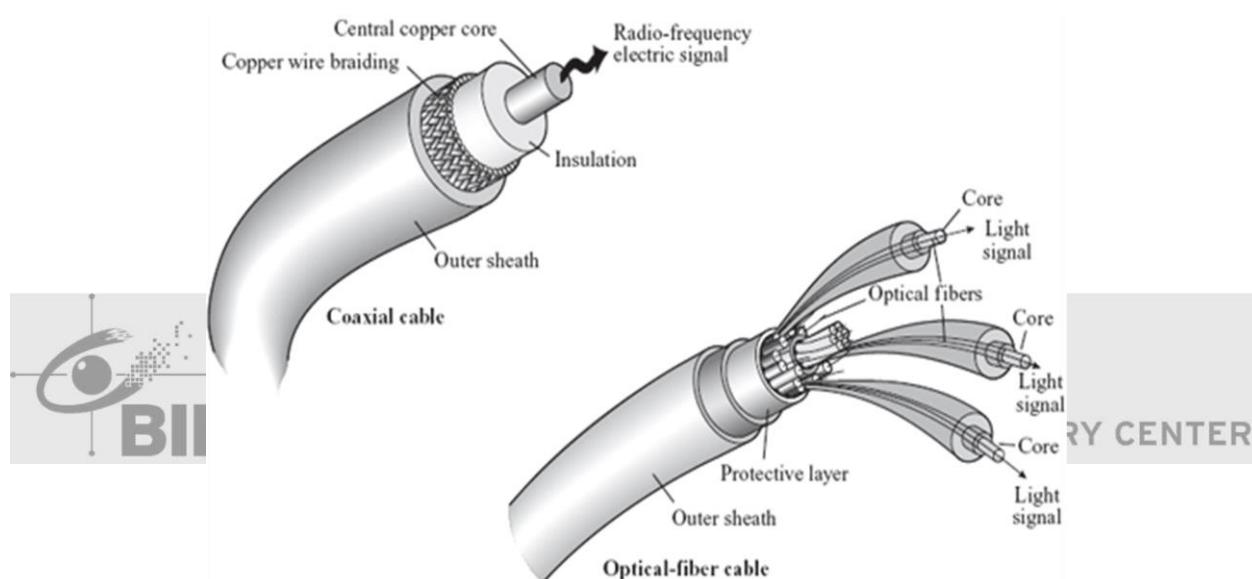
Terdapat beberapa media dalam jaringan komputer di antaranya adalah sebagai berikut.

- Kabel

Ada beberapa jenis kabel yang banyak digunakan dan menjadi standard dalam penggunaannya untuk komunikasi data dalam jaringan komputer. Setiap jenis kabel mempunyai kemampuan dan spesifikasi yang berbeda.

Tiga jenis kabel yang umum digunakan adalah :

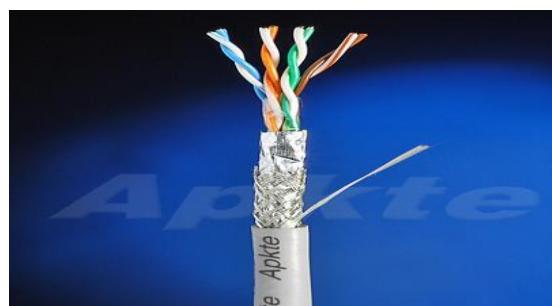
- *Coaxial*



- *Twisted Pair*

*Twisted Pair* adalah jenis kabel yang dua konduktornya digabungkan dengan tujuan untuk mengurangi atau meniadakan gangguan elektromagnetik dari luar.

Ada 2 jenis kabel *Twisted Pair*, yaitu UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*). Perbedaan antara kedua jenis kabel tersebut adalah pada bagian dalam dari kabel, STP memiliki lapisan di bagian dalam kabel sedangkan UTP tidak.



- *Fiber Optic*

Pada fiber optic, transmisi data dilakukan dengan menggunakan cahaya, berbeda dengan copper cable (kabel tembaga: UTP, STP, coaxial) yang menggunakan sinyal listrik. Hal tersebut menghasilkan jarak tempuh yang lebih jauh dan kecepatan yang lebih tinggi serta tidak terpengaruh terhadap cuaca, panas dan juga elektromagnetik sehingga kabel fiber optic dapat memberikan performa serta kapasitas yang jauh lebih tinggi dari kabel tembaga, oleh karena itu kabel fiber optic biasanya digunakan untuk koneksi jarak jauh maupun koneksi yang memerlukan kecepatan tinggi seperti pada backbone dan interkoneksi antar daerah.

#### 1.4. Perangkat-Perangkat Jaringan Komputer

- Repeater

Repeater berfungsi untuk memperpanjang rentang jaringan dengan cara memperkuat sinyal elektronik. Repeater dapat digunakan untuk sinyal analog maupun digital dan biasanya digunakan untuk transmisi data jarak jauh. Dan dapat juga digunakan untuk menggabungkan beberapa segmen suatu jaringan yang besar, misalnya apabila menggunakan kabel terdapat keterbatasan, maka Repeater sangat dibutuhkan dalam hal ini.



- Hub

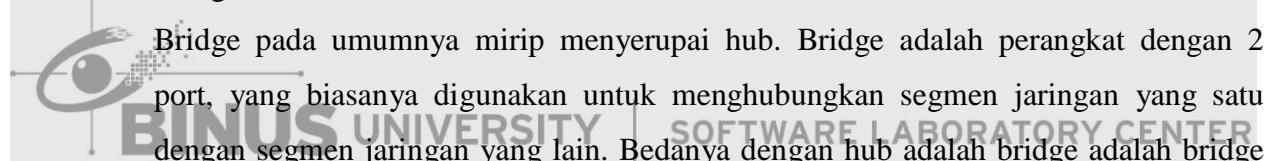
Hub adalah sebuah perangkat yang menyediakan suatu jalur fisik bagi suatu sinyal untuk dapat menyeberang dari satu kabel ke kabel berikutnya. Pada dasarnya, hub

merupakan repeater dengan banyak port, maka hub **hanya menguatkan sinyal listrik** yang masuk ke dalam salah satu portnya, dan meneruskan sinyal itu ke semua port yang lain.

Karena hub hanya bekerja menguatkan sinyal tanpa melakukan pemrosesan apapun, maka tiap-tiap port pada hub selalu merupakan bagian dari segmen jaringan (*collision domain* yang sama).



- Bridge

Bridge pada umumnya mirip menyerupai hub. Bridge adalah perangkat dengan 2 port, yang biasanya digunakan untuk menghubungkan segmen jaringan yang satu dengan segmen jaringan yang lain. Bedanya dengan hub adalah bridge adalah bridge melaksanakan pemeriksaan terhadap data yang datang, dan membuat keputusan apakah data itu boleh dilewatkan atau tidak. Bridge bekerja pada lapisan 2 OSI (misalnya MAC Address).

- Switch

Sekilas switch sangat mirip dengan hub, tetapi keduanya berbeda. Switch ini adalah perkembangan dari hub dan bridge, punya port banyak seperti hub dengan cara kerja seperti bridge. Pada switch, frame diteruskan berdasarkan MAC address yang disimpan dalam table MAC Address yang dimiliki switch. Switch bekerja pada layer 2 (*Data Link*) pada model OSI.

Cara kerja switch:

- ✓ Pada saat frame diterima switch, akan diperiksa apakah MAC address (dalam table MAC Address) yang dituju tersambung pada port yang sama dengan MAC address pengirim.
- ✓ Jika pada port yang sama maka pengiriman frame tidak diteruskan.

- ✓ Jika tidak, maka frame akan diteruskan ke port jaringan yang mengandung MAC address tujuan.
- ✓ Dengan demikian terbentuk jalur logikal dalam switch antar membuat dua buah komputer/end-device yang berkomunikasi, sehingga perangkat jaringan lainnya tidak terganggu. Dengan demikian pada switch kecepatannya tidak terbagi-bagi, melainkan masing - masing port memiliki bandwidth yang penuh sehingga kecepatan transfer data pun akan menjadi lebih tinggi dibandingkan dengan hub.

Pada awalnya, switch merupakan perangkat bridge dengan banyak port. Namun, kini switch memiliki perbedaan secara fungsional. Pertama, switch dapat menangani beberapa sambungan sekaligus. Artinya switch dapat mengirim dan menerima frame-frame secara bersamaan (full-duplex). Kedua, switch memiliki sejumlah buffer (memori sementara) yang digunakan untuk menampung frame-frame, sehingga frame-frame itu dapat dikirimkan kembali. Fungsi ini bermanfaat jika terjadi kepadatan trafik jaringan.



- **Unmanageable switch.**

Unmanageable switch hampir sama dengan hub tetapi jauh lebih cepat dan data hanya dikirimkan kepada port yang memiliki jaringan yang dituju. Switch ini adalah perangkat yang tinggal pakai, tidak memerlukan pengaturan sama sekali.

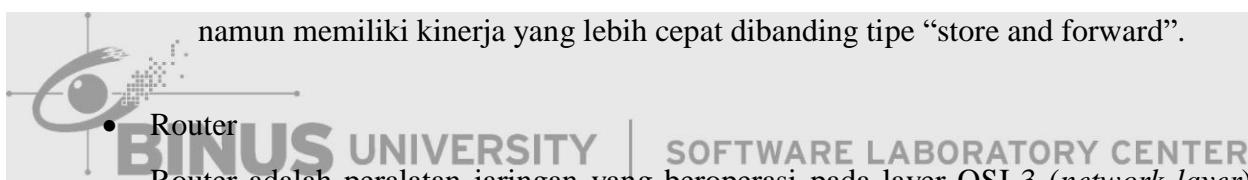
- **Manageable switch**

Manageable switch tidak hanya memiliki kemampuan yang sama, juga ditambah dengan kemampuan untuk membuat Virtual LAN dengan melakukan setting terhadap switch, sehingga dapat diatur pengiriman data hanya dari dan ke jaringan tertentu.



Berdasarkan cara untuk meneruskan data, switch dibedakan menjadi 2 tipe:

- Switch “*Store and forward*” (simpan dan teruskan) menerima dan menyimpan seluruh frame secara utuh di dalam buffer, sebelum mengirimkan kembali frame tersebut. Hal ini memungkinkan switch membaca dan menghitung checksum yang ada pada akhir frame untuk memastikan bahwa frame tidak rusak.
- Switch “*cut through*” (lewaskan saja) hanya membaca alamat tujuan dan mengirimkan kembali frame tersebut, termasuk frame yang mengalami kerusakan, namun memiliki kinerja yang lebih cepat dibanding tipe “store and forward”.



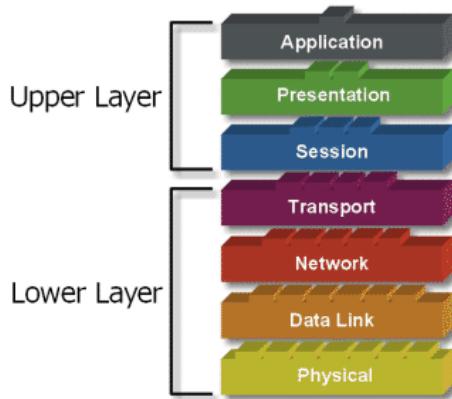
Router adalah peralatan jaringan yang beroperasi pada layer OSI 3 (*network layer*).

Beberapa router bergabung, menghubungkan beberapa segment jaringan atau bahkan seluruh jaringan. Router mengirimkan data berdasarkan informasi pada layer 3.



## 1.4. 7 OSI Layer

Model *Open Systems Interconnection* (OSI) diciptakan oleh *International Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. OSI dibuat sebagai standard komunikasi agar perangkat yang berbeda manufaktur dapat saling berkomunikasi. Standard ini dikembangkan agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien.



Terdapat 7 layer pada model OSI. Setiap layer bertanggung jawab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk memaketkan data menjadi frame-frame, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.

Model Layer OSI dibagi dalam dua group: “upper layer” dan “lower layer”. “Upper layer” fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Lower layer adalah intisari komunikasi data melalui jaringan aktual, bagaimana data dikirimkan dari perangkat yang satu ke perangkat yang lain.

Berikut dijelaskan 3 layer paling bawah dari 7 OSI Layer.

### Layer 1 OSI: *Physical Layer*

*Physical Layer* adalah layer paling bawah dari layer model OSI. Layer ini berisi standar-standar untuk menghubungkan komputer kepada media transmisi yang sesungguhnya. Contohnya: Membahas bagaimana frame dikonversi ke dalam bentuk bit-bit singnal listrik maupun gelombang radio tergantung media yang digunakan.

Tujuan utama dari layer Physical adalah:

- Menspesifikasikan standar untuk berinteraksi dengan media jaringan.
- Menspesifikasikan kebutuhan media untuk jaringan.

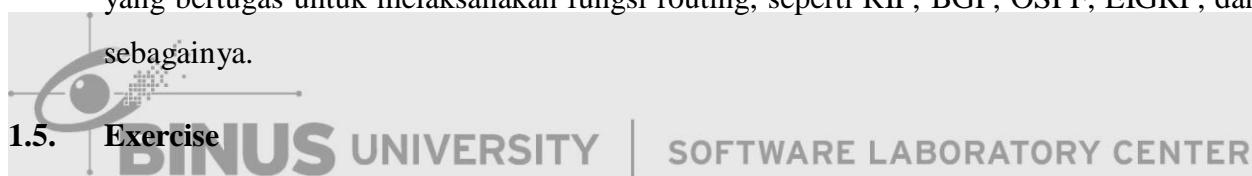
- Format sinyal elektrikal untuk transmisi lewat media jaringan.
- Sinkronisasi transmisi sinyal.
- Deteksi error selama transmisi.

### **Layer 2 OSI: Data Link Layer**

Lapisan Data Link bertanggung jawab untuk memaketkan data dari lapisan di atasnya menjadi frame-frame transmisi, dan mentransmisikan via medium. Untuk melaksanakan hal ini, seperangkat aturan dan prosedur harus didefinisikan untuk mengontrol aliran data dan error, dan mengalokasikan alamat-alamat fisik ke semua perangkat yang ada dalam jaringan. Alokasi alamat dapat dilakukan dengan MAC Address.

### **Layer 3 OSI: Network Layer**

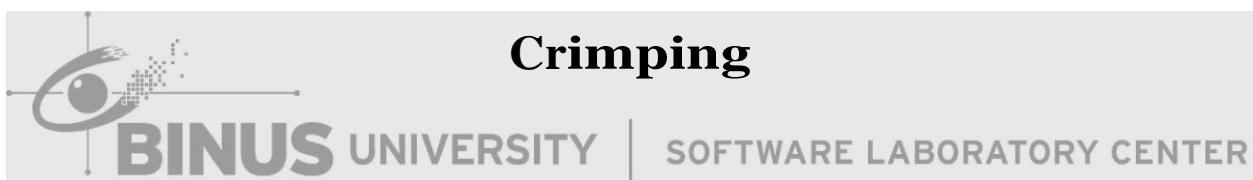
Lapisan Jaringan bertugas dalam membentuk rute komunikasi dari suatu simpul ke simpul lainnya dalam suatu jaringan. Oleh karenanya, perlu dibuat alokasi alamat global yang unik untuk perangkat komputer (misalnya dengan IP address) dan diperlukan protokol yang bertugas untuk melaksanakan fungsi routing, seperti RIP, BGP, OSPF, EIGRP, dan sebagainya.



1. Apakah yang dimaksud dengan jaringan komputer?
2. Faktor-faktor apa saja yang harus dipertimbangkan dalam menentukan suatu topologi jaringan?
3. Apa yang akan terjadi jika koneksi pada suatu komputer pada jaringan bus terputus? Bagaimana jika jaringan tersebut merupakan jaringan *ring*, *star*, atau *mesh*?
4. Kabel fiber *optic* dapat dibedakan menjadi 2 mode, yaitu ***single mode*** dan ***multimode***. Jelaskan perbedaan dari *single mode* dan *multimode*.
5. Apakah guna *shield* (pelindung) pada kabel *twisted pair*?
6. Apakah yang dimaksud dengan LAN? Apa perbedaannya dengan WAN?
7. Jelaskan mengenai hub, switch dan router dan perbedaannya masing-masing!
8. Tuliskan cara kerja switch serta tulis dan jelaskan dua jenis switch!
9. Di mana letak layer *Physical* di OSI layer? Tuliskan tujuan utama layer *physical*!
10. Dimanakah letak kabel, repeater, hub, bridge, switch, dan router masing-masing pada lapisan 7 layer OSI?

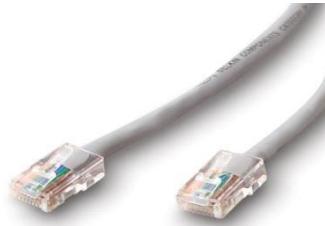
## **Chapter 02**

### **Crimping**



## 2.1 Kabel UTP

Kabel UTP (*Unshielded Twisted Pair*) merupakan kabel yang paling sering digunakan. Di dalamnya terdapat pasangan kabel yang disusun spiral alias saling berlilitan (*twisted pair*) dan tidak memiliki pelindung (*unshielded*) sehingga kurang tahan terhadap interferensi elektromagnetik dan cahaya fluoresensi.



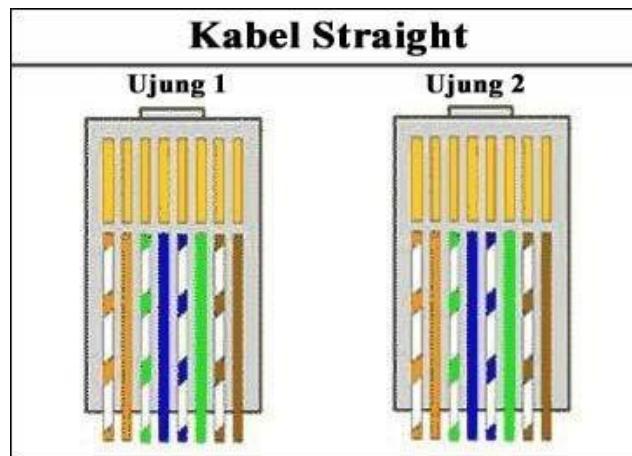
Kabel UTP dispesifikasi menjadi 7 golongan, yaitu kategori 1, hingga kategori 7. Kategori yang paling sering dijumpai adalah:

- CAT2: umumnya digunakan untuk sambungan telepon dalam gedung. Sebuah plug RJ-11 dipakai untuk tiap ujungnya
- CAT3: digunakan pada jaringan Ethernet 10Base-T. Ujung kabelnya dipasangkan dengan plug RJ-45, yang mirip dengan RJ-11, namun memiliki 8 buah kawat (4 pasang) ketimbang hanya 4 buah (2 pasang).
- CAT5: spesifikasi minimum untuk FastEthernet 100Base-T. Digunakan pada banyak jaringan komputer modern. Kabel ini juga menggunakan plug RJ-45.

## 2.2 Jenis-jenis Kabel UTP CAT-5

### ➤ Straight Through Cable (patch cable)

- ✓ Digunakan untuk menghubungkan device yang berbeda jenis. Contoh : komputer dengan switch.

**Ujung 1 Standard (568B)**

Pin 1 Putih-Orange

Pin 2 Orange

Pin 3 Putih-Hijau

Pin 4 Biru

Pin 5 Biru-putih

Pin 6 Hijau

Pin 7 Putih-Cokelat

Pin 8 Cokelat

**Ujung 2 Standard(568B)**

Pin 1 Putih-Orange

Pin 2 Orange

Pin 3 Putih-Hijau

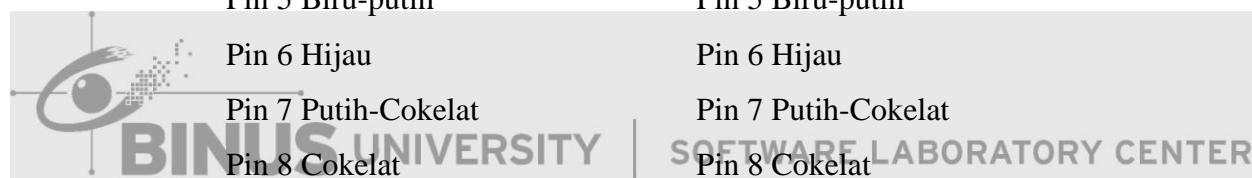
Pin 4 Biru

Pin 5 Biru-putih

Pin 6 Hijau

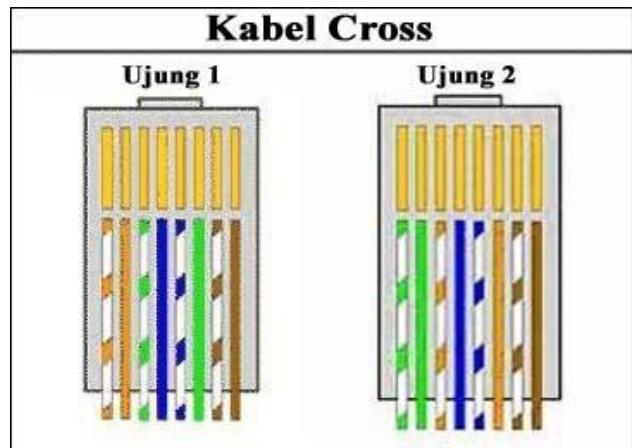
Pin 7 Putih-Cokelat

Pin 8 Cokelat



### ➤ Cross Over Cable

- ✓ Digunakan untuk menghubungkan device yang berjenis sama. Contoh : komputer dengan komputer.

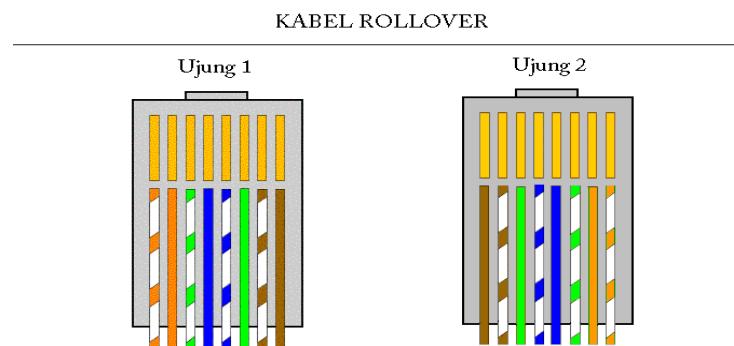


Ujung 1 Standard (568B)	Ujung 2 Cross(568A)
Pin 1 Putih-Orange	Pin 1 Putih – Hijau
Pin 2 Orange	Pin 2 Hijau
Pin 3 Putih-Hijau	Pin 3 Putih – Orange
Pin 4 Biru	Pin 4 Biru
Pin 5 Biru-putih	Pin 5 Biru – Putih
Pin 6 Hijau	Pin 6 Orange
Pin 7 Putih-Cokelat	Pin 7 Putih – Cokelat
Pin 8 Cokelat	Pin 8 Cokelat

### ➤ Rollover Cable

- ✓ Digunakan untuk menghubungkan sebuah terminal komputer ke port *router console*. Port console adalah port yang terdapat pada beberapa perangkat jaringan yang digunakan untuk mengkonfigurasi perangkat tersebut. Port console tidak digunakan untuk komunikasi data pada jaringan.

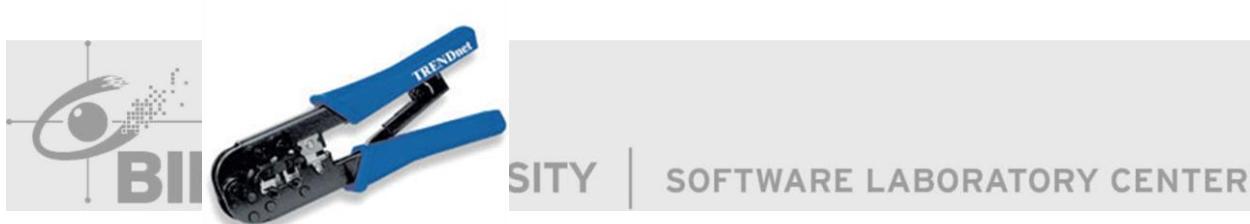
Kabel ini biasanya datar (dan berwarna biru muda) untuk membantu membedakannya dari jenis lain pemasangan kabel jaringan. Diberi nama *rollover* karena *pinouts* pada salah satu ujung dibalikkan dari ujung yang lain, seakan kawat telah di-*rollover* dan kita melihatnya dari sisi lain. Kabel *rollover* ini lebih dikenal sebagai kabel *Yost* atau lebih tepat yang "*YostSerialDevice Wiring Standar*".



<b>Ujung 1 Standard</b>	<b>Ujung 2 Rollover</b>
Pin 1 Putih-Orange	Pin 1 Cokelat
Pin 2 Orange	Pin 2 Putih-Cokelat
Pin 3 Putih-Hijau	Pin 3 Hijau
Pin 4 Biru	Pin 4 Biru-putih
Pin 5 Biru-putih	Pin 5 Biru
Pin 6 Hijau	Pin 6 Putih-Hijau
Pin 7 Putih-Cokelat	Pin 7 Orange
Pin 8 Cokelat	Pin 8 Putih-Orange

### 2.3 Cara Crimping Kabel

1. Persiapkan peralatan yang dibutuhkan, yaitu sebagai berikut :
  - a. Crimping tool



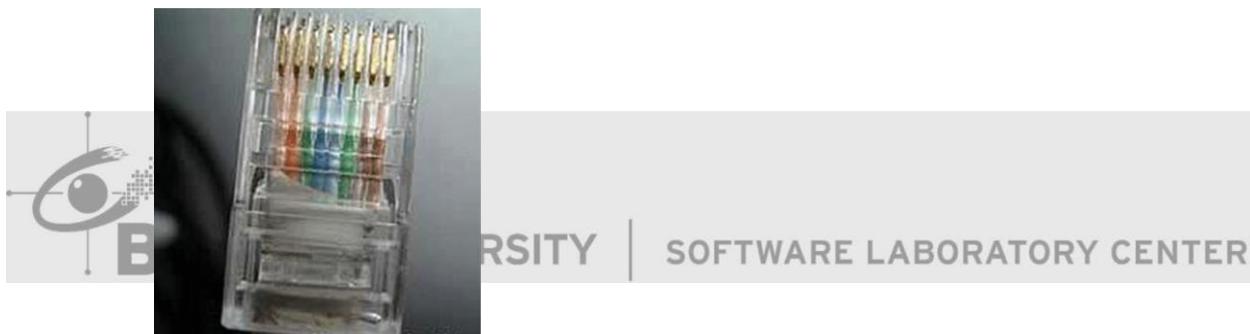
- b. Kabel UTP (Unshielded Twisted Pair)



c. RJ-45



2. Kupas ujung-ujung dari kabel UTP menggunakan *Crimping tool*.
3. Urutkan warna-warnanya sesuai dengan syarat dan ketentuan urutan warna pada masing-masing kabel (telah dijabarkan di subbab di atas).
4. Memotong kabel dengan rapi menggunakan *Crimping tool*.
5. Memasukkan kabel ke konektor RJ-45 hingga ujung kabel terlihat pada bagian depan konektor RJ-45



6. Mengunci kabel RJ-45 dengan cara memasukkannya ke *Crimping tool* untuk mengepress sehingga terpasang sempurna ke konektor RJ-45.
7. Tes kabel dengan mencolokkan kabel langsung ke komputer.



### Testing Kabel

Untuk pengecekan, coba hubungkan 2 buah computer dengan kabel LAN yang telah kita buat, lalu coba gunakan sintaks **ping <ip address computer>**

Contoh :

```

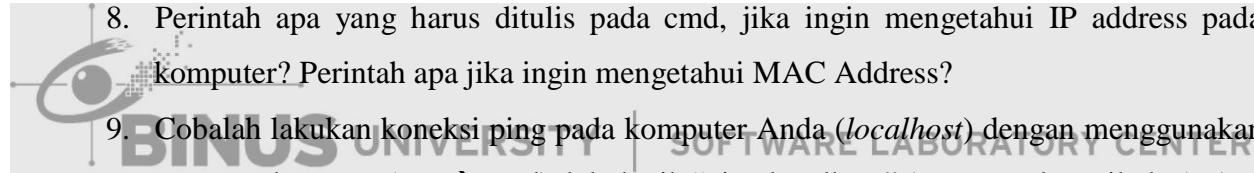
C:\WINDOWS\system32\cmd.exe
D:>ping 10.22.121.113
Pinging 10.22.121.113 with 32 bytes of data:
Reply from 10.22.121.113: bytes=32 time<1ms TTL=128

Ping statistics for 10.22.121.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:>

```

Untuk mengetahui ip address dari suatu komputer, gunakan perintah **IPCONFIG** pada cmd.

## 2.4 Exercise

1. Tuliskan urutan warna standar pada kabel *straight*, *cross*, dan *rollover*!
  2. Kapan kabel *straight* dan kabel *cross* digunakan?
  3. Jelaskan langkah-langkah *crimping* kabel!
  4. Jelaskan maksud dari pewarnaan pada kabel! Ditujukan untuk fungsi apakah warna oranye, hijau, biru, dan coklat?
  5. Jelaskan maksud dari *striped* (kabel belang) dengan kabel yang *solid* (tidak belang)! Mengapa masing-masing dari pasang kabel harus dipilin (*twisted*)?
  6. Jenis kabel apakah (*straight/cross*) yang harus digunakan untuk menghubungkan perangkat-perangkat di bawah.
    - PC dengan laptop
    - PC dengan switch
    - Switch dengan router
  7. Jelaskan fungsi dari NIC!
- 
8. Perintah apa yang harus ditulis pada cmd, jika ingin mengetahui IP address pada komputer? Perintah apa jika ingin mengetahui MAC Address?
  9. Cobalah lakukan koneksi ping pada komputer Anda (*localhost*) dengan menggunakan command prompt (run → cmd), lalu ketik “ping localhost” (tanpa tanda petik dua). Apa yang dimaksud dengan ping berdasarkan percobaan yang baru saja Anda lakukan, serta berikan pula penjelasan apa yang dimaksud dengan IP 127.0.0.1!
  10. Cobalah melakukan ping ke 10.22.64.15. Tuliskan apa yang Anda lihat! Apa syarat suatu koneksi dikatakan bagus dan jelaskan hasil statistik ping tersebut!

## **Chapter 03**

### **Introduction to TCP/IP and Subnetting**



### 3.1. TCP/IP

*Transmission Control Protocol/Internet Protocol* (TCP/IP) adalah suatu protokol (aturan) yang memungkinkan kumpulan komputer dapat berkomunikasi dan bertukar data di dalam suatu jaringan.

Fungsi umum TCP adalah memecah pesan-pesan menjadi beberapa paket sehingga bisa dikirimkan dan juga menyatukan kembali (*reassemble*) paket-paket itu kembali pada stasiun tujuan. Fungsi umum IP adalah menangani alamat-alamat yang ada pada paket yang dikirimkan sehingga dapat paket dapat menuju tujuan yang benar.

### 3.2. IP Addressing

IP address (Alamat IP) adalah suatu bilangan yang secara unik mendefinisikan setiap host yang ada pada jaringan IP.

IP address terdiri dari 32-bit bilangan biner. Sebagai contoh, IP address dapat ditulis sebagai berikut: 11000000101010001000100000011100. Untuk mempermudah penulisan, digunakan format notasi desimal bertitik (*dotted-decimal notation*) yang mengelompokkan 32-bit menjadi 4 kelompok yang masing-masing 8-bit (oktet atau byte) dan ditulis dalam bilangan desimal. Dengan demikian, contoh di atas dapat ditulis menjadi 192.168.136.28.

Tujuan penggunaan ip address adalah memungkinkan komunikasi antar jaringan. Setiap ip address terbagi menjadi dua bagian:

- **Network ID (netid):** mengidentifikasi di jaringan mana host komputer itu berada.
- **Host ID (hostid):** mengidentifikasi device spesifik pada jaringan yang berada pada jaringan yang ditunjukkan oleh Network ID.

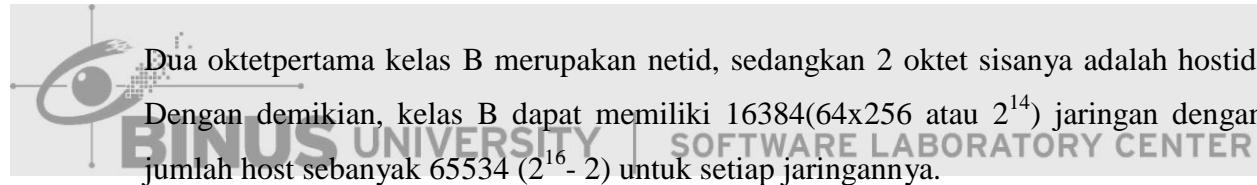
Protokol IP menggolongkan IP address menjadi 5 kelas: A, B, C, D, dan E. Kelas A hingga C berbeda dalam hal porsi netid dan hostid. Kelas D digunakan untuk keperluan multicast, sedangkan kelas E digunakan untuk kepentingan eksperimen.

Kelas	Mulai	Hingga	Bit pertama	Jumlah bit untuk netid	Jumlah jaringan	Jumlah Host per jaringan	Default Subnet Mask
A	1. 0. 0. 0 netid hostid	126. 255. 255. 255. netid hostid	0	8	126	16777214	255.0.0.0
B	128. 0. 0. 0 netid hostid	191. 255. 255. 255. netid hostid	10	16	16384	65534	255.255.0.0
C	192. 0. 0. 0 netid hostid	223. 255. 255. 255. netid hostid	110	24	2097152	254	255.255.255.0
D	224. 0. 0. 0	239. 255. 255. 255.	1110	-	-	-	-
E	240. 0. 0. 0	255. 255. 255. 255.	1111	-	-	-	-

- Kelas A

IP address kelas A didesain untuk jaringan-jaringan besar. Oktet (8-bit) pertama kelas A merupakan netid, sedangkan 3 oktet sisanya adalah hostid. Dengan demikian, kelas A dapat memiliki 126 jaringan dengan jumlah host  $16777214$  ( $2^{24} - 2$ ) untuk setiap jaringannya.

- Kelas B

Dua oktet pertama kelas B merupakan netid, sedangkan 2 oktet sisanya adalah hostid. Dengan demikian, kelas B dapat memiliki  $16384$  ( $64 \times 256$  atau  $2^{14}$ ) jaringan dengan jumlah host sebanyak  $65534$  ( $2^{16} - 2$ ) untuk setiap jaringannya.

- Kelas C

Tiga oktet pertama kelas C merupakan netid, sedangkan oktet terakhir adalah hostid. Dengan demikian, kelas C dapat memiliki  $2097152$  ( $32 \times 256 \times 256$  atau  $2^{21}$ ) jaringan dengan jumlah host sebanyak  $254$  ( $2^8 - 2$ ) untuk setiap jaringannya.

- Kelas D

Alamat IP kelas D dicadangkan untuk skema **multicast**, yaitu kemampuan untuk mengirimkan sebuah paket ke sekelompok perangkat yang tergabung ke dalam sebuah grup **multicast** yang sama.

- Kelas E

Alamat IP kelas E dicadangkan untuk keperluan eksperimen dan tidak digunakan.

Komponen penting dari IP addressing adalah subnet mask. Subnet mask adalah bilangan 32-bit (sama seperti ip address) yang berperan untuk membantu router dalam membedakan antara bagian jaringan dan bagian host dari suatu ip. Secara lebih spesifik, router melaksanakan operasi AND antara ip address yang bersangkutan dengan subnet mask.

Suatu *subnet mask* dapat dituliskan di posisi akhir setelah alamat ip. Sebagai contoh, suatu alamat 192.168.2.0 dengan *subnet mask* 255.255.255.0 dapat dituliskan menjadi 192.168.2.0/24 dimana 24 adalah jumlah bit 1 yang ada pada *subnet mask*.

Suatu host tidak boleh memiliki ip address di mana semua bit dari hostid adalah 0. Sebagai contoh: 192.168.20.0 (kelas C) atau 10.14.0.0 (kelas B). IP address di mana semua bit hostnya 0 digunakan sebagai ***network address*** (alamat jaringan). IP address 192.168.20.0 merujuk ke jaringan 192.168.20.

Suatu host juga tidak boleh memiliki ip address di mana semua bit hostid adalah 1. Sebagai contoh: 10.255.255.255 (kelas A), atau 10.14.255.255 (kelas B) atau 192.168.20.255 (kelas C). IP address di mana semua bit hostid-nya adalah 1 digunakan sebagai ***broadcast address***(alamat broadcast). Broadcast address merujuk ke semua host yang ada pada jaringan yang bersangkutan. Misalnya, ip address 192.168.20.255 merujuk ke semua host yang ada pada jaringan 192.168.20.

Contoh Soal:

Diberikan suatu ip address 137.21.15.70. Tentukan:

- a. kelas ip address tersebut,
- b. subnetmask defaultnya,
- c. network address dan broadcast addressnya.
- d. Apakah 137.21.15.80 berada pada jaringan yang sama?
- e. 137.22.10.1 berada pada jaringan yang sama?

Jawab:

Kelas ip address dari 137.21.15.70 adalah kelas B, karena berada dalam range 128-191.x.y.z. Subnet mask defaultnya adalah 255.255.0.0 (subnet mask default untuk kelas B). Network addressnya 137.21.0.0 dan broadcast addressnya 137.21.255.255. Ip address 137.21.15.80 juga memiliki alamat jaringan 137.21.0.0, oleh karenanya berada pada jaringan yang sama, sedangkan 137.22.10.1 memiliki alamat jaringan 137.22.0.0 sehingga berada pada jaringan yang berbeda.

Perlu diketahui bahwa ada beberapa ip address yang tidak dapat digunakan untuk pengalamanan:

- IP 127.0.0.0 tidak dapat digunakan untuk pengalamanan jaringan. 127.0.0.1 dipakai untuk merujuk ke perangkat itu sendiri, sehingga dikenal dengan *localhost* atau alamat *loopback*.
- Oktet pertama pada suatu ip address tidak dapat seluruhnya terdiri atas bit-bit 0. Misalnya 0.0.0.68 atau 0.0.1.1. Ip dari 0.0.0.68 merujuk ke terminal host nomor 68 pada jaringan lokal.
- IP 0.0.0.0 merujuk ke host yang sedang digunakan.
- IP 255.255.255.255 adalah sebuah alamat broadcast, dan merujuk ke semua host yang ada pada jaringan lokal.

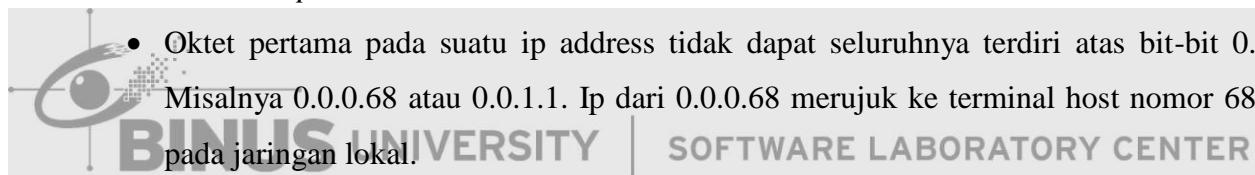
### 3.3. Subnetting

Subnetting adalah pembagian suatu kelompok alamat IP menjadi beberapa network ID lain dengan jumlah host yang lebih kecil, yang disebut subnet (subnetwork).

#### a. FLSM Subnetting (Fixed Length Subnet Mask)

Langkah-langkah untuk melakukan subnetting suatu jaringan:

1. Menentukan Subnet Mask Baru
2. Menentukan IP Host tiap Jaringan



Contoh :

➤ **Contoh dengan cara 1:**

Soal:

Suatu perusahaan memiliki alamat ip **192.168.1.0** ingin membuat jaringan. Jaringan pertama digunakan untuk bagian **Admin** membutuhkan jaringan yang dapat menampung **15 komputer** sedangkan jaringan kedua untuk bagian **Operational** membutuhkan jaringan yang dapat menampung **33 komputer**. Masing-masing divisi membutuhkan sekitar 40 komputer. Tentukan subnet mask yang baru yang dapat digunakan untuk mengakomodasi kebutuhan perusahaan tersebut! Tentukan alokasi IP address untuk masing-masing divisi!

NA (Network Address) = 192.168.1.0

SM (Subnet Mask) = 24 = 11111111.11111111.11111111.00000000

= 255.255.255.0 -> class C

Requirements:

- Admin section membutuhkan **15 hosts**
- Operational section membutuhkan **33 hosts**

**1. Cari jaringan dengan jumlah komputer/host terbesar**

Jumlah komputer terbesar yang dibutuhkan ada pada jaringan bagian Operasional **33 hosts**

**2. Tentukan Subnet mask yang baru**

Rumus:  $2^h - 2 \geq$  jumlah host pada jaringan

Example:

$$2^h - 2 \geq 33$$

$$2^6 - 2 \geq 33$$

$$64 - 2 \geq 33$$

$$62 \geq 33$$

$$h = 6$$

Rumus untuk mencari subnet mask yang baru:

$$\mathbf{n = 32 - b - h}$$

b = total bit **1** dari subnet mask lama

$$n = 32 - 24 - 6$$

= 2 (tambahkan bit 1 sebanyak 2 kepada subnet mask yang lama)

new Subnet Mask = 11111111.11111111.11111111.**11**000000

$$= 255.255.255.192$$

## 2. Determine each network IP Host

Gunakan rumus ini:  $2^{\text{total zero bit that remaining in new Subnet Mask}}$

$$2^6 = 64$$

Result for IP Host partition in each network as follows:

No.	IP Host	Network Address	Broadcast Address
1	192.168.1.0 – 192.168.1.63	192.168.1.0	192.168.1.63
2	192.168.1.64 – 192.168.1.127	192.168.1.64	192.168.1.127
3	192.168.1.128 – 192.168.1.191	192.168.1.128	192.168.1.191
4	192.168.1.192 – 192.168.1.255	192.168.1.192	192.168.1.255

- IP address pertama dalam setiap jaringan digunakan untuk **Network Address**
- IP address terakhir dalam setiap jaringan digunakan untuk **Broadcast Address**
- Jaringan No. 1 diberikan untuk bagian **Admin** yang memiliki range alamat IP yang dapat digunakan 192.168.1.1 – 192.168.1.62 dengan **Network Address** 192.168.1.0 and **Broadcast Address** 192.168.1.63
- Jaringan No. 2 diberikan untuk bagian **Operational** yang memiliki range alamat IP yang dapat digunakan 192.168.1.65 – 192.168.1.126 dengan **Network Address** 192.168.1.64 dan **Broadcast Address** 192.168.1.127
- Jaringan No. 3 and 4 tidak terpakai karena jaringan yang dibutuhkan hanya 2 jaringan.

➤ **Contoh dengan cara 2 (Jika ingin dibagi menjadi sejumlah  $n$  jaringan):**

Suatu perusahaan memiliki alamat ip 192.168.1.0 **ingin membuat 2 buah jaringan**. Jaringan pertama digunakan untuk divisi Finance sedangkan jaringan kedua untuk Divisi Operasional. Masing-masing divisi membutuhkan sekitar 40 komputer. Tentukan subnet mask yang baru yang dapat digunakan untuk mengakomodasi kebutuhan perusahaan tersebut! Tentukan alokasi IP address untuk masing-masing divisi!

Jawab:

192.168.1.0 merupakan ip address kelas C dengan default subnet mask 255.255.255.0.

1. Menentukan Subnet Mask Baru

Gunakan Rumus :  $2^n \geq$  jumlah jaringan

Dimana n adalah jumlah bit 1 yang ditambahkan pada subnet mask yang lama.

$$2^n \geq 2$$

$$n = 1$$

Subnet Mask yang lama = 11111111.11111111.11111111.00000000  
 $= 255.255.255.0.$

Tambahkan sebanyak n bit 1 pada subnet mask yang lama. Maka, tambahkan sebanyak 1

$$\text{Subnet Mask yang baru} = 11111111.11111111.11111111.\mathbf{1}0000000  
= 255.255.255.128$$

2. Menentukan IP Host tiap Jaringan

Gunakan Rumus : jumlah host tiap jaringan =  $2^m$

Dimana **m** adalah banyaknya bit 0 pada subnet mask yang baru

$$\text{Subnet Mask yang baru} = 11111111.11111111.11111111.\mathbf{10000000}$$

Jumlah nol yang tersisa pada Subnet Mask yang baru adalah 7.

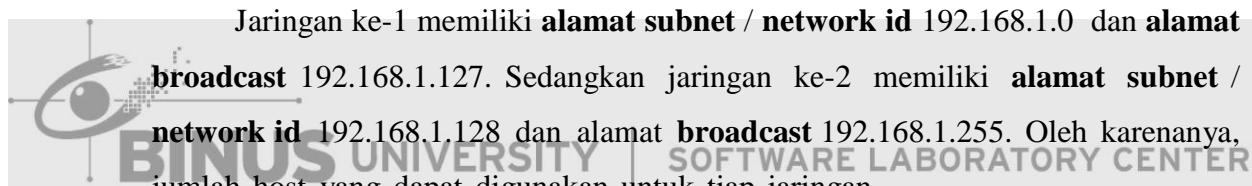
Jadi, jumlah host tiap jaringan =  $2^7 = 128$

Jadi pembagian IP Host tiap jaringannya adalah sebagai berikut.

Jaringan ke	IP Host	Penggunaan
1	192.168.1.0 – 192.168.1.127	Divisi Finance
2	192.168.1.128 – 192.168.1.255	Divisi Operasional

Penjelasan:

Divisi Finance dan Operasional dapat saling dipertukarkan antara jaringan ke-1 dan ke-2. Dalam jawaban di atas, divisi Finance berada pada jaringan ke-1 yang memiliki kisaran ip dari 192.168.1.0 hingga 192.168.1.127 sedangkan divisi Operasional berada pada jaringan ke-2 yang memiliki kisaran IP dari 192.168.1.128 hingga 192.168.1.255.

 Jaringan ke-1 memiliki **alamat subnet / network id** 192.168.1.0 dan **alamat broadcast** 192.168.1.127. Sedangkan jaringan ke-2 memiliki **alamat subnet / network id** 192.168.1.128 dan alamat **broadcast** 192.168.1.255. Oleh karenanya, jumlah host yang dapat digunakan untuk tiap jaringan adalah **128 – 2 = 126** host.

Jaringan	Network Address	Broadcast Address	Range host yang dapat digunakan
1	192.168.1.0	192.168.1.127	192.168.1.1 – 192.168.1.126
2	192.168.1.128	192.168.1.255	192.168.1.129 – 192.168.1.254

IP address 192.168.1.0 dapat bermakna ganda, yaitu sebagai alamat jaringan 192.168.1.0/24 dan sebagai alamat jaringan 192.168.1.0/25. IP address 192.168.1.255 juga bermakna ganda, yaitu sebagai broadcast address jaringan 192.168.1.255/24 dan sebagai broadcast address untuk subnet 192.168.1.255/25. Disinilah terlihat peran dari subnet mask / prefix yaitu mendefinisikan range address dari suatu jaringan.

Protokol routing *classfull* (berklasifikasi) tidak menyertakan informasi subnet mask di dalam updating routinya sehingga tidak mengerti perbedaan /24 dengan /26. Oleh

karenanya, di dalam RFC 950, dokumen asli yang pertama kali mendefinisikan subnet- subnet ini, penggunaan alamat subnet “*all zeros*” (seluruhnya terdiri dari bit 0) dan “*all ones*” (seluruhnya terdiri dari bit 1) tidak diizinkan.

Dewasa ini, telah digunakan protokol *classless* (tanpa klasifikasi) sehingga dapat dengan mudah membedakan antara 192.168.1.0/24 ataupun 192.168.1.0/26. Dengan demikian, tidak ada lagi batasan teknis untuk menggunakan subnet “*all-zeros*” atau “*allones*”.

### b. VLSM (Variable Length Subnet Mask)

VLSM adalah teknik subnetting dimana tiap subnet bisa memiliki ukuran subnet yang berbeda-beda dan memungkinkan untuk membuat subnet sesuai jumlah host yang diperlukan saja sehingga tidak membuang resource secara percuma.

Contoh soal:

Suatu perusahaan memiliki alamat ip 172.16.0.0/16 ingin membuat 3 buah jaringan. Jaringan pertama yang digunakan divisi Finance membutuhkan 2000 komputer, jaringan kedua yang digunakan Divisi Operasional membutuhkan 500 komputer sedangkan jaringan ketiga yang digunakan oleh Divisi Penelitian membutuhkan 3000 komputer. Tentukan subnet mask yang baru yang dapat digunakan untuk mengakomodasi kebutuhan perusahaan tersebut! Tentukan alokasi IP address untuk masing-masing divisi!

Jawab:

IP = 172.16.0.0/16 (class B)

Subnet Mask = 11111111.11111111.00000000.00000000



1. Urutkan berdasarkan jumlah host (dari yang terbesar ke yang terkecil)

Divisi Penelitian: 3000 komputer

Divisi Finance: 2000 komputer

Divisi Operasional: 500 komputer

Urutan ini juga akan sama dengan urutan pengerjaan pada langkah-langkah berikutnya

2. Mencari subnet baru pada tiap jaringan

Gunakan rumus:  $2^h - 2 \geq \text{jumlah komputer atau host}$

Untuk mendapatkan jumlah subnet mask yang baru gunakan rumus

$$n = 32 - b - h$$

**b** = total bit **1** dari subnet mask lama

Lalu dilanjutkan dengan rumus: **s + n**

Dimana s adalah subnet mask yang lama

- a. Divisi Penelitian

$$2^h - 2 \geq 3000$$

$$h \geq 3002$$

$$2^{12} \geq 3002$$

$$h = 12$$

Mencari subnet mask baru:

**b** = 16 (IP class B)

$$n = 32 - 16 - 12$$

= 4 (tambahkan bit 1 kepada subnet mask lama sebanyak n)

Subnet mask baru adalah /20 atau 11111111.11111111.**11110000.00000000**

- b. Divisi Finance

$$2^h - 2 \geq 2000$$

$$2^h \geq 2002$$

$$2^{11} \geq 2002$$

$$h = 11$$



Mencari subnet mask baru:

$$b = 16 \text{ (IP class B)}$$

$$n = 32 - 16 - 11$$

= 5 (tambahkan bit 1 kepada subnet mask lama sebanyak n)

Subnet mask baru adalah /21 atau 11111111.11111111.**11111000.00000000**

- c. Divisi Operasional

$$2^h - 2 \geq 500$$

$$2^h \geq 502$$

$$2^9 \geq 502$$

$$h = 9$$

Mencari subnet mask baru:

$$b = 16 \text{ (IP class B)}$$

$$n = 32 - 16 - 9$$

= 7 (tambahkan bit 1 kepada subnet mask lama sebanyak n)

Subnet mask baru adalah /23 atau 11111111.11111111.**11111110.00000000**

3. Mencari IP Address yang bisa digunakan pada tiap jaringan

Untuk menentukan jumlah host tiap jaringan gunakan rumus:  $2^m$

Dimana m adalah banyaknya bit 0 pada subnet mask yang baru

Subnet mask divisi **Penelitian** yang baru adalah

11111111.11111111.11110000.00000000

Jumlah nol pada subnet mask yang baru adalah 12. Jadi jumlah host pada divisi penelitian adalah  $2^{12} = 4096$



Subnet mask divisi **Finance** yang baru adalah

11111111.11111111.11110000.00000000

Jumlah nol pada subnet mask yang baru adalah 11. Jadi jumlah host pada divisi penelitian adalah  $2^{11} = 2048$

Subnet mask divisi **Operasional** yang baru adalah

11111111.11111111.11111110.00000000

Jumlah nol pada subnet mask yang baru adalah 9. Jadi jumlah host pada divisi penelitian adalah  $2^9 = 512$

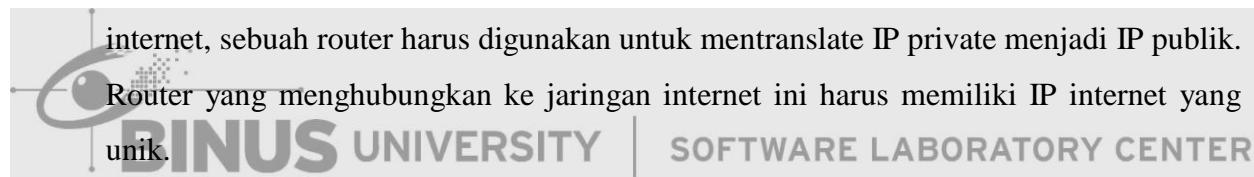
**Jaringan pertama selalu dimulai dari IP yang diberikan sedangkan jaringan lainnya dimulai setelah broadcast address jaringan sebelumnya**

Jaringan	Network Address	Broadcast Address	Range host yang dapat digunakan
Penelitian	172.16.0.0/20	172.16.15.255/20	172.16.0.1/20 – 172.16.15.254/20
Finance	172.16.16.0/21	172.16.23.255/21	172.16.16.1/21 – 172.16.23.254/21

Operasional	172.16.24.0/23	172.16.25.255/23	172.16.24.1/23 – 172.16.25.254/23
-------------	----------------	------------------	--------------------------------------

### 3.4. Private IP Address

Private IP address adalah IP address yang tidak tersambung (atau tidak memiliki *presence* di internet). Jaringan yang menggunakan Private IP address disebut sebagai jaringan private / Private Network. IP Private ini tidak akan dirouting di internet. IP private dapat digunakan secara bebas untuk jaringan lokal, berbeda dengan IP public yang secara penggunaan harus teregister ke IP registrar. Agar jaringan ini dapat terhubung ke internet, sebuah router harus digunakan untuk mentranslate IP private menjadi IP publik.



Berikut adalah range IP address private untuk masing-masing kelas:

- Kelas A: 10.0.0.0 – 10.255.255.255
- Kelas B: 172.16.0.0 – 172.31.255.255
- Kelas C: 192.168.0.0 – 192.168.255.255

Penggunaan IP privat memiliki keuntungan dalam penghematan IP yang digunakan untuk internet. Selain itu, penggunaan IP privat juga bertujuan untuk keamanan jaringan dan data. Secara default, router tidak mengizinkan traffic dari luar untuk memasuki jaringan privat, kecuali jika terminal dalam jaringan privat meminta data tersebut.

### 3.5. Mac Address

Media Access Control (MAC) Address adalah alamat 6 byte yang digunakan untuk secara unik mengidentifikasi perangkat-perangkat pada jaringan Ethernet. MAC address seringkali disebut juga sebagai *physical address* (alamat fisik) karena alamat MAC bergantung pada *Network Interface Card* (NIC).

Sebagai contoh alamat MAC yaitu 00:A3:03:51:0E:AC. Tiga byte pertama, 00:A3:03, merupakan kode vendor yang ditetapkan oleh IEEE. Jadi, setiap vendor pabrikan memiliki kode yang unik. Tiga byte terakhir, 51:0E:AC, merupakan kode yang ditetapkan oleh vendor. Oleh karenanya setiap alamat MAC pasti unik.

Alamat MAC tidak digunakan sebagai pengalaman jaringan karena alasan skalabilitas. Pada MAC Address, perangkat-perangkat jaringan tidak dapat dikelompokkan ke dalam segmen jaringan. Sebagai akibatnya, tabel-tabel rute harus memuat semua alamat MAC dari semua perangkat yang ada, yang membuatnya tidak praktis.

MAC Address digunakan untuk pengiriman dari node ke node (perangkat ke perangkat), seperti komputer ke router atau komputer ke komputer. IP address tujuan ditranslate terlebih dahulu menjadi MAC Address tujuan. Protokol yang digunakan untuk translasi dari IP Address ke MAC Address adalah ARP (*Address Resolution Protocol*).

### 3.6. Frame dan Paket

Suatu data yang akan dikirimkan dalam suatu jaringan akan dipecah-pecah menjadi suatu unit data berupa bit-bit agar dapat ditransmisikan melalui medium transmisi (misalnya kabel). **Frame** adalah suatu unit trasmisi data yang berada pada lapisan data-link (lapisan 2). Frame memiliki struktur logikal terhadap bit-bit sehingga setiap perangkat dapat membaca informasi yang ada di dalamnya. Di dalam frame terhadap informasi **paket** (informasi yang ada pada lapisan 3 OSI).

Misalnya, format dari frame Ethernet adalah sebagai berikut.

Preamble	Start of Frame	Destination MAC Address	Source MAC Address	Ether Type	Payload	CRC Checksum
----------	----------------	-------------------------	--------------------	------------	---------	--------------

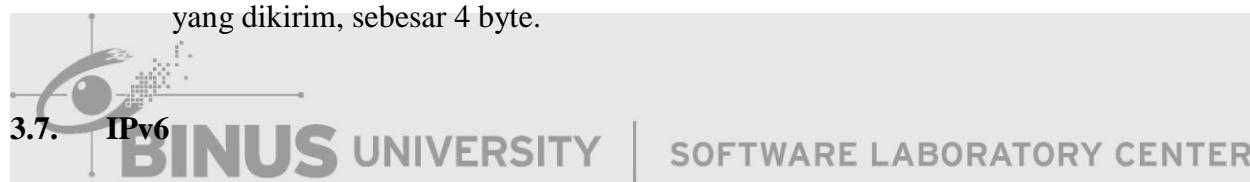
- **Preamble** adalah pola bit yang berfungsi untuk mengsinkronisasikan perangkat jaringan dalam berkomunikasi. Panjang preamble adalah 7 byte, dengan pola 10101010....
- **Start of Frame (SOF)** adalah bit-bit yang berfungsi untuk memberitahukan device bahwa isi frame berada pada bit yang berikutnya. SOF terdiri dari 1 byte dan berakhir dengan bit 11, misalnya 10101011.

- **Destination Mac Address** adalah informasi tentang MAC Address tujuan sebesar 6 byte.
- **Source MAC Address** adalah informasi tentang MAC Address pengirim sebesar 6 byte.
- **Ether Type** adalah tipe dari frame Ethernet yang dikirim, sebesar 2 byte.
- **Payload** adalah isi data dari frame. Payload disebut juga sebagai **paket** atau **datagram** (jika menggunakan unreliable protocol seperti UDP). Payload inilah yang disebut sebagai informasi pada layer 3 OSI. Ukuran payload ini beragam, antara 46 hingga 1500 byte.

Contoh format paket yang ada pada protokol TCP:

IP Header	IP Destination Address	IP Source Address	TCP Destination Port	TCP Source Port	TCP Header and data	TCP CRC	IP CRC
-----------	------------------------	-------------------	----------------------	-----------------	---------------------	---------	--------

- **CRC (Cyclic Redundancy Check)** bit yang menandakan validitas dari suatu frame yang dikirim, sebesar 4 byte.



Meningkatnya kebutuhan internet membuat jumlah alamat yang tersisa pada sistem IP sebelumnya, yaitu IPv4, menjadi semakin menipis. Oleh karenanya, dikembangkan IPv6 atau IPng (*IP next generation*) yang terdiri atas format 128-bit (16 oktet) ketimbang IPv4 yang hanya 4 oktet.

Contoh IPv6 adalah sebagai berikut.

105.100.215.50.255.255.255.0.0.32.136.150.5.255.255

IPv6 di atas dapat ditulis dalam bentuk notasi hexadesimal dengan titik dua di mana tiap-tiap kelompok 1-bit dituliskan dalam nilai hexadesimal dan dipisahkan oleh sebuah tanda titik-dua. Dengan demikian, alamat di atas dapat ditulis menjadi:

6964 : D732 : FFFF : FFFF : 0 : 2088 : 9605 : FFFF

Lebih jauh lagi, jika terdapat dua buah nilai 0 yang muncul berturut-turut dalam alamat, maka dua buah tanda titik-dua digunakan untuk merepresentasikan bilangan nol tersebut. Contoh:

6964 : 0 : 0 : 0 : 0 : 0 : 0 : FFFF

dapat direpresentasikan sebagai:

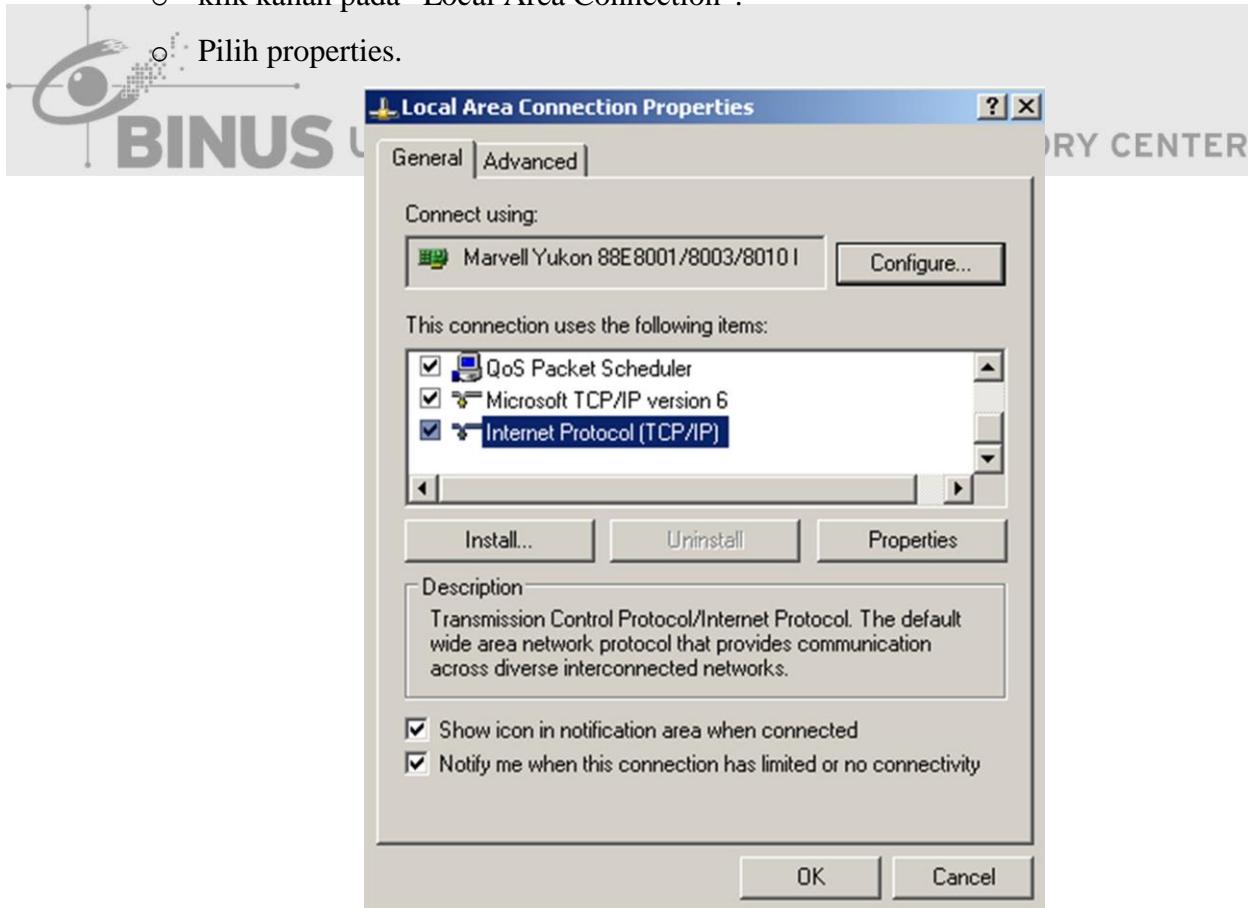
6964 : : FFFF

### 3.8. Aktivitas Percobaan

Untuk aktivitas percobaan ini, hanya menggunakan 1 jaringan. Misalnya menggunakan IP dari **jaringan 2 (192.168.1.64 – 192.168.1.127)**.

Berikut ini langkah-langkah dalam melakukan percobaan :

1. Hubungkan setiap komputer dengan switch dengan menggunakan kabel LAN.
2. Kemudian setting IP untuk setiap komputer, dengan langkah-langkah sebagai berikut:
  - o Untuk men-setting IP, kita dapat melakukannya melalui menu “Network Connections”.
  - o klik kanan pada “Local Area Connection”.

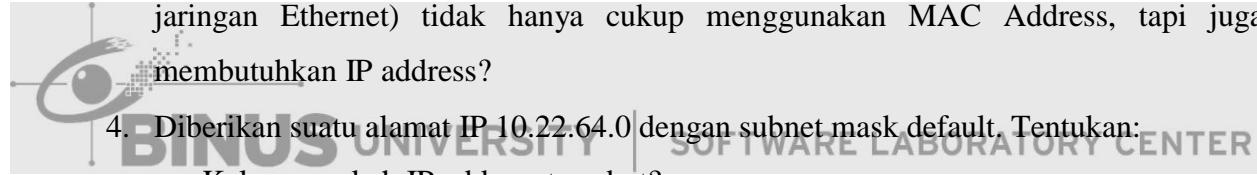


- Pilih Internet Protocol (TCP/IP) seperti yang terlihat pada gambar di atas
  - Lalu klik Properties
  - Kemudian masukkan IP dan Subnet Masknya
3. Kemudian lakukan pengecekan terhadap jaringan yang telah kita buat dengan menggunakan “ping”.

### 3.9. Exercise

1. Jelaskan fungsi dari TCP/IP!

Berdasarkan lapisan 7 OSI later, di lapisan manakah TCP/IP berada?

2. Jelaskan kegunaan dari subnet mask!
3. Apa kegunaan dari IP address? Apa kegunaan dari MAC address? Suatu komputer memiliki alamat IP, namun mengapa komputer itu tetap membutuhkan MAC address? Mengapa komputer yang ingin mengirimkan paket antar komputer (pada jaringan Ethernet) tidak hanya cukup menggunakan MAC Address, tapi juga membutuhkan IP address?
4. Diberikan suatu alamat IP 10.22.64.0 dengan subnet mask default. Tentukan:
  - a. Kelas manakah IP address tersebut?
  - b. Termasuk IP publik atau IP privat?
  - c. Subnet mask,
  - d. Network address dan broadcast address,
  - e. Berapa jumlah host yang dapat digunakan pada jaringan tersebut?
  - f. Apakah host dengan IP address 10.22.255.255 dapat berada pada jaringan yang sama dengan IP tersebut.
5. Subnetting memiliki 2 tujuan utama, yaitu dilihat dari segi *space* dan segi *performance*. Jelaskan maksud dari kedua tujuan tersebut!
6. Suatu perusahaan memiliki *network address* 154.20.0.0/16 dan ingin membagi IP address tersebut agar dapat mengakomodasi minimal 20 jaringan (subnet). Tentukan banyak jaringan yang terbentuk dari hasil subnetting! Tentukan subnet mask yang baru! Berapa banyak host yang dapat digunakan untuk tiap subnet?

7. Untuk menyediakan lebih banyak subnet, suatu alamat kelas C diberi subnet mask 255.255.255.128.
  - a. Berapa banyak subnet yang tersedia?
  - b. Berapa banyak host dalam tiap subnet?
  - c. Tuliskan apa saja subnetnya!
8. Suatu jaringan IP dengan alamat jaringan 192.168.130.0 menggunakan subnet mask 255.255.255.224. Di subnet manakah tiap-tiap perangkat di bawah ini berada?
  - a. 192.168.130.10
  - b. 192.168.130.65
  - c. 192.168.130.100
  - d. 192.168.130.179
  - e. 192.168.130.222
  - f. 192.168.130.225
9. Jika suatu jaringan dilakukan subnetting menghasilkan beberapa subnet, atas dasar pertimbangan apakah subnet pertama dan subnet terakhir tidak digunakan?
10. Apa perbedaan IP publik dan IP privat? Bagaimanakah cara mendapatkan IP publik? Siapa pihak yang bertanggung jawab dalam menyediakan IP publik tersebut?
11. ARP adalah protokol yang digunakan untuk melaksanakan resolusi alamat IP menjadi alamat fisik. Terdapat 2 tipe ARP, yaitu *ARP request* dan *ARP response*. Jelaskan cara kerja kedua tipe ARP tersebut!
12. Apa perbedaan frame dan paket?

## **Chapter 04**

### **Router Configuration**

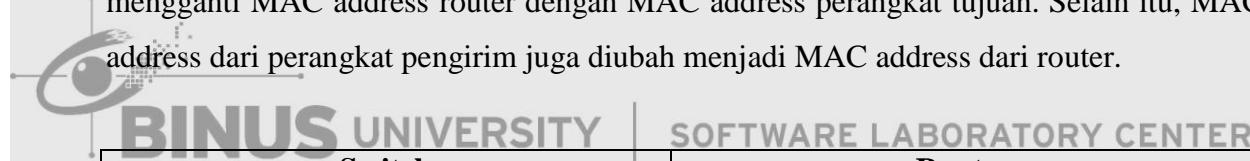


#### 4.1. Router

**Router** adalah suatu perangkat jaringan yang bekerja pada lapisan ke 3 (*network layer*) layer OSI, yaitu mengirimkan paket data dari jaringan yang satu ke jaringan yang lain yang berbeda. Dengan kata lain, router adalah penghubung antar 2 jaringan yang berbeda. Berbeda dengan switch yang bekerja pada lapisan ke-2 (*data link layer*) OSI. Switch tidak dapat meneruskan paket menuju jaringan yang berbeda dengan jaringan pengirimnya.

Cara kerja router yaitu membaca informasi ip address dari paket yang diterimanya dan meneruskan ke jaringan yang dituju. Router berbeda dengan switch. Switch tidak dapat membaca ip address, melainkan MAC address. Switch hanya meneruskan frame ke alamat MAC address yang dituju.

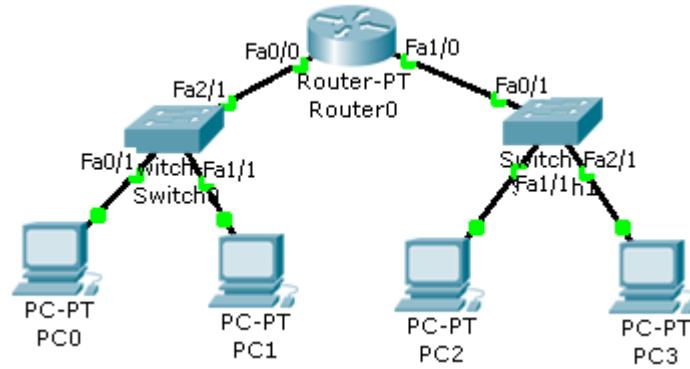
Perlu diketahui juga bahwa router melakukan modifikasi terhadap MAC address pada frame. Ketika suatu frame ditujukan ke router, maka MAC address tersebut ditujukan ke MAC address router, kemudian router meneruskan frame tersebut dengan mengganti MAC address router dengan MAC address perangkat tujuan. Selain itu, MAC address dari perangkat pengirim juga diubah menjadi MAC address dari router.



Switch	Router
Berfungsi untuk menghubungkan perangkat-perangkat jaringan	Berfungsi untuk menghubungkan antar jaringan yang berbeda agar dapat saling berkomunikasi.
Bekerja dengan MAC address (lapisan 2 OSI)	Bekerja dengan IP address (lapisan 3 OSI)
Tidak memiliki IP address	Memiliki IP address
Hanya meneruskan frame dari perangkat yang satu ke perangkat yang lain	Melakukan modifikasi frame agar dapat meneruskan paket ke jaringan berbeda.

#### 4.2. Konfigurasi Router dengan Packet Tracer (Contoh Kasus)

Buatlah 2 buah jaringan seperti gambar di bawah ini (dapat melalui simulasi di Packet Tracer)



#### Informasi Jaringan :

##### PC:

- IP PC0 : 192.168.1.2/24
- IP PC1 : 192.168.1.3/24
- IP PC2 : 192.168.2.2/24
- IP PC3 : 192.168.2.3/24

 **Router0**

SOFTWARE LABORATORY CENTER

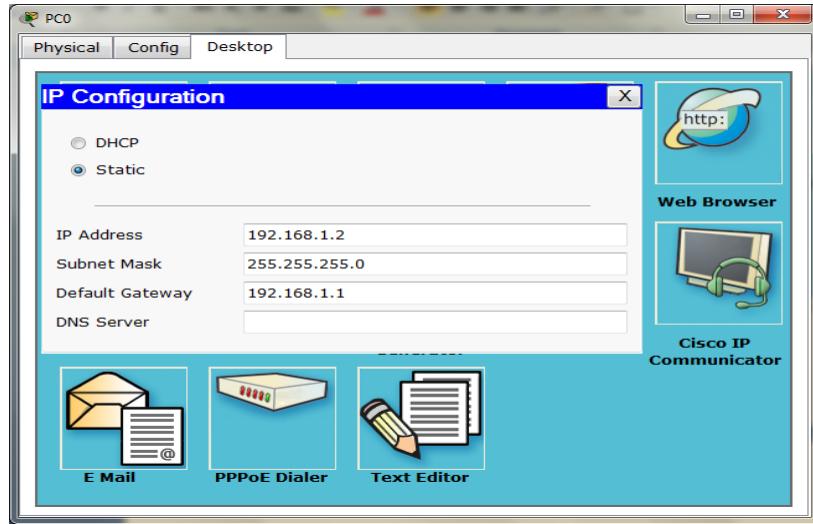
- IP FastEthernet 0/0 : 192.168.1.1/24
- IP FastEthernet 1/0 : 192.168.2.1/24

#### Jawaban:

Pertama-tama, buatlah topologi seperti yang digambarkan.

Kemudian, setting IP masing-masing komputer dengan langkah-langkah sebagai berikut :

1. Klik pada PC0, lalu pilih tab Desktop.
2. Pilih IP Configuration, lalu isikan IP Address, Subnet Mask, dan Default Gateway sesuai dengan yang telah diberikan. Subnet Mask adalah /24 yang berarti 24 bit, yaitu 255.255.255.0. Default gateway diisi dengan IP dari router yang berfungsi sebagai penghubung jaringan luar, yaitu IP FastEthernet 0/0, 192.168.1.1.



3. Tutup kotak dialog PC dan lakukan hal yang sama pada semua PC untuk melakukan setting IP Address masing-masing PC.

Setting Router dengan langkah-langkah sebagai berikut:

1. Klik pada router di simulasi packet tracer, lalu pilih tap Command Line Interface (CLI)

2. Masukkan perintah sesuai dengan yang diberikan di bawah.

```

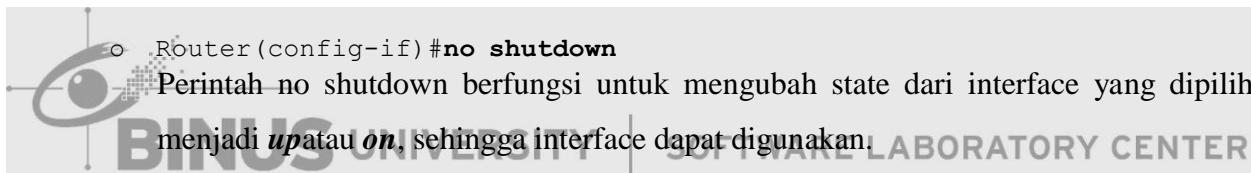
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#exit

```

Penjelasan:

- Router>**enable**  
Router memiliki beberapa mode. Ketika pertama kali dinyalakan, router berada dalam *user mode/read-only mode*. Mode ini ditandai dengan tanda lebih besar (>). Perintah **enable** berfungsi untuk berpindah dari *user mode* ke *privilege mode* yang ditandai dengan tanda pagar (#).

- Router#**configure terminal**  
Perintah configure terminal berfungsi untuk beralih dari *privilege mode* ke *global configuration mode*.
- Router(config)#**interface FastEthernet0/0**  
Pada mode konfigurasi, perintah **interface** digunakan untuk memilih interface mana yang akan dikonfigurasi. Interface dalam hal ini dapat berupa koneksi fisik Ethernet atau Serial. Perintah **interface FastEthernet0/0** berarti memilih yang port Ethernet pertama atau “0” pada FastEthernet card yang pertama atau “0”. Jika ingin memilih port Ethernet yang pertama atau “0” pada FastEthernet card yang kedua atau “1”, maka ketikan perintah **interface FastEthernet1/0**.
- Router(config-if)#**ip address 192.168.1.1 255.255.255.0**  
Perintah **ip address 192.168.1.1 255.255.255.0** berfungsi untuk mengeset IP address dari interface yang bersangkutan dengan 192.168.1.1 dan dengan subnet mask 255.255.255.0.



- **exit**  
Perintah **exit** digunakan untuk kembali ke mode sebelumnya. Misalnya dari mode konfigurasi, jika diketikkan perintah **exit**, maka akan kembali ke mode privilege yang ditandai dengan tanda pagar (#).

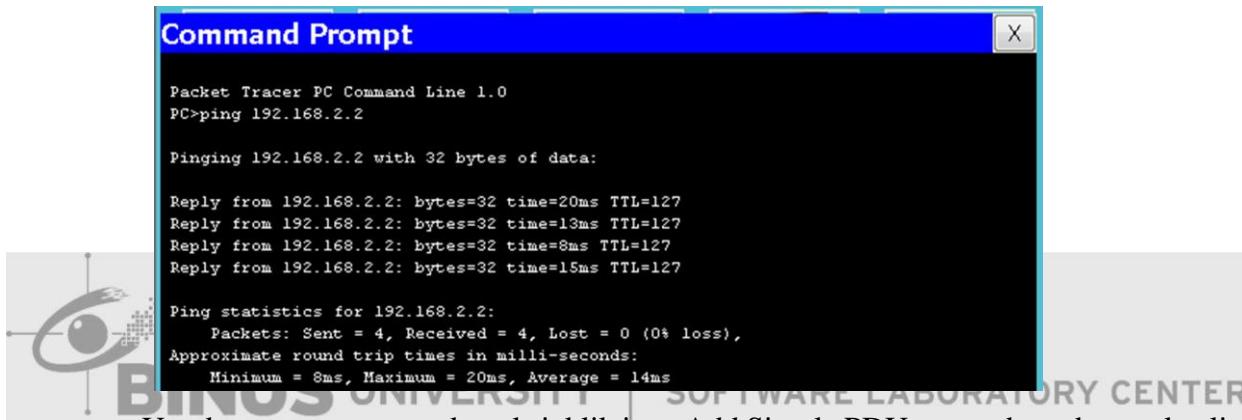
Perintah-perintah lain yang umum dipakai:

- Router#**show running-config**  
Perintah show running-config dipakai untuk melihat konfigurasi yang sedang berjalan pada router, misalnya status interface, ip address dari interface.
- Router(config-if)#**no ip address <ip address><subnet mask>**  
Perintah di atas digunakan untuk menghapus konfigurasi ip address dengan subnet mask pada suatu interface.
- Router#**write memory**  
Jika suatu router dimatikan dan dinyalakan kembali, maka konfigurasi yang sebelumnya suda diset akan hilang. Perintah **write memory** bertujuan untuk

menyimpan konfigurasi riuter ke dalam *Non Volatile Memory* (NVRAM) sehingga konfigurasinya dapat di-*load* ketika router di-*restart*.

Untuk mengetahui apakah perangkat yang satu sudah terkoneksi dengan perangkat yang lain, gunakan tes ping. Tes ping pada Packet Tracer dapat dilakukan dengan salah satu dari cara berikut.

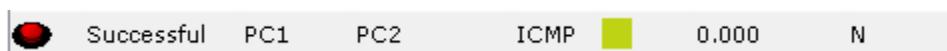
- Klik salah satu komputer (misalnya PC1), kemudian pilih tab **Desktop**. Pilih icon **Command Prompt**. Lalu, ketikkan perintah ping, misalnya **ping 192.168.2.2**. Jika komputer PC1 dan 192.168.2.2 (PC2) sudah terkoneksi, maka akan diterima pesan tanggapan (*reply*).



- Untuk mempercepat tes koneksi, klik icon Add Simple PDU yang ada pada panel paling kanan.



Kemudian, klik komputer yang ingin mengirim pesan dan klik kembali komputer yang menjadi tujuan. Untuk mengetahui apakah sudah pengiriman berhasil atau tidak (terkoneksi atau tidak), dapat diketahui dari pesan yang ada jendela PDU list yang ada di bagian kanan bawah.



Untuk menghapus pesan informasi yang ada pada PDU list, klik tombol Delete.



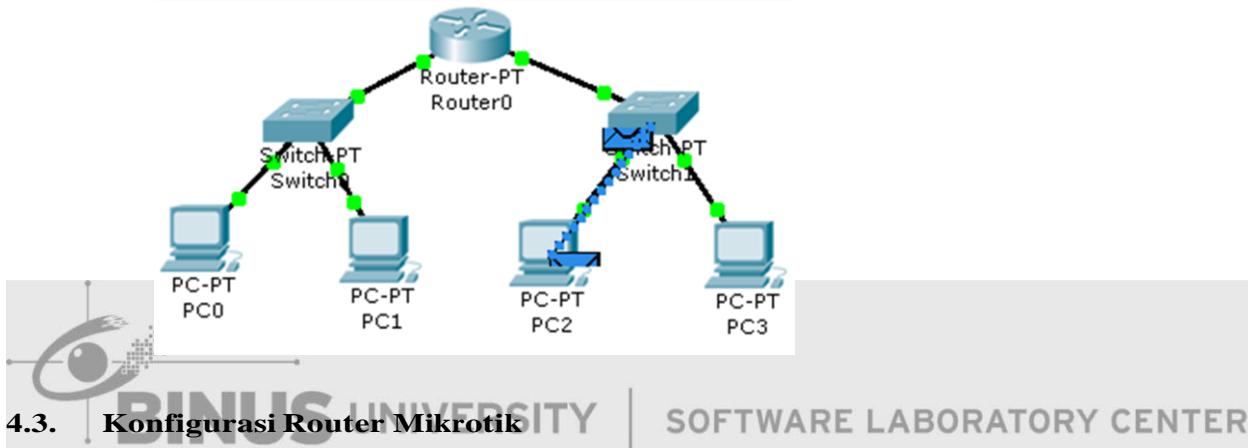
- Untuk mengetahui pergerakan dari pesan yang dikirim, gunakan mode Simulasi. Perhatikan tab yang aktif di bagian bawah, saat ini yang aktif adalah tab **Realtime**

(*default*). Aktifkan tab **Simulation** di belakang tab Realtime dengan cara mengklik iconnya.



Ubahlah **Edit Filters** menjadi **ICMP**. ICMP (*Internet Control Message Protocol*) merupakan tipe pesan yang dikirim, jika dilakukan perintah ping.

Kemudian, klik tombol **Auto Capture / Play** untuk memulai simulasi.

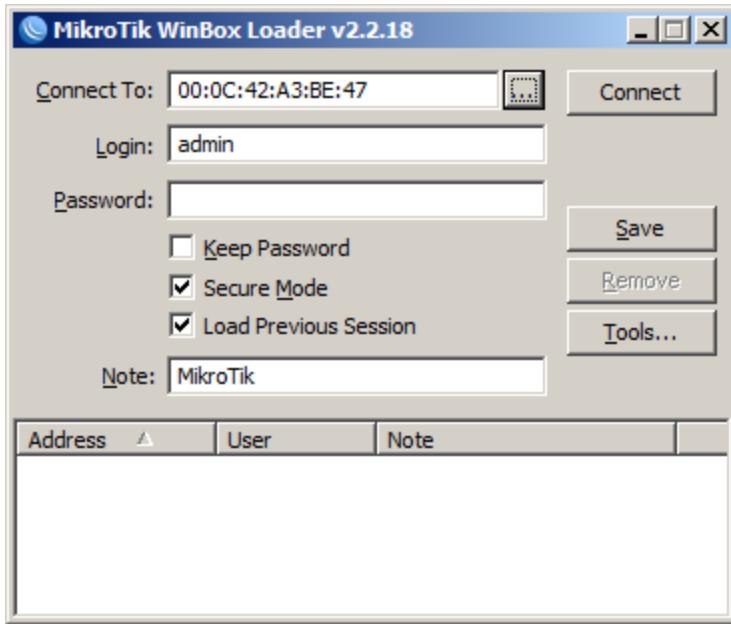


#### 4.3. Konfigurasi Router Mikrotik

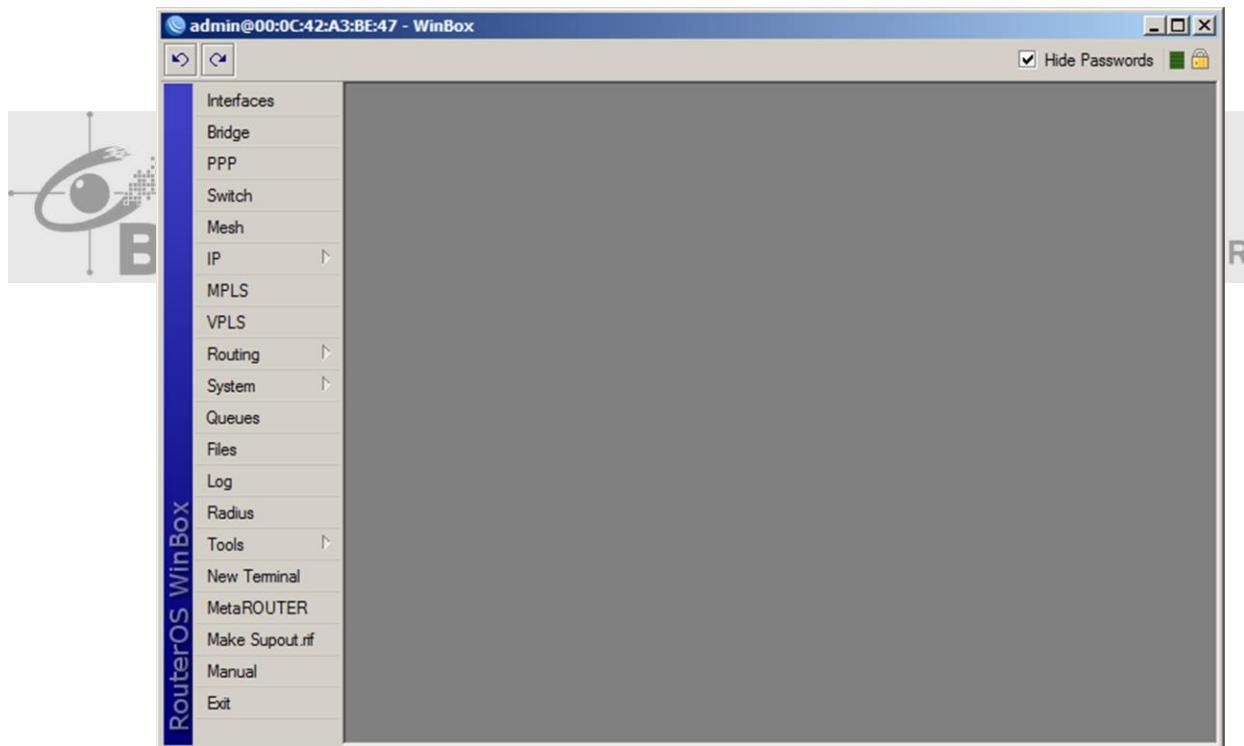
Seperti halnya dengan konfigurasi router pada packet tracer. Konfigurasi pada router mikrotik memiliki konsep yang serupa, namun hanya berbeda perintah yang digunakan.

Berikut adalah cara konfigurasi pada router mikrotik (versi OS 4.14):

1. Download program winbox dari situs <http://www.mikrotik.co.id/download.php>. Winbox yang digunakan adalah winbox-2.2.18.
  2. Hubungkan sebuah komputer yang memiliki interface ethernet dengan salah satu port ethernet pada router.
  3. Jalankan program winbox dari PC yang terhubung dengan router.
  4. Pilih tanda ... pada **Connect To** untuk memilih MAC Address dari interface router.
  5. Login dengan memasukkan username dan password.
- Secara default, username adalah **admin** dan password adalah <kosong>.



6. Tampilan ketika sudah login adalah sebagai berikut.



7. Klik **New Terminal** untuk melakukan perintah konsole.

Berikut perintah-perintah dasar yang digunakan pada MikroTik:

1. **[admin@MikroTik]>system reset-configuration**

Digunakan untuk melakukan reset ke konfigurasi awal.

2. **[admin@MikroTik] > system identity set name="bluejack"**

Digunakan untuk mengubah nama router menjadi "bluejack"

3. **[admin@MikroTik] > interface ethernet enable ether1**

atau

**[admin@MikroTik] > interface ethernet enable 0**

Digunakan untuk mengaktifkan interface ethernet pada interface dengan nama ether1 atau interface dengan nomor ke-0.

4. **[admin@MikroTik] > interface ethernet print**

Digunakan untuk melihat konfigurasi interface

5. **[admin@MikroTik] > interface ethernet set ether1 name="Test"**

atau

**[admin@MikroTik] > interface ethernet set 0 name="Test"**

Digunakan untuk mengubah nama yang sebelumnya ether1 (defaultnya sebagai nomor ke-0) menjadi Test.

6. **[admin@MikroTik] > ip address print**

Digunakan untuk melihat konfigurasi ip address

7. **[admin@MikroTik] > ip address add interface=ether1 address=10.22.64.1/8**

**network=10.0.0.0 broadcast=10.255.255.255**

Digunakan untuk menambahkan interface ether1 dengan alamat ip 10.22.64.1 dengan subnet mask 8 bit, yaitu 255.0.0.0.

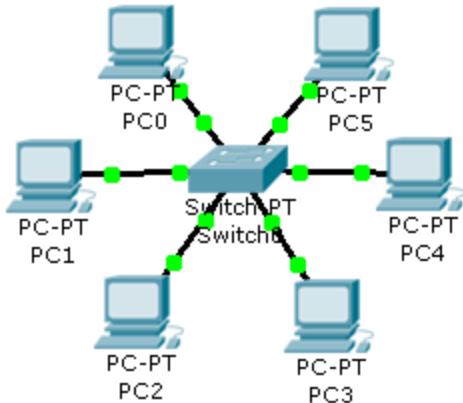
8. **[admin@MikroTik] > ip address set interface=ether1 address=192.168.0.1/24**

**network=192.168.0.255 broadcast=192.168.0.255**

Digunakan untuk mengubah interface ether1 menjadi 192.168.0.1 sebagai alamat ip dan 255.255.255.0 sebagai subnet mask.

#### 4.4. Exercise

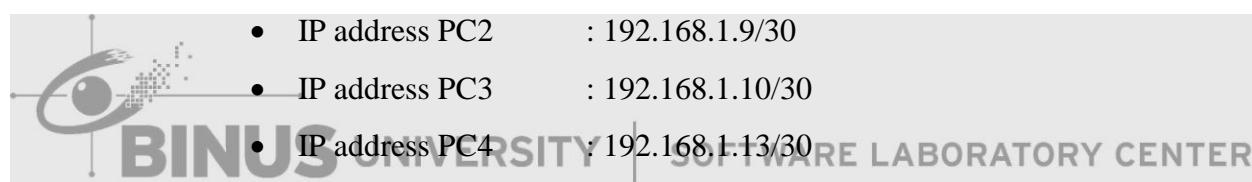
- Diketahui topologi sebagai berikut.



**Informasi Jaringan :**

**PC:**

- IP address PC0 : 192.168.1.5/30
- IP address PC1 : 192.168.1.6/30
- IP address PC2 : 192.168.1.9/30
- IP address PC3 : 192.168.1.10/30
- IP address PC4 : 192.168.1.13/30
- IP address PC5 : 192.168.1.14/30

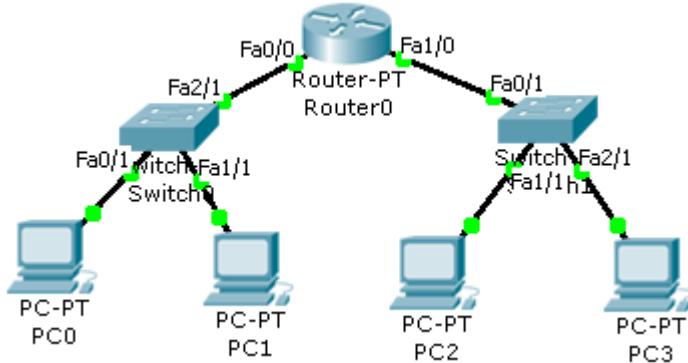


Jelaskan mengapa PC0 tidak dapat mengirimkan pesan ke PC2!

Berapa banyak jaringan yang ada pada topologi di atas?

- Sebut dan jelaskan mode-mode yang dimiliki router!
- Jelaskan perintah:
  - enable**
  - configure terminal**
  - no shutdown**
  - write mem**
  - ip forwarding**
- Suatu perusahaan memiliki *network address* kelas A. Perusahaan ingin membuat 3 buah jaringan yang ingin saling terkoneksi menggunakan router. Rancanglah sistem jaringan perusahaan tersebut dengan menggunakan packet tracer.

5. Diketahui topologi sebagai berikut.



#### Informasi Jaringan :

##### PC:

- IP address PC0 : 192.168.1.2/24  
MAC address PC0 : 0090.21D7.A8A6
- IP address PC1 : 192.168.1.3/24  
MAC address PC1 : 0001.6477.9C3A
- IP address PC2 : 192.168.2.2/24  
MAC address PC2 : 0002.4A3D.18A5
- IP address PC3 : 192.168.2.3/24  
MAC address PC3 : 0050.0F4C.ACC1

##### Router0

- IP address FastEthernet 0/0 : 192.168.1.1/24
- MACaddress FastEthernet 0/0 : 000A.F390.2041
- IP address FastEthernet 1/0 : 192.168.2.1/24
- MACaddress FastEthernet 1/0 : 0060.47D8.6009

Jika PC0 mengirim suatu pesan ke komputer PC3, maka pesan (dalam bentuk frame) akan melalui lintasan PC0-switch0-router-switch1-PC3. Setiap frame memiliki informasi MAC address dan IP address. Lengkapi tabel di bawah untuk menjelaskan informasi setiap frame dari node ke node.

Dari – Tujuan	MAC address pengirim	MAC address penerima	IP address pengirim	IP address penerima
PC0 ke switch0	...	...	...	...
Switch0 ke router	...	...	...	...
Router ke switch1	...	...	...	...
Switch1 ke PC3	...	...	...	...

## **Chapter 05**

### **Routing**

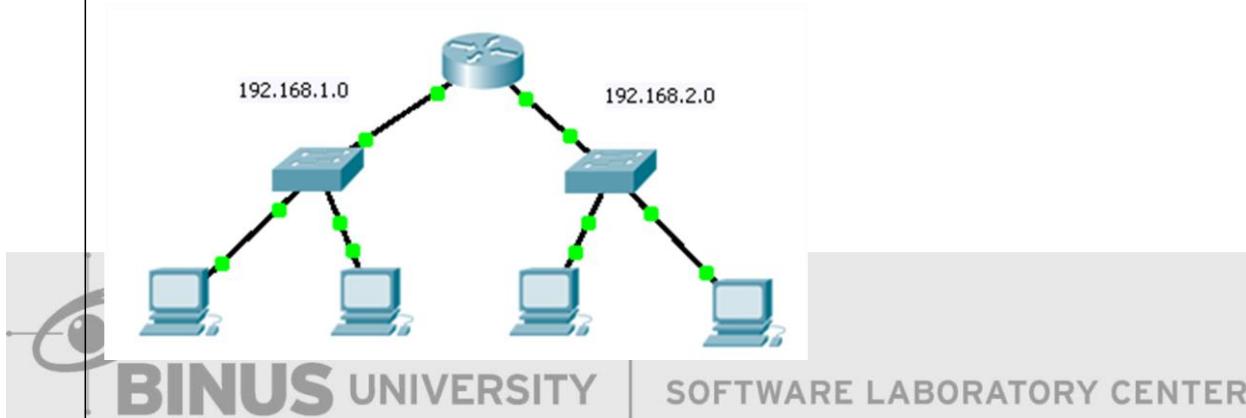


### 5.1. Routing

Router bekerja dengan cara membaca informasi IP address dari paket yang diterimanya, kemudian meneruskan paket itu ke jalur tujuannya. Penentuan jalur inilah yang disebut dengan **routing**.

Untuk dapat menentukan jalur yang tepat untuk suatu paket, suatu router memiliki memori di dalamnya yang digunakan untuk menyimpan hubungan antara tujuan paket dan jalur mana yang akan dilaluinya. Informasi jalur-jalur ini disimpan dalam bentuk entri-entri sebuah tabel, dinamakan sebagai **tabel routing**.

Diberikan sebuah contoh:



Sebuah router terhubung dengan dua buah jaringan. Routing table dari router dapat diketahui dengan command `show ip route`, maka dapat ditampilkan routing table dari router adalah sebagai berikut.

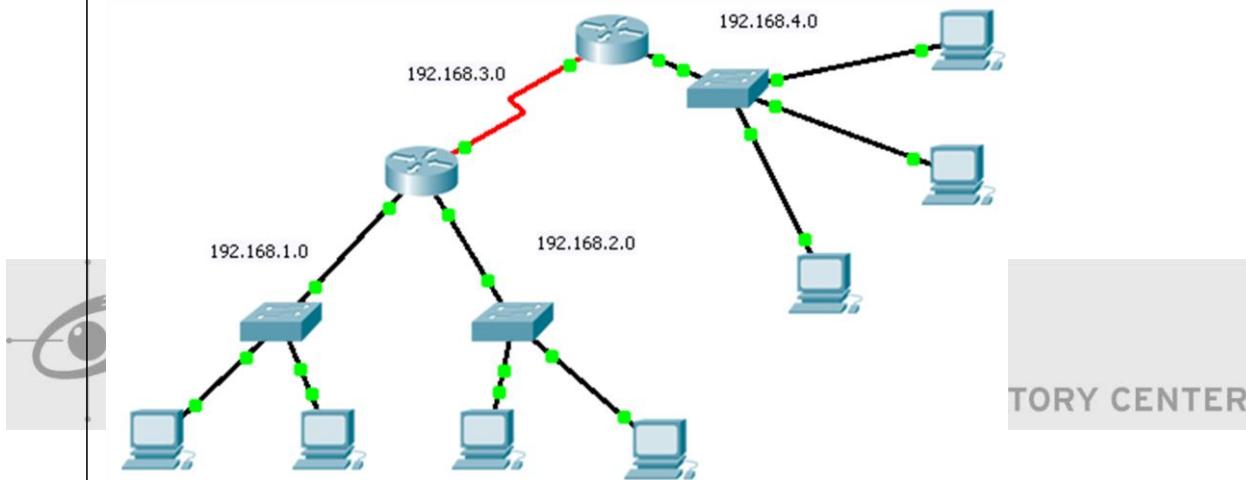
```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
```

(Simbol **C** berarti router terhubung langsung dengan jaringan/Directly Connected Route).

Dengan memanfaatkan tabel ini, jika suatu paket dengan alamat tujuan ke perangkat pada jaringan 192.168.1.0, misalnya ke 192.168.1.5, maka router akan meneruskannya ke FastEthernet 0/0. Sebaliknya, jika suatu paket ingin menuju ke perangkat pada jaringan 192.168.2.0, misalnya menuju 192.168.2.100, maka router akan meneruskan paket itu ke FastEthernet1/0.

Entri pada tabel routing akan terbentuk secara default jika suatu jaringan langsung terkoneksi ke router. Namun, hal ini akan menjadi masalah jika banyak jaringan harus saling terhubung satu sama lain sehingga tidak mungkin sebuah router dapat mengakomodasi semua kebutuhan tersebut. Oleh karenanya, dibutuhkan lebih dari 1 router agar dapat mengakomodasi kebutuhan jaringan yang banyak. Namun, dengan hal ini, routing menjadi hal yang rumit, karena kini router tidak langsung terhubung (*directly connected*) ke semua jaringan.

Ilustrasi masalah:



Terdapat 4 buah jaringan. Router pertama terhubung langsung ke jaringan 192.168.1.0, 192.168.2.0, dan 192.168.3.0, sedangkan router kedua terhubung langsung ke jaringan 192.168.3.0 dan 192.168.4.0. Hal ini dapat diketahui dari command `show ip route`.

Untuk router pertama, jika show ip route:

- C 192.168.1.0/24 is directly connected, FastEthernet0/0
- C 192.168.2.0/24 is directly connected, FastEthernet1/0
- C 192.168.3.0/24 is directly connected, Serial2/0

Untuk router kedua, jika show ip route:

- C 192.168.3.0/24 is directly connected, Serial2/0
- C 192.168.4.0/24 is directly connected, FastEthernet0/0

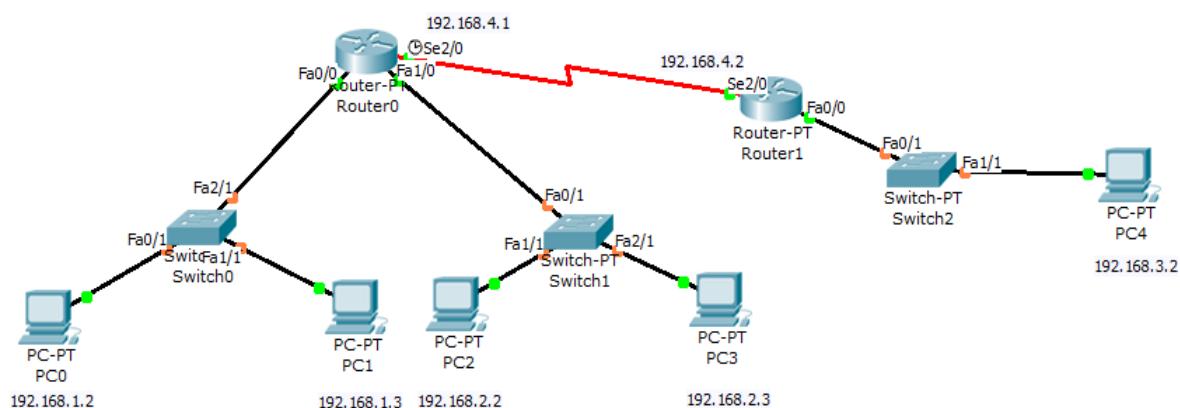
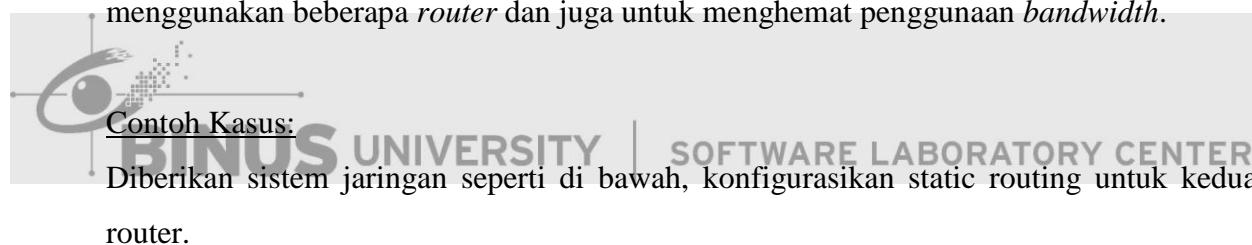
Sebagai contoh, jika suatu paket dengan tujuan ke jaringan 192.168.4.0, misalnya menuju 192.168.4.3, masuk ke router pertama, maka informasi jaringan ini tidak ditemukan dalam tabel routingnya, sehingga paket tersebut akan di-drop. Padahal, jika paket diteruskan ke jalur pada jaringan 192.168.3.0 (Serial2/0), maka paket akan sampai ke tujuannya.

Oleh karenanya, selain dengan langsung terhubung (*directly connected*), penentuan jalur / routing dilakukan dengan mekanisme lain, yaitu:

1. Static Routing
2. Dynamic routing

## 5.2. Static Routing

*Static routing* adalah salah satu cara untuk membuat tabel *routing*/ proses pemilihan *path* ke jaringan lain secara **manual**. Static routing ini berguna untuk jaringan sederhana yang menggunakan beberapa *router* dan juga untuk menghemat penggunaan *bandwidth*.



Jawaban:

Langkah-langkah yang perlu dilakukan:

1. Isi masing-masing IP Address PC sesuai dengan yang soal.

2. Lakukan konfigurasi untuk Router0 dan Router1 untuk setiap port FastEthernet.
3. Kemudian lakukan konfigurasi Router untuk port Serial dengan mengikuti langkah-langkah perintah berikut:

**\*KONFIGURASI SERIAL2/0 PADA ROUTER0\***

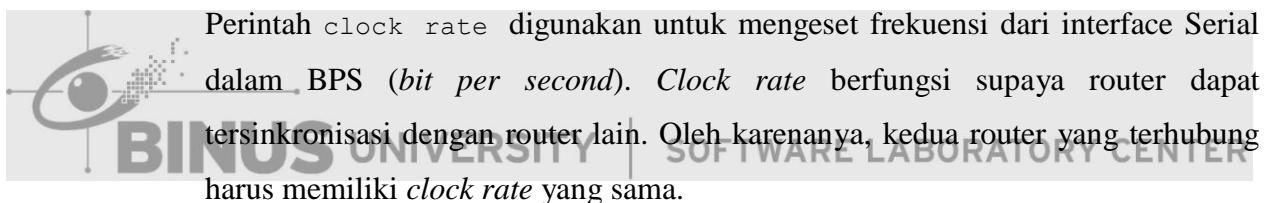
```
Router>enable
Router#configure terminal
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

**\*KONFIGURASI SERIAL2/0 PADA ROUTER1\***

```
Router>enable Router#configure
terminal Router(config)#interface
Serial2/0
Router(config-if)#ip address 192.168.4.2 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Penjelasan:

- o clock rate 64000



4. Lakukan konfigurasi static routing untuk kedua router.

**\*KONFIGURASI STATIC ROUTING PADA ROUTER0\***

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.4.2
```

**\*KONFIGURASI STATIC ROUTING PADA ROUTER1\***

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.4.1
```

Penjelasan:

- o `ip route 192.168.3.0 255.255.255.0 192.168.4.2`

Perintah `ip route` digunakan untuk menambahkan entri rute yang baru ke dalam tabel routing. Perintah `ip route 192.168.3.0 255.255.255.0 192.168.4.2`

digunakan untuk menambahkan entri rute jaringan 192.168.3.0/24 untuk menuju 192.168.4.2.

- Untuk melihat hasil tabel routing, gunakan perintah `show ip route`.

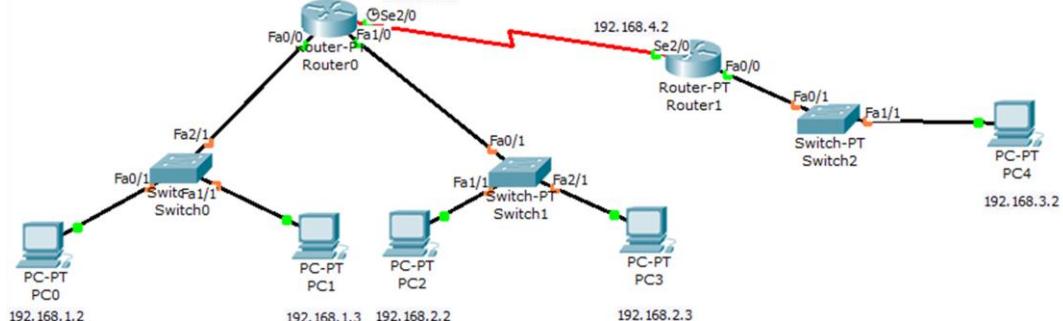
**\*TABLE ROUTING PADA ROUTER0\***

```
Router>enable
Router#configure terminal
Router#show ip route
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
S    192.168.3.0/24 [1/0] via 192.168.4.2
C    192.168.4.0/24 is directly connected, Serial2/0
```

**\*TABLE ROUTING PADA ROUTER1\***

```
Router>enable
Router#configure terminal
Router#show ip route
S    192.168.1.0/24 [1/0] via 192.168.4.1
S    192.168.2.0/24 [1/0] via 192.168.4.1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial2/0
```

Dengan penambahan entri secara statik / manual seperti di atas, maka semua jaringan kini dapat saling terkoneksi.



Diilustrasikan bahwa paket datang dari PC0 ingin menuju PC4, maka ketika paket tersebut memasuki router0, maka router0 akan mengecek tabel routingnya dan menemukan bahwa kini entri terhadap jaringan 192.168.3.0 sudah ada di tabel, maka router0 akan meneruskannya ke 192.168.4.2 sesuai dengan tabel tersebut. Kemudian, ketika paket itu masuk ke router1, router1 akan langsung meneruskannya ke PC4.

Sebaliknya, jika PC4 ingin berkirim data ke PC0, maka ketika paket memasuki router1, maka router1 akan mengecek tabel routingnya dan menemukan bahwa entri

terhadap jaringan 192.168.1.0 ada pada tabel, maka router1 akan meneruskan paket itu ke 192.168.4.1 sesuai dengan tabel routing yang dimilikinya.

Static routing digunakan karena alasan kemudahan konfigurasi, keamanan, overhead resources yang kecil. Tetapi untuk jaringan yang kompleks, static routing tidak dapat dipakai. Seandainya, terjadi perubahan network, misalnya terdapat rute yang putus maka tabel routing harus di-update secara manual untuk semua router yang ada dalam sistem. Oleh karenanya, dalam hal ini, digunakan dynamic routing untuk meng-update tabel routing secara dinamis.

### 5.3. Dynamic Routing

Static routing memiliki kelemahan jika ukuran jaringan terlalu besar dan jika terjadi banyak perubahan konfigurasi jaringan dari waktu ke waktu. Alternatif lainnya yaitu menggunakan *dynamic routing*. *Dynamic routing* dibangun berdasarkan informasi yang dikumpulkan oleh protokol *routing*. Protokol ini didesain untuk mendistribusikan informasi yang secara **dinamis** mengikuti perubahan kondisi jaringan.

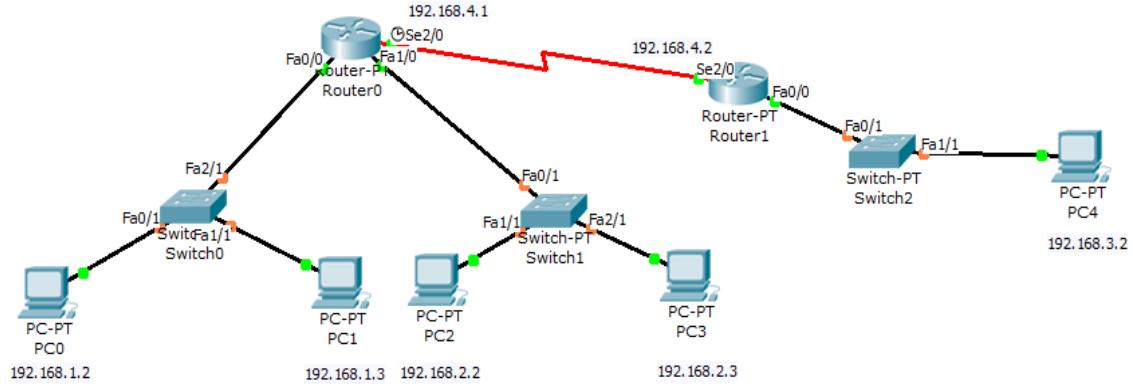


Pada layer TCP/IP, router dapat menggunakan protokol routing untuk membentuk routing melalui suatu algoritma. Beberapa protokol routing antara lain:

1. **RIP** → menggunakan protokol *routing interior* dengan algoritma *distance vector*
2. **IGRP** → menggunakan protokol *routing interior* dengan algoritma Cisco *distance vector*
3. **OSPF** → menggunakan protokol *routing interior* dengan algoritma *link state*
4. **EIGRP** → menggunakan protokol *routing interior* dengan algoritma *advanced Cisco distance vector*.

Contoh kasus:

Diberikan sistem jaringan seperti di bawah, konfigurasikan dynamic routing untuk kedua router menggunakan protokol RIP.



Jawaban:

Langkah-langkah yang perlu dilakukan:

1. Isi masing-masing IP Address PC sesuai dengan yang soal.
2. Lakukan konfigurasi untuk Router0 dan Router1 untuk setiap port FastEthernet dan port Serial.
3. Lakukan konfigurasi dynamic routing untuk kedua router.

```
*KONFIGURASI DYNAMIC ROUTING PADA ROUTER0*
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.4.0

*KONFIGURASI DYNAMIC ROUTING PADA ROUTER1*
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
```

Penjelasan:

- **Router rip**

Perintah `router rip` digunakan untuk masuk ke dalam konfigurasi RIP.

- **network 192.168.1.0**

Perintah di atas digunakan agar memasukkan jaringan 192.168.1.0 ke dalam protokol rip. Selanjutnya, protokol rip akan melakukan algoritma dengan mendistribusikan jaringan 192.168.1.0 ke router-router lainnya. Pada router0,

dilakukan tiga kali perintah network, karena router0 terhubung secara langsung ke 3 jaringan.

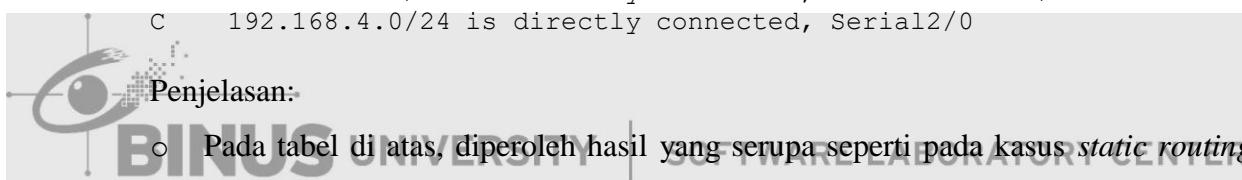
- Untuk melihat hasil tabel routing, gunakan perintah `show ip route`.

**\*TABEL ROUTING PADA ROUTER0\***

```
Router>enable
Router#configure terminal
Router#show ip route
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:02, Serial2/0
C    192.168.4.0/24 is directly connected, Serial2/0
```

**\*TABEL ROUTING PADA ROUTER1\***

```
Router>enable
Router#configure terminal
Router#show ip route
R    192.168.1.0/24 [120/1] via 192.168.4.1, 00:00:16, Serial2/0
R    192.168.2.0/24 [120/1] via 192.168.4.1, 00:00:16, Serial2/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial2/0
```



- Pada tabel di atas, diperoleh hasil yang serupa seperti pada kasus *static routing*, namun diperoleh secara dinamis (tanda R berarti entri tabel didapat dari hasil protokol RIP).
- 00:00:02 merupakan waktu, berapa lama entri rute ini berada pada tabel. Setiap 30 detik, waktu akan kembali menjadi 00:00:00.

Protokol RIP bekerja dengan algoritma *distance vector*. Setiap 30 detik, suatu router (misalnya router A) akan memberitahukan kepada router-router tetangganya mengenai informasi jaringan yang langsung terhubung dengannya. Router tetangga akan mengupdate informasi dalam tabel routing yang dimilikinya dari informasi yang diperoleh, kemudian akan mendistribusikan informasi tersebut ke sekitarnya lagi. Hingga akhirnya informasi ini dikembalikan ke router A, dan router A akan mengupdate tabel routingnya lagi. Jika diperlukan router A perlu untuk mengirimkan kembali informasi tabel routingnya hingga terjadi konvergensi jaringan. Konvergensi

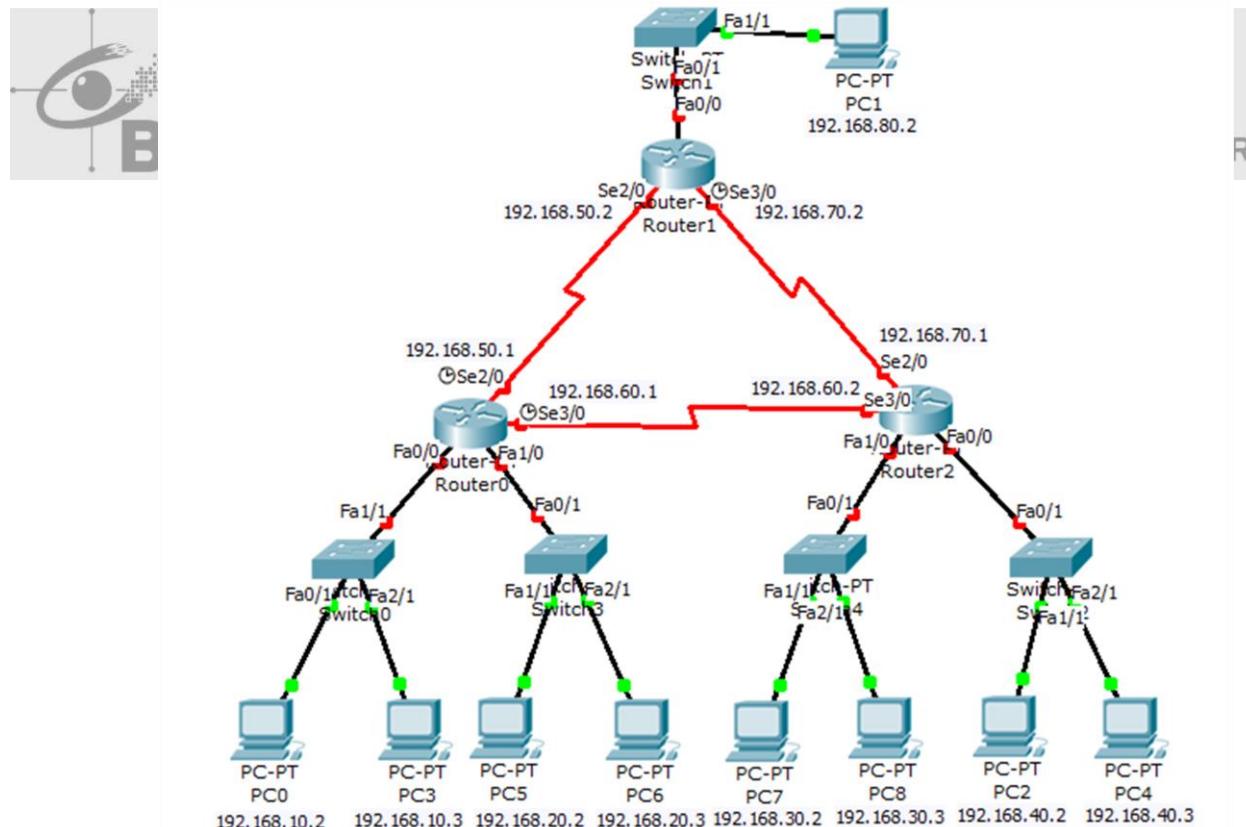
jaringan adalah kondisi di mana semua router dalam jaringan sudah sepakat dalam menentukan jalur terbaik.

RIP bekerja dengan menghitung hop. Hop adalah jarak antar router. Jika router saling tersambung, maka jaraknya adalah 1 hop. Jika di antara dua buah router terdapat sebuah router, maka jaraknya 2 hop. Dalam RIP, penentuan entri tabel didasarkan pada jalur dengan hop terkecil.

#### 5.4. Exercise

1. Apa yang dimaksud dengan *static* dan *dynamic routing*? Jelaskan kelebihan dan kekurangannya masing-masing!
2. Apa kegunaan clock rate pada konfigurasi serial?
3. Jelaskan kelebihan dan kekurangan dari protokol routing yang ada meliputi protokol RIP, OSPF, EIGRP, dan IGRP!

*Perhatikan gambar di bawah ini untuk menjawab soal nomor 4 dan 5!*



4. Buatlah konfigurasi router dengan static routing!
5. Buatlah konfigurasi router dengan dynamic routing!

## **Chapter 06**

### **Access List**



## 6.1. Pengenalan Access List

ACL (*Access List*) adalah aturan-aturan yang digunakan untuk mengizinkan (*permit*) atau menolak (*deny*) paket menuju ke tujuan tertentu. Proses untuk melewatkkan dan menolak paket ini terjadi pada interface di router.

Access list mempunyai beberapa fungsi, misalnya:

- Membatasi *traffic* jaringan dan meningkatkan kerja jaringan. Misalnya, access list memblok *traffic* video sehingga dapat menurunkan beban jaringan dan meningkatkan kerja jaringan.
- Mengatur aliran *traffic*. Access list mampu memblok update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
- Mampu memberikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan untuk mengakses jaringan tersebut.
- Memutuskan jenis *traffic* mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, *traffic* email dilayani, *traffic* telnet diblok.
- Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.
- Memilih host-host yang diijinkan atau diblok dalam mengakses segmen jaringan. Misal, access list mengijinkan atau memblok FTP atau HTTP.

Berdasarkan kemampuan filternya, ACL dibagi menjadi 2:

### a. Standard Access List

Standard Access List merupakan suatu access list yang hanya dapat melakukan filter berdasarkan alamat sumber (*source address*). Misalnya, jika sumbernya dari 192.168.1.2 maka akan ditolak, namun standard access list tidak dapat melakukan filter terhadap alamat tujuan dari paket, tipe paket (protokol yang digunakan), dan nomor port.

### b. Extended Access List

Extended Access List merupakan pengembangan dari standard access list. Selain bisa melakukan filter pada alamat sumber, namun juga dapat melakukan filter berdasarkan tujuan paket, tipe/protokol yang digunakan, dan nomor port.

Untuk mendefinisikan access list, digunakan nomor dari 1 hingga 199, sekaligus nomor tersebut mendefinisikan apakah access list yang digunakan adalah standard atau extended. Selain nomor, access list juga bisa didefinisikan menggunakan nama (tipe string), sehingga lebih mudah dikenal.

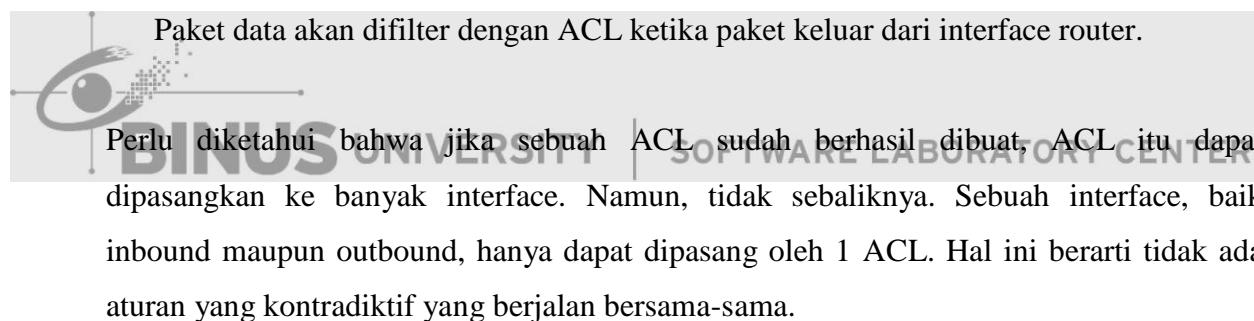
Rentang Nomor	List Type
1-99	Regular IP List
100-199	Extended IP List

Sesudah suatu ACL dibentuk, maka ACL pun bisa dipasangkan pada interface di router. Pemasangan pada interface dapat dilakukan dengan 2 cara:

**a. Inbound**

Paket data akan difilter dengan ACL ketika paket masuk ke dalam interface router.

**b. Outbound**

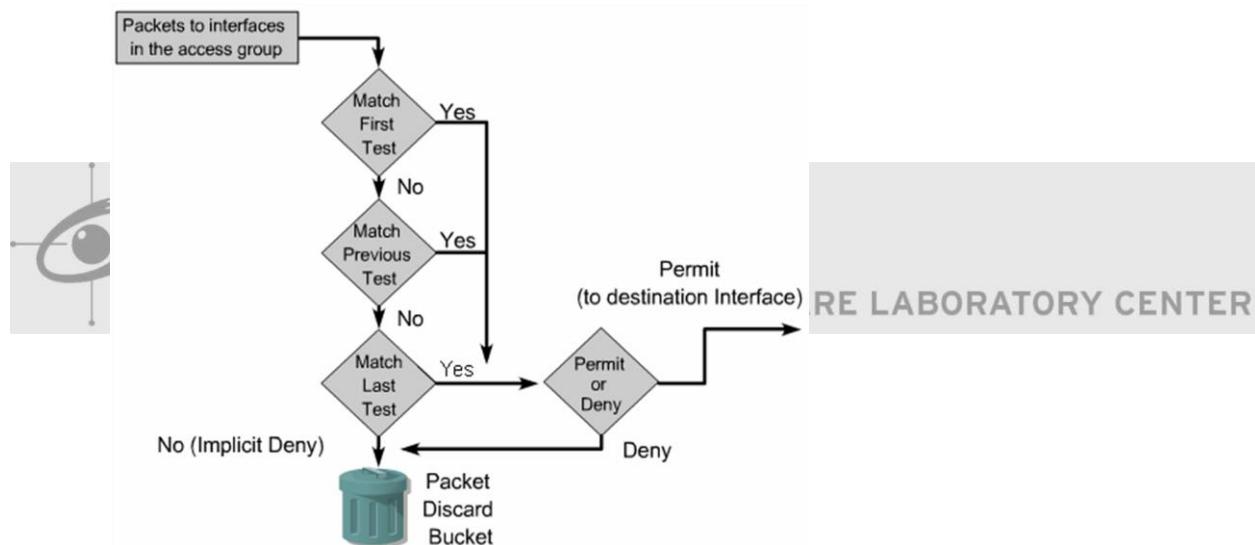


Berikut adalah pedoman / aturan dalam membuat access list:

- Harus memiliki satu access list per protokol per arah.
- Standard access list sebaiknya diaplikasikan ke tujuan terdekat.
- Extended access list sebaiknya diaplikasikan ke asal terdekat.
- *Inbound* dan *outbound* interface harus dilihat dari port arah masuk router.
- Pernyataan akses diproses secara sequential dari atas ke bawah sampai ada yang cocok. Jika tidak ada yang cocok maka paket ditolak dan dibuang.
- Rule dalam access list dibaca secara berurutan (*sequential*) berdasarkan nomor index dari rule. Jika tidak terdapat rule yang cocok maka secara default akan di *deny*.
- Access list yang dimasukkan harus difilter dengan urutan spesifik ke umum. Host tertentu harus ditolak dulu dan grup atau umum kemudian.

- Kondisi cocok dijalankan dulu. Dijinkan atau ditolak dijalankan jika ada pernyataan yang cocok.
- Baris baru selalu ditambahkan di akhir access list. Perintah **no access-list x** akan menghapus semua daftar.
- Access list berupa IP akan dikirim sebagai pesan ICMP host unreachable ke pengirim dan akan dibuang.

## 6.2. Cara Kerja Access List



Suatu access list sebenarnya merupakan kumpulan aturan-aturan, sehingga bisa lebih dari 1 aturan yang ada pada access list. Contoh, diberikan sebuah access list standard dengan nomor 35 yang memiliki 2 aturan / *test*:

Standard IP access list 35

deny host 192.168.1.2

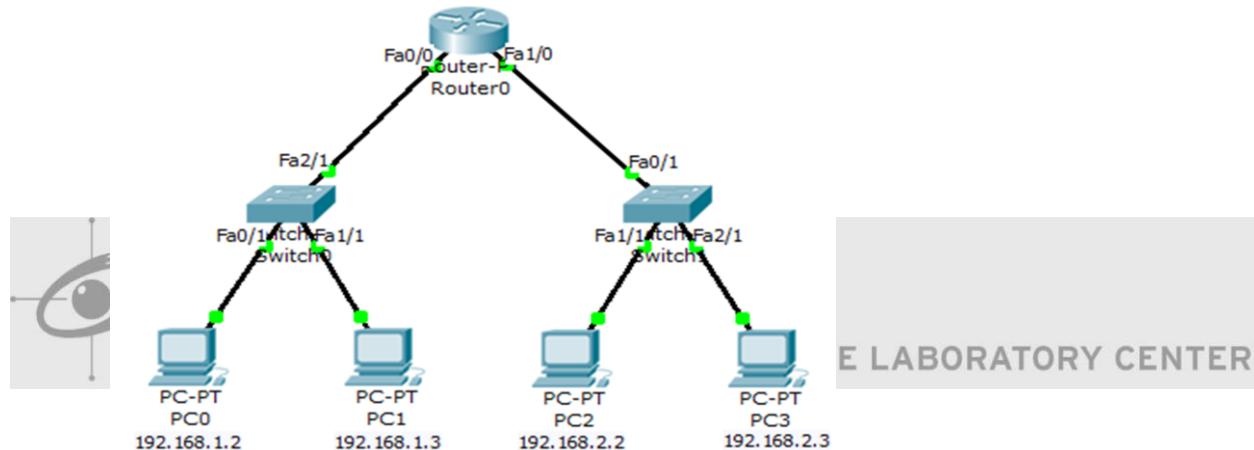
permit host 192.168.1.3

ACL bekerja dari atas ke bawah. Dengan demikian, ketika suatu paket difilter dengan ACL tersebut, maka akan dicek pertama kali apakah paket berasal dari 192.168.1.2. Jika

ya, maka paket akan di-*deny* (sesuai dengan ketentuan test pertama) dan test baris berikutnya tidak perlu dicek. Namun, jika paket tidak berasal dari 192.168.1.2, maka test baris kedua akan dilakukan, cek paket apakah berasal dari 192.168.1.3. Jika ya, maka paket akan di-*permit* / dilewatkan. Namun, jika tidak berasal dari 192.168.1.3, maka paket secara default akan ditolak / di-*deny*. Aturan *deny* ini selalu ada di akhir dari access list yang dibuat dan tidak terlihat pada konfigurasi yang disebut implicit deny.

### 6.3. Kasus untuk Standard Access List

*Deny / tolak paket (hanya) ke 192.168.1.2 dengan menggunakan standard access list, lalu tampilkan access list yang telah dibuat tersebut!*



**Jawab:**

1. Buatlah topologi seperti di atas, setting ip address untuk semua PC dan semua port fastEthernet pada Router.
2. Buatlah suatu access list. Klik pada router, lalu masuk bagian CLI. Gunakan perintah **access-list**.

```
Router>enable
Router#configure terminal
Router(config)#access-list 10 deny host 192.168.1.2
Router(config)#access-list 10 permit any
Router(config)#exit
```

Penjelasan:

- Perintah **access list 10 deny host 192.168.1.2** berfungsi untuk membentuk suatu standard access list nomor 10. Pada ACL ini, ditambahkan

sebuah aturan untuk menolak paket yang berasal dari host dengan ip address 192.168.1.2.

- Perintah **access-list 10 permit any** berfungsi untuk menambahkan aturan di bawah aturan **deny host 192.168.1.2** yang telah dibuat sebelumnya. Jika aturan ini tidak dibuat, maka host selain 192.168.1.2 secara default akan di-*deny*. Oleh karenanya, aturan ini perlu ditambahkan agar host yang lain di-*permit*.
3. Untuk melihat access list yang telah dibuat, dapat digunakan perintah **show access-list**.

```
Router#show access-lists
Standard IP access list 10
    deny host 192.168.1.2
    permit any
```

Penjelasan:

- Gunakan perintah **show access-list 10** untuk menampilkan access list hanya nomor 10.

#### 4. Pasang / attach access list yang sudah dibuat ke interface pada router.

```
Router#configure terminal
Router(config)#interface fastEthernet0/0
Router(config-if)#ip access-group 10 in
```

Penjelasan:

- Perintah **ip access-group 10 in** berfungsi untuk memasang aturan access-list nomor 10 secara inbound pada interface fastEhternet0/0. Inbound berarti aturan ACL akan bekerja ketika suatu paket masuk ke router melalui fastEhternet0/0.

#### 5. Tampilkan informasi pada interface dengan perintah **show ip interface**.

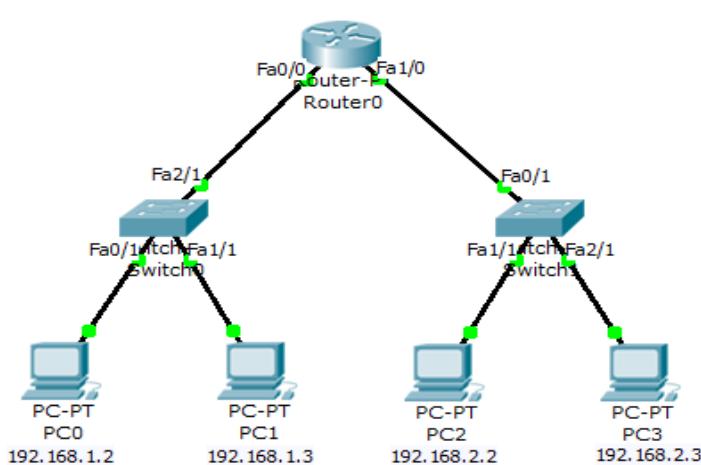
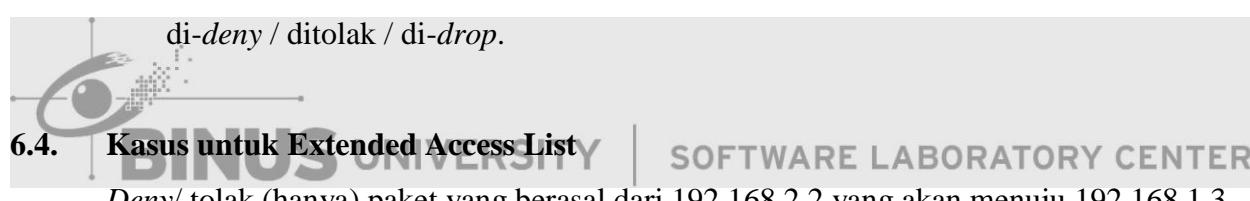
```
Router#show ip interface
```

```

Router#show ip interface
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is 10
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled

```

Dapat dilihat bahwa access-list nomor 10 sudah terpasang pada interface FastEthernet0/0 secara inbound. Kini, jika suatu paket masuk pada ke router melalui interface fa0/0, paket itu akan dicek. Jika berasal dari 192.168.1.2, maka paket akan di-denied / ditolak / di-drop.



**Jawab:**

1. Buatlah topologi seperti di atas, setting ip address untuk semua PC dan semua port fastEthernet pada Router.
2. Buatlah suatu access list. Klik pada router, lalu masuk bagian CLI. Gunakan perintah **access-list**.

```
Router>enable
Router#configure terminal
Router(config)#access-list 120 deny ip host 192.168.2.2 host
192.168.1.3 Router(config)#access-list 120 permit ip any any
Router(config)#exit
```

Penjelasan:

- Untuk membuat extended access list, maka digunakan nomor access list di antara 100 hingga 199. Dalam kasus ini, digunakan nomor 120.
- Perintah `access-list 120 deny ip host 192.168.2.2 host 192.168.1.3` digunakan untuk membuat *extended access-list* dengan nomor 120 dengan aturan untuk “*deny*” atau menolak paket dengan tipe “*ip*” (semua protokol) jika paket berasal dari host dengan ip 192.168.2.2 yang akan menuju host dengan ip 192.168.1.3.
- Karena secara default, access list akan menambahkan *deny ip any any* untuk aturan yang tidak cocok dengan *test* sebelumnya, maka ditambahkan perintah `permit ip any any` pada access-list nomor 120.

3. Pasang / attach access list yang sudah dibuat ke interface pada router.

```
Router#configure terminal
```

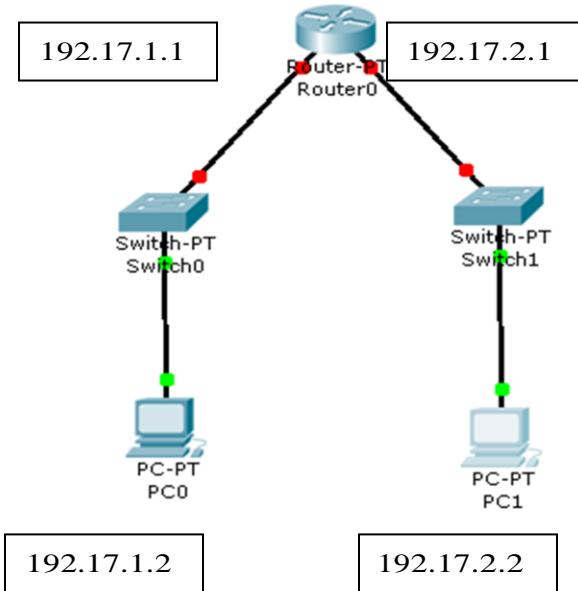
```
Router(config)#interface fastEthernet1/0
Router(config-if)#ip access-group 120 in
```

Penjelasan:

- Perintah `ip access-group 120 in` berfungsi untuk memasang aturan access-list nomor 120 secara *inbound* pada interface fastEhernet1/0.

## 6.5. Exercise

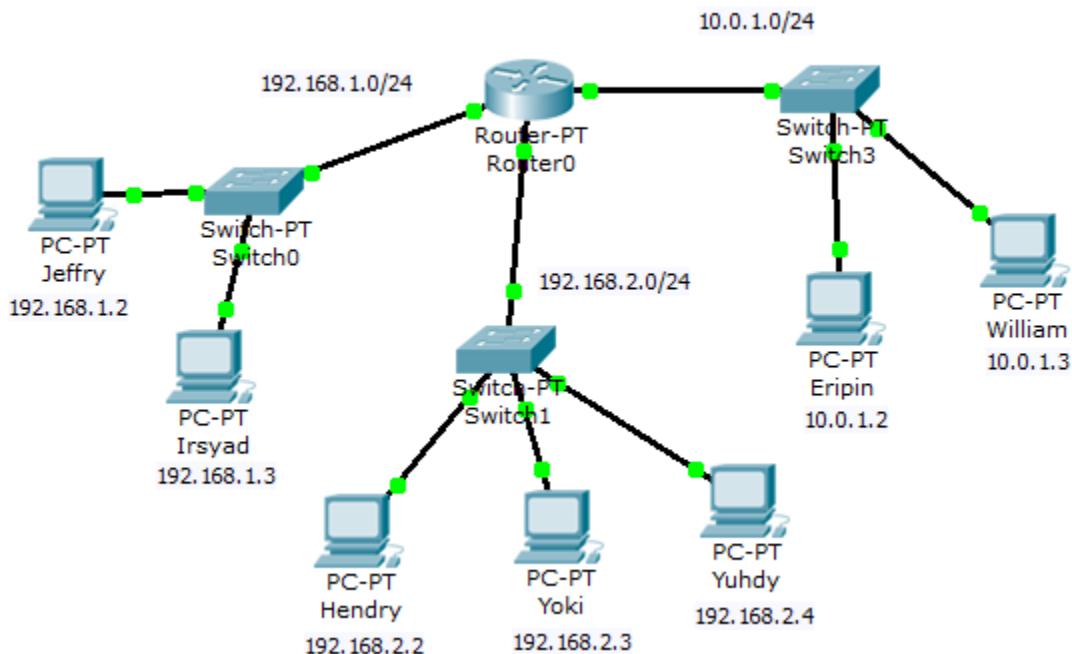
- Buatlah topologi seperti gambar dibawah ini



 Buatlah IP Standard Access-List dengan nomor 10 agar PC1 tidak bisa mengakses PC manapun.

**BINUS UNIVERSITY** | SOFTWARE LABORATORY CENTER

- Buatlah topologi seperti gambar di bawah.



Buatlah access-list dengan ketentuan sebagai berikut:

- Router akan menolak semua paket yang berasal dari PC Jeffry.
- Router akan menolak paket dari PC Yoki dan PC Yuhdy yang akan menuju PC Irsyad.
- Jaringan 10.0.1.0 hanya menerima paket ICMP yang berasal dari jaringan 192.168.2.0. (beri nama “icmp-jar2” untuk aturan ini).



## **Chapter 07**

### **VLAN**



## 7.1. VLAN

VLAN (Virtual LAN) merupakan cara untuk membagi suatu jaringan menjadi seolah-olah berbeda jaringan dengan cara membagi broadcast domain. Setiap VLAN memiliki nomor dan nama untuk identifikasi. Setiap host yang berada dalam suatu nomor VLAN hanya dapat berkomunikasi dengan host lain yang memiliki nomor VLAN yang sama.

VLAN biasanya dibuat pada switch, dan dipasangkan di interface pada switch. Untuk memasangkan VLAN pada switch, terdapat 2 mode yaitu:

### 1. Mode Access

Mode access hanya dapat melewaskan (tag) 1 vlan, contoh penggunaannya adalah untuk perangkat *end device* (PC, Laptop, ...) atau ke switch non-manageable atau wireless.

### 2. Mode Trunk

Mode trunk dapat melewaskan 2 vlan atau lebih (beberapa), contoh penggunaannya adalah untuk koneksi antar switch dengan beberapa vlan.

## 7.2. Contoh kasus VLAN

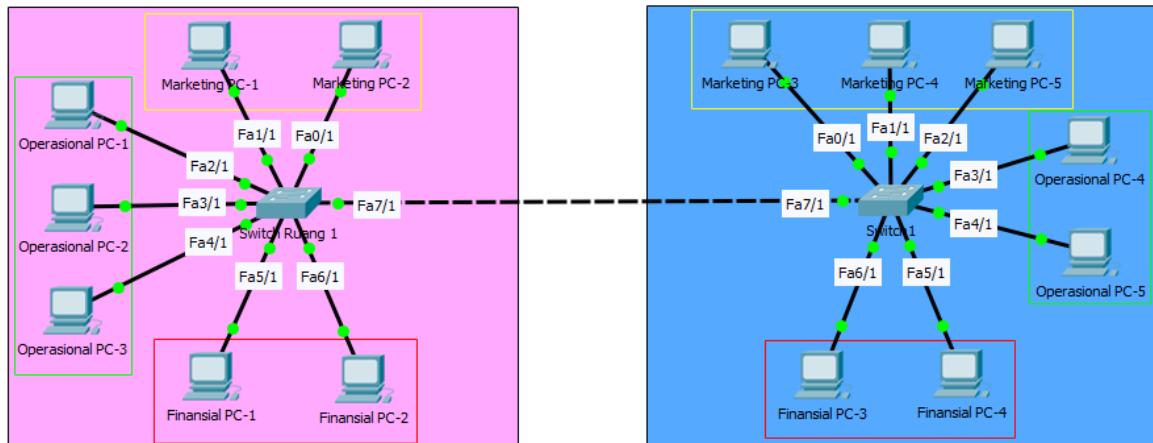
Terdapat suatu jaringan 192.168.1.0/24 yang ingin dibagikan untuk 3 divisi:

1. Divisi operasional, menggunakan range IP 192.168.1.10 – 192.168.1.50
2. Divisi marketing, menggunakan range IP 192.168.1.110 – 192.168.1.150
3. Divisi finansial, menggunakan range IP 192.168.1.210 – 192.168.1.250

Terdapat 2 ruang dimana masing-masing ruang memiliki 1 buah switch dan switch kedua ruang tersebut saling terhubung, spesifikasi ruangannya adalah sebagai berikut:

1. Ruang 1
  - Terdapat 3 komputer untuk divisi operasional
  - Terdapat 2 komputer untuk divisi marketing
  - Terdapat 2 komputer untuk divisi finansial
2. Ruang 2
  - Terdapat 2 komputer untuk divisi operasional
  - Terdapat 3 komputer untuk divisi marketing
  - Terdapat 2 komputer untuk divisi finansial

Berdasarkan requirement di atas, buatlah agar komputer-komputer untuk divisi yang sama dapat saling terhubung walaupun berbeda ruang, dan komputer untuk divisi yang berbeda tidak dapat saling terhubung!



Jawab:

### 1. Buat VLAN untuk masing-masing divisi

Pembuatan VLAN dilakukan pada switch, jadi kita akan membuat VLAN untuk masing-masing divisi di **Switch Ruang 1** dan **Switch Ruang 2**.

- **Cara 1 (Menggunakan Command)**

1. Klik Switch Ruang 1 => Pilih tab CLI => Masuk ke configure terminal

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

2. Buat VLAN menggunakan command berikut:

```
Switch(config)#vlan 10
Switch(config-vlan)#name Operasional
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Finansial
Switch(config-vlan)#exit
Switch(config)#
```

Penjelasan command:

1. **vlan [nomor vlan]** => membuat vlan dengan nomor yang ditulis

**vlan 10** => membuat vlan dengan nomor 10 dan masuk ke konfigurasi vlan  
**vlan 20** => membuat vlan dengan nomor 20 dan masuk ke konfigurasi vlan  
**vlan 30** => membuat vlan dengan nomor 30 dan masuk ke konfigurasi vlan  
Range nomor vlan yang diijinkan adalah 1-4094. Jika sudah masuk ke konfigurasi vlan, maka prompt akan berubah menjadi **Switch(config-vlan)#[/b]**.

2. **name [nama vlan]** => mengubah nama vlan

**name Operasional** => mengubah nama vlan menjadi Operasional untuk vlan 10

**name Marketing** => mengubah nama vlan menjadi Marketing untuk vlan 20

**name Finansial** => mengubah nama vlan menjadi Finansial untuk vlan 30

Untuk mengubah nama vlan, kita harus masuk ke konfigurasi dari vlan yang ingin diubah namanya dengan menggunakan command pertama. Pastikan prompt nya adalah Switch(config-vlan)#.

3. Cek apakah VLAN sudah terbuat menggunakan command berikut:

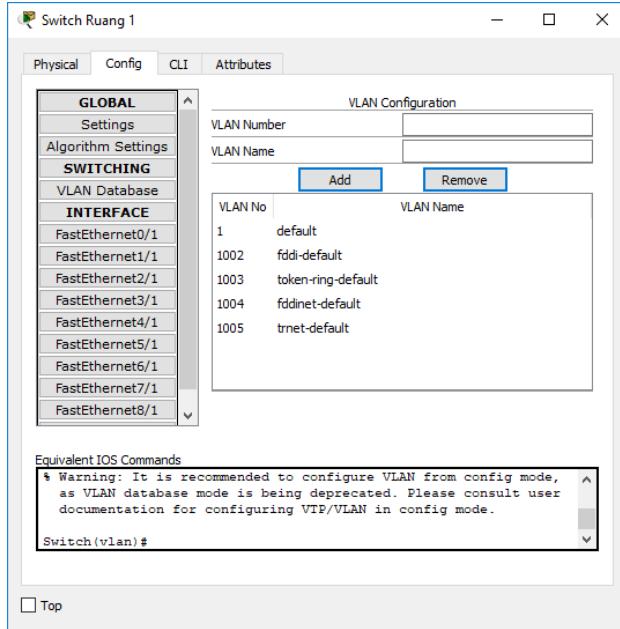
Switch#show vlan brief		
VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa1/1,
Fa2/1, Fa3/1		Fa4/1, Fa5/1,
Fa6/1, Fa7/1		Fa8/1, Fa9/1
10 Operasional	active	
20 Marketing	active	
30 Finansial	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Penjelasan command:

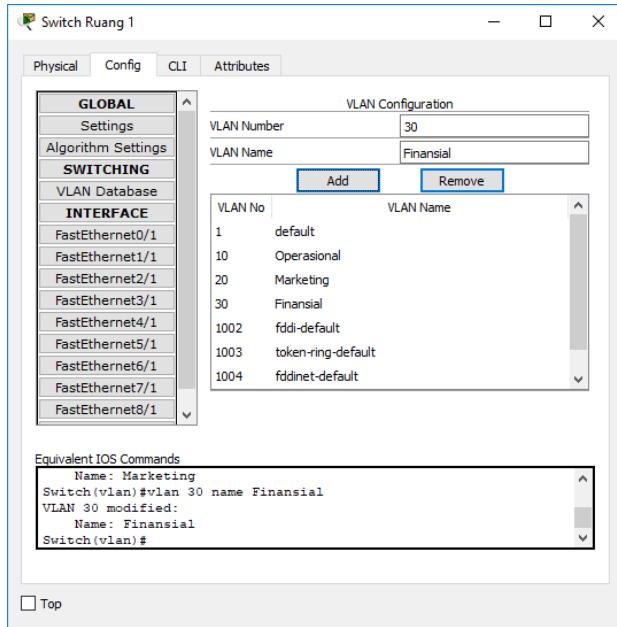
1. Keluar dari configure terminal dengan command “**exit**”, hingga prompt menjadi Switch#
2. Ketik “**show vlan brief**” untuk menampilkan semua VLAN yang ada di switch tersebut dan VLAN untuk masing-masing divisi sudah terbuat dengan nomor VLAN 10, 20, dan 30

### - Cara 2 (Lewat GUI)

1. Klik Switch Ruang 1 => Pilih tab Config => Pilih menu VLAN Database



2. Buat VLAN dengan memasukan **VLAN Number** dan **VLAN Name**, lalu tekan Add. Semua VLAN yang ada akan terlihat di list. Walaupun hal ini dilakukan menggunakan GUI, packet tracer secara otomatis mengeksekusi command via CLI. Dapat dilihat pada window CLI kecil di bagian bawah.



### 2. Assign VLAN ke masing-masing divisi

Untuk memberikan VLAN ke PC di masing-masing divisi, pertama kita harus mengetahui dulu nama interface di switch yang mengarah ke PC masing-masing divisi.

- Switch Ruang 1:
  - PC Divisi Marketing: Fa0/1, Fa1/1
  - PC Divisi Operasional: Fa2/1, Fa3/1, Fa4/1
  - PC Divisi Finansial: Fa5/1, Fa6/1
- Switch Ruang 2:
  - PC Divisi Marketing: Fa0/1, Fa1/1, Fa2/1
  - PC Divisi Operasional: Fa3/1, Fa4/1
  - PC Divisi Finansial: Fa5/1, Fa6/1
- **Cara 1 (Menggunakan Command)**

1. Klik Switch Ruang 1 => Pilih tab CLI => Masuk ke configure terminal

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

2. Masuk ke konfigurasi interface => Ubah port mode menjadi access => Set nomor vlan yang sesuai dengan command berikut

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

```

Ulangi langkah ini hingga semua interface yang mengarah ke PC di masing-masing divisi diberikan nomor vlan yang sesuai.

Penjelasan command:

1. **interface [interface]** => masuk ke konfigurasi interface

**interface fa0/1** => masuk ke konfigurasi interface fa0/1

Jika sudah masuk ke konfigurasi interface maka prompt akan berubah menjadi **Switch(config-if)#**

2. **switchport mode [mode]** => mengubah mode port

**switchport mode access** => mengubah mode port dari interface fa0/1 menjadi access

3. **switchport access vlan [nomor vlan]** => memberikan nomor vlan ke port

**switchport access vlan 20** => memberikan vlan nomor 20 untuk interface fa0/1

### Tambahan:

- Jika ingin masuk ke konfigurasi dari beberapa interface sekaligus, dapat menggunakan command berikut:

```
Switch(config)#interface range fa5/1 , fa6/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#

```

Penjelasan command:

1. **interface range [interface-1] , [interface-2] , ... , [interface-n]** => masuk ke konfigurasi beberapa interface

Jika sudah masuk ke konfigurasi interface maka prompt akan berubah menjadi Switch(config-if-range)#. Semua perubahan yang dilakukan di dalam sini akan berpengaruh pada semua interface yang dituliskan dalam range.

3. Cek apakah interface sudah diberi nomor vlan yang benar dengan command berikut

```
Switch#show vlan brief

VLAN Name                               Status      Ports
--- -----
1   default                             active     Fa7/1, Fa8/1,
Fa9/1
10  Operasional                         active     Fa2/1, Fa3/1,
Fa4/1
20  Marketing                           active     Fa0/1, Fa1/1
30  Finansial                           active     Fa5/1, Fa6/1
1002 fddi-default                       active
1003 token-ring-default                 active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#

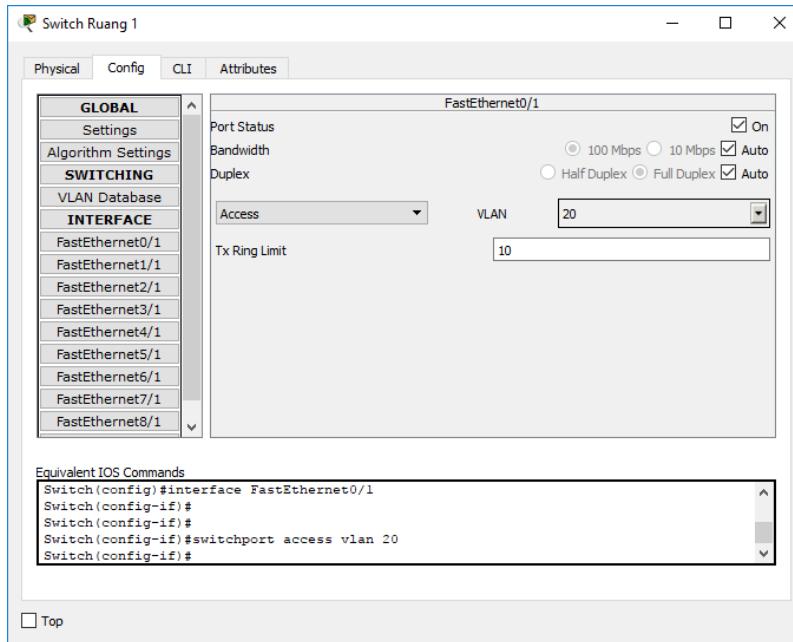
```

Penjelasan command:

1. Keluar dari configure terminal dengan command “**exit**”, hingga prompt menjadi Switch#
2. Ketik “**show vlan brief**” untuk menampilkan interface apa saja yang terpasang dalam masing-masing vlan. Pastikan sesuai dengan interface di masing-masing divisi.

### - Cara 2 (Lewat GUI)

1. Klik Switch Ruang 1 => Pilih tab Config => Pilih interface yang ingin diubah nomor vlan-nya => Ubah port mode nya menjadi access (secara default sudah access) => Ubah nomor vlan-nya sesuai dengan yang seharusnya



Ulangi langkah ini hingga semua interface yang mengarah ke PC di masing-masing divisi diberikan nomor vlan yang sesuai.

### 3. Ubah mode port dari interface yang menghubungkan antar Switch

Interface yang menghubungkan 2 buah Switch harus diberi mode **trunk** agar saat ada PC dari suatu divisi mengirim pesan, switch yang menerima pesan dapat meneruskan pesan ke switch lainnya, sehingga switch lainnya dapat meneruskan pesan ke PC dengan divisi yang sama walau berbeda switch. Karena mode trunk dapat melewatkkan 2 vlan atau lebih. Pertama kita harus mengetahui interface apa saja yang menghubungkan antar **Switch Ruang 1** dan **Switch Ruang 2**.

- Switch Ruang 1: Fa7/1
- Switch Ruang 2: Fa7/1

- **Cara 1 (Menggunakan Command)**

1. Klik Switch Ruang 1 => Pilih tab CLI => Masuk ke configure terminal

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

2. Masuk ke konfigurasi interface => Ubah port mode trunk

```
Switch(config)#interface fa7/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#[/pre]

```

Penjelasan command:

1. **interface [interface]** => masuk ke konfigurasi interface

**interface fa7/1** => masuk ke konfigurasi interface fa7/1

Jika sudah masuk ke konfigurasi interface maka prompt akan berubah menjadi **Switch(config-if)#[/pre]**

2. **switchport mode [mode]** => mengubah mode port

**switchport mode trunk** => mengubah mode port dari interface fa7/1 menjadi trunk

3. Set nomor vlan yang diijinkan lewat dengan command berikut

Agar pesan dari masing-masing divisi dapat diteruskan ke switch lain, maka nomor VLAN 10, 20, dan 30 harus ditambahkan ke list nomor vlan yang diijinkan lewat pada interface7/1 di **Switch Ruang 1** dan **Switch Ruang 2**. Secara default, mode port trunk akan mengijinkan semua nomor VLAN yang terdaftar di dalam switch tersebut.

- Menambahkan nomor vlan

```
Switch(config)#interface fa7/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#switchport trunk allowed vlan add 20
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#[/pre]
```

**switchport trunk allowed vlan add [nomor vlan]** => menambahkan nomor vlan ke list nomor vlan yang diijinkan

- Menghapus nomor vlan dari list

```
Switch(config)#interface fa7/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan remove 10
Switch(config-if)#+
```

**switchport trunk allowed vlan remove [nomor vlan]** => menghapus nomor vlan dari list nomor vlan yang diijinkan

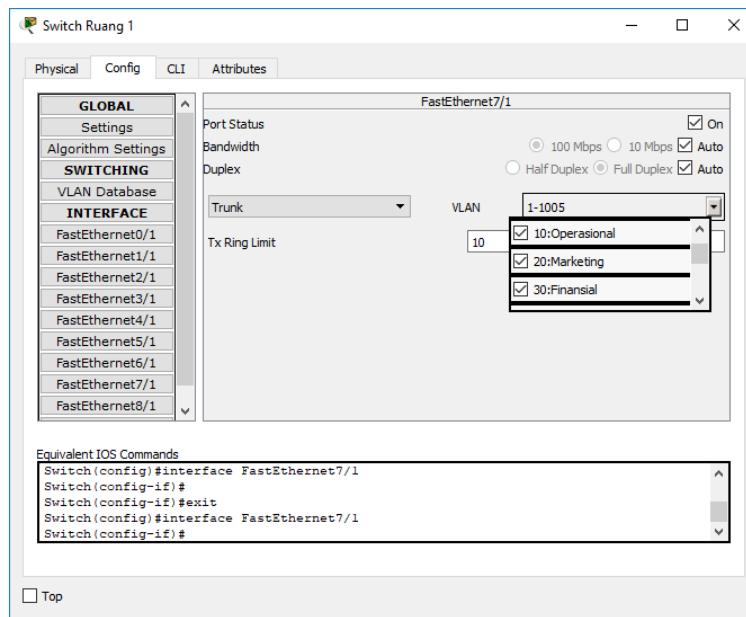
- Menambahkan range nomor vlan

```
Switch(config)#interface fa7/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10-30
Switch(config-if)#+
```

**Switchport trunk allowed vlan [lower range]-[upper range]** => menambahkan nomor vlan menggunakan range

#### - Cara 2 (Lewat GUI)

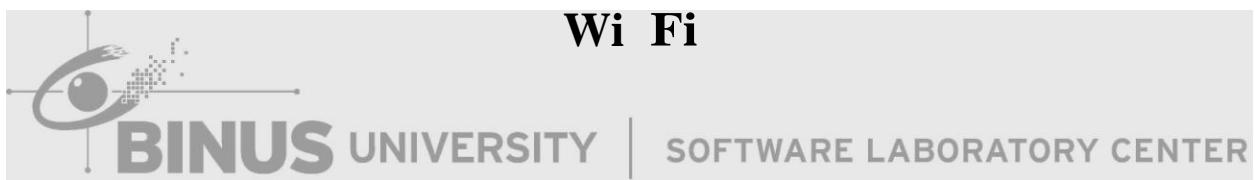
1. Klik Switch Ruang 1 => Pilih tab Config => Pilih interface FastEthernet7/1 => Ubah port modenya menjadi trunk => Set nomor vlan yang diijinkan lewat (nomor VLAN masing-masing divisi harus ditambahkan)



Lakukan langkah ini pada interface Fa7/1 di **Switch Ruang 1** dan **Switch Ruang 2**

## **Chapter 08** **(materi tambahan)**

### **Wi Fi**



## 8.1. WiFi



Wi-Fi (*Wireless Fidelity*) merupakan teknologi jaringan tanpa kabel yang menggunakan gelombang radio untuk mentransfer datanya. Wi-Fi tidak hanya digunakan pada komputer, tetapi juga pada alat-alat lain seperti *notebook*, *smartphone*, *mobile device*, *multimedia device*, dan lain-lain. Awalnya Wi-Fi ditujukan untuk penggunaan perangkat nirkabel dan jaringan Local Area Network (LAN), namun saat ini lebih banyak digunakan untuk penggunaan internet.

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Saat ini terdapat 5 variasi yaitu :

No	Spesifikasi	Kecepatan	Frekuensi Band	Kompatibilitas
1	802.11a	54 Mbps	5 GHz	a
2	802.11b	11 Mbps	2.4 Ghz	b
3	802.11g	54 Mbps	2.4 Ghz	b, g
4	802.11n	300 Mbps	2.4 Ghz	b, g, n
5	802.11ac	1.3 Gbps	5 Ghz	a, n

Untuk mengakses koneksi Wi-Fi terdapat 2 cara yaitu :

### 1. Ad-Hoc

Cara Ad-Hoc bekerja dengan cara menghubungkan beberapa komputer secara langsung, atau istilah lainnya *peer to peer*. Cara Ad-Hoc memiliki kekurangan yaitu hanya bisa menangani sedikit *client* 2 atau 3 komputer saja, koneksi yang tidak stabil, dan jangkauannya kecil. Kelebihannya yaitu murah, karena tidak memerlukan alat tambahan sebagai konsentrator seperti *access point*.

### 2. Infrastruktur

Menggunakan *Access Point* sebagai konsentrator untuk menghubungkan dan mengatur lalu lintas data. Kekurangannya yaitu memerlukan biaya untuk perangkat Access Point. Kelebihannya yaitu dapat menangani banyak client, koneksi relatif stabil, jangkauan relatif luas (tergantung perangkatnya).

### Kelebihan Wi-Fi

1. Kemudahan akses. Pengguna dapat terhubung ke jaringan dalam suatu area secara bersamaan, tanpa direpotkan oleh kabel-kabel.
2. Pengguna yang ingin terhubung ke jaringan cukup membawa PDA, *smartphone*, *notebook* atau *tablet PC* yang berkemampuan Wi-Fi.
3. Banyaknya *acces point* atau *hotspot* di area-area seperti *café*, *restaurant*, dan lain-lain.

### Kekurangan Wi-Fi

1. Memiliki resiko di-*hack* oleh hacker untuk mencuri *password* Wi-Fi
2. Penggunaan *battery* yang lebih tinggi jika dibandingkan dengan penggunaan standar.
3. Memiliki cakupan area yang terbatas
4. Performa kurang stabil dibandingkan dengan penggunaan kabel karena faktor gangguan, kekuatan sinyal, dsb.

## 8.2. Konsep konfigurasi WiFi

Pada dasarnya, terdapat 3 faktor utama konfigurasi wifi supaya dapat terhubung, yaitu:

### 1. Frekuensi

Perangkat-perangkat yang akan dihubungkan melalui wireless haruslah bekerja pada frekuensi yang sama. Hal ini juga mempengaruhi kompatibilitas standard wireless, contohnya wireless standard 802.11a yang bekerja di frekuensi 5Ghz tidak akan bisa terhubung dengan perangkat yang bekerja dengan standard 802.11b yang mana bekerja di frekuensi 2.4 Ghz. Selain itu frekuensi juga berhubungan dengan interference jaringan wireless jika di area tersebut banyak perangkat yang menggunakan perangkat wireless di channel frekuensi yang sama atau berpotongan. Perangkat wireless client akan mengikuti channel frekuensi yang telah diset pada wireless access point.

### 2. SSID

SSID atau Service Set Identifier adalah identitas dari suatu jaringan wireless yang dipancarkan oleh sumber wireless. SSID haruslah sama supaya perangkat wireless dapat terhubung.

### 3. Security

Saat ini terdapat berbagai jenis security untuk mengamankan wireless. Berdasarkan perkembangannya saat ini terdapat security mode WEP, WPA, hingga yang terakhir WPA2. Untuk dapat terhubung perangkat wireless harus dapat memenuhi kebutuhan security yang dikonfigurasi, misalnya pada security WEP maka password yang digunakan harus sesuai, pada WPA2-enterprise maka username dan password harus valid.

Ada beberapa tipe keamanan wireless, yaitu:

- a) *No Authentication (Disabled)* yaitu jaringan yang dibuat tanpa autentikasi atau dengan kata lain pengguna dapat mengakses jaringan hotspot anda tanpa harus memasukkan *password*.
- b) WEP (*Wired Equivalent Privacy*) yaitu tipe pengamanan jaringan yang lebih lama, yang dapat mendukung perangkat-perangkat lama. Cara kerja dari tipe ini yaitu informasi yang telah dienkripsi dengan *key* ini dikirimkan dari satu komputer ke komputer lain melalui jaringan. Sehingga, WEP mudah di-crack.
- c) WPA dan WPA2 (*Wi-Fi Protected Access*) yaitu WPA mengenkripsi informasi dan memastikan bahwa kunci keamanan jaringan belum diubah. WPA juga mengautentikasi pengguna untuk membantu memastikan bahwa hanya orang yang berwenang yang dapat mengakses jaringan. Terdapat 2 tipe autentikasi WPA yaitu WPA dan WPA2. WPA dibuat untuk bekerja dapat bekerja dengan semua adaptornya *wireless*, tetapi WPA juga mungkin tidak dapat bekerja dengan *router* lama atau *access point*. WPA2 lebih aman dari WPA, tetapi tidak dapat bekerja dengan beberapa *network adapter* yang lama. WPA dibuat untuk digunakan dengan sebuah server autentikasi 802.1X, yang mendistribusikan *key* yang berbeda untuk setiap pengguna. Hal ini disebut sebagai WPA-Enterprise atau WPA2-Enterprise. Hal ini juga dapat digunakan dalam mode *pre-shared key* (PSK), dimana setiap pengguna diberikan *passphrase* yang sama. Hal ini disebut sebagai WPA-Personal atau WPA2-Personal.

Mode Personal dan Enterprise:

- a) Mode personal biasanya digunakan untuk jaringan wireless kecil seperti untuk rumah. Pada mode personal, suatu password yang disebut *Pre-Shared Key* (PSK) digunakan oleh user saat mau terhubung ke jaringan dan semua user menggunakan password yang sama.

- b) Mode enterprise biasanya digunakan untuk jaringan di lingkungan kerja. Pada mode enterprise, data autentikasi diatur secara terpusat pada RADIUS server. Keuntungan dalam menggunakan mode ini adalah setiap user dapat diberikan hak akses yang berbeda, tergantung dari hak akses user yang mereka gunakan untuk terhubung ke jaringan.

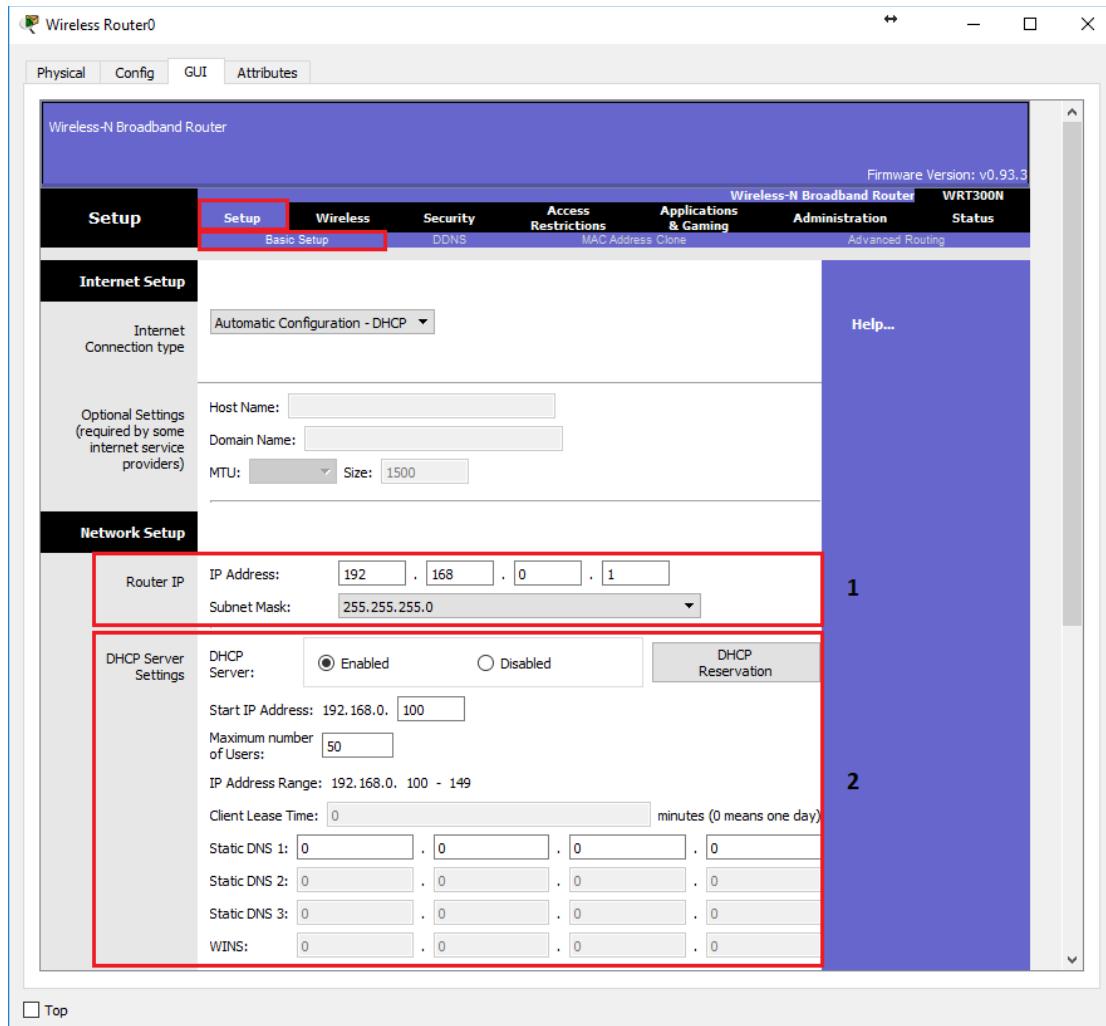
### 8.3. Setting WiFi di Packet Tracer

#### A. Setting Router Wireless

1. Buat sebuah wireless router (WRT300N)



2. Klik Router yang sudah terbuat, lalu masuk ke tab GUI untuk melakukan setting wireless



Penjelasan:

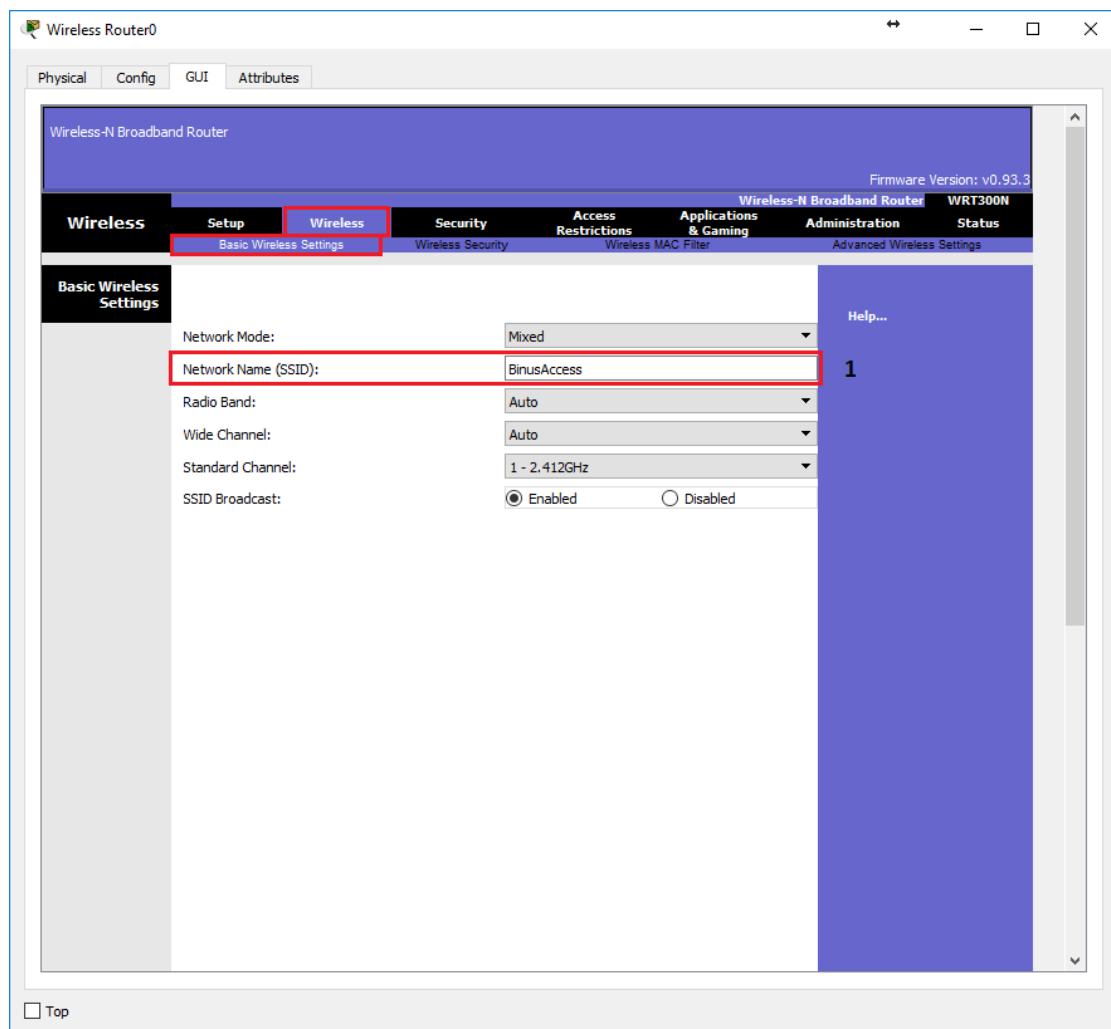
### 1. Router IP

- IP Address: IP address dari router, akan menjadi IP gateway dari client yang terhubung

- Subnet Mask: Subnet Mask dari IP Router

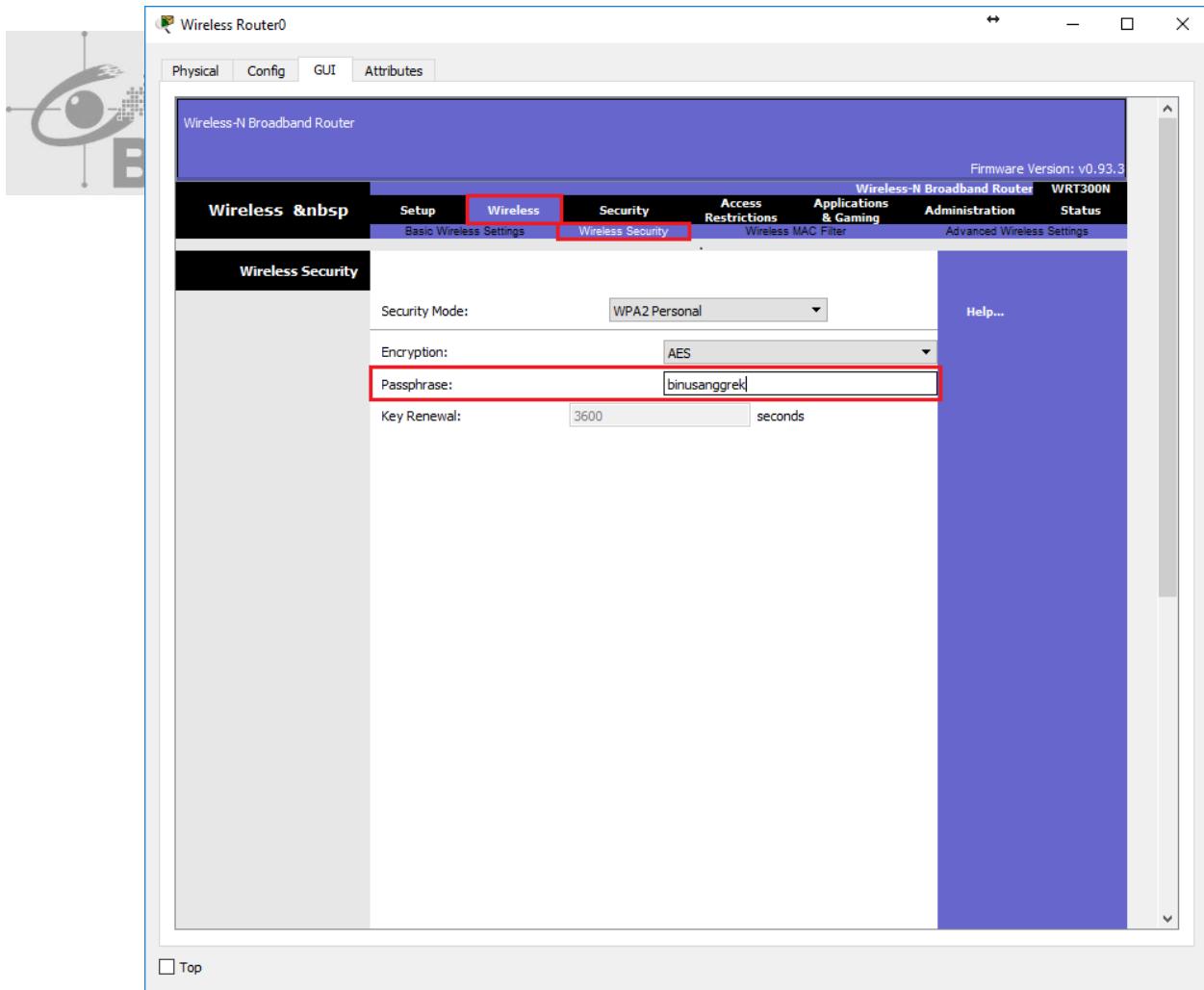
### 2. DHCP Server Settings

- Enable / Disable DHCP
- Start IP Address: Menentukan IP address awal yang akan diberikan untuk client yang terhubung
- Maximum number of Users: Jumlah user yang dapat terhubung secara bersamaan
- Static DNS: IP DNS server, akan menjadi DNS server dari client yang terhubung



Penjelasan:

- SSID: Mengubah nama jaringan dari WiFi

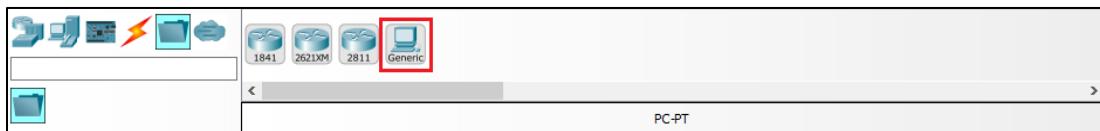


Penjelasan:

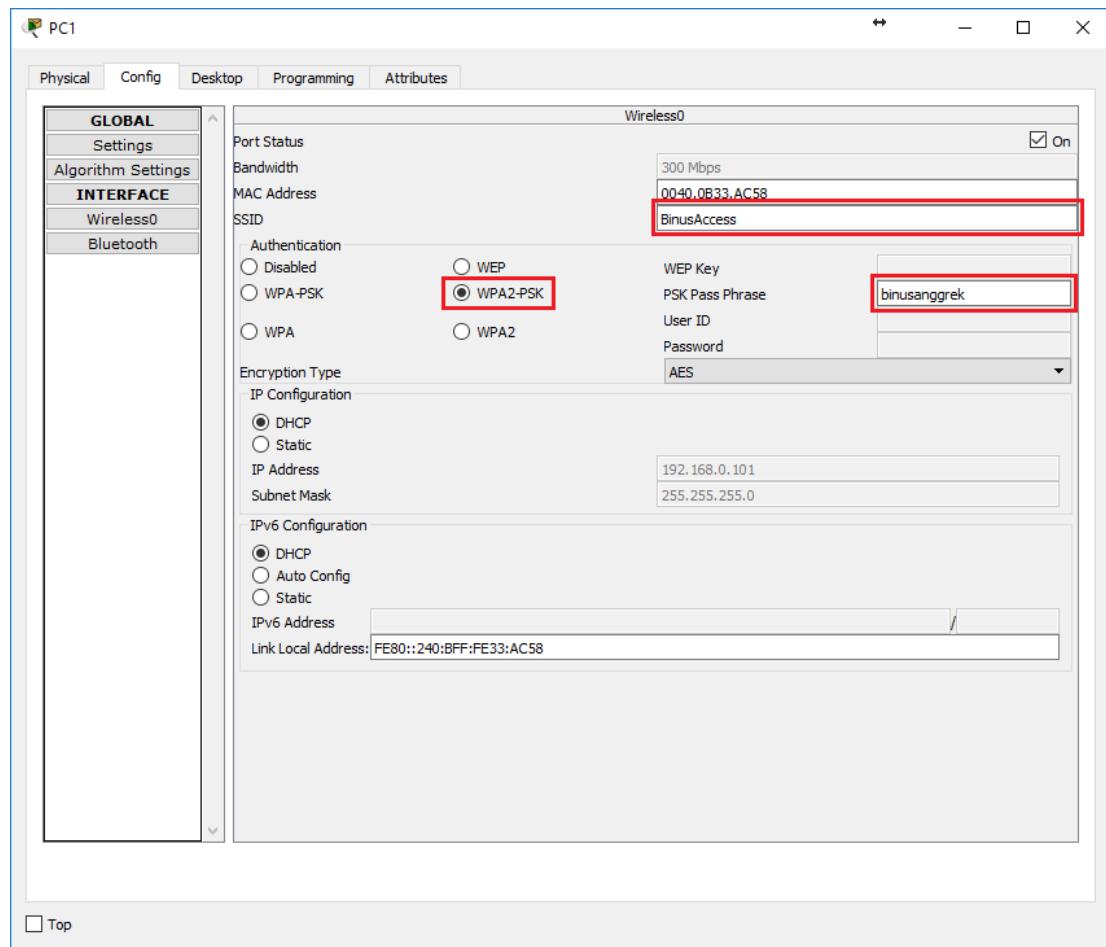
- Passphrase: password untuk terhubung ke wifi

## B. Terhubung ke WiFi

1. Buat sebuah wireless PC



2. Klik PC yang sudah dibuat => pilih tab Config => pilih interface Wireless lalu masukan data WiFi yang ingin dihubungkan



Penjelasan:

- SSID: SSID dari WiFi yang ingin dihubungkan, sebelumnya SSID nya di set menjadi BinusAccess
- Authentication: sebelumnya kita memilih WPA2 Personal, maka disini kita pilih yang WPA2-PSK (PSK adalah *Pre-Shared Key*)
- PSK Pass Phrase: password yang digunakan untuk terhubung ke jaringan

## **REFERENCES**

Benedetti, R., Anderson, A., *Head First Networking*, O'Reilly Media, 2009.

Tittel, Ed., *Schaum's Outline of Computer Networking*, Mc. Graw Hill, 2002.

<https://www.nusa.net.id/blog/article/standar-protokol-jaringan-wireless-ieee-802-11/>

