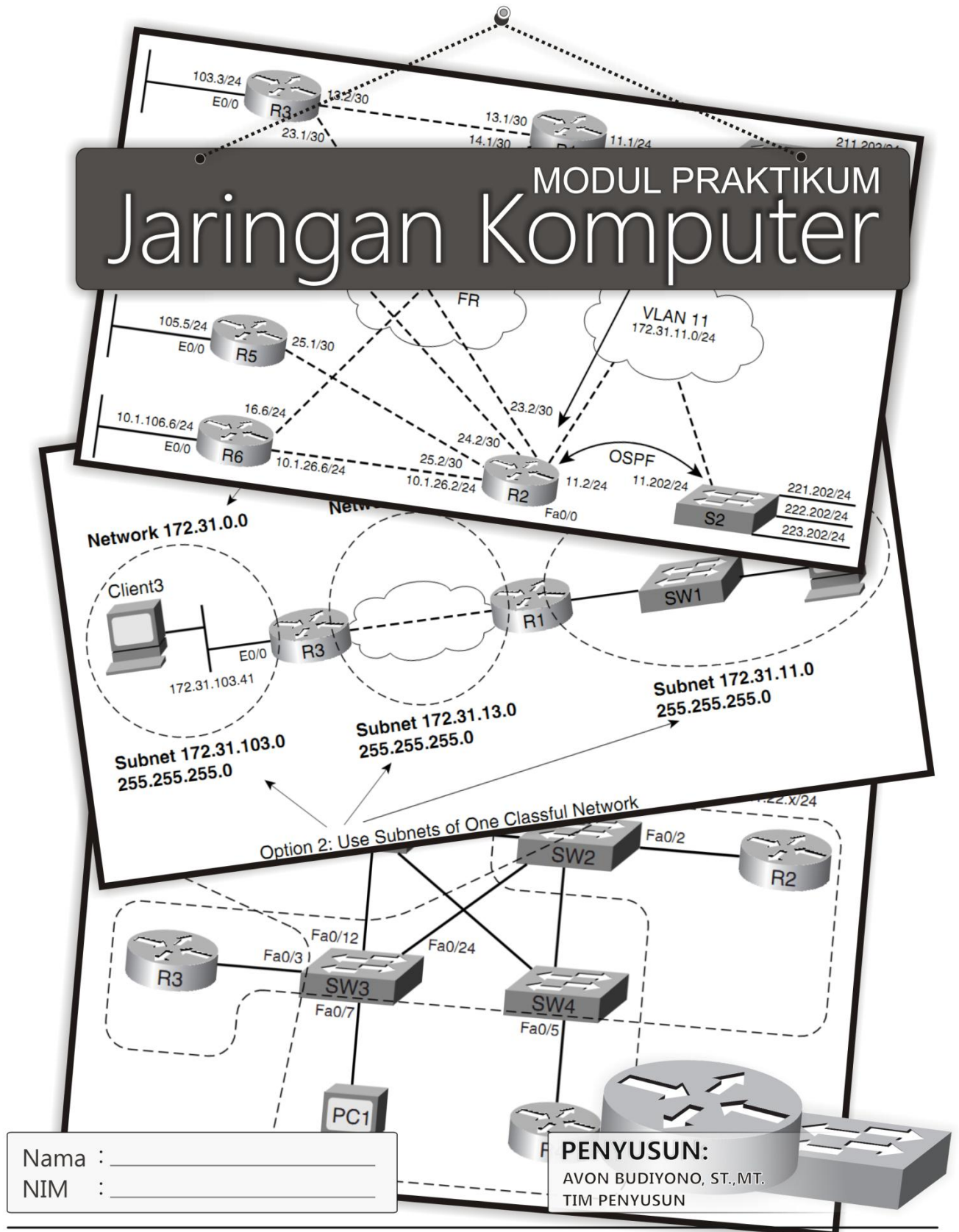


MODUL PRAKTIKUM Jaringan Komputer



Nama : _____
NIM : _____

PENYUSUN:

AVON BUDIYONO, ST.,MT.
TIM PENYUSUN



Laboratorium
Sistem Operasi dan Jaringan Komputer
Program Studi Sistem Informasi
Fakultas Rekayasa Industri
Institut Teknologi Telkom

Headquarter
Gedung H110 (Belakang GSG)
Jl. Telekomunikasi No. 1 Terusan Buah Batu, Dayeuh Kolot, Bandung
Jawa Barat, Indonesia

<http://sisjarlabs.org>



**INSTITUT TEKNOLOGI
TELKOM**

MODULE 1

Router Basic Configuration and Static Routing

I. Tujuan praktikum

1. Praktikan mampu menguasai teori konseptual router.
2. Praktikan mampu menguasai berbagai perintah dasar pada router.
3. Praktikan mampu mengkonfigurasi router pada jaringan sederhana.
4. Praktikan dapat membuat konfigurasi dalam sebuah simulator (Packet Tracer).
5. Praktikum mampu mengoperasikan piranti Cisco (Router dan IOS).
6. Membuat jaringan sederhana berdasarkan diagram topologi jaringan yang dibuat.
7. Menghapus konfigurasi ketika *startup* dan *me-load* router ke kondisi awal.
8. Menjalankan perintah-perintah standar konfigurasi pada router.
9. Mengkonfigurasi dan mengaktifkan interface Serial dan Ethernet
10. Mendapatkan informasi untuk menemukan sebab dari koneksi yang kurang baik antar *device*.
11. Mengkonfigurasi *static route* menggunakan *intermediate address* dan *exit interface*, serta membandingkan hasilnya.
12. Mengkonfigurasi *default static route* dan *summary static route*
13. Mendokumentasikan implementasi jaringan

II. Alat dan bahan

1. Set PC Desktop/Notebook
2. OS Berbasis Windows (XP/Vista/Seven)
3. Cisco Packet Tracer (Preinstalled)
4. Flash Player Plugin (Preinstalled)
5. Cisco CCNA Discovery (CCNA 2)

III. Konfigurasi Dasar Router

Perkembangan teknologi informasi dahulu tidaklah sepesat masa sekarang. Penyebaran informasi yang lambat dianggap menjadi salah satu alasan yang paling berpengaruh. Pada saat itu, jaringan yang terpisah-pisah serta berbeda jenis membuat informasi tidak bisa menyebar secara cepat antar sumber informasi. Selain itu, kemampuan lingkup jaringan pada saat itu masih terbatas dalam jarak yang begitu kecil sehingga sulit dan mahal sekali membuat jaringan yang bisa mencakup wilayah yang lebih luas.

Dengan kondisi yang seperti itulah muncul gagasan untuk menciptakan alat yang mampu mengakomodasi jaringan yang lebih luas dan mempersatukan berbagai jenis jaringan, hingga nantinya lahirlah alat yang dinamakan router. Router inilah yang menjawab permasalahan keterbatasan jarak dan perbedaan jenis jaringan dalam membuat suatu jaringan yang mencakup wilayah besar.

Pengertian Router:

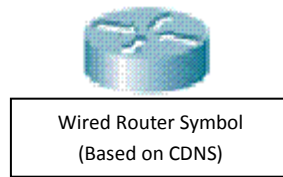
Router adalah network layer device yang mampu menghubungkan dua jaringan lokal (LAN) berbeda atau lebih (internetwork) dalam sebuah lingkup yang lebih luas (WAN) sehingga memungkinkan pertukaran informasi di dalamnya. Dalam sudut pandang berbeda, router memungkinkan transfer paket data dari suatu jaringan ke jaringan lainnya berdasarkan protokol yang bekerja pada OSI layer network (TCP/IP layer internet).

Sesuai layer tempat router berada, maka cara kerja dari router memiliki standarisasi protokol yang berlaku pada layer tersebut. Protokol yang dimaksud adalah TCP/IP Protocol, oleh sebab itu semua router bekerja dengan berbasis IP sekalipun modul interface pada layer di bawahnya berbeda jenis.

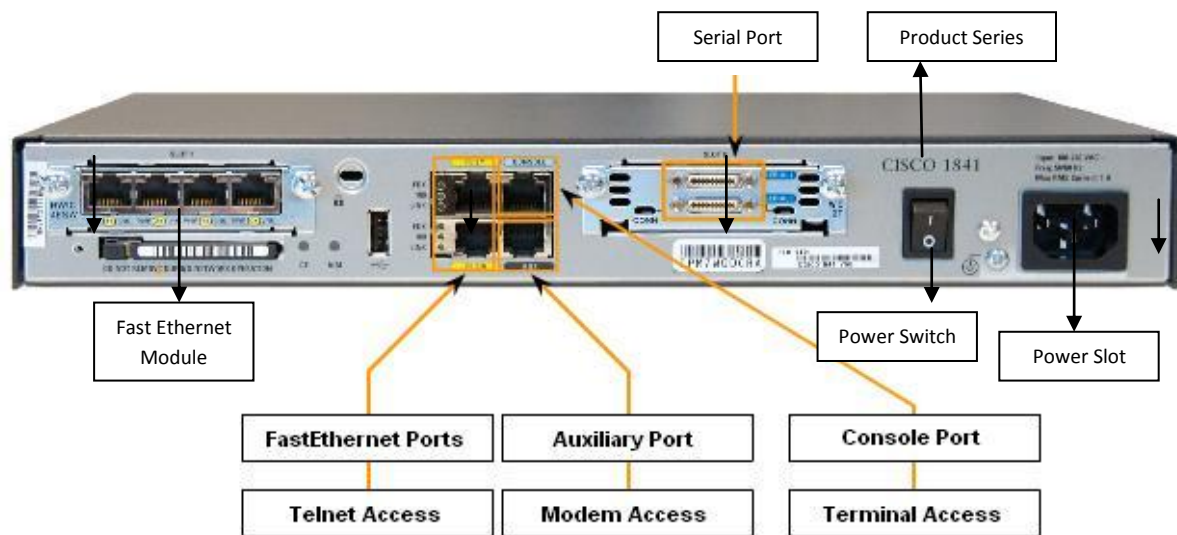
Fungsi Router:

1. Sebagai intermediary device bagi end-user devices dalam menyediakan sambungan ke jaringan luar yang lebih luas.
2. Menghubungkan dua buah jaringan atau lebih dengan interface module yang berbeda.
3. Menentukan jalur terbaik dalam mengirimkan paket data antar jaringan, dan lain sebagainya.

Simbol Router pada Common Data Network Symbols (Berlaku di Seluruh Dunia)



Salah Satu Penampakan Router, sampel CISCO router (Tampak Belakang)



Pengenalan Perusahaan Cisco

Cisco System Incorporation merupakan salah satu vendor terbesar di dunia yang menyediakan solusi lengkap dalam hal jaringan komputer. Berbagai piranti yang dirilis oleh Cisco mendominasi infrastruktur jaringan komputer di dunia. Lebih dari itu Cisco juga membuat standarisasi jaringan komputer yang menjadi acuan pokok berbagai lembaga di dunia baik secara teoretis maupun praktis.

Cisco pun memiliki akademi pendidikan jaringan komputer. Bagi mereka yang berhasil lulus akan diberikan sertifikat oleh Cisco yang diakui secara global bahwa mereka telah mampu menguasai jaringan komputer baik secara teori maupun implementasi di lapangan.

Kebutuhan akan tenaga profesional jaringan komputer bersertifikat khususnya Cisco begitu diminati oleh banyak perusahaan di dunia. Oleh sebab itu, praktikum jaringan komputer di Sisjar Laboratorium mengacu pada Cisco Academy dengan

harapan mampu menghasilkan praktikan dengan kualitas yang mendekati profesional pemegang sertifikat Cisco serta memiliki kompetensi hardskill dan softskill agar bisa bersaing di dunia kerja kelak.

Jika Anda memiliki minat di bidang jaringan komputer, manfaatkan momentum ini sebaik mungkin!

Pengenalan Cisco IOS (Internetwork Operating System)

Sama halnya dengan komputer, sebuah router tidak berfungsi apa-apa tanpa ada sistem operasi bersamanya. Khusus untuk network device yang dimiliki Cisco, telah disiapkan sebuah sistem operasi yang secara universal bisa dipakai di semua device Cisco. Dengan adanya Cisco IOS, kita dapat mengkonfigurasi router Cisco untuk berbagai keperluan.

Cisco IOS dapat dioperasikan dengan interface terminal khusus yang telah dibuat oleh Cisco, dengan kata lain berbasis CLI (Command Line Interface). Tidak seperti OS pada komputer, ukuran IOS tidak begitu besar dan tersimpan dalam sebuah flash memory. Penggunaan flash memory memungkinkan IOS dapat beroperasi lebih cepat, menyediakan non-volatile storage, hingga pemutakhiran versi. Pembelajaran beberapa syntax dasar IOS adalah syarat wajib untuk bisa mengkonfigurasi router Cisco.

Pengenalan Cisco Packet Tracer

Cisco Packet Tracer merupakan aplikasi simulasi yang disediakan oleh Cisco untuk membangun jaringan komputer virtual dengan berbagai piranti buatan Cisco. Hal ini sangat menguntungkan dari berbagai aspek bagi mereka yang memiliki hasrat TERBATAS (waktu, biaya, dan resiko) dalam menguasai materi praktis sertifikasi Cisco. Keberadaan Cisco Packet Tracer diharapkan memberikan angin segar bagi mereka yang ingin bereksperimen kreatif mungkin dengan memanfaatkan berbagai piranti Cisco. Tentunya hal ini memudahkan juga bagi mereka yang ingin serius menempuh jalur sertifikasi agar prosentase peluang kelulusan dapat optimal.

Preview dari Interface Cisco IOS:

```
Router0
Physical Config CLI
IOS Command Line Interface

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :
##### [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

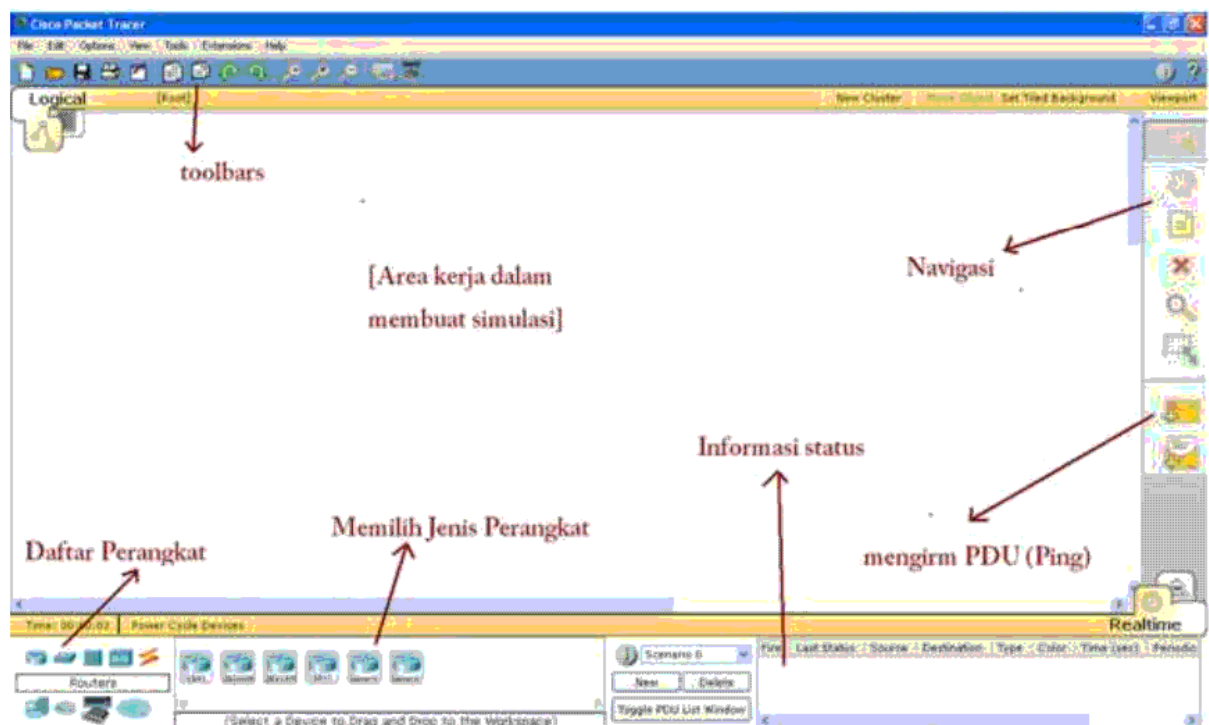
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Preview dari Cisco Packet Tracer:



Tahapan Pengoperasian IOS

Setelah sebelumnya mengenal fungsi dan peran IOS, kini tiba saatnya kita mempelajari bagaimana mengoperasikan router dengan mengendalikannya melalui IOS. Kita akan mulai dari beberapa tahapan, mulai dari persiapan hingga pada posisi router siap dikonfigurasi.

Ada 3 Cara untuk mengakses IOS:

1. Console

Disediakan port console untuk mengakses IOS secara langsung dari router. Walaupun ini untuk mengkonfigurasi secara jarak jauh (remote), tetapi console satu-satunya cara mengkonfigurasi jika router mengalami hang atau error.

2. Telnet/SSH

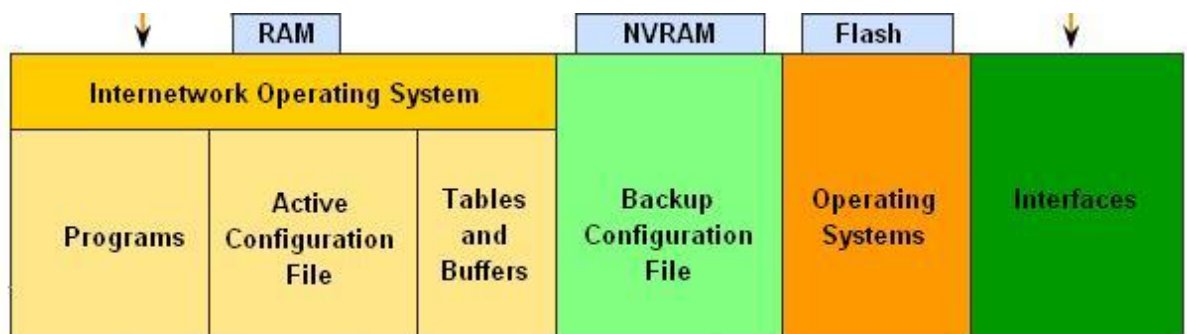
Cara ini dikategorikan remote, dalam arti harfiah IOS tidak diakses secara langsung tetapi melalui jaringan lokal (LAN) yang terhubung langsung dengan router. Bisa juga diartikan melakukan remote terhadap default gateway.

3. AUX Port

Cara ini lebih mendekati pengertian remote, karena IOS bisa diakses dari jarak yang sangat jauh menggunakan koneksi dial-up dengan modem yang tersambung ke router. Disisi lain, Aux dapat dijadikan alternatif jika terjadi kerusakan pada port console.

Prakonfigurasi Router

Ada dua piranti lunak yang terpasang pada sebuah router, yang pertama IOS itu sendiri yang terdapat pada flash memory. Kemudian ada configuration file yang tersimpan pada NVRAM. Piranti yang kedua berfungsi sebagai checkpoint agar setelan router yang telah dibuat dapat dipakai lagi sekalipun router mengalami restart atau crash. Perlu diingat dalam membuat checkpoint agar selalu terkini sehingga jika router mati atau crash dapat kembali ke kondisi terakhir. Untuk lebih jelas dapat dilihat pada bagan di bawah ini:



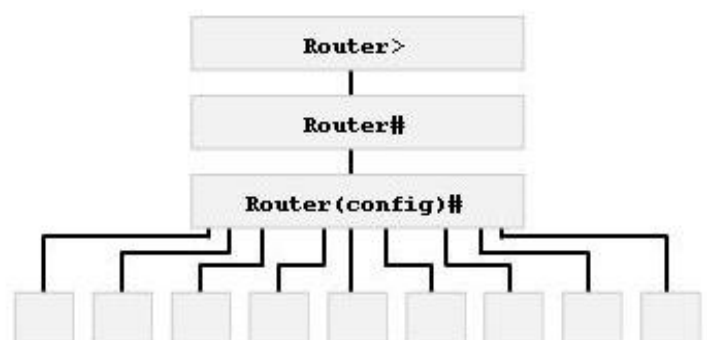
Hirarki pada IOS :

User EXEC mode

Privileged EXEC mode

Global configuration mode

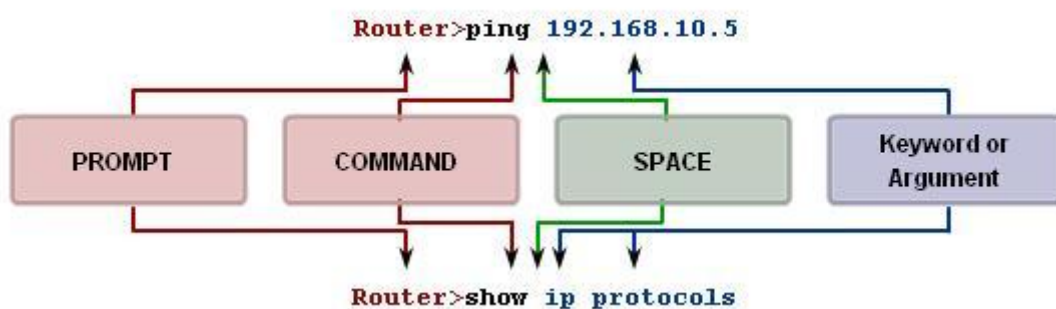
Specific configuration mode



Mirip dengan vi editor pada UNIX, IOS pun memiliki mode akses yang bertingkat, yaitu:

- User Executive Mode (User EXEC)
Perintah dasar yang bisa dilakukan oleh semua user termasuk dalam mode ini. Misalnya: ping, enable (untuk masuk mode privileged), dsb. Pada router ditandai dengan prompt **router>**
- Privileged Executive Mode (Privileged EXEC)
Semua perintah user EXEC termasuk dalam mode ini ditambah dengan beberapa syntax lain yang hanya bisa dipakai oleh admin. Misalnya: configure (untuk masuk mode global configuration), dsb. Pada router ditandai dengan prompt **router#**
- Global Configuration Mode (config)
Global configuration memuat berbagai syntax yang mengatur kerja internal device Cisco secara umum (maka disebut global). Misalnya: karena yang kita ingin konfigurasi adalah router, maka contohnya adalah **router rip** (untuk mengatur router bekerja dengan rip) Pada router ditandai dengan prompt **Router(config)#**
- Specific Configuration Modes (config-if)
Disini syntax IOS yang spesifik sesuai untuk device yang terkait. Semisal router, maka hanya syntax untuk mengatur kerja router saja yang dapat diperintahkan. Misalnya syntax network, version, dsb. Pada router ditandai dengan prompt **Router(config-router)#**

Struktur Syntax IOS pada CLI (Command Line Interface)



IOS Error Message and Error Handling

Sama halnya dengan kebanyakan penggunaan CLI, seorang user maupun admin sekalipun tidak akan luput dari kesalahan dalam membentuk syntax. Setidaknya ada tiga kesalahan yang umum dilakukan oleh mereka:

- Ambiguous command
syntax ini tidak dikenali oleh IOS.
Contoh: `JtextLabel()`
- Incomplete command
syntax ini sudah benar tetapi argumen tidak ada atau masih salah.
Contoh: `clock set <tanpa ada argumen>`
- Incorrect command
syntax sudah lengkap hanya saja tidak sesuai format yang dikenali.
Contoh: `clock set 12:12:12 25 6`(angka 6 akan ditandai salah harusnya 'MAY')

Perintah – perintah konfigurasi dasar Cisco IOS Router

Purpose	Command
Enter the global configuration mode.	configure terminal Example: Router> enable Router# <code>configure terminal</code> Router(config)#
Specify the name for the router.	hostname name Example: Router(config)# hostname Router1 Router(config)#
Specify an encrypted password to prevent unauthorized access to the privileged exec mode.	enable secret <i>password</i> Example: Router(config)# enable secret cisco Router(config)#
Specify a password to prevent	password <i>password</i>

unauthorized access to the console.

login

Example:

```
Router(config)# line con 0  
Router(config-line)# password class  
Router(config-line)# login  
Router(config)#
```

Specify a password to prevent
unauthorized telnet access.

password*password*

login

Example:

```
Router(config)# line vty 0 4  
Router(config-line)# password class  
Router(config-line)# login  
Router(config-line)#
```

Router vty lines: 0 4

Switch vty lines: 0 15

Configure the MOTD banner.

Banner motd %

Example:

```
Router(config)# banner motd %  
Router(config)#
```

Configure an interface.

Example:

Router- interface is OFF by default

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

Switch- interface is ON by default

```
Router(config-if)# description  
description
```

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

address mask

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

```
Router(config-if)#
```

Save the configuration to NVRAM.

copy running-config startup-config

Example:

```
Router# copy running-config startup-  
config
```

```
Router#
```

IV. Routing Statis

Static Routing merupakan proses pemilihan jalur yang dilakukan secara manual, dengan cara menambahkan route – route pada routing table di setiap router. Dilakukan oleh administrator jaringan.

Routing statis memiliki keuntungan – keuntungan sebagai berikut :

- Tidak ada overhead (waktu pemrosesan) pada CPU router, yang berarti anda mungkin dapat membeli router yang lebih murah dari pada router dinamis.
- Tidak ada bandwidth yang digunakan antara router, yang berarti anda dapat menghemat uang untuk link WAN.
- Routing statis menambah keamanan, karena administrator dapat memilih untuk mengizinkan akses routing ke network tertentu saja.

Routing statis memiliki kerugian – kerugian sebagai berikut :

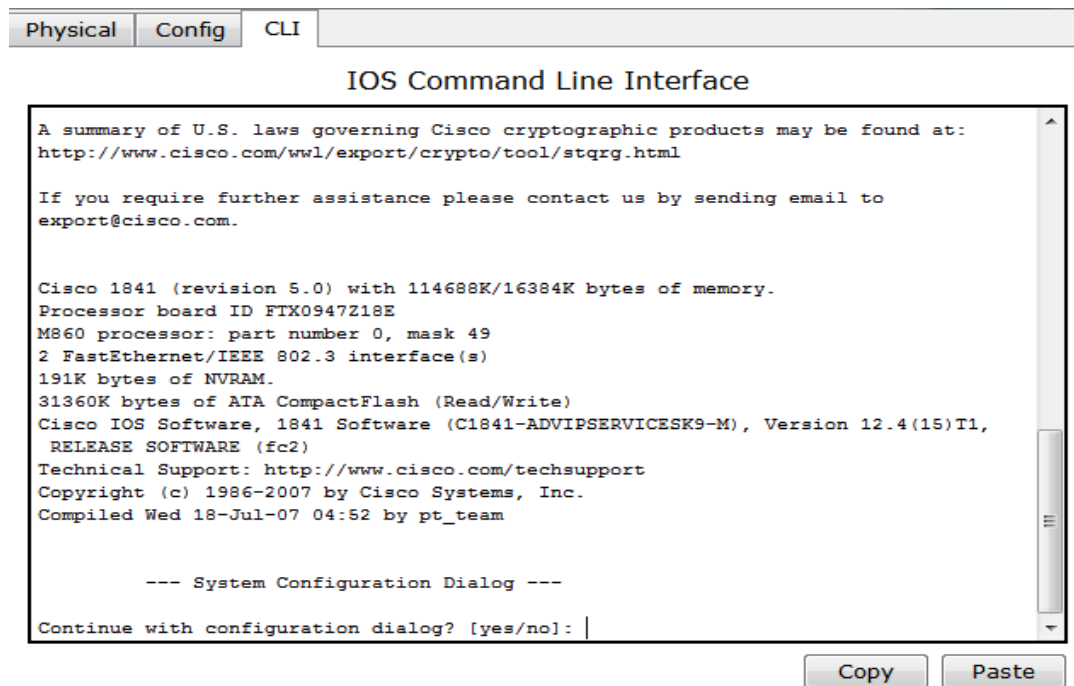
- Administrator harus benar – benar memahami internetwork dan bagaimana setiap router dihubungkan untuk dapat mengkonfigurasi router dengan benar.
- Jika sebuah network ditambah ke internetwork, administrator harus menambahkan sebuah route ke semua router secara manual.
- Routing statis tidak sesuai untuk network – network yang besar karena menjaganya akan menjadi sebuah pekerjaan full-time sendiri.

Routing statis terdiri atas tiga macam:

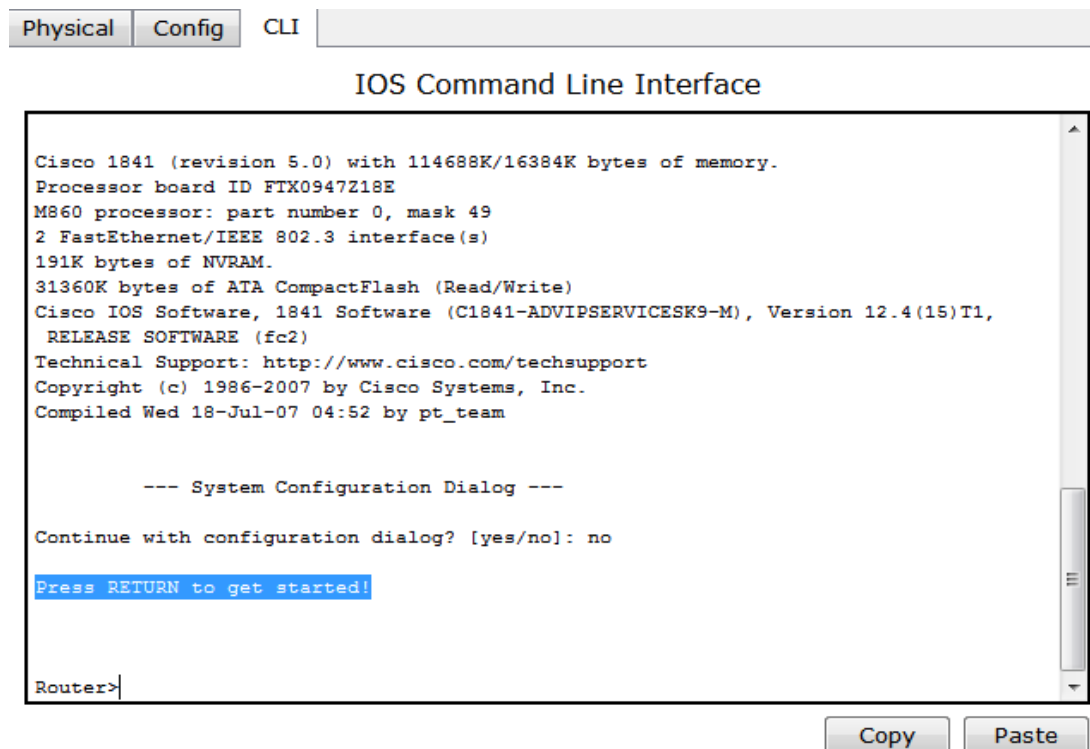
- Next Hop Address
 - Suatu router A akan mengirimkan paket menuju alamat jaringan lain melalui ip address router lain yang berada diantara router A dengan alamat tujuan.
- Exit Interface
 - Suatu router A akan mengirimkan paket menuju alamat jaringan lain melalui salah satu interface aktif pada router A dimana interface tersebut menuju pada alamat tujuan.
- Default Static Route
 - Sebuah router menggunakan static route default jika tidak ada rute yang lebih baik (atau spesifik) untuk mem-forward packet ke alamat tujuan.

V. Pedoman Dasar Konfigurasi Esensial Router

1. Lakukan konfigurasi pada Router
 - a. Klik pada gambar Router hingga muncul form dan pilih menu CLI, sehingga tampilan seperti berikut:



- b. Pada dialog yang muncul ketik NO



- c. Mengaktifkan hak akses EXEC mode: **ditandai dengan prompt #**

```
Router>enable  
Router#
```

- d. Masuk ke global configuration mode: **ditandai dengan prompt (config)#**

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

- e. Mengganti nama router:

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

- f. Mengatur password pada EXEC mode:

```
Syntax: enable secret <password>  
R1 (config) #enable secret jarkom  
R1 (config) #
```

- g. Mengatur password console pada router:

```
Disini kita gunakan password cisco  
R1 (config) #line console 0  
R1 (config-line) #password cisco  
R1 (config-line) #login  
R1 (config-line) #exit  
R1 (config) #
```

- h. Mengkonfigurasi interface FastEthernet 0/0 dengan alamat IP 192.168.1.1/24

```
R1 (config) #interface fastethernet 0/0  
R1 (config-if) #ip address 192.168.1.1 255.255.255.0  
R1 (config-if) #no shutdown
```

Hasilnya:

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

- i. Mengkonfigurasi interface serial 0/0/0 dengan alamat IP 192.168.2.1/24

Jangan lupa set clock rate 64000

```
R1(config-if)#interface serial 0/0/0
```

```
R1(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
R1(config-if)#clock rate 64000
```

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

```
R1(config-if)#
```

- j. Gunakan command end untuk kembali ke awal:

```
R1(config-if)#end
```

```
R1#
```

- k. Simpan konfigurasi dari R1:

```
R1#copy running-config startup-config
```

```
Building configuration...
```

```
[OK]
```

```
R1#
```

2. Melakukan pengujian Router

Lakukan pengujian dengan commands berikut ini dan lakukan analisa sendiri

a. R1#**show running-config**

b. R1#**show startup-config**

c. R1# **show interfaces fastEthernet 0/0**

d. R1#**show version**

e.

3. Penggunaan command ping

Command ping di gunakan untuk mengetahui apakah ada koneksi atau tidak.

- a. Tes koneksi R1 terhadap PC yang ber-ip 192.168.1.10/24

```
R1#ping 192.168.1.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/79/91 ms
```


VI. Langkah-langkah praktikum

Dalam praktikum kali ini, kita akan membuat jaringan seperti yang disajikan pada topologi diagram dan tabel pengalamatan sebagai berikut :

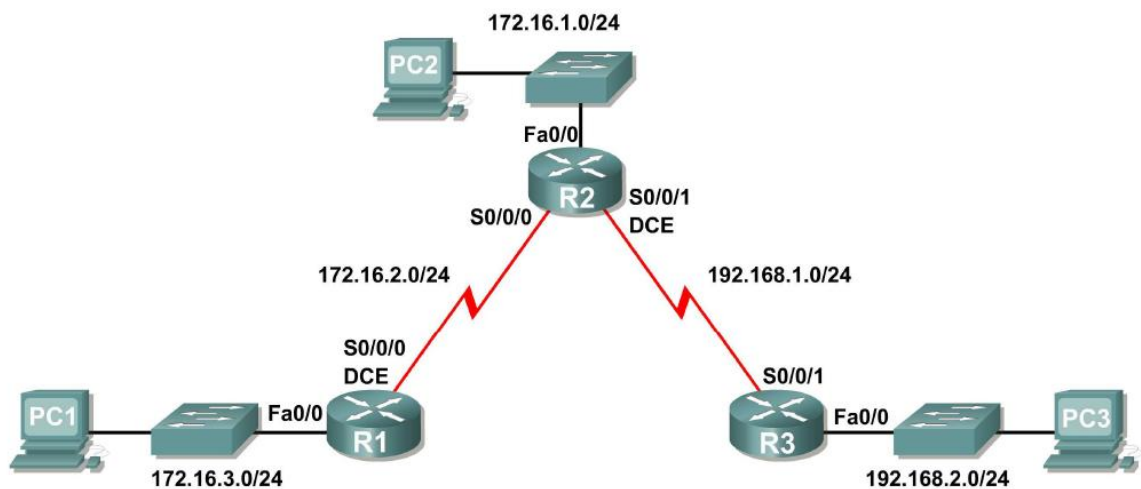


Table Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.3.1	255.255.255.0	N/A
	S0/0/0	172.16.2.1	255.255.255.0	N/A
R2	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.2.2	255.255.255.0	N/A
	S0/0/1	192.168.1.2	255.255.255.0	N/A
R3	FA0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A
PC1	NIC	172.16.3.10	255.255.255.0	172.16.3.1
PC2	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC3	NIC	192.168.2.10	255.255.255.0	192.168.2.1

Tabel pengalamatan dari topologi diatas

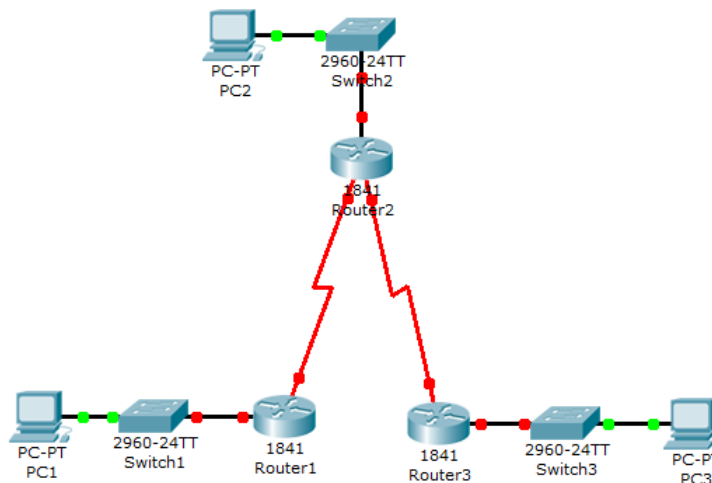
Praktikum akan dimulai dengan menghubungkan setiap *devicesesuai* dengan topologi diatas. Kemudian kita akan melakukan konfigurasi dasar yang dibutuhkan untuk konektivitas jaringan. Gunakan IP address sesuai dengan tabel diatas untuk mencoba skema pengalamatan ke masing-masing *device*. Setelah menyelesaikan konfigurasi dasar, ujliah konektivitas antar *device* dalam jaringan tersebut. Pengujian pertama yakni koneksi antar *device* yang terhubung secara langsung, dilanjutkan uji

koneksi antar *device* yang tidak terhubung secara langsung. *Static route* harus dikonfigurasi pada router untuk komunikasi *end-to-end* karena router disini akan berperan cukup penting dalam transfer data antar network. Kita akan mengkonfigurasi *static route* yang dibutuhkan untuk mengizinkan komunikasi antar host. Perhatikan tabel routing setelah setiap *static route* ditambahkan untuk mengetahui bagaimana tabel routing berubah.

Task 1 : Pengkabelan, menghapus, dan me-load ulang router

Langkah-langkah :

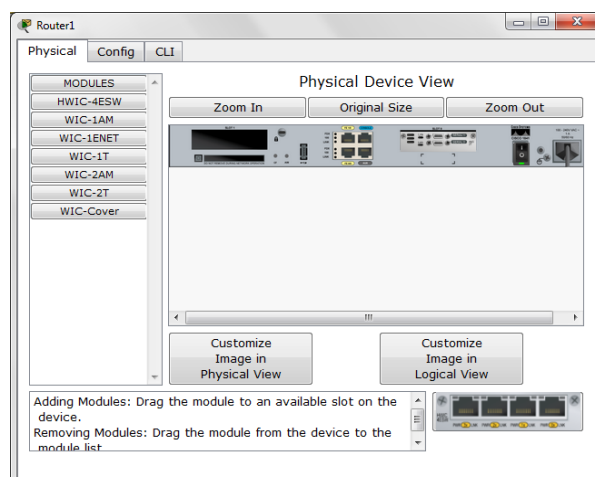
1. Hubungkan setiap *device* dengan kabel sesuai dengan diagram diatas. (hasil seperti dibawah ini)



2. Hapus konfigurasi tiap router

Untuk menghapus konfigurasi tiap router, gunakan perintah `erase startup-config`, kemudian reload.

Caranya, klik ke salah satu router (misal, 1841 Router1), muncul gambar berikut :



Kemudian pada tab CLI, terlebih dahulu kita masuk sebagai privileged user, ketikkan perintah enable, selanjutnya ketikkan perintah erase startup-config, akhiri dengan menekan [Enter] untuk konfirmasi yes :

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Lanjutkan dengan mengetikkan perintah reload, kemudian konfirmasi perintah dengan [Enter], akhiri dengan mengetikkan no untuk konfirmasi berikutnya :

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
##### [OK]
          Restricted Rights Legend

. . . . .
. . . . .
. . . . .

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
```

Ulangi langkah diatas untuk setiap router yang digunakan.

Task 2 : Melakukan konfigurasi dasar router

Langkah-langkah :

1. Gunakan perintah konfigurasi global

Pada router, masuk ke mode konfigurasi global dan atur perintah konfigurasi global dasar dengan :

- Hostname
- no ip domain-lookup
- enable secret

Caranya, masuk ke salah satu router (misalnya 1841 Router1) kemudian pada tab CLI (setelah terlebih dahulu masuk pada mode privileged user) ketikkan configure terminal :

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

Kemudian atur hostname-nya, misalnya test :

```
Router(config)#hostname test
test(config)#
```

Lanjutkan dengan perintah no ip domain-lookup, akhiri dengan enable secret (misalnya passwordnya adalah test) :

```
test(config)#no ip domain-lookup
test(config)#enable secret 0 test
test(config)#
```

Ulangi pada setiap router yang digunakan, dengan mengatur nama yang berbeda tentunya.

2. Atur password untuk console dan virtual terminal pada setiap router

Gunakan perintah :

- password
- login

Untuk mengatur password untuk console, terlebih dahulu masuk sebagai privileged user, kemudian masuk ke pengaturan console dengan perintah line console 0, dilanjutkan dengan mengetik password <nama passwordnya>, lalu login, akhiri dengan exit :

```
test(config)#line console 0
test(config-line)#password test
test(config-line)#login
test(config-line)#exit
test(config)#
```

Gunakan cara yang sama untuk mengatur password untuk virtual terminal, diawali dengan masuk ke pengaturan virtual terminal melalui perintah line vty 0 4:

```
test(config)#line vty 0 4
test(config-line)#password test
test(config-line)#login
test(config-line)#exit
test(config)#
```

Ulangi konfigurasi pada setiap router yang digunakan.

Task 3 : Menginterpretasikan output dari debug

Langkah-langkah :

1. Pada 1841 Router1 jalankan perintah debug ip routing (setelah sebelumnya masuk privileged mode) :

```
test#debug ip routing
IP routing debugging is on
test#
```

2. Masuk ke mode konfigurasi interface untuk LAN interface dari 1841 Router1. Kita akan mengatur IP address untuk interface FastEthernet 0/0, masukkan IP-nya 172.16.3.1 dan subnet 255.255.255.0, kemudian hidupkan interface tersebut :

```
test#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
test(config)#interface fastethernet 0/0
test(config-if)#ip address 172.16.3.1 255.255.255.0
test(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RT: interface FastEthernet0/0 added to routing tableRT: SET_LAST_RDB for 172.16.3.0/24
    NEW rdb: is directly connected

RT: add 172.16.3.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.3.0/24
test(config-if)#
```

3. Cek status IP routing pada 1841 Router1 dengan perintah show ip route :

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

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
test#
```

4. Atur konfigurasi interface WAN 1841 Router1 yang terhubung ke 1841 Router2 (koneksi antar router menggunakan interface serial, gunakan IP 172.16.2.1 dan subnet 255.255.255.0). Atur juga agar clock rate-nya 64000 :

```

test#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
test(config)#interface Serial0/0/0
test(config-if)#ip address 172.16.2.1 255.255.255.0
test(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
test(config-if)#clock rate 64000
test(config-if)#

```

5. Atur konfigurasi interface WAN 1841 Router2 yang terhubung ke 1841 Router1 (gunakan IP 172.16.2.2 dan subnet 255.255.255.0) :

```

test2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
test2(config)#interface serial 0/0/0
test2(config-if)#ip address 172.16.2.2 255.255.255.0
test2(config-if)#no shutdown

test2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
test2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

RT: interface Serial0/0/0 added to routing tableRT: SET_LAST_RDB for 172.16.2.0/
24
    NEW rdb: is directly connected

RT: add 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.2.0/24
test2(config-if)#

```

6. Cek status IP routing pada 1841 Router1 dan 1841 Router2 :

Pada 1841 Router1 :

```

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

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
test#

```

Pada 1841 Router2 :

```
test2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
test2#
```

7. Terakhir matikan debugging pada setiap router, menggunakan perintah no debug ip routing :

```
test#no debug ip routing
IP routing debugging is off
test#

test2#no debug ip routing
IP routing debugging is off
test2#
```

Task 4 : Lengkapi konfigurasi interface router

Langkah-langkah :

1. Periksa dan selesaikan konfigurasi interface pada 1841 Router2 sesuai dengan tabel pengalamatan yang kita gunakan :

```
test2(config)#interface fastethernet 0/0
test2(config-if)#ip address 172.16.1.1 255.255.255.0
test2(config-if)#no shutdown

test2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
test2(config-if)#exit
test2(config)#interface serial 0/0/1
test2(config-if)#ip address 192.168.1.2 255.255.255.0
test2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
test2(config-if)#exit
test2(config)#
```


2. Konfigurasi setiap interface yang digunakan pada 1841 Router3 sesuai dengan tabel pengalamatan :

```
test3(config)#interface serial 0/0/1
test3(config-if)#ip address 192.168.1.1 255.255.255.0
test3(config-if)#no shutdown

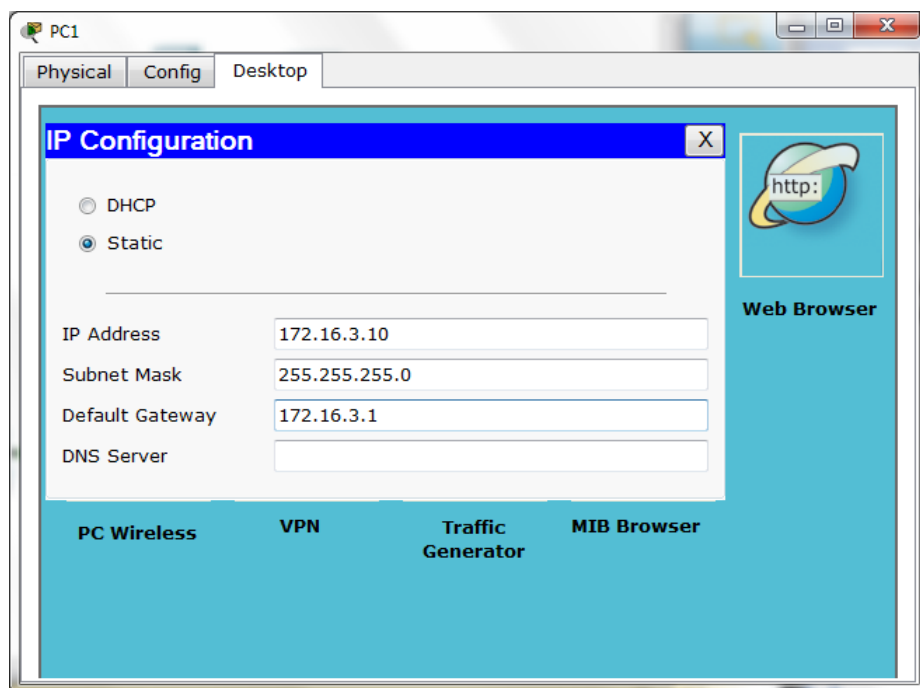
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
test3(config-if)#exit
test3(config)#interface fastethernet 0/0
test3(config-if)#ip address 192.168.2.1 255.255.255.0
test3(config-if)#no shutdown

test3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
test3(config-if)#exit
test3(config)#
```

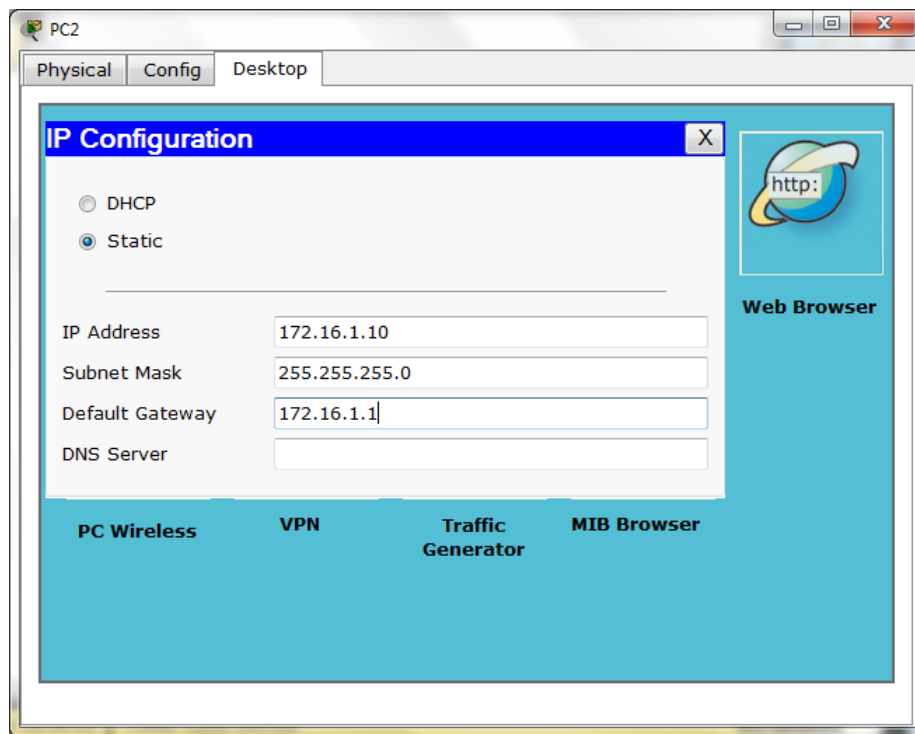
Task 5 : Atur IP address pada setiap PC

Langkah-langkah :

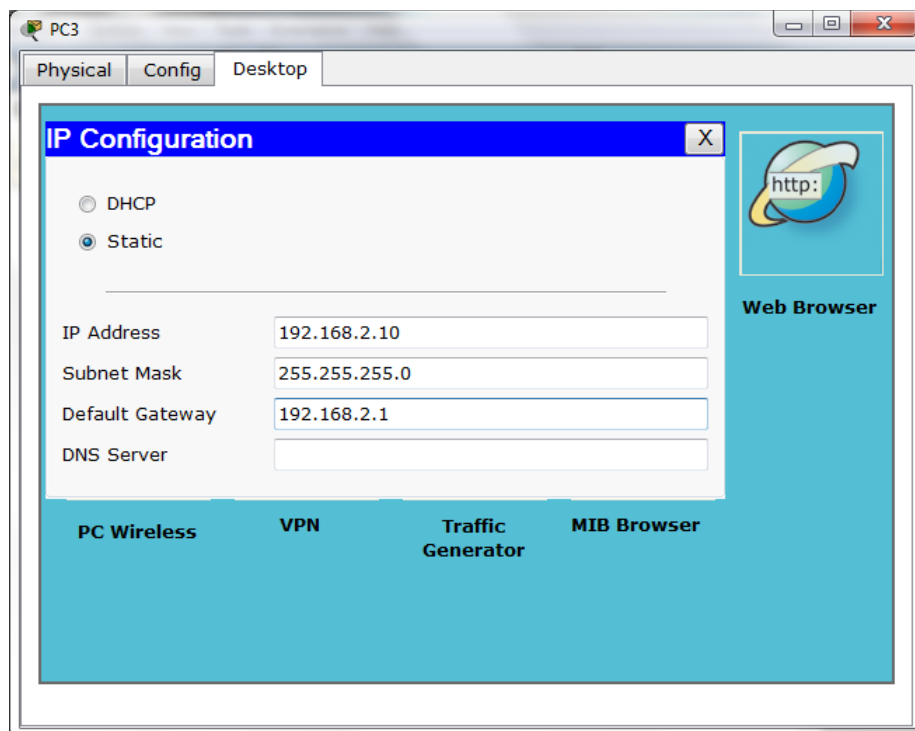
1. Atur PC1 dengan IP address 172.16.3.10/24 dan default gateway 172.16.3.1



2. Atur PC2 dengan IP address 172.16.1.10/24 dan default gateway 172.16.1.1



3. Atur PC3 dengan IP address 192.168.2.10/24 dan default gateway 192.168.2.1

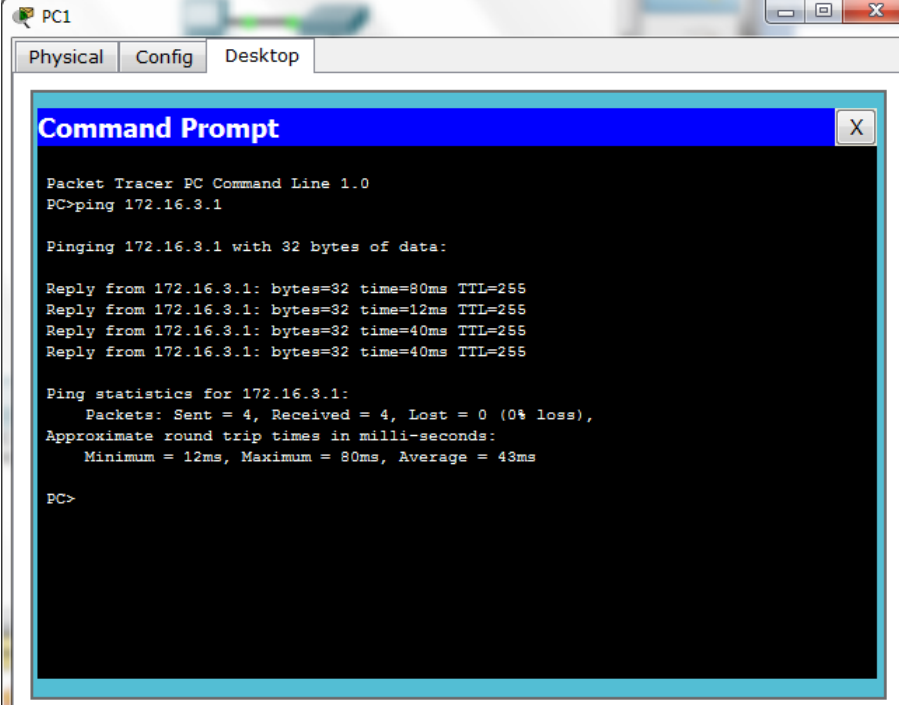


Task 6 : Menguji koneksi antara host dengan default gateway-nya dan koneksi antar router.

(Catatan : pengujian bisa juga menggunakan simulasi pengiriman simple PDU.)

Langkah-langkah :

1. Ujilah koneksi antara host dengan default gateway-nya dengan menggunakan perintah ping :



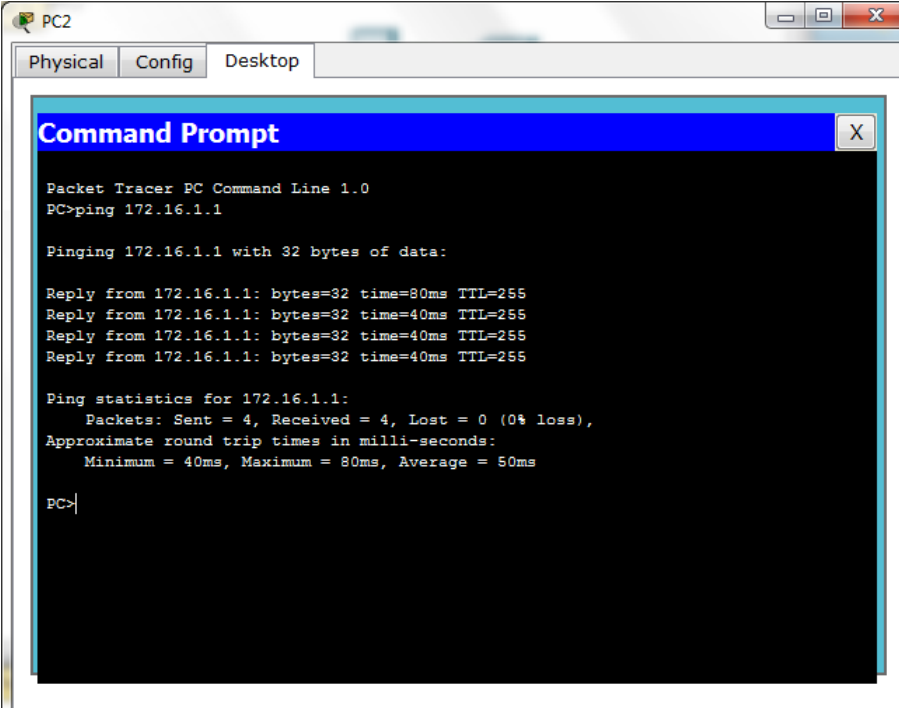
```
PC1
Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 172.16.3.1: bytes=32 time=80ms TTL=255
Reply from 172.16.3.1: bytes=32 time=12ms TTL=255
Reply from 172.16.3.1: bytes=32 time=40ms TTL=255
Reply from 172.16.3.1: bytes=32 time=40ms TTL=255

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 80ms, Average = 43ms

PC>
```



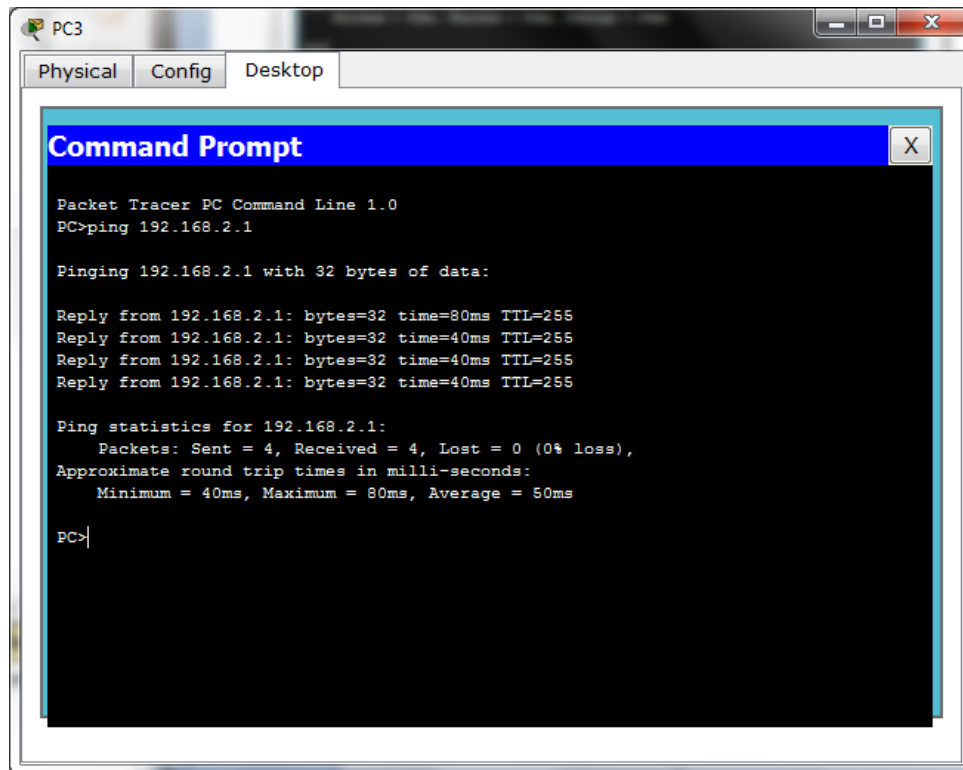
```
PC2
Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time=80ms TTL=255
Reply from 172.16.1.1: bytes=32 time=40ms TTL=255
Reply from 172.16.1.1: bytes=32 time=40ms TTL=255
Reply from 172.16.1.1: bytes=32 time=40ms TTL=255

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 80ms, Average = 50ms

PC>
```



2. Dengan metode yang sama, ujliah koneksi antar router :

Pada 1841 Router1 :

```
test>ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/12/20 ms

test>|
```

Pada 1841 Router2 :

```
test2>ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

test2>

test2>ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/18/20 ms

test2>|
```

Pada 1841Router3 :

```
test3>ping 192.168.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/17/20 ms
```

```
test3>
```

3. Sekarang, cobalah analisis, apakah setiap host sudah terhubung dan dapat berkomunikasi satu sama lain? Jelaskan analisis tersebut!

Task 7 : Memperoleh informasi dari setiap router.

Langkah-langkah :

1. Cek status setiap interface pada 1841 Router2 dengan perintah show ip interface brief :

```
test2>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.16.1.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	172.16.2.2	YES	manual	up	up
Serial0/0/1	192.168.1.2	YES	manual	up	up
Vlan1	unassigned	YES	manual	administratively down	down

```
test2>
```

2. Tampilkan informasi tabel routing untuk setiap router :

Pada 1841 Router1 :

```
test>show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 2 subnets
```

```
C 172.16.2.0 is directly connected, Serial0/0/0
```

```
C 172.16.3.0 is directly connected, FastEthernet0/0
```

```
test>
```

Pada 1841 Router2 :

```
test2>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets
C      172.16.1.0 is directly connected, FastEthernet0/0
C      172.16.2.0 is directly connected, Serial0/0/0
C     192.168.1.0/24 is directly connected, Serial0/0/1
test2>
```

Pada 1841 Router3 :

```
test3>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C     192.168.1.0/24 is directly connected, Serial0/0/1
C     192.168.2.0/24 is directly connected, FastEthernet0/0
test3>
```

3. Dari informasi diatas, apa saja yang dapat anda simpulkan?

Task 8 : Konfigurasi Static Route menggunakan alamat Next-Hop

Langkah-langkah :

1. Gunakan syntax berikut untuk mengkonfigurasi static route dengan next-hop yang sudah ditetapkan :

ip route*network-address**subnet-mask**ip-address*

Dengan ketentuan :

- *network-address* merupakan tujuan alamat network yang akan ditambahkan ke tabel routing
- *subnet-mask* merupakan subnet mask dari *network-address*
- *ip-address* merupakan IP address router yang dijadikan next-hop.

Pada 1841 Router3, atur static route ke network 172.16.1.0 melalui interface Serial 0/0/1 dari 1841 Router2 sebagai next-hop-nya :

```
test3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.2
test3(config)#
```

2. Cek tabel routing-nya untuk memastikan static route telah di-update :

```
test3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
S      172.16.1.0 [1/0] via 192.168.1.2
C      192.168.1.0/24 is directly connected, Serial0/0/1
C      192.168.2.0/24 is directly connected, FastEthernet0/0
test3#
```

Simpulkan, apakah terjadi perubahan pada tabel routing? Jelaskan!

3. Sekarang, cobalah menggunakan ping untuk mengecek koneksi antara PC3 dan PC2, apakah berhasil? Jelaskan!

4. Pada 1841 Router2, atur static route untuk mencapai jaringan 192.168.2.0 :

```
test2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
test2(config)#
```

5. Cek tabel routing-nya untuk memastikan static route telah di-update :

```
test2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets
C      172.16.1.0 is directly connected, FastEthernet0/0
C      172.16.2.0 is directly connected, Serial0/0/0
C      192.168.1.0/24 is directly connected, Serial0/0/1
S      192.168.2.0/24 [1/0] via 192.168.1.1
test2#
```


6. Sekarang, cobalah kembali menggunakan ping untuk mengecek koneksi antara PC3 dan PC2, apakah berhasil? Jelaskan!

Task 9 : Konfigurasi static route menggunakan exit-interface

Untuk mengkonfigurasi static route dengan exit-interface yang sudah ditentukan sebelumnya, gunakan syntax berikut :

ip route *network-address subnet mask exit-interface*

Dengan ketentuan :

- *network-address* merupakan tujuan alamat network yang akan ditambahkan ke tabel routing
- *subnet-mask* merupakan subnet mask dari *network-address*
- *exit-interface* merupakan interface "keluar" yang akan digunakan untuk mem-forward packet ke network tujuan.

Langkah-langkah :

1. Pada 1841 Router3, atur static route untuk mem-forward packet yang akan menuju network 172.16.2.0 menggunakan interface Serial 0/0/1 sebagai exit-interface-nya :

```
test3(config)#ip route 172.16.2.0 255.255.255.0 Serial0/0/1
test3(config)#
```

2. Lakukan cek tabel routing-nya :

```
test3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 2 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
S       172.16.2.0 is directly connected, Serial0/0/1
C       192.168.1.0/24 is directly connected, Serial0/0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
test3#
```

Pengecekan dapat dilakukan dengan mengetik perintah show running-config, untuk melihat perintah apa saja yang baru saja dieksekusi.

3. Pada 1841 Router2, atur static route untuk mem-forward packet yang akan menuju network 172.16.3.0 menggunakan interface Serial 0/0/0 sebagai exit-interface-nya :

```
test2(config)#ip route 172.16.3.0 255.255.255.0 Serial0/0/0
test2(config)#
```

4. Lakukan cek tabel routing-nya :

```
test2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
C      172.16.1.0 is directly connected, FastEthernet0/0
C      172.16.2.0 is directly connected, Serial0/0/0
S      172.16.3.0 is directly connected, Serial0/0/0
C      192.168.1.0/24 is directly connected, Serial0/0/1
S      192.168.2.0/24 [1/0] via 192.168.1.1
test2#
```

5. Ujilah koneksi antara PC2 ke PC1, menggunakan ping. Apakah berhasil? Analisis dan jelaskan!

Task 10 : Konfigurasi Static Route Default

Pada langkah-langkah sebelumnya, kita telah mengkonfigurasi router untuk rute tujuan tertentu. Tetapi kenyataannya, apakah kita perlu melakukan langkah yang sama apabila kita ingin mengatur rute di internet? Tentu saja tidak, karena sangat tidak efisien baik untuk administrator jaringan, maupun router itu sendiri. Untuk memperkecil ukuran tabel routing, maka digunakanlah static route default. Sebuah router menggunakan static route default jika tidak ada rute yang lebih baik (atau spesifik) untuk mem-forward packet ke alamat tujuan.

Untuk memahami apa itu static route default, kita bisa asumsikan 1841 Router1 sebagai host dan 1841 Router2 sebagai default gateway-nya. Artinya jika 1841 Router1 memiliki packet yang akan di-forward, namun tujuan packet tersebut tidak terdapat pada setiap jaringan yang terhubung pada 1841 Router1, maka packet tersebut akan di-forward ke default gateway-nya, dalam hal ini 1841 Router2. Dengan kata lain, 1841 Router1 memiliki static route default yakni 1841 Router2. Kita akan mencoba mengkonfigurasi static route default, dengan syntax sebagai berikut :

```
ip route 0.0.0.0 0.0.0.0 {ip-address | interface }
```

Langkah-langkah :

1. Konfigurasi 1841 Router1 agar memiliki static route default, dengan interface Serial 0/0/0 sebagai next-hop-nya :

```
test(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
test(config)#
```

2. Kemudian cek pada tabel routing :

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

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

    172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 172.16.2.2
test#
```

Sekarang 1841 Router1 sudah memiliki rute default, yakni *Gateway of last resort*, yang mana akan mem-forward semua paket yang tidak diketahui tujuannya, "keluar" dari Serial 0/0/0 yang mana terhubung pada 1841 Router2 (172.16.2.2)

3. Ujilah koneksi antara PC2 dan PC1, apakah berhasil? Uji pula koneksi antara PC 3 dan PC1! Jelaskan!

Task 11 : Konfigurasi summary static route

Kita bisa mengkonfigurasi static route lain pada 1841 Router3 untuk network 172.16.3.0. Namun, 1841 Router3 telah memiliki static route untuk network 172.16.2.0/24 dan 172.16.1.0/24. Karena ketiga jaringan tadi berlokasi cukup dekat, kita bisa menyimpulkannya menjadi satu rute. Ini bisa mengurangi ukuran tabel routing, yang tentunya menambah efisiensi router dalam mem-forward packet.

Perhatikan ketiga network tadi, kita ubah ke level binary :

```
172.16.1.0    10101100.00010000.0000000001.00000000
172.16.2.0    10101100.00010000.0000000010.00000000
172.16.3.0    10101100.00010000.0000000011.00000000
```

Jika kita "mematikan" bit dari bit ke-22 sampai bit paling kanan (tidak ditandai dengan area kuning, "mematikan" berarti mengubah semua angka binary tersebut menjadi 0), akan muncul prefix :172.16.0.0.

Kemudian kita "menghidupkan" bit dari kiri sampai bit ke-22 (ditandai dengan area kuning, "menghidupkan" berarti mengubah semua angka binary tersebut menjadi 1, sehingga didapat bit mask-nya : 11111111.11111111.11111100.00000000

Konversi bits diatas, sehingga didapat mask-nya :255.255.252.0

Langkah-langkah :

1. Konfigurasi summary static route pada 1841 Router3, dengan summary route

172.16.0.0/22

```
test3(config)#ip route 172.16.0.0 255.255.252.0 192.168.1.2
test3(config)#
```

2. Cek tabel routing-nya :

```
test3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S    172.16.0.0/22 [1/0] via 192.168.1.2
S    172.16.1.0/24 [1/0] via 192.168.1.2
S    172.16.2.0/24 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
test3#
```

Terlihat adanya penambahan summary route pada tabel routing.

3. Menghapus static route pada 1841 Router3

Kita akan menghapus 2 static route, karena rute tersebut sudah "disimpulkan" ke rute yang kita konfigurasi pada langkah sebelumnya.

```
test3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
test3(config)#no ip route 172.16.2.0 255.255.255.0 Serial0/0/1
test3(config)#
```

4. Cek kembali tabel routing-nya :

```
test3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/22 is subnetted, 1 subnets
S       172.16.0.0 [1/0] via 192.168.1.2
C       192.168.1.0/24 is directly connected, Serial0/0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
test3#
```

Apa yang bisa anda simpulkan, dari data tabel routing milik 1841 Router3?

5. Ujilah koneksi antara PC3 dan PC1, apakah berhasil?

Anda bisa me-review ulang langkah-langkah diatas, untuk dapat lebih memahami static route dan juga syntax-syntax yang digunakan.

MODULE 2

Dynamic Routing – RIPv1, RIPv2, EIGRP

I. Tujuan Praktikum

- Praktikan mengetahui konsep dasar dynamic routing.
- Praktikan mengetahui kelebihan dan kekurangan dari dynamic routing.
- Praktikan dapat melakukan simulasi konfigurasi router pada jaringan dengan menggunakan dynamic routing (dalam praktikum ini menggunakan packet tracer).
- Praktikan mengetahui perbedaan penggolongan link-state dan distance vector pada algoritma dinamic routing.
- Praktikan dapat melakukan simulasi konfigurasi router pada jaringan dengan menggunakan algoritma dinamic routing (dalam praktikum ini menggunakan packet tracer).
- Praktikan mengetahui kelebihan dan kekurangan dari algoritma dinamic routing RIPv1, RIPv2, EIGRP.

II. Alat dan Bahan

- Alat tulis
- Komputer
- Software Cisco Packet Tracer Latest Version

III. Landasan Teori

A. Routing Protocol

Routing merupakan inti dari setiap jaringan data, memindahkan informasi melalui sebuah internetwork dari *source* ke *destination*. *Network device* yang bertanggung jawab dalam melakukan fungsi routing tersebut dikenal dengan sebutan *Router*. Untuk dapat memindahkan/meneruskan data *network* asal ke *network* tujuan, *Router* perlu mengenali *network-network* yang terhubung dengannya. *Router* mengenali *remote networks* melalui *routing protocols*, baik *static routing* maupun *dynamic routing protocol*.

B. Static Routing

Static Routing merupakan proses pemilihan jalur yang dilakukan secara manual, dengan cara menambahkan route – route pada routing table di setiap router. Dilakukan oleh administrator jaringan.

Routing statis memiliki keuntungan – keuntungan sebagai berikut :

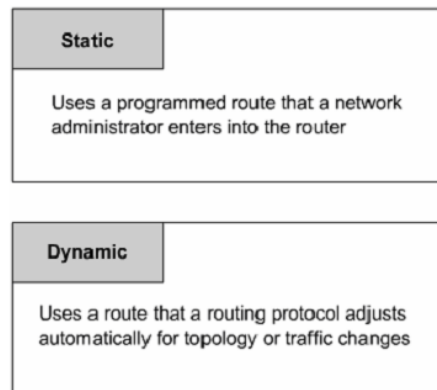
- Tidak ada *overhead* (waktu pemrosesan) pada CPU router, yang berarti anda mungkin dapat membeli router yang lebih murah dari pada router dinamis.
- Tidak ada bandwidth yang digunakan antara router, yang berarti anda dapat menghemat uang untuk link WAN.
- Routing statis menambah keamanan, karena administrator dapat memilih untuk mengizinkan akses routing ke network tertentu saja.

Routing statis memiliki kerugian – kerugian sebagai berikut :

- Administrator harus benar – benar memahami *internetwork* dan bagaimana setiap router dihubungkan untuk dapat mengkonfigurasi router dengan benar.
- Jika sebuah network ditambah ke *internetwork*, administrator harus menambahkan sebuah route ke semua router secara manual.
- Routing statis tidak sesuai untuk network – network yang besar karena menjaganya akan menjadi sebuah pekerjaan full-time sendiri.

C. Dynamic Routing

Dynamic Routing merupakan proses pemilihan jalur yang dilakukan secara otomatis oleh *gateway* atau router yang bersangkutan. Diterapkan pada jaringan yang memiliki banyak *gateway* atau router. Kelebihannya *Dynamic Routing* juga dia selalu mengupdate secara otomatis table routing yang tersedia pada dirinya.



Gambar 2.1 Perbedaan statis dan dinamis routing

Ketika router menggunakan routing dinamik informasi ini dipelajari dari router yang lain. Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual. Jika routing yang digunakan adalah statis, maka konfigurasinya harus dilakukan secara manual, administrator jaringan harus memasukkan atau menghapus rute statis jika terjadi perubahan topologi. Pada jaringan skala besar, jika tetap menggunakan routing statis, maka akan sangat membuang waktu administrator jaringan untuk melakukan update table routing. Karena itu routing statis hanya mungkin dilakukan untuk jaringan skala kecil. Sedangkan routing dinamik bisa diterapkan di jaringan skala besar dan membutuhkan kemampuan lebih dari administrator.

Pada routing dinamis, sebuah protocol pada satu router berkomunikasi dengan protocol yang sama yang bekerja di router tetangga. Router kemudian akan saling melakukan update tentang semua network yang mereka ketahui dan mendapatkan informasi tersebut ke routing tabel. Jika suatu perubahan terjadi di network, maka *Protocol Routing* dinamis secara otomatis akan memberitahukan semua router tentang apa yang terjadi. Jika routing statis digunakan, maka seorang administrator bertanggung jawab untuk melakukan update semua perubahan tersebut.

Pada *Dynamic Routing* terdapat *Dynamic Routing protocol*. *Protocol Routing* adalah program yang mengubah informasi yang digunakan untuk membangun routing table. Secara keseluruhan, protokol routing pada dinamik routing dapat kita kelompokkan menjadi dua Jenis yaitu:

- a. *Interior Routing protocol*, digunakan sebagai protokol routing di dalam suatu *autonomous system*. Pada TCP/IP routing, istilah *autonomous system* memiliki arti yang formal, yakni suatu kumpulan network dan *gateway* yang memiliki mekanisme internal sendiri dalam mengumpulkan informasi routing dan memberikannya kepada yang lain. Misalnya, Routing Information Protocol (RIP), Hello, Shortest Path First (SPF) dan Open Shortest Path First (OSPF).
- b. *Exterior Routing protocol* digunakan sebagai protokol routing untuk mempertukarkan informasi routing antar *autonomous system*. Informasi routing yang dikirimkan antar *autonomous system* disebut reachability information, yakni informasi mengenai network apa saja yang dapat dicapai melalui suatu *autonomous system*. Misalnya, Exterior Gateway Protocol (EGP) dan Border Gateway Protocol (BGP).

Berikut ini adalah beberapa contoh algoritma yang digunakan dalam protocol dinamik routing, yaitu:

1. Distance Vektor

Protokol ini menentukan jalur terbaik ke sebuah network dengan menilai jarak. Setiap kali suatu paket melalui sebuah router disebut Hop. Rute dengan Hop yang paling sedikit ke network yang dituju, akan menjadi rute terbaik. Algoritma distance vector ini mengirimkan isi routing table yang lengkap ke router-router tetangganya, yang kemudian menggabungkan entri-entri di routing table yang diterima tersebut dengan routing table yang mereka miliki untuk melengkapi routing table router tersebut. Contoh protocol : RIP, IGRP

2. Link State

Pada protocol ini setiap router akan menciptakan tiga buah tabel secara terpisah. Satu table mencatat perubahan dari network-network yang terhubung langsung, satu table lain menentukan topologi dari keseluruhan *internetwork*, dan tabel terakhir digunakan sebagai routing tabel. Router

yang link-state mengetahui lebih banyak tentang *internetwork* dibandingkan semua jenis *routing protocol* yang distance-vektor. Algoritma yang dipakai oleh link-state yaitu algoritma dijkstra dimana jalur terpendekakan dibangun berdasarkan jalur-jalur terbaik dan disimpan di table routing. Tetapi kelemahan dari link state yaitu membutuhkan resource yang besar seperti memory yang besar untuk menyimpan table routing. Contoh protocol : OSPF.

D. Dynamic Routing Protocol

a. RIP

RIP mengirimkan routing table yang lengkap ke semua interface yang aktif setiap 30 detik, RIP hanya menggunakan jumlah hop untuk menentukan cara terbaik ke sebuah network *remote*, tetapi RIP secara default memiliki jumlah hop maksimum yang di izinkan, yaitu 15 hop. Hal tersebut berarti nilai 16 dianggap tidak terjangkau (*unreachable*). RIP bekerja dengan baik di network-network yang kecil, tetapi RIP tidak efisien pada network yang besar dengan link WAN yang lambat atau pada network yang memiliki jumlah router yang banyak.

RIP versi 1 menggunakan hanya *classful routing*, yang berarti semua alat di network harus menggunakan subnetmask yang sama, hal tersebut dikarenakan RIP versi 1 tidak mengirimkan update dengan informasi subnetmask didalamnya. RIP versi 2 menyediakan sesuatu yang disebut *prefix routing*, dan bisa mengirimkan informasi subnetmask bersama dengan update-update dari route.

RIP Timers

RIP menggunakan tiga jenis timer yang berbeda untuk mengatur unjuk kerjanya yaitu :

1. Route Update Timer , Interval antar update biasanya 30 detik secara periodik dimana router mengirimkan sebuah copy yang lengkap dari routing table-nya ke semua router terdekat.
2. Route Invalid Timer, Timer ini menentukan jangka waktu yang harus lewat (180 detik) sebelum sebuah router menentukan bahwa sebuah rute menjadi tidak valid.

3. Holddown Timer, Timer ini men-set interval waktu di mana informasi routing ditahan (*holddown state*), defaultnya adalah 180 detik.
4. Route Flish Time, Timer ini men-set waktu antara sebuah route menjadi tidak valid dan penghapusannya dari routing table (240 detik).

b. EIGRP

Sebelum adanya EIGRP (*Enhanced interior gateway routing protocol*) diawali dengan IGRP (*interior gateway routing protocol*). IGRP adalah sebuah *routing protocol* jenis distance vector milik cisco. IGRP dan EIGRP diciptakan untuk mengatasi masalah – masalah yang ada pada RIP.

Enhanced interior gateway routing protocol (EIGRP) adalah sebuah *protocol distance vector* yang classless dan yang sudah ditingkatkan (*enhanced*), yang memberikan keunggulan dibandingkan dengan IGRP. EIGRP menggunakan konsep *autonomous system* untuk menggambarkan kumpulan dari router – router yang contiguous (berentetan, sebelah menyebelah) yang menjalankan *routing protocol* yang sama dan berbagi informasi routing. Selain itu EIGRP juga memasukkan subnet mask ke dalam update route-nya.

Beberapa fitur utama yang ada pada IEGRP :

- ✓ Mendukung IP, IPX, dan AppleTalk melalui modul – modul yang bersifat *protocol dependent* (bergantung pada protocol).
- ✓ Pencarian network tetangga (*neighbor discover*) yang dilakukan dengan efisien.
- ✓ Komunikasi melalui reliable transport protocol.
- ✓ Pemilihan jalur terbaik melalui Difussing Update Algorithm (DUAL)

EIGRP cocok digunakan untuk network – network besar. Hal ini disebabkan karena EIGRP mampu untuk :

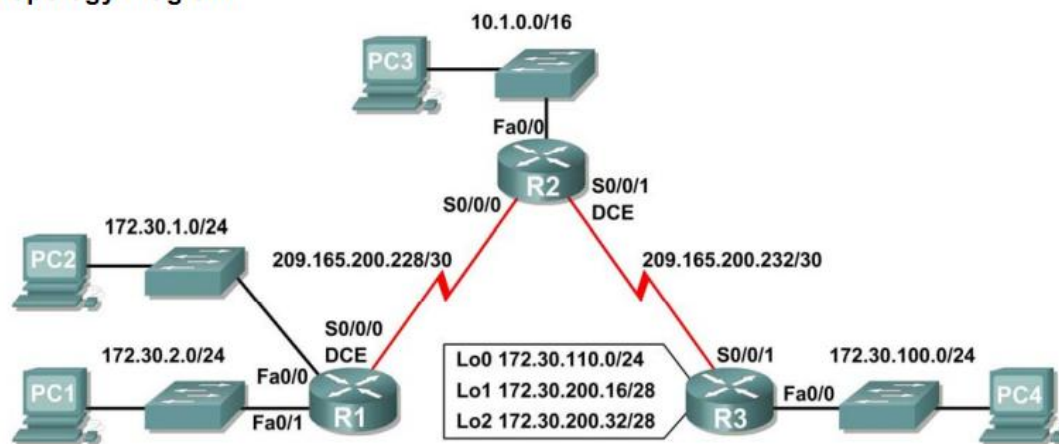
- ✓ Mendukung banyak *autonomous system* pada satu router.
- ✓ Mendukung VLSM (Variable Length Subnet Mask) dan summarization.
- ✓ Mencari route dan memeliharanya.

IV.Praktikum

A. Praktikum Dinamic Routing

✓ RIPv2

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	N/A
	Fa0/1	172.30.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
R2	Fa0/0	10.1.0.1	255.255.0.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.233	255.255.255.252	N/A
R3	Fa0/0	172.30.100.1	255.255.255.0	N/A
	S0/0/1	209.165.200.234	255.255.255.252	N/A
	Lo0	172.30.110.1	255.255.255.0	N/A
	Lo1	172.30.200.17	255.255.255.240	N/A
	Lo2	172.30.200.33	255.255.255.240	N/A
PC1	NIC	172.30.1.10	255.255.255.0	172.30.2.1
PC2	NIC	172.30.2.10	255.255.255.0	172.30.1.1
PC3	NIC	10.1.0.10	255.255.0.0	10.1.0.1
PC4	NIC	172.30.100.10	255.255.255.0	172.30.100.1

Skenario

Pada jaringan yang ditampilkan dalam Diagram Topologi terdapat jaringan yg tdk berhubungan (*discontiguous network*) yaitu 172.30.0.0 dimana jaringan tersebut telah di subneting menggunakan VLSM. Subnet 172.30.0.0 secara fisik dan logic dibagi oleh setidaknya satu jaringan *classful* atau jaringan yang lebih besar lainnya, dalam kasus ini

jaringan tersebut adalah dua buah jaringan serial yaitu 209.165.200.232/30 dan 209.165.200.228/30.

Hal ini dapat menjadi masalah ketika routing protokol yang digunakan tidak memuat informasi yang cukup untuk membedakan masing-masing subnet. RIPv2 adalah sebuah routing protocol classless yang dapat digunakan untuk menyediakan informasi subnet mask pada saat melakukan *routing update*. Sehingga akan memungkinkan informasi subnet VLSM dapat disebarluaskan ke seluruh jaringan.

Tugas 1: Pengkabelan, Menghapus dan Mereload Router.

Langkah – langkah (Langkah Awal Menggunakan RIPv1):

1. Pengkabelan jaringan.

Hubungkan dan lakukan pengkabelan antar device yang ada pada jaringan sesuai dengan yang tergambar dalam Diagram Topologi. Lakukan Konfigurasi IP pada jaringan. Untuk interface loopback sendiri pada Router 3, dapat disetting dengan command berikut ini :

```
Router(config)#interface Loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Router(config-if)#ip address 172.30.110.1 255.255.255.0
Router(config-if)#exit
```

```
Router(config)#interface Loopback 1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
Router(config-if)#ip address 172.30.200.17 255.255.255.240
Router(config-if)#exit
```

```
Router(config)#interface Loopback 2
%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
Router(config-if)#ip address 172.30.200.33 255.255.255.240
Router(config-if)#exit
Router(config)#
```

2. Hapus konfigurasi pada setiap router.

Menghapus konfigurasi pada masing-masing router menggunakan perintah

```
Router# erase startup-config
```

dan kemudian

```
Router# reload router
```

Jawab no, jika diminta untuk menyimpan perubahan.

Tugas 2: Memasukan Script ke dalam Router.

Langkah – langkah :

1. Masukan script berikut ke dalam R1.

```
Router(config)#router rip
Router(config-router)#passive-interface FastEthernet 0/0
Router(config-router)#passive-interface FastEthernet 0/1
Router(config-router)#network 172.30.0.0
Router(config-router)#network 209.165.200.0
Router(config-router)#
```

2. Masukan script berikut ke R2.

```
Router(config)#router rip
Router(config-router)#passive-interface FastEthernet 0/0
Router(config-router)#network 10.0.0.0
Router(config-router)#network 209.165.200.0
Router(config-router)#
```

3. masukan script berikut ke dalam R3.

```
Router(config)#router rip
Router(config-router)#passive-interface FastEthernet 0/0
Router(config-router)#network 172.30.0.0
Router(config-router)#network 209.165.200.0
Router(config-router)#
```

Tugas 3: Memeriksa status jaringan.

Langkah – langkah :

1. Verifikasi apakah kedua jaringan serial telah aktif (*up*).

Untuk melakukan verifikasi gunakan perintah `show ip interface brief` pada R2.

```
R2#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	209.165.200.229	YES	manual	up	up
Serial0/0/1	209.165.200.233	YES	manual	up	up
Vlan1	unassigned	YES	manual	administratively down	down

2. Cek konektivitas dari R2 ke Host dalam LAN R1 dan R3.

Contoh : Lakukan ping dari R2 ke komputer pada R1.

```
R2#ping [ip address PC1].
```

3. Cek konektivitas antar PC dalam jaringan.

4. Melihat *routing table* di R2.

Kedua router R1 dan R3 menginformasikan rute ke jaringan 172.30.0.0/16; karena itu, ada dua entri untuk jaringan pada *routing table* R2. *Routing table* di R2 ini hanya menampilkan alamat jaringan utama *classfull* dari 172.30.0.0. Ini berarti *routing table* tidak menunjukkan bahwa *subnet jaringan* yang digunakan pada LAN melekat pada R1 dan R3.

Ketik perintah :

```
R2#show ip route
```

Output :

```
10.0.0.0/16 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:24, Serial0/0/0
      [120/1] via 209.165.200.234, 00:00:15, Serial0/0/1
209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
C    209.165.200.232 is directly connected, Serial0/0/1
```

5. Memeriksa *routing table* pada R1.

Kedua router R1 dan R3 dikonfigurasi dengan interfaces 172.30.0.0 pada jaringan yg tdk berhubungan (*discontiguous network*) . Dalam skenario ini, subnet 172.30.0.0 secara fisik dan logic dibagi oleh dua jaringan serial 209.165.200.228/30 dan 209.165.200.232/30. *Classfull routing protokol* seperti RIPv1 akan meringkas jaringan pada batas jaringan utama. Kedua router R1 dan R3 akan meringkas subnet 172.30.0.0/24 menjadi 172.30.0.0/16. Karena rute ke 172.30.0.0/16 telah terhubung langsung dan karena R1 tidak memiliki rute khusus untuk subnet 172.30.0.0 pada R3, maka paket yang ditujukan ke jaringan LAN di R3 tidak akan diteruskan dengan benar. Akibatnya, apabila kita melakukan ping dari PC1 ke PC4, maka akan gagal.

Ketik perintah :

```
R1#show ip route
```

Output :


```

R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
    172.30.0.0/24 is subnetted, 2 subnets
C    172.30.1.0 is directly connected, FastEthernet0/0
C    172.30.2.0 is directly connected, FastEthernet0/1
    209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0

```

6. Memeriksa *routing table* pada router R3.

R3 hanya menunjukkan subnet 172.30.100/24, 172.30.110/24, 172.30.200.16/28, dan 172.30.200.32/28 untuk jaringan 172.30.0.0. R3 tidak memiliki rute untuk subnet 172.30.0.0 subnet pada R1.

Ketik perintah :

```
R3#show ip route
```

Output :

```

R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
C    209.165.200.232 is directly connected, Serial0/0/1

```

7. Memeriksa paket RIP v1 yang diterima oleh R2

Gunakan perintah `debug ip rip` untuk menampilkan update routing RIP. R2 menerima rute 172.30.0.0 dengan 1 hop baik dari R1 dan R3. Karena *cost metrics* dari kedua rute adalah sama, kedua rute ditambahkan kedalam *routing table* R2. Karena RIPv1 adalah sebuah routing protocol yang classfull, tidak ada informasi subnet mask yang dikirim di dalam update.

Ketik perintah :

```
R2#debug ip rip
```

Output :

```

RIP protocol debugging is on
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
    172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
    172.30.0.0 in 1 hops

```

R2 hanya mengirim rute untuk LAN 10.0.0.0 dan dua koneksi serial ke R1 dan R3. R1 dan R3 tidak menerima informasi apapun mengenai rute subnet 172.30.0.0.

```

RIP: sending v1 update to 255.255.255.255 via Serial0/0/1
(209.165.200.233)
RIP: build update entries
      network 10.0.0.0 metric 1
      network 209.165.200.228 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
(209.165.200.229)
RIP: build update entries
      network 10.0.0.0 metric 1
      network 209.165.200.232 metric 1

```

Setelah selesai, matikan debugging dengan cara :

R2#undebug all

Tugas 4: Konfigurasi RIP Version 2.

Langkah – langkah :

1. Gunakan perintah versi 2 untuk mengaktifkan RIP versi 2 pada setiap router.

Ketik perintah :

```

R2(config)#router rip
R2(config-router)#version 2

```

```

R1(config)#router rip
R1(config-router)#version 2

```

```

R3(config)#router rip
R3(config-router)#version 2

```

Pesan pada RIPv2 mengandung informasi subnet mask di field dalam *routing update*. Hal ini memungkinkan subnet dan mask tersebut untuk dimasukkan dalam *routing update*. Namun, pada defaultnya RIPv2 merangkum jaringan pada batas jaringan besar seperti pada RIPv1 akan tetapi subnet mask tersebut dimasukkan dalam update.

2. Pastikan bahwa RIPv2 berjalan pada router. Debug ip rip menunjukkan protokol ip dan menunjukkan semua perintah aktif yang dapat digunakan untuk mengkonfirmasi bahwa RIPv2 telah aktif. Output dari perintah show ip protocols untuk R1 ditampilkan di bawah ini.

Ketikkan perintah :

R1# show ip protocols

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
FastEthernet0/0      2     2
FastEthernet0/1      2     2
Serial10/0/0         2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  172.30.0.0
  209.165.200.0
Passive Interface(s):
  FastEthernet0/0
  FastEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  209.165.200.229    120
Distance: (default is 120)
```

Tugas 5: Memeriksa Peringkasan Rute otomatis (*Automatic Summarization*).

LAN yang tersambung ke R1 dan R3 masih terdiri dari jaringan yg tidak berhubungan. R2 masih menunjukkan dua jalur biaya yang sama dengan jaringan 172.30.0.0/16 pada tabel routing. R2 masih hanya menunjukkan alamat jaringan classful utama dari 172.30.0.0 dan tidak menunjukkan salah satu subnet untuk jaringan ini.

Ketikkan perintah:

R2#show ip route

Output :

```
      10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
R       172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:07, Serial10/0/0
          [120/1] via 209.165.200.234, 00:00:08, Serial10/0/1
      209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial10/0/0
C       209.165.200.232 is directly connected, Serial10/0/1
```

R1 masih hanya menunjukkan subnetnya sendiri untuk jaringan 172.30.0.0. R1 belum memiliki rute untuk subnet 172.30.0.0 di R3.

Ketikkan perintah:

R1#show ip route

Output :

```

R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
    172.30.0.0/24 is subnetted, 2 subnets
C    172.30.1.0 is directly connected, FastEthernet0/0
C    172.30.2.0 is directly connected, FastEthernet0/1
    209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0

```

R3 masih hanya menunjukkan subnetnya sendiri untuk jaringan 172.30.0.0. R3 belum memiliki rute untuk subnet 172.30.0.0 di R1.

Ketikkan perintah:

R3#show ip route

Output :

```

R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
C    209.165.200.232 is directly connected, Serial0/0/1

```

Tugas 6: Menonaktifkan Automatic Summarization.

Perintah `no auto-summary` digunakan untuk menonaktifkan *automatic summarization* pada RIPv2. Setelah menonaktifkan *auto summarization* pada semua router, maka router tidak akan lagi meringkas rute dalam batas jaringan besar.

Ketikkan perintah:

R2(config)#router rip

R2(config-router)#no auto-summary

R1(config)#router rip

R1(config-router)#no auto-summary

R3(config)#router rip

R3(config-router)#no auto-summary

Perintah `show ip route` dan `ping` dapat digunakan untuk memverifikasi apakah *automatic summarization* sudah tidak aktif.

Tugas 7: Memeriksa Routing Tables.

Jaringan LAN yang terhubung dengan R1 dan R3 sekarang harus masuk dalam ketiga *routing table*. Ketikkan perintah :

R2#show ip route

Output :

```
10.0.0.0/16 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 is variably subnetted, 7 subnets, 3 masks
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:01:28, Serial0/0/0
    [120/1] via 209.165.200.234, 00:01:56, Serial0/0/1
R    172.30.1.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R    172.30.2.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R    172.30.100.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.110.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.200.16/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R    172.30.200.32/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
C    209.165.200.232 is directly connected, Serial0/0/1R2#
```

R1#show ip route

Output :

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:02:13, Serial0/0/0
R    10.1.0.0/16 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.30.1.0/24 is directly connected, FastEthernet0/0
C    172.30.2.0/24 is directly connected, FastEthernet0/1
R    172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
```

R3#show ip route

Output :

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:02:28, Serial0/0/1
R    10.1.0.0/16 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
R    172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R    172.30.1.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
R    172.30.2.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
C    209.165.200.232 is directly connected, Serial0/0/1
```

Tugas 8: Verifikasi Konektivitas Jaringan.

Langkah – langkah :

1. Cek konektivitas antara router R2 ke PC.

R2#ping [ip address PC] .

2. Cek konektivitas antar PC dalam jaringan.

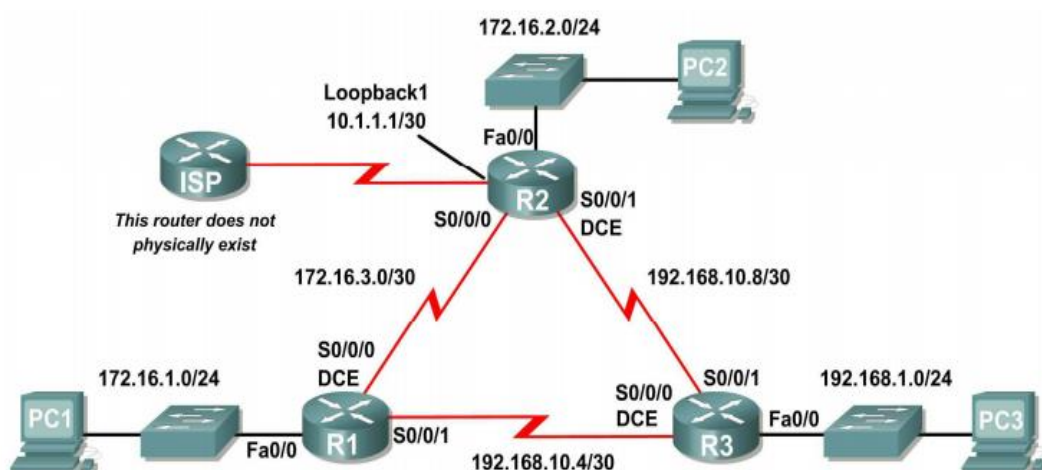
Tugas 9: Dokumentasi

Dari setiap router, simpan output dari perintah-perintah berikut dalam file dengan format text (.txt)

- show running-config
- show ip route
- show ip interface brief
- show ip protocols

✓ EIGRP

Konfigurasi Dasar EIGRP



Addressing table

device	interface	IP address	subnet mask	default gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	Lo1	10.1.1.1	255.255.255.252	N/A
R3	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A

	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Persiapan jaringan

- a. Buat topologi jaringan seperti pada gambar di atas.
 - b. Hapus semua konfigurasi yang ada pada setiap router.
 - c. Nonaktifkan peringkasan otomatis pada router.
 - d. Konfigurasi peringkasan manual pada router.
 - e. Konfigurasi default route statis.
 - f. menyebarkan default EIGRP rute ke tetangga.
 - g. Dokumentasi konfigurasi EIGRP
1. Konfigurasi mengaktifkan Serial dan *Ethernet Address*
 - a. Konfigurasi interfaces pada Router 1 (R1), Router 2 (R2), dan Router 3 (R3)
 - b. Cek *IP Address* dan *Interfaces* dengan mengetikan `commandshow ip interface brief`.
 - c. Konfigurasi Ethernet Interface pada PC1, PC2, dan PC3
 - d. Cek konfigurasi PC dengan cara ping ke *default gateway*
 2. Konfigurasi EIGRP pada Router R1.
 - a. Aktifkan EIGRP

Gunakan perintah `eigrp router` dalam mode konfigurasi global untuk mengaktifkan EIGRP pada router R1. Akhiri dengan angka 1 sebagai parameter `autonomous-system`.

```
R1(config)#router eigrp 1
```
 - b. Konfigurasi classful jaringan 172.16.0.0


```
R1(config-router)#network 172.16.0.0
```

```
R1(config-router)#
```

router akan mulai mengirimkan pesan keluar berupa update dari EIGRP pada setiap jaringan interface 172.16.0.0. Update EIGRP akan dikirim keluar dari FastEthernet0 / 0 dan Serial0/0/0 karena keduanya berada pada subnet 172.16.0.0

- c. Konfigurasi router untuk menginformasikan jaringan 192.168.10.4/30 yang ada pada interface Serial0/0/1.

Gunakan option wildcard-mask pada command network agar yang di informasikan oleh interface hanya subnetnya bukan keseluruhan jaringan 192.168.10.0 .

Wildcard-mask bisa di ibaratkan sebagai kebalikan dari subnet mask. Untuk menghitungnya sebagai berikut:

```
255.255.255.255
- 255.255.255.252 kurangi dengan subnet mask-nya
-----
0. 0. 0. 3 => wildcard-mask
```

```
R1(config-router)# network 192.168.10.4 0.0.0.3
R1(config-router)#
```

Setelah itu kembalikan dalam mode EXEC khusus dan simpan konfigurasinya ke NVRAM.

```
R1(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

3. Konfigurasi EIGRP pada router 2 dan router 3

- a. Aktifkan EIGRP routing pada router 2 seperti pada router 1.

```
R2(config)#router eigrp 1
R2(config-router)#
```

- b. Konfigurasi classful jaringan 172.16.0.0

```
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1
(Serial0/0/0) is up:new adjacency
```

Perhatikan bahwa DUAL mengirim pesan pemberitahuan ke konsol yang menyatakan bahwa hubungan tetangga dengan EIGRP router lain telah dibentuk.

- c. Konfigurasi router untuk menginformasikan jaringan **192.168.10.8/30** yang ada pada interface Serial0/0/1. Lakukan seperti pada router 1.

```
R2(config-router)#network 192.168.10.8 0.0.0.3  
R2(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console R2#
```

- d. Konfigurasikan router 3 seperti router 1 dan router 2 namun dengan IP **192.168.10.4 dan 192.168.10.8**

```
R3(config)#router eigrp 1  
R3(config-router)#network 192.168.1.0  
R3(config-router)#network 192.168.10.4 0.0.0.3  
R3(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5  
(Serial0/0/0) is up:  
new adjacency  
R3(config-router)#network 192.168.10.8 0.0.0.3  
R3(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9  
(Serial0/0/1) is up:  
new adjacency  
R3(config-router)#end  
%SYS-5-CONFIG_I: Configured from console by console R3#
```

Perhatikan bahwa ketika jaringan untuk link serial dari R3 ke R1 dan R3 ke R2 ditambahkan ke EIGRP konfigurasi, DUAL mengirim pesan pemberitahuan ke konsol yang menyatakan bahwa hubungan tetangga dengan EIGRP router lain telah dibentuk.

Lakukan uji koneksi antar PC dari tiap jaringan !!

4. Verifikasi operasi EIGRP
- a. Lihat jaringan tetangga

Pada router R1, gunakan perintah **show ip eigrp neighbors** untuk melihat tabel tetangga dan memverifikasi bahwa EIGRP telah membentuk kedekatan dengan router R2 dan R3.

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 172.16.3.2 Ser0/0/0 10 00:36:51 40 500 0 13
1 192.168.10.6 Ser0/0/1 11 00:26:51 40 500 0 4
R1#
```

b. Lihat informasi routing protocol

Pada router R1, gunakan perintah **show ip protocols** untuk melihat informasi tentang routing protokol operasi.

```
R1#show ip protocols
Routing Protocol is "eigrp 1 "
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 1
Automatic network summarization is in effect
Automatic address summarization:
Maximum path: 4
Routing for Networks:
172.16.0.0
192.168.10.4/30
Routing Information Sources:
Gateway Distance Last Update
172.16.3.2 90 4811399
192.168.10.6 90 5411677
Distance: internal 90 external 170
```

Perhatikan bahwa output menentukan proses ID yang digunakan oleh EIGRP. Ingat, ID proses harus menjadi sama pada semua router untuk EIGRP untuk mendirikan adjacencies tetangga dan berbagi informasi routing.

5. Periksa EIGRP route pada table routing.

a. Lihat routing table yang ada pada router 1

EIGRP rute dilambangkan dalam tabel routing dengan D, yang merupakan singkatan dari DUAL (Diffusing Update Algorithm), yang merupakan algoritma routing yang digunakan oleh EIGRP.

```
R1#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M -  
mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter  
area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type  
2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E -  
EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-  
IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
```

```
D 172.16.0.0/16 is a summary, 01:16:19, Null0
```

```
C 172.16.1.0/24 is directly connected, FastEthernet0/0
```

```
D 172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20,  
Serial0/0/0
```

```
C 172.16.3.0/30 is directly connected, Serial0/0/0
```

```
D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:06:18,  
Serial0/0/1
```

```
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
```

```
D 192.168.10.0/24 is a summary, 01:06:07, Null0
```

```
C 192.168.10.4/30 is directly connected, Serial0/0/1
```

```
D 192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07,  
Serial0/0/1  
R1#
```

Perhatikan bahwa jaringan induk 172.16.0.0/16 adalah variabel yang dijadikan subnet dengan tiga rute cabang baik / 24 atau / 30. Juga perhatikan bahwa EIGRP secara otomatis termasuk ringkasan rute ke Null0 untuk 172.16.0.0/16 jaringan. Rute 172.16.0.0/16 tidak benar-benar merupakan jalan untuk mencapai induk jaringan, 172.16.0.0/16. Jika paket ditujukan untuk 172.16.0.0/16 tidak sesuai dengan salah satu dari 2 cabang rute, maka paket akan dikirim ke interface Null0.

```
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks  
D 172.16.0.0/16 is a summary, 01:16:19, Null0  
C 172.16.1.0/24 is directly connected, FastEthernet0/0  
D 172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20,  
Serial0/0/0  
C 172.16.3.0/30 is directly connected, Serial0/0/0
```

Jaringan 192.168.10.0/24 juga memiliki variasi subnetted dan mencakup rute Null0.

```
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks  
D 192.168.10.0/24 is a summary, 01:06:07, Null0  
C 192.168.10.4/30 is directly connected, Serial0/0/1  
D 192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07,  
Serial0/0/1
```

b. Lihat routing table yang ada pada router 3

Tabel routing digunakan untuk menunjukkan bahwa R3 R1 dan R2 secara otomatis meringkas jaringan 172.16.0.0/16 dan mengirimnya sebagai update routing tunggal. Karena ringkasan otomatis, R1 dan R2 tidak menyebarkan subnet individu. Pada R3 akan melalui dua rute yang sama jaraknya ketika menuju 172.16.0.0/16 baik dari R1 ataupun R2, kedua rute tersebut dimasukkan ke dalam tabel routing.

```
R3#show ip route
```

```
<output omitted>
```

```
D 172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:15:35,  
Serial0/0/0  
[90/2172416] via 192.168.10.9, 01:15:22, Serial0/0/1  
C 192.168.1.0/24 is directly connected, FastEthernet0/0  
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks  
D 192.168.10.0/24 is a summary, 01:15:22, Null0  
C 192.168.10.4/30 is directly connected, Serial0/0/0  
C 192.168.10.8/30 is directly connected, Serial0/0/1  
R3#
```

Lakukan Pengiriman Paket dari PC3 ke PC2 dengan mode simulasi, secara berulang kali. Apa yang terjadi ?

6. Konfigurasi EIGRP metrics

a. Lihat informasi EIGRP metric

Nilai yang akan ditampilkan adalah bandwidth, delay, reliability dan load atau beban dari router tersebut.

```
R1#show interface serial0/0/0
```

```
Serial0/0/0 is up, line protocol is up (connected)
```

```
Hardware is HD64570
```

```
Internet address is 172.16.3.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,  
load 1/255
```

```
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

```
<output omitted>
```

b. Modifikasi bandwidth dari serial interface

Bandwidth metric default dari setiap serial interface adalah 1544 Kbits.

Untuk praktikum ini, hubungan antara R1 dan R2 akan dikonfigurasi dengan bandwidth 64 kbps, dan link antara R2 dan R3 akan dikonfigurasi dengan bandwidth 1024 kbps. Gunakan perintah bandwidth untuk memodifikasi bandwidth interface serial dari setiap router.

R1 router:

```
R1(config)#interface serial0/0/0
```

```
R1 (config-if) #bandwidth 64
```

R2 router:

```
R2 (config) #interface serial0/0/0
```

```
R2 (config-if) #bandwidth 64
```

```
R2 (config) #interface serial0/0/1
```

```
R2 (config-if) #bandwidth 1024
```

R3 router:

```
R3 (config) #interface serial0/0/1
```

```
R3 (config-if) #bandwidth 1024
```

Lakukan Pengiriman Paket dari PC3 ke PC2 dengan mode simulasi, secara berulang kali. Apa yang terjadi ?

Catatan: Perintah **bandwidth** hanya memodifikasi bandwidth metrik yang digunakan oleh routing protokol, bukan bandwidth linkfisik.

c. Verifikasi dari modifikasi bandwith

Gunakan command **show ip interface** untuk melakukan verifikasi bandwith yang telah dimodifikasi.

```
R1#show interface serial0/0/0
```

```
Serial0/0/0 is up, line protocol is up (connected)
```

```
Hardware is HD64570
```

```
Internet address is 172.16.3.1/30
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255,  
load 1/255
```

```
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

```
<output omitted>
```

```
R2#show interface serial0/0/0
```

```
Serial0/0/0 is up, line protocol is up (connected)
```

```
Hardware is HD64570
```

```
Internet address is 172.16.3.2/30
```

```
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255,  
load 1/255
```

```

Encapsulation HDLC, loopback not set, keepalive set (10 sec)
<output omitted>
R3#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.10.9/30
MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255,
load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
<output omitted>

```

Catatan: gunakan perintah **no bandwidth** untuk mengembalikan bandwidth pada kondisi defaultnya.

7. Periksa jaringan penerus (successor) dan kelayakan jarak

Periksa jarak jaringan penerus dan kelayakan dalam tabel routing di R2.

Lakukan dengan perintah **show ip route**

```

R2#show ip route
<output omitted>
10.0.0.0/30 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback1
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:00:52, Null0
D 172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52,
Serial0/0/0
C 172.16.2.0/24 is directly connected, FastEthernet0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11,
Serial0/0/1
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:00:11, Null0
D 192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C 192.168.10.8/30 is directly connected, Serial0/0/1
R2#

```

Dari table routing pada R2 dapat dilihat rute mana yang sebaiknya dipilih oleh PC 1 untuk mengirimkan pakatnya.

8. Menentukan apakah R1 adalah Penerus yang layak untuk Rute dari R2 ke Jaringan 192.168.1.0.

Sebuah rute penerus yang layak adalah rute tetangga yang memiliki jalur cadangan yang layak. Untuk menjadi rute penerus layak, R1 harus memenuhi kondisi kelayakan. Kondisi kelayakan (FC) adalah ketika jarak jaringan tetangga dilaporkan ke jaringan yang kurang layak dari router lokal ke jaringan dengan tujuan yang sama.

- a. Periksa table routing pada R1

```
R1#show ip route
<output omitted>
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:42:59, Null0
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:43:00,
Serial0/0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2172416] via 192.168.10.6,
00:42:26, Serial0/0/1
192.168.10.0/24 is variably subnetted, 3 subnets, 2
masks
D 192.168.10.0/24 is a summary, 00:42:20, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6,
00:42:20,
Serial0/0/1
R1#
```

- b. Periksa table routing pada R2

```
R2#show ip route
<output omitted>
10.0.0.0/30 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback1
```



```

172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:00:52, Null0
D 172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52,
Serial0/0/0
C 172.16.2.0/24 is directly connected, FastEthernet0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/3014400] via 192.168.10.10,
00:00:11, Serial0/0/1
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:00:11, Null0
D 192.168.10.4/30 [90/3523840] via 192.168.10.10,
00:00:11, Serial0/0/1
C 192.168.10.8/30 is directly connected, Serial0/0/1
R2#

```

9. Periksa table topologi routing EIGRP

a. Lihat tabel topologi EIGRP.

Gunakan perintah `show ip eigrp topology` untuk melihat tabel topologi EIGRP di R2.

```

R2#show ip eigrp topology
IP-EIGRP Topology Table for AS 1
Codes: P - Passive, A - Active, U - Update, Q - Query, R
- Reply,
r - Reply status
P 172.16.2.0/24, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
via Connected, Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
via Summary (28160/0), Null0
P 192.168.10.0/24, 1 successors, FD is 3011840
via Summary (3011840/0), Null0
P 172.16.1.0/24, 1 successors, FD is 40514560

```

```
via 172.16.3.1 (40514560/28160), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
via 192.168.10.10 (3014400/28160), Serial0/0/1
via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
via 192.168.10.10 (3523840/2169856), Serial0/0/1
R2#
```

b. Lihat informasi detail dari topologi EIGRP

Tambahkan parameter jaringan untuk melihat informasi secara detail.

```
R2#show ip eigrp topology 192.168.1.0
```

```
IP-EIGRP (AS 1): Topology entry for 192.168.1.0/24
State is Passive, Query origin flag is 1, 1 Successor(s),
FD is 3014400
Routing Descriptor Blocks:
192.168.10.10 (Serial0/0/1), from 192.168.10.10, Send
flag is 0x0
Composite metric is (3014400/28160), Route is Internal
Vector metric:
Minimum bandwidth is 1024 Kbit
Total delay is 20100 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
172.16.3.1 (Serial0/0/0), from 172.16.3.1, Send flag is
0x0
Composite metric is (41026560/2172416), Route is Internal
Vector metric:
Minimum bandwidth is 64 Kbit
Total delay is 40100 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 2
R2#
```

10. Non aktifkan peringkasan otomatis dari EIGRP

a. Periksa table routing pada router 3

Perhatikan R3 yang tidak menerima rute individu untuk 172.16.1.0/24, 172.16.2.0/24 dan 172.16.3.0/24. Sebaliknya, tabel routing hanya memiliki ringkasan rute ke alamat jaringan classful dari 172.16.0.0/16 melalui router R1. Hal ini akan menyebabkan paket yang seharusnya untuk 172.16.2.0/24 dikirim melalui router R1 tidak dikirim langsung ke router R2.

```
R3#show ip route
```

```
<output omitted>
```

```
D 172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:21:54,  
Serial0/0/0
```

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

```
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
```

```
D 192.168.10.0/24 is a summary, 01:21:47, Null0
```

```
C 192.168.10.4/30 is directly connected, Serial0/0/0
```

```
C 192.168.10.8/30 is directly connected, Serial0/0/1
```

```
R3#
```

Perhatikan bahwa jarak dari R2 yang lebih tinggi dari jarak layak dari R1.

b. Periksa topologi IP dari EIGRP

```
R3#show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS 1
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R -  
Reply,
```

```
r - Reply status
```

```
P 192.168.1.0/24, 1 successors, FD is 28160  
via Connected, FastEthernet0/0
```

```
P 192.168.10.4/30, 1 successors, FD is 2169856  
via Connected, Serial0/0/0
```

```
P 192.168.10.0/24, 1 successors, FD is 2169856  
via Summary (2169856/0), Null0
```

```
P 172.16.0.0/16, 1 successors, FD is 2172416  
via 192.168.10.5 (2172416/28160), Serial0/0/0
```

```
via 192.168.10.9 (3014400/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3011840
via Connected, Serial0/0/1
```

- c. Nonaktifkan automatic summarization pada ketiga router yang ada.

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
R2(config)#router eigrp 1
R2(config-router)#no auto-summary
R3(config)#router eigrp 1
R3(config-router)#no auto-summary
```

- d. Periksa ulang table routing pada R3

Perhatikan rute individu untuk 172.16.1.0/24, 172.16.2.0/24, dan sekarang subnet 172.16.3.0/24 telah ada dan ringkasan rute Null tidak lagi terdaftar.

```
R3#show ip route
<output omitted>
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.1.0/24 [90/2172416] via 192.168.10.5, 00:02:37,
Serial0/0/0
D 172.16.2.0/24 [90/3014400] via 192.168.10.9, 00:02:39,
Serial0/0/1
D 172.16.3.0/30 [90/41024000] via 192.168.10.9, 00:02:39,
Serial0/0/1
[90/41024000] via 192.168.10.5, 00:02:37, Serial0/0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/0
C 192.168.10.8/30 is directly connected, Serial0/0/1
R3#
```

11. Konfigurasi Manual Peringkasan

a. Tambahkan loopback address pada router 3

Tambahkan dua alamat loopback, 192.168.2.1/24 dan 192.168.3.1/24, ke router R3. Virtual interface ini akan digunakan untuk mewakili jaringan secara manual yang diringkas bersama dengan 192.168.1.0/24.

```
R3(config)#interface loopback1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state
to upR3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#interface loopback2
%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2,
changed state
to up
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#
```

b. Tambahkan jaringan 192.168.3.0 dan 192.168.2.0 untuk konfigurasi EIGRP pada R3.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
```

c. Verifikasi rute yang terbaru

```
R1#show ip route
<output omitted>
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07,
Serial0/0/1
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:15:07,
Serial0/0/1
```

```

D 192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:01:07,
Serial0/0/1
D 192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:00:57,
Serial0/0/1
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1
R1#

```

- d. Aplikasikan peringkasan manual untuk outbound interfaces.

Rute ke 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 jaringan dan dapat diringkaskan dalam yang 192.168.0.0/22 jaringan tunggal. Gunakan ip eigrp ringkasan-alamat sebagai nomor network address subnet-mask summarization perintah untuk mengkonfigurasi manual pada masing-masing outbound interface terhubung ke tetangga EIGRP.

```

R3(config)#interface serial0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0
255.255.252.0
R3(config-if)#interface serial0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0
255.255.252.0
R3(config-if)#

```

- e. Verifikasi rute ringkasan

```

R1#show ip route
<output omitted>
172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07,
Serial0/0/1
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.0.0/22 [90/2172416] via 192.168.10.6, 00:01:11,
Serial0/0/1

```

```
192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1
R1#
```

12. Konfigurasi dan penyebaran Rute Default statis.

a. Konfigurasi static default route pada router 2

Gunakan alamat loopback yang telah dikonfigurasi untuk mensimulasikan link ke ISP sebagai interface keluar.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R2(config)#
```

b. Masukkan static route pada update dari EIGRP

```
R2(config)#router eigrp 1
R2(config-router)#redistribute static
R2(config-router)#
```

c. Lakukan verifikasi terhadap static default route

Lihat tabel routing pada router R1 untuk memverifikasi bahwa static default route sedang didistribusikan melalui EIGRP.

```
R1#show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
```

```
192.168.10.0/30 is subnetted, 2 subnets
C      192.168.10.4 is directly connected, Serial0/0/1
D      192.168.10.8 [90/3523840] via 192.168.10.6,
01:06:01, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      172.16.1.0/24 is directly connected, FastEthernet0/0
```

```
D      172.16.2.0/24 [90/3526400] via 192.168.10.6,  
01:05:39, Serial0/0/1  
C      172.16.3.0/30 is directly connected, Serial0/0/0  
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:02:14,  
Serial0/0/1  
D      192.168.0.0/22 [90/2172416] via 192.168.10.6, 01:05:38,  
Serial0/0/1
```

13. Dokumentasi

Lakukan dokumentasi pada setiap router kemudian simpan dalam format .txt

- show running-config
- show ip route
- show ip interface brief
- show ip protocols

MODULE 3

Dynamic Routing – OSPF

V. Tujuan Praktikum

- Praktikan mengetahui konsep dasar dynamic routing.
- Praktikan mengetahui kelebihan dan kekurangan dari dynamic routing.
- Praktikan dapat melakukan simulasi konfigurasi router pada jaringan dengan menggunakan dynamic routing (dalam praktikum ini menggunakan packet tracer).
- Praktikan mengetahui perbedaan penggolongan link-state dan distance vector pada algoritma dinamic routing.
- Praktikan dapat melakukan simulasi konfigurasi router pada jaringan dengan menggunakan algoritma dinamic routing (dalam praktikum ini menggunakan packet tracer).
- Praktikan mengetahui kelebihan dan kekurangan dari algoritma dinamic routing OSPF.

VI. Alat dan Bahan

- Alat tulis
- Komputer
- Software Cisco Packet Tracer Latest Version

VII. Landasan Teori

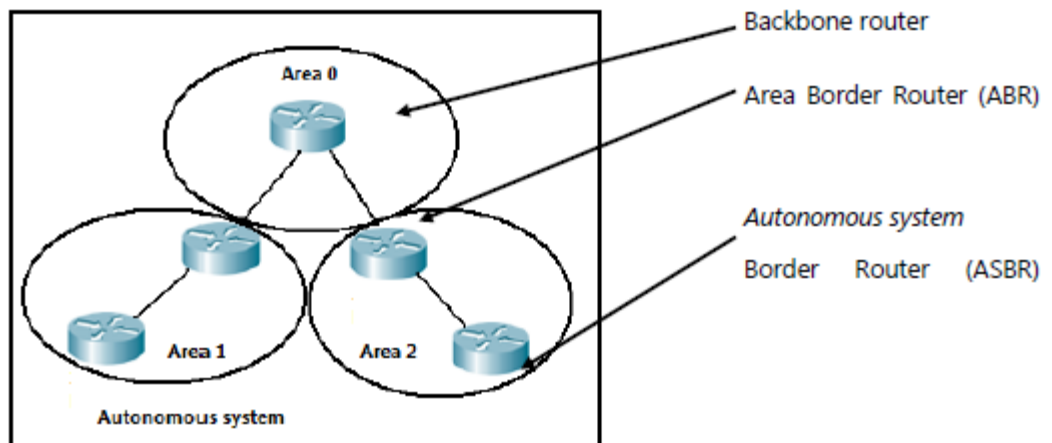
OSPF

Open Shortest Path First (OSPF) didesain sebagai pengganti dari RIP dan mengambil dari versi sebelumnya dari Intermediate System to Intermediate System (IS-IS). OSPF adalah protocol yang handal dengan fasilitas least-cost routing, multipath routing dan load balancing. Penentuan jalur tercepat dan terbaik pada jaringan dihitung dengan metode algoritma Dijkstra. Pertama, sebuah pohon jalur terpendek (shortest path tree) akan di bangun, dan kemudian routing table akan diisi dengan jalur-jalur terbaik yang dihasilkan dari pohon tersebut. OSPF melakukan coverage dengan cepat dan OSPF mendukung multiple route dengan cost (biaya) yang sama, ke tujuan yang sama.

OSPF memberikan kontribusi pada sebuah protocol yang cepat, scalable, dan kuat yang dapat ditetapkan secara aktif pada ribuan network produksi. OSPF seharusnya dirancang dengan cara hierarkis, yang pada dasarnya berarti bahwa anda dapat memisahkan *internetwork* yang lebih besar menjadi *internetwork – internetwork* yang lebih kecil yang disebut dengan *area*. Ini adalah rancangan terbaik untuk OSPF. Alasan untuk menciptakan OSPF dalam rancangan hierarkis, antara lain :

- Untuk mengurangi *overhead* (waktu pemrosesan) routing.
- Untuk mempercepat *convergence*
- Untuk membatasi ketidakstabilan network disebuah area dari network saja

Lihat gambar dibawah ini :



Gambar tersebut menunjukkan sebuah rancangan yang sederhana yang khas OSPF. Perhatikan bahwa setiap router terhubung ke backbone yang disebut *area 0*, atau *area backbone*. OSPF harus memiliki sebuah area 0, dan semua router harus terhubung ke area ini jika memungkinkan, tetapi router – router yang menghubungkan area – area lain ke backbone di dalam sebuah AS disebut *Area Border Routers* (ABRs). Meskipun pemilihan paling sedikit satu interface harus berada di area 0.

OSPF bekerja didalam sebuah *autonomous system*, tetapi juga menghubungkan banyak *autonomous system* bersama. Router yang menghubungkan beberapa AS bersama disebut sebuah *Autonomous system Border Router* (ASBR).

Terminologi OSPF

Berikut ini adalah istilah – istilah penting OSPF yang harus dipahami :

Link Sebuah *link* adalah sebuah network atau sebuah interface router yang ditempatkan pada sebuah network. Ketika sebuah interface ditambahkan ke proses OSPF, ia dianggap oleh OSPF sebagai sebuah link. Link ini atau interface, akan memiliki informasi status yang berkaitan dengannya (status hidup atau mati) dan memiliki satu atau lebih alamat IP.

Router ID *Router ID* (RID) adalah sebuah alamat IP yang digunakan untuk mengidentifikasi router. Cisco memilih menggunakan RID dengan menggunakan alamat IP tertinggi dari semua interface loopback yang

dikonfigurasi. Jika tidak ada interface loopback yang terkonfigurasi dengan alamat – alamat IP, OSPF akan memilih alamat IP tertinggi dari semua interface-interface fisik yang aktif.

Neighbors *Neighbors* adalah dua atau lebih router yang memiliki sebuah interface pada sebuah network yang sama, seperti dua router yang terhubung pada sebuah link serial point- to-point.

Adjacency *Adjacency* atau kedekatan adalah sebuah hubungan antara dua buah router OSPF yang mengizinkan pertukaran langsung dari update – update route.

Neighborship Database *Neighborship Database* adalah daftar dari semua router OSPF, dimana paket hello dari router tersebut sudah terlihat. Berbagai detail, termasuk router ID dan statusnya, dipelihara pada setiap router didalam *Neighborship Database*.

Topology Database *Topology Database* mengandung informasi dari semua paket *Link State Advertisement* (LSA) yang telah diterima untuk sebuah area. Router menggunakan informasi dari topology database sebagai input kedalam algoritma Dijkstra yang menghitung jalur terpendek ke semua network.

Link State Advertisement *Link State Advertisement (LSA)* adalah paket data OSPF yang mengandung informasi link-state dan informasi routing yang dibagi diantara router-router OSPF. Sebuah router OSPF akan bertukar paket – paket LSA hanya dengan router-router dimana ia telah menetapkan adjacency.

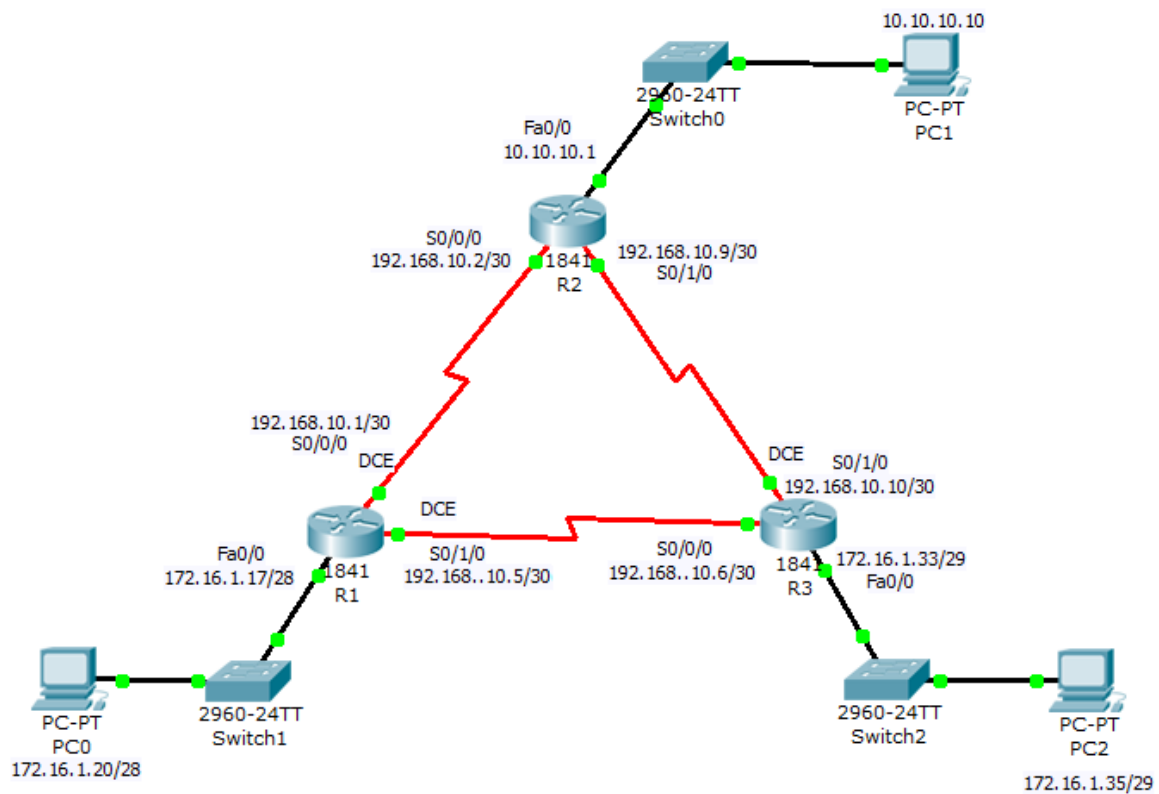
OSPF areas sebuah area OSPF adalah pengelompokan dari network dan router yang *contiguous* (berentetan). Semua router diarea yang sama berbagi sebuah Area ID yang sama. Karena sebuah router dapat menjadi sebuah anggota dari banyak area pada satu kesempatan, maka area ID diasosiasikan dengan interface tertentu di router. Ini akan mengizinkan beberapa interface untuk masuk ke area 1, sementara interface yang lain masuk ke area 0. Semua router di area yang sama memiliki tabel topologi yang sama. Ketika mengkonfigurasi OSPF, anda harus ingat bahwa harus ada area 0, dan biasanya ini di konfigurasi untuk router-router yang terhubung ke backbone

dari network. Area jg memainkan sebuah peranan dalam menetapkan sebuah organisasi network yang hierarkis, sesuatu yang meningkatkan skalabilitas OSPF.

VIII. Praktikum

B. Praktikum Dinamic Routing

Konfigurasi Dasar OSPF



Addressing Table (Lihat tabel terlampir di bawah)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

Langkah 1 : Siapkan Jaringan

1. Buat topologi jaringan seperti gambar diatas
2. Hapus semua konfigurasi yang ada pada router

Langkah 2 : Konfigurasi mengaktifkan Serial dan *Ethernet Address*

1. Konfigurasi interfaces pada Router 1 (R1), Router 2 (R2), dan Router 3 (R3)
2. Cek *IP Address* dan *Interfaces*
3. Konfigurasi Ethernet Interface pada PC1, PC2, dan PC3
4. Cek konfigurasi PC dengan cara ping ke *default gateway*

Langkah 3 : Konfigurasi OSPF pada Router 1 (R1)

1. Gunakan perintah Router OSPF dalam *global configuration mode* untuk mengaktifkan OSPF pada Router 1. Masukkan proses ID 1 untuk parameter proses-ID.

```
R1(config)#router ospf 1
```

```
R1(config-router)#
```

2. Konfigurasi jaringan LAN

Setelah berada dalam sub-mode konfigurasi Router OSPF, lakukan konfigurasi jaringan LAN 172.16.1.16/28 untuk dimasukkan dalam *update* OSPF yang dikirim keluar dari Router 1 (R1).

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
```

```
R1(config-router)#
```

3. Konfigurasi router untuk menyatakan jaringan 192.168.10.0/30 dikaitkan pada interface Serial0/0/0.

```
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
```

```
R1(config-router)#
```

4. Konfigurasi router untuk menyatakan jaringan 192.168.10.4/30 dikaitkan pada interface Serial0/0/1.

```
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

```
R1(config-router)#
```

5. Kembali ke EXEC mode

```
R1(config-router)#end
```

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

```
R1#
```

Langkah 4 : Konfigurasi router pada Router 2 (R2) dan Router 3 (R3)

1. Enable OSPF routing pada R2 dengan menggunakan perintah ospf.

Gunakan process ID 1.

```
Router(config)#router ospf 1
```

```
Router(config-router)#
```

2. Konfigurasi router untuk menyatakan jaringan LAN 10.10.10.0/24 dalam OSPF *update*.

```
Router(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

```
Router(config-router)#
```

3. Konfigurasi router untuk menyatakan jaringan 192.168.10.0/30 dikaitkan pada interface Serial0/0/0.

```
Router(config-router)#network 192.168.10.0 0.0.0.3 area 0
```

```
Router(config-router)#
```

```
00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on  
Serial0/0/0 from EXCHANGE to FULL, Exchange Done
```

Perhatikan bahwa jaringan untuk link serial dari R1 ke R2 yang ditambahkan ke konfigurasi OSPF, router mengirimkan pesan pemberitahuan ke konsol yang menyatakan bahwa hubungan tetangga dengan OSPF router lainnya telah dibentuk.

4. Konfigurasi router untuk menyatakan jaringan 192.168.10.8/30 dikaitkan pada interface Serial0/0/1.

```
Router(config-router)#network 192.168.10.8 0.0.0.3 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by consoleSaa
```

5. Konfigurasi OSPF router pada Router 3 (R3)

Gunakan proses ID 1. Konfigurasi router untuk menyatakan ketiga jaringan terhubung secara langsung. Ketika selesai, kembali ke EXEC mode.

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#
00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on
Serial0/0/0 from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
R3(config-router)#
00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on
Serial0/0/1 from EXCHANGE to FULL, Exchange Done
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Saat jaringan dari R3 ke R1 dan R3 ke R2 sudah ditambahkan pada konfigurasi OSPF, router tersebut mengirimkan *notification* ke *console*, yang menyatakan hubungan tetangga dengan router OSPF lainnya telah dibangun.

Langkah 5 : Konfigurasi IDs OSPF Router

OSPF Router ID digunakan untuk mengidentifikasi secara unik dalam OSPF router routing domain. Router Cisco menurunkan ID Router di dalam salah satu dari tiga cara dan dengan mengutamakan:

1. Alamat IP dikonfigurasi dengan perintah OSPF router-id.
2. Alamat IP tertinggi dari setiap alamat loopback dari router.
3. Alamat IP tertinggi aktif pada salah satu interfaces fisik router. Memeriksa IDs Router yang ada dalam topologi.

R3#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 192.168.10.10

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

<output omitted>

R3#show ip ospf

Routing Process "ospf 1" with ID 192.168.10.10

Supports only single TOS(TOS0) routes

Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

<output omitted>

R3#show ip ospf interface

FastEthernet0/0 is up, line protocol is up

Internet address is 172.16.1.33/29, Area 0

Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST,
Cost:

1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.10.10, Interface address
172.16.1.33

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5

Hello due in 00:00:00

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

<output omitted>

1. Gunakan *loopback addresses* untuk mengubah IDs router

```
R1(config)#interface loopback 0
```

```
R1(config-if)#ip address 10.1.1.1 255.255.255.255
```

```
R2(config)#interface loopback 0
```

```
R2(config-if)#ip address 10.2.2.2 255.255.255.255
```

```
R3(config)#interface loopback 0
```

```
R3(config-if)#ip address 10.3.3.3 255.255.255.255
```

2. Gunakan perintah `#show ip ospf` untuk memeriksa IDs router yang diganti.

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.3.3.3	0	FULL/ -	00:00:30	192.168.10.6
Serial0/0/1				
10.2.2.2	0	FULL/ -	00:00:33	192.168.10.2
Serial0/0/0				

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.3.3.3	0	FULL/ -	00:00:36	
192.168.10.10				
Serial0/0/1				
10.1.1.1	0	FULL/ -	00:00:37	192.168.10.1
Serial0/0/0				

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.2.2.2	0	FULL/ -	00:00:34	192.168.10.9
Serial0/0/1				
10.1.1.1	0	FULL/ -	00:00:38	192.168.10.5
Serial0/0/0				

3. Gunakan perintah `router-id` untuk mengubah ID router pada Router 1 (R1).

Beberapa versi IOS tidak tersedia untuk perintah `router-id`.

```
R1(config)#router ospf 1
```

```
R1(config-router)#router-id 10.4.4.4
```

Reload or use "clear ip ospf process" command, for this to take effect

Perintah tersebut digunakan router ospf yang sudah aktif (memiliki router tetangga).

Router-ID baru digunakan pada proses OSPF dengan cara restart secara manual

Untuk manual restart proses OSPF, gunakan perintah ip OSPF proses yang jelas.

```
R1#(config-router)#end
```

```
R1# clear ip ospf process
```

```
Reset ALL OSPF processes? [no]:yes
```

```
R1#
```

4. Gunakan perintah show ip ospf neighbor pada router R2 untuk memverifikasi bahwa router-ID R1 telah berubah.

```
R2#show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address
```

```
Interface
```

```
10.3.3.3 0 FULL/ - 00:00:36 192.168.10.10
```

```
Serial0/0/1
```

```
10.4.4.4 0 FULL/ - 00:00:37 192.168.10.1
```

```
Serial0/0/0
```

5. Hapus konfigurasi router ID

```
R1(config)#router ospf 1
```

```
R1(config-router)#router-id 10.4.4.4
```

Reload or use "clear ip ospf process" command, for this to take effect

6. Restart proses ospf dengan perintah clear ip ospf process

```
R1(config-router)#end
```

```
R1# clear ip ospf process
```

```
Reset ALL OSPF processes? [no]:yes
```

Langkah 6 : Verifikasi operasi OSPF

1. Pada router R1, Gunakan perintah "show ip ospf neighbor" untuk melihat informasi tentang tetangga OSPF router R2 dan R3. Anda harus dapat melihat neighbor ID dan IP address dari setiap router berdekatan, dan interface yang digunakan R1 untuk mencapai OSPF tetangga.

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
10.2.2.2	0	FULL/-	00:00:32	192.168.10.2
Serial0/0/0				
10.3.3.3	0	FULL/-	00:00:32	192.168.10.6
Serial0/0/1				

```
R1#
```

2. Pada router R1, gunakan perintah show ip protokol untuk melihat informasi tentang operasi protokol routing.

Perhatikan bahwa informasi yang telah dikonfigurasi pada Tugas sebelumnya, seperti protokol, process ID, neighbor ID, dan jaringan, muncul dalam output. IP address dari para tetangga yang berdekatan juga ditampilkan.

```
R1#show ip protocols
```

```
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.16.1.16 0.0.0.15 area 0
192.168.10.0 0.0.0.3 area 0
192.168.10.4 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
10.2.2.2 110 00:11:43
10.3.3.3 110 00:11:43
Distance: (default is 110)
R1#
```

Langkah 7 : Periksa rute OSPF dalam Tabel Routing

```
R1#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
 inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
 Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
 C 10.1.1.1/32 is directly connected, Loopback0
 O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:01:02, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
 C 172.16.1.16/28 is directly connected, FastEthernet0/0
 O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:12, Serial0/0/1
 192.168.10.0/30 is subnetted, 3 subnets
 C 192.168.10.0 is directly connected, Serial0/0/0
 C 192.168.10.4 is directly connected, Serial0/0/1
 O 192.168.10.8 [110/128] via 192.168.10.6, 00:01:12, Serial0/0/1
 [110/128] via 192.168.10.2, 00:01:02, Serial0/0/0
 R1#

Langkah 8 : Konfigurasi Biaya OSPF

1. Gunakan perintah show ip route pada router R1 untuk melihat biaya OSPF untuk mencapai jaringan 10.10.10.0/24.

R1#**show ip route**

<output omitted>

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
 C 10.1.1.1/32 is directly connected, Loopback0
 O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:16:56,
 Serial0/0/0
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
 C 172.16.1.16/28 is directly connected, FastEthernet0/0
 O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:17:06,
 Serial0/0/1
 192.168.10.0/30 is subnetted, 3 subnets
 C 192.168.10.0 is directly connected, Serial0/0/0
 C 192.168.10.4 is directly connected, Serial0/0/1

```
O 192.168.10.8 [110/128] via 192.168.10.6, 00:17:06,  
Serial0/0/1  
[110/128] via 192.168.10.2, 00:16:56, Serial0/0/0  
R1#
```

2. Gunakan perintah `show interfaces serial0/0/0` pada router R1 untuk melihat bandwidth interface Serial 0/0/0.

```
R1#show interfaces serial0/0/0  
Serial0/0/0 is up, line protocol is up (connected)  
Hardware is HD64570  
Internet address is 192.168.10.1/30  
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,  
load  
1/255  
Encapsulation HDLC, loopback not set, keepalive set (10 sec)  
Last input never, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0 (size/max/drops); Total output drops: 0  
<output omitted>
```

Biasanya pada serial link, bandwidth metric akan default 1544 kbits. Jika ini bukan bandwidth sebenarnya dari serial link, bandwidth perlu diubah sehingga biaya OSPF dapat dihitung dengan benar.

3. Gunakan perintah `bandwidth` untuk mengubah bandwidth interface serial router R2 dan R1 ke bandwidth yang sebenarnya, 64 kbps.

R1 router:

```
R1(config)#interface serial0/0/0  
R1(config-if)#bandwidth 64  
R1(config-if)#interface serial0/0/1  
R1(config-if)#bandwidth 64
```

R2 router:

```
R2(config)#interface serial0/0/0  
R2(config-if)#bandwidth 64  
R2(config)#interface serial0/0/1  
R2(config-if)#bandwidth 64
```

- Gunakan perintah `show ip ospf interface` pada router R1 untuk memverifikasi biaya dari link serial.

```
R1#show ip ospf interface
```

```
<output omitted>
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet address is 192.168.10.1/30, Area 0
```

```
Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT,
```

```
Cost:
```

```
1562
```

```
Transmit Delay is 1 sec, State POINT-TO-POINT,
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40,
```

```
Retransmit 5
```

```
Hello due in 00:00:05
```

```
Index 2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 1, maximum is 1
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 1 , Adjacent neighbor count is 1
```

```
Adjacent with neighbor 10.2.2.2
```

```
Suppress hello for 0 neighbor(s)
```

```
Serial0/0/1 is up, line protocol is up
```

```
Internet address is 192.168.10.5/30, Area 0
```

```
Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT,
```

```
Cost:
```

```
1562
```

```
Transmit Delay is 1 sec, State POINT-TO-POINT,
```

```
<output omitted>
```

- Gunakan perintah `ip ospf cost` untuk mengkonfigurasi biaya OSPF pada router R3

```
R3(config)#interface serial0/0/0
```

```
R3(config-if)#ip ospf cost 1562
```

```
R3(config-if)#interface serial0/0/1
```

```
R3(config-if)#ip ospf cost 1562
```

- Gunakan perintah `show ip ospf interface` pada router R3 untuk memverifikasi bahwa biaya link pada masing-masing link Serial sekarang 1562.

```
R3#show ip ospf interface
```

```
<output omitted>
```

```

Serial0/0/1 is up, line protocol is up
Internet address is 192.168.10.10/30, Area 0
Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT,
Cost:
1562
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:06
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 10.2.2.2
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 192.168.10.6/30, Area 0
Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT,
Cost:
1562
Transmit Delay is 1 sec, State POINT-TO-POINT,
<output omitted>

```

Langkah 9 : Mendistribusikan sebuah OSPF Default Route

1. Konfigurasi alamat loopback pada router R1 untuk mensimulasikan link ke ISP

```

R1(config)#interface loopback1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed
state to up
R1(config-if)#ip address 172.30.1.1 255.255.255.252

```
2. Konfigurasi static route default pada router R1

```

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R1(config)#

```
3. Gunakan perintah `default-information originate` untuk memasukkan rute statis pada update OSPF yang dikirim dari router R1.


```
R1(config)#router ospf 1
```

```
R1(config-router)#default-information originate
```

```
R1(config-router)#
```

4. Lihat tabel routing pada router R2 untuk memverifikasi default route statis yang didistribusikan melalui OSPF.

```
R2#show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 192.168.10.1 to network 0.0.0.0
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
C 10.2.2.2/32 is directly connected, Loopback0
```

```
C 10.10.10.0/24 is directly connected, FastEthernet0/0
```

```
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
O 172.16.1.16/28 [110/1563] via 192.168.10.1, 00:29:28,  
Serial0/0/0
```

```
O 172.16.1.32/29 [110/1563] via 192.168.10.10, 00:29:28,  
Serial0/0/1
```

```
192.168.10.0/30 is subnetted, 3 subnets
```

```
C 192.168.10.0 is directly connected, Serial0/0/0
```

```
O 192.168.10.4 [110/3124] via 192.168.10.10, 00:25:56,  
Serial0/0/1
```

```
[110/3124] via 192.168.10.1, 00:25:56, Serial0/0/0
```

```
C 192.168.10.8 is directly connected, Serial0/0/1
```

```
O*E2 0.0.0.0/0 [110/1] via 192.168.10.1, 00:01:11, Serial0/0/0
```

```
R2#
```

Langkah 10 : Dokumentasi

Lakukan dokumentasi pada setiap router kemudian simpan dalam format .txt

- Running configuration
- Routing table
- Interface summarization
- Output from show ip protocols

MODULE 4

VLAN Configuration with VTP

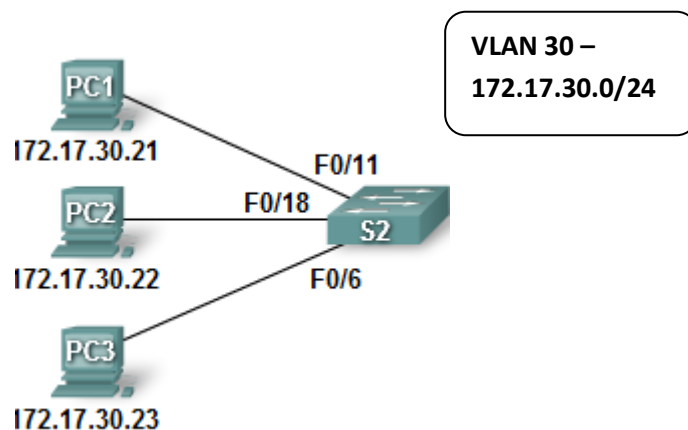
Tujuan :

- Memahami konsep Virtual LAN
- Memahami konsep Switch Port Mode
- Memahami konsep Trunking pada VLAN
- Memahami konsep VTP
- Dapat mengkonfigurasi VLAN menggunakan VTP
- Melakukan *troubleshoot* pada permasalahan VLAN

LANDASAN TEORI

Pengertian VLAN

Virtual Local Area Network, atau yang disebut VLAN (selanjutnya akan disebut VLAN) merupakan sebuah teknik untuk memisahkan subnet IP secara logis. VLAN akan membagi broadcast domain dengan memperbolehkan beberapa jaringan atau subjaringan berada dalam sebuah jaringan. Pada gambar berikut ditunjukkan sebuah VLAN dengan tiga computer.



Gambar 1 Contoh implementasi VLAN sederhana

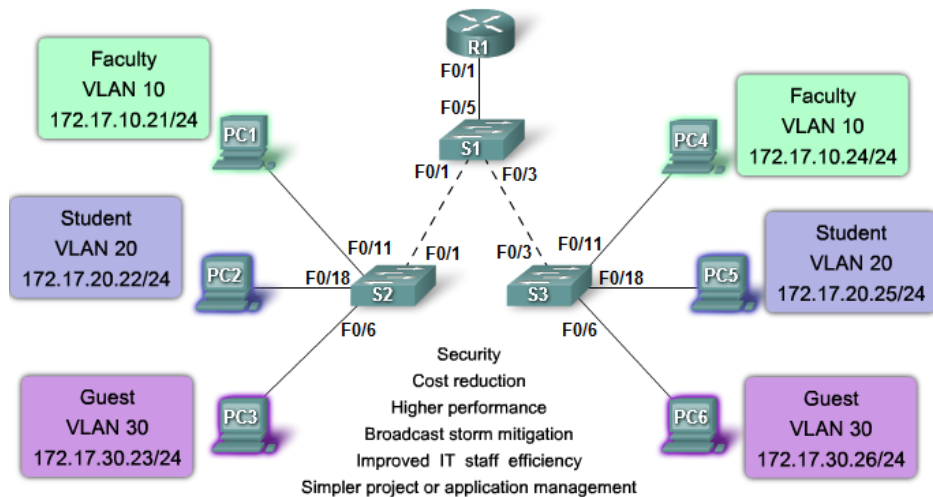
Komputer-komputer tersebut untuk dapat berkomunikasi harus memiliki IP address dan subnet mask yang sesuai pada VLAN tersebut. Switch yang digunakan harus dikonfigurasi untuk VLAN dan setiap port di dalam VLAN harus diset agar sesuai. Sebuah port switch dengan VLAN tunggal disebut access port. Harap diperhatikan, komputer-komputer yang tersambung secara fisik pada sebuah switch tidak selalu dapat langsung berkomunikasi. Perangkat pada dua jaringan dan subjaringan harus berkomunikasi melalui sebuah router (yang berada pada layer 3), baik yang menggunakan

VLAN atau tidak. VLAN tidak selalu dibutuhkan untuk menggunakan beberapa jaringan atau sub jaringan pada sebuah jaringan switching, akan tetapi terdapat beberapa keuntungan dengan digunakannya VLAN.

Keuntungan penggunaan VLAN

Produktivitas pengguna dan adaptabilitas jaringan adalah penunjang pertumbuhan dan kesuksesan bisnis. Pengimplementasian VLAN membuat sebuah jaringan lebih fleksibel untuk mendukung bisnis. Keuntungan-keuntungan utama menggunakan VLAN adalah sebagai berikut.

1. **Security**, dengan menggunakan VLAN kelompok pengguna yang memiliki data-data yang bersifat sensitive dapat dipisahkan dari pengguna lain pada jaringan yang sama. Hal ini akan mengurangi adanya kemungkinan pembobolan keamanan.
2. **Cost reduction**, adanya pengurangan biaya untuk upgrade perangkat jaringan yang mahal serta efisiensi yang didapat dari penggunaan bandwidth dan uplink.
3. **Higher performance**, membagi jaringan pada layer 2 kedalam beberapa kelompok secara logik mengurangi traffic pada jaringan dan meningkatkan performansi.
4. **Broadcast storm mitigation**, membagi sebuah jaringan kedalam VLAN mengurangi jumlah perangkat yang terlibat ketika terjadi broadcast storm (suatu keadaan ketika seluruh computer mengirimkan broadcast message yang membuat traffic pada jaringan padat). Hal ini dikarenakan dengan penggunaan VLAN maka akan membagi broadcast domain pada jaringan.
5. **Improved IT staff efficiency**, VLAN memudahkan pengelolaan jaringan. Karena user dengan kebutuhan yang sama dikelompokkan kedalam sebuah VLAN. Selain itu digunakannya penamaan juga memudahkan pengelola dalam mengidentifikasi user sebuah VLAN (dapat dilihat pada gambar di bawah)
6. **Simpler project or application management**, VLAN mengumpulkan user dan perangkat jaringan sesuai kebutuhan. Dengan membedakan perangkat atau user yang memiliki fungsi berbeda memudahkan pengelolaan pekerjaan yang terspesialisasi.



Gambar 2 Bernagai keuntungan yang didapatkan dengan menggunakan VLAN

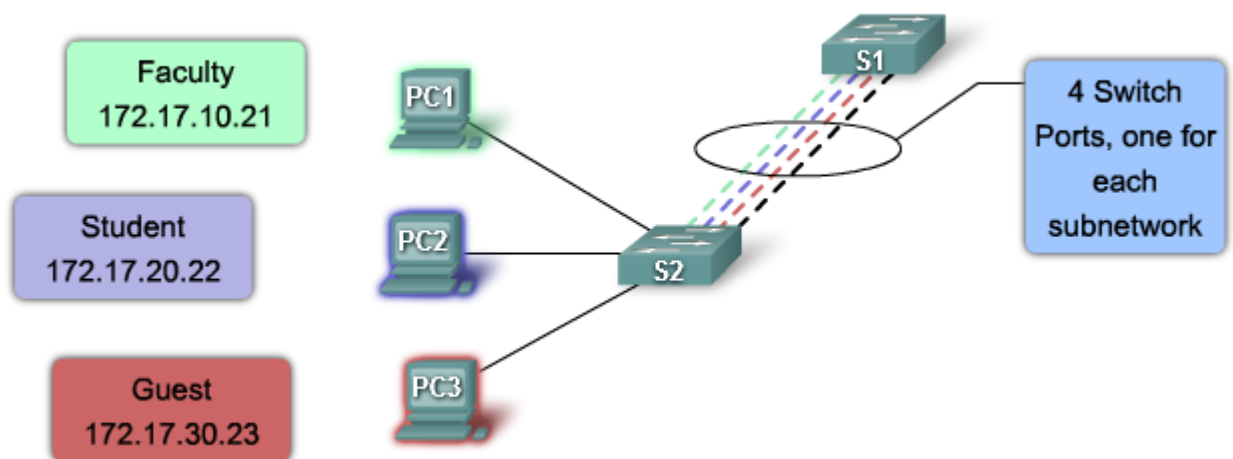
Switch Port Mode

Ketika melakukan konfigurasi VLAN, anda harus memberikan nomor ID untuk VLAN tersebut, selain itu anda juga dapat memberikannya sebuah nama (opsional). Pada saat mengimplementasikan VLAN, kita akan mencocokkan port dengan VLAN yang spesifik. Kita dapat mengkonfigurasi sebuah port ke dalam sebuah VLAN dengan meng-assign membership mode sesuai VLAN yang telah dispesifikasikan. Sebuah port dapat dikonfigurasi untuk mendukung tipe VLAN sebagai berikut:

1. **Static VLAN**, port-port pada switch diassign secara manual ke dalam VLAN. Static VLAN dapat dikonfigurasi menggunakan Cisco CLI. Konfigurasi static VLAN ini akan dilakukan berikutnya pada modul ini.
2. **Dynamic VLAN**, mode ini tidak banyak digunakan dan tidak akan dibahas pada praktikum ini. Bagaimanapun, ada baiknya kita mengetahui apa itu dynamic VLAN. Sebuah dynamic port VLAN membership dikonfigurasi menggunakan VLAN Membership Policy Server (VMPS). Dengan menggunakan VMPS, assign switch port dengan VLAN akan dilakukan secara dinamis sesuai dengan source MAC address yang tersambung dengan port. Keuntungannya adalah ketika kita memindahkan host dari satu port ke port lain pada switch di jaringan, switch tersebut akan secara otomatis melakukan assign port yang tersambung kedalam VLAN yang sesuai untuk host tersebut
3. **Voice VLAN**, mode ini akan memperbolehkan penggunaan IP phone pada VLAN. Sebelum melakukan konfigurasi voice VLAN pada port, lakukan konfigurasi VLAN untuk voice dan VLAN untuk data. Mode ini tidak akan dipelajari pada modul ini.

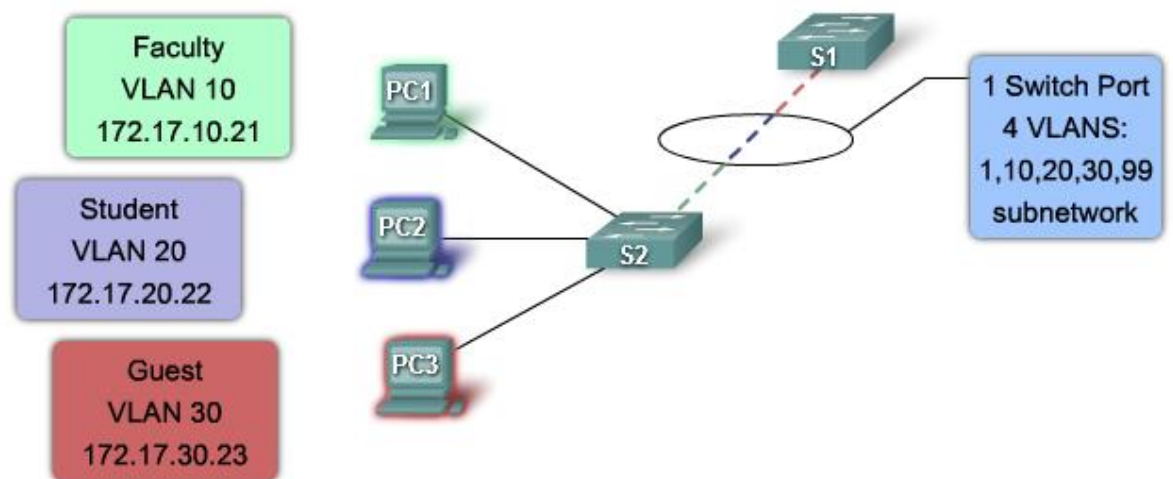
VLAN Trunk

Trunk merupakan link point-to-point antara satu atau lebih interface Ethernet switch dan perangkat jaringan lain, baik router atau switch. Ethernet trunk membawa traffic dari beberapa VLAN ke dalam satu link. Perhatikan gambar di bawah ini, diperlihatkan bahwa untuk memforward paket dari VLAN yang berbeda dibutuhkan satu link untuk masing-masing subnet. Hal ini tentu tidak efisien dilihat dari biaya yang dikeluarkan untuk masing-masing link.



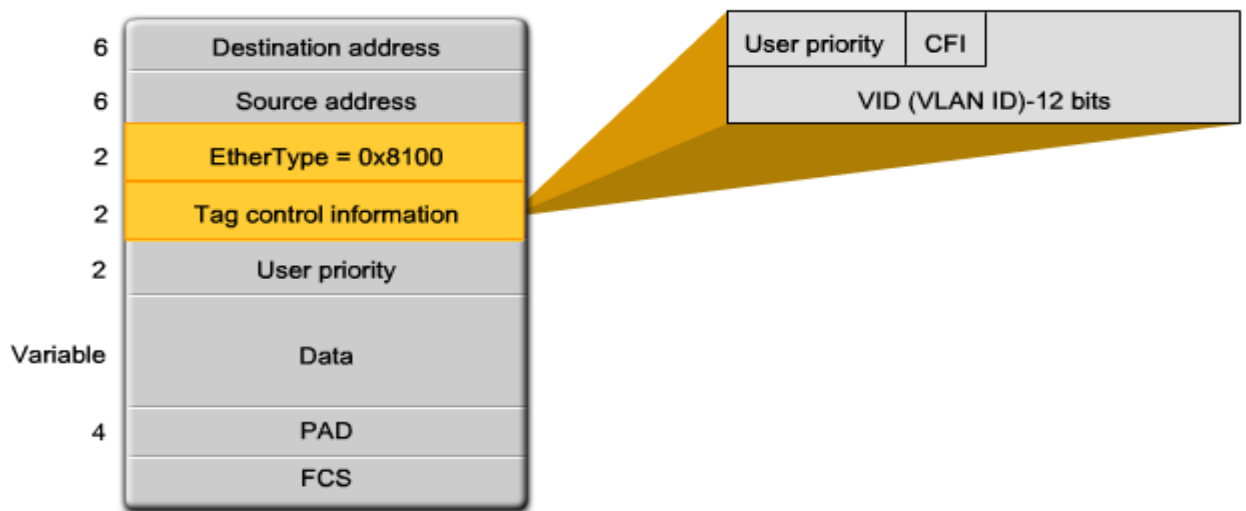
Gambar 3 Implementasi VLAN tanpa Ethernet trunk

Maka dari itu kita dapat menggunakan Ethernet trunk sebagai solusi atas masalah di atas. Dengan menggunakan trunk, keempat link VLAN dapat dikumpulkan ke dalam satu link (lihat gambar di bawah).



Gambar 4 Implementasi VLAN dengan Ethernet trunk

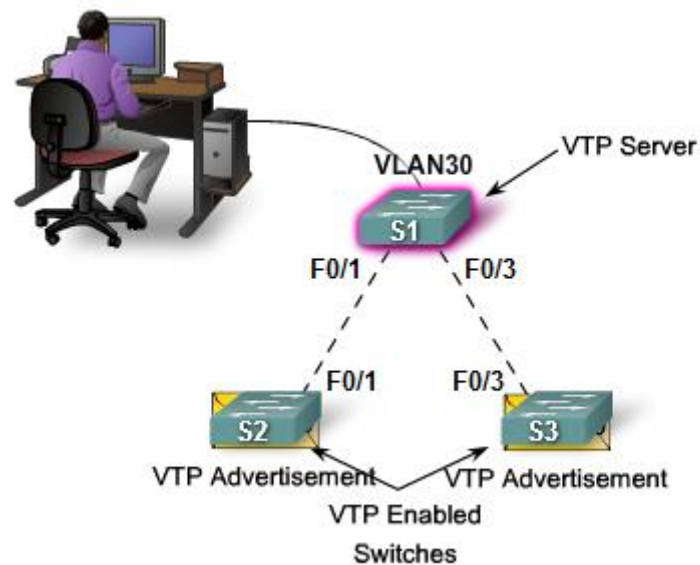
Namun harap diperhatikan, switch merupakan perangkat yang bekerja di layer 2 dan hanya meneruskan paket menggunakan Ethernet frame header. Untuk itu digunakanlah 802.1Q frame tagging yang akan menambahkan tanda pada frame header asli sesuai VLAN masing-masing. Sehingga semua frame akan dapat dilewatkan pada satu link dan VLAN mengenali frame mana yang merupakan miliknya. Cisco mendukung IEEE 802.1Q untuk mengatur trunk pada interface Fast Ethernet dan Gigabit Ethernet.



Gambar 5 Penambahan tag VLAN ID pada frame header

VTP

Virtual LAN Trunking Protocol merupakan sebuah protokol yang memeperbolehkan user untuk melakukan konfigurasi VLAN pada switch lain dalam jaringan. Switch dapat dikonfigurasi oleh VTP server dan VTP client. VTP hanya dapat digunakan pada normal-range VLAN (VLAN dengan ID dari 1 sampai 1005). Cara kerja VTP adalah dengan mendistribusikan dan menyesuaikan informasi mengenai VLAN ke seluruh switch yang menggunakan VTP. Hal ini akan mengurangi adanya kemungkinan kesalahan maupun inkonsistensi konfigurasi. VTP akan menyimpan konfigurasi VLAN dalam database yang disebut vlan.dat



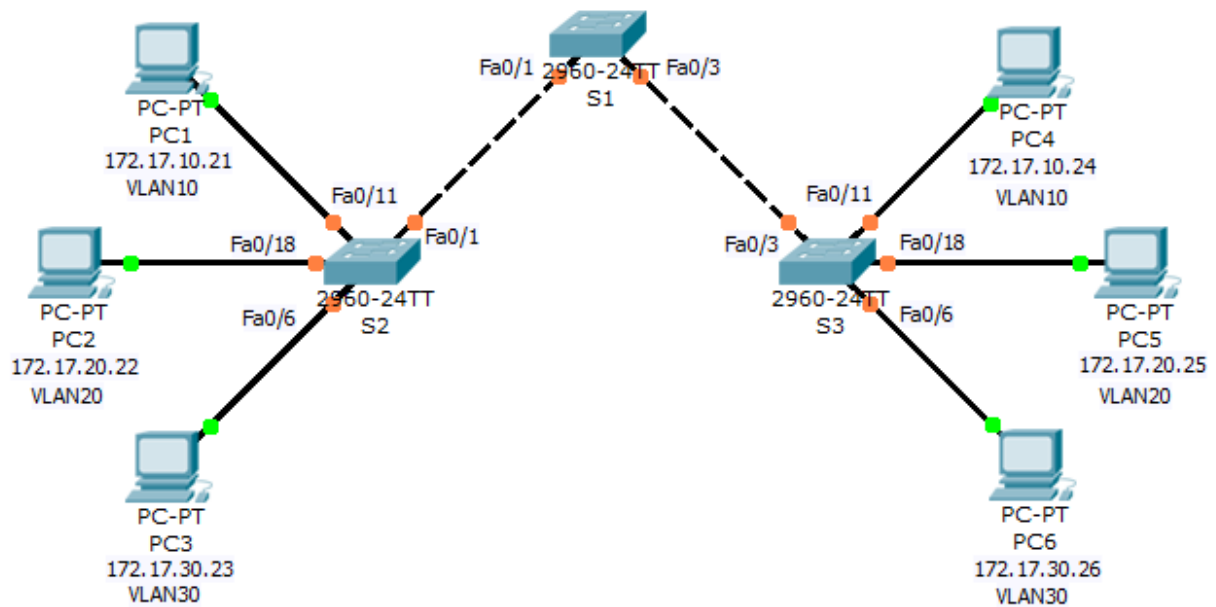
Gambar 6 Penggunaan VTP pada konfigurasi VLAN

Beberapa hal yang harus dipahami mengenai VTP antara lain:

1. **VTP Domain**, merupakan metoda untuk membatasi VTP dalam mendistribusikan konfigurasinya.
2. **VTP Server**, VTPmode yang menjadikan switch sebuah server yang mendistribusikan konfigurasi ke switch-switch yang telah menggunakan VTP. VTP server akan menyimpan informasi seluruh VLAN pada sebuah domain dalam NVRAM. Pembuatan, penghapusan, dan rename VLAN dapat dilakukan pada server.
3. **VTP Client**, VTP mode ini berfungsi sama seperti server yaitu menyebarkan konfigurasi. Namun tidak seperti VTP server, VTP client tidak dapat digunakan untuk membuat, menghapus, maupun menamai VLAN

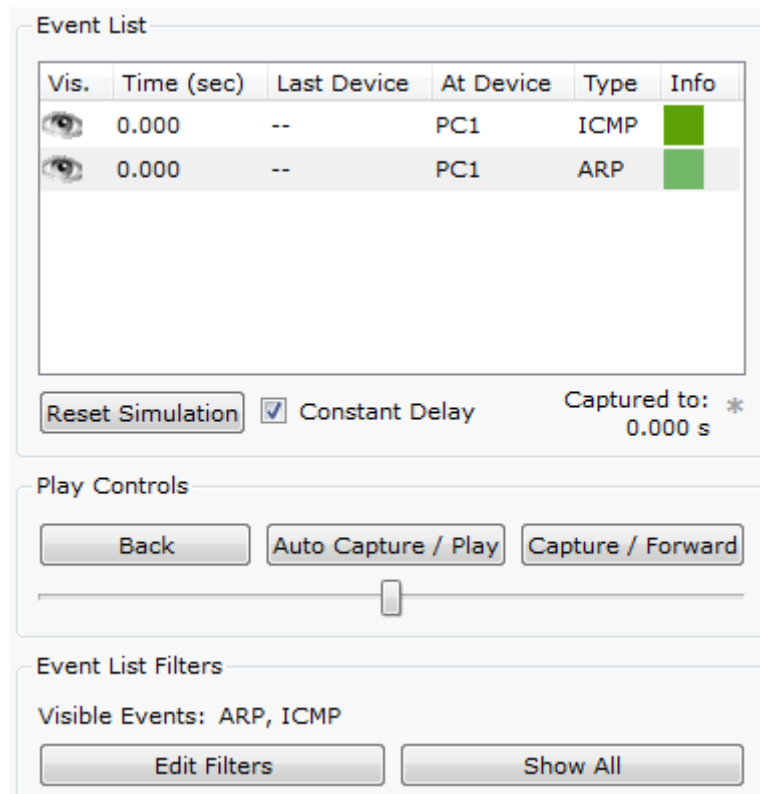
PRAKTIKUM

Dalam praktik modul ini, praktikan akan mencoba bagaimana melakukan konfigurasi VLAN menggunakan VTP. Namun sebelum itu ada baiknya kita mengetahui bagaimana perbedaan yang terdapat pada jaringan dengan subnet yang menggunakan VLAN dan tidak. Kegiatan praktikum akan menggunakan topologi seperti di bawah ini:



Langkah-langkah praktikum

1. Buatlah topologi seperti gambar di atas, sesuaikan juga pengaturan IP address untuk setiap end device sehingga seperti yang telah ditunjukkan
2. Setelah semua interface yang tersambung aktif (berwarna hijau) lanjutkan ke langkah berikutnya
3. Lakukan ping dari PC1 ke PC6, pada realtime mode gunakan **Add Simple PDU** tool. Klik PC1 lalu PC6. Lalu pada simulation mode klik **Capture/Forward** button untuk melihat langkah-langkah pada proses ping yang dilakukan. Perhatikan ARP request yang berjalan pada jaringan. Apakah yang terjadi?



Gambar 7 Gunakan Capture/Forward button untuk meninjau proses ping

4. Sebelum melakukan konfigurasi VLAN, lakukan konfigurasi VTP terlebih dahulu. Periksa apakah switch telah berfungsi sebagai VTP server menggunakan command sebagai berikut:

S1#show vtp status

```
Number of existing VLANs      : 9
VTP Operating Mode           : Server
VTP Domain Name              :
VTP Pruning Mode             : Disabled
VTP V2 Mode                  : Disabled
VTP Traps Generation         : Disabled
MD5 digest                   : 0x13 0xFF 0xFC 0x81 0xFC 0x34 0x53 0x00
Configuration last modified by 0.0.0.0 at 3-1-93 00:07:13
```

5. Setelah itu buat sebuah VTP domain dengan mengetikkan command sebagai berikut:

S1#configure

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
```

S1(config)#vtp domain sisjar

```
Changing VTP domain name from NULL to sisjar
```

S1(config)#exit

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

S1#show vtp status

```
VTP Version                  : 2
Configuration Revision        : 8
Maximum VLANs supported locally : 255
Number of existing VLANs      : 9
VTP Operating Mode            : Server
```

```

VTP Domain Name           : sisjar
VTP Pruning Mode          : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x7B 0x98 0x4C 0x90 0x59 0x6D 0x08 0x0C
Configuration last modified by 0.0.0.0 at 3-1-93 00:15:16S1#configure

```

6. Setelah itu konfigurasi versi dari VTP ke versi 1 dengan mengetikkan perintah berikut

```
S1(config)#vtp version 1
```

```
VTP mode already in V1.
```

7. Setelah itu ubah VTP mode pada switch 2 dan switch 3 menjadi client dan ubah VTP domainnya menjadi sisjar dengan mengetikkan perintah berikut

```
S2(config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
```

```
S2(config)#vtp domain sisjar
```

```
Changing VTP domain name from NULL to sisjar
```

```
S3(config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
```

```
S3(config)#vtp domain sisjar
```

```
Changing VTP domain name from NULL to sisjar
```

8. Pada switch 1 konfigurasikan VLAN dengan ID **10, 20, dan 30**. Serta nama secara berurutan

OS, Network, dan Research

```
S1#configure
```

```
Configuring from terminal, memory, or network [terminal]?
```

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

```
S1(config)#vlan 10
```

```
S1(config-vlan)#name OS
```

```
S1(config-vlan)#end
```

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

```
S1#configure
```

```
Configuring from terminal, memory, or network [terminal]?
```

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

```
S1(config)#vlan 20
```

```
S1(config-vlan)#name Network
```

```
S1(config-vlan)#end
```

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

```
S1#configure
```

```
Configuring from terminal, memory, or network [terminal]?
```

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

```
S1(config)#vlan 30
```

```
S1(config-vlan)#name Research
```

```
S1(config-vlan)#end
```

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

9. Setelah itu konfirmasikan bahwa vlan yang diinputkan telah berhasil dibuat

```
S1#show vlan brief
```

```

VLAN Name                               Status    Ports

```

1	default	active	Gig1/1, Gig1/2
10	OS	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17
20	Network	active	Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
30	Research	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
99	Management&Native	active	Fa0/2, Fa0/4, Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

10. Berikutnya lakukan konfigurasi trunk pada S1 (f0/1, f0/3), S2 (f0/1), s3(f0/3) dengan mengetikkan perintah berikut

Switch 1

```
S1(config)#interface f0/1
```

```
S1(config-if)#switchport mode trunk
```

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

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

```
S1(config-if)#switchport trunk native vlan 99
```

```
S1(config-if)#switchport trunk allowed vlan add 10
```

```
S1(config-if)#switchport trunk allowed vlan add 20
```

```
S1(config-if)#switchport trunk allowed vlan add 30
```

```
S1(config)#interface f0/3
```

```
S1(config-if)#switchport mode trunk
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

```
S1(config-if)#switchport trunk native vlan 99
```

```
S1(config-if)#switchport trunk allowed vlan add 10
```

```
S1(config-if)#switchport trunk allowed vlan add 20
```

```
S1(config-if)#switchport trunk allowed vlan add 30
```

Switch 2

```
S2(config)#interface f0/1
```

```
S2(config-if)#switchport mode trunk
```

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

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

```
S2(config-if)#switchport trunk native vlan 99
```

```
S2(config-if)#switchport trunk allowed vlan add 10
```

```
S2(config-if)#switchport trunk allowed vlan add 20
```

```
S2(config-if)#switchport trunk allowed vlan add 30
```

Switch 3

```
S1(config)#interface f0/3
```

```
S1(config-if)#switchport mode trunk
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

```
S1(config-if)#switchport trunk native vlan 99
```

```
S1(config-if)#switchport trunk allowed vlan add 10
```

```
S1(config-if)#switchport trunk allowed vlan add 20
```

```
S1(config-if)#switchport trunk allowed vlan add 30
```

11. Berikutnya periksa pada setiap switch daftar vlan yang ada menggunakan **show vlan brief**. Apakah semua switch memiliki daftar yang sama?
12. Berikutnya pada switch 2 dan switch 3 lakukan assign setiap port untuk vlan yang sesuai pada topologi

Switch 2

```
S2(config)#interface f0/11
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 10
```

```
S2(config-if)#exit
```

```
S2(config)#interface f0/18
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 20
```

```
S2(config-if)#exit
```

```
S2(config)#interface f0/6
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 30
```

```
S2(config-if)#exit
```

Switch 3

```
S2(config)#interface f0/11
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 10
```

```
S2(config-if)#exit
```

```
S2(config)#interface f0/18
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 20
```

```
S2(config-if)#exit
```

```
S2(config)#interface f0/6
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 30
```

```
S2(config-if)#exit
```

13. Berikutnya lakukan kembali langkah ke-3. Setelah itu perhatikan, apakah yang berbeda dari pengamatan sebelumnya.

MODULE 5

STP Implementation & Inter-VLAN Routing

Tujuan :

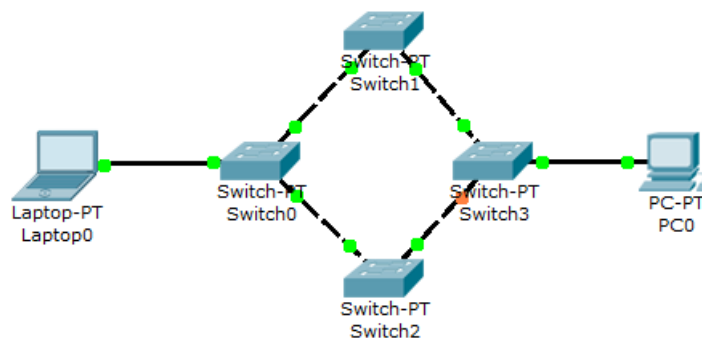
- Memahami peran dari *redundancy* dalam jaringan konvergen
- Memahami bagaimana *Spanning Tree Protocol* (STP) bekerja terutama mengatasi *loop* pada layer 2 dalam jaringan konvergen
- Memahami apa saja 3 unsur penting dalam algoritma STP
- Memahami bagaimana *routing* yang dilakukan agar antar VLAN dapat berkomunikasi satu sama lain dalam jaringan konvergen
- Dapat mengkonfigurasi inter-VLAN *routing* agar setiap *end-device* dapat saling berkomunikasi pada VLAN yang berbeda
- Melakukan *troubleshoot* pada permasalahan terkait inter-VLAN *routing*

Alat & Bahan :

- ✓ Komputer/Laptop yang terinstal aplikasi Packet Tracer.

Tentang STP dan *Redundancy*, adakah keterkaitannya?

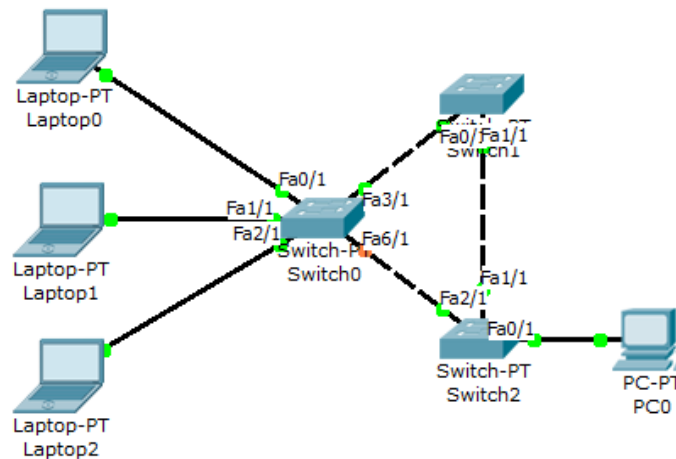
Sebelum mengenal apa itu STP, sebaiknya kita memahami terlebih dahulu apakah *redundancy*, serta bagaimana perannya dalam sebuah jaringan konvergen. *Redundancy*, dalam definisi Indonesia yang berarti sesuatu yang berlebih, merupakan suatu kondisi dalam jaringan komputer dimana terdapat multi-jalur dari sebuah titik sumber untuk menuju ke titik penerima *packet*. Sederhananya adalah seperti berikut :



Misalnya, sebuah transmisi data terjadi dari Laptop0 ke PC0. Perhatikan bahwa Laptop0 memiliki 2 jalur pilihan untuk menuju PC0 (melalui Switch1 dan Switch2). Jika Switch1 menjadi jalur utama dalam transmisi data tersebut, maka setiap kali komunikasi terjadi antara Laptop0 dan PC0 akan

selalu melalui Switch1. Namun, ketika jalur pada Switch1 mengalami masalah (ada masalah pada kabel antara Switch0 dan Switch1, kabel antara Switch1 dan Switch3, atau pada Switch1 itu sendiri) maka jalur pada Switch2 menjadi jalur alternatif komunikasi antara Laptop0 dan PC0.

Sederhananya, dengan adanya *redundancy* tersebut, maka komunikasi data dalam sebuah jaringan dapat tetap terakomodasi (adanya jalur utama dan jalur *backup*). Namun apa yang terjadi ketika *redundancy* dalam sebuah jaringan bertugas sebaliknya (mengacaukan sistem transmisi data seperti *loop*)? Berikut contohnya :



Beberapa kondisi yang mungkin terjadi dikarenakan adanya *redundancy* yang tidak dapat terkontrol :

1. Loop pada Layer 2 :

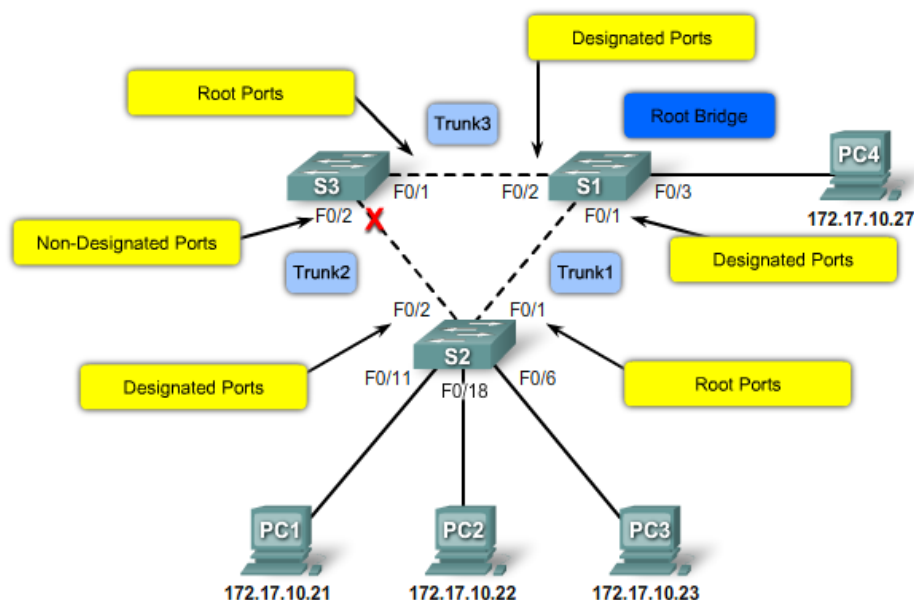
- Ketika Laptop0 ingin mem-broadcastpacket, ia terlebih dahulu mengirim packet ke Switch0.
- Switch0 menerima packet, mencatat bahwa Laptop0 terdapat pada Fa0/1 (berdasarkan informasi dari packet), lalu mem-forwardpacket tersebut ke semua link yang aktif (kecuali link pengirim).
- Switch1 menerima packet dari Switch0, mencatat bahwa Laptop0 terdapat pada Fa0/1, lalu mem-forward packet tersebut ke Switch2. Switch2 juga menerima packet dari Switch0, mencatat bahwa Laptop0 terdapat pada Fa2/1, lalu mem-forward packet tersebut ke Switch1.
- Switch1 menerima packet dari Switch2, begitu pula sebaliknya, kemudian masing-masing mencatat keberadaan Laptop0 berdasarkan informasi packet yang diterimanya (Switch1 meng-update keberadaan Laptop0 pada Fa1/1, Switch2 meng-update keberadaan Laptop0 pada Fa1/1), dilanjutkan dengan masing-masing mem-forward packet ke Switch2. Dari sini kekacauan mulai terjadi.
- Switch2 menerima packet dari Switch1 dan Switch2, kemudian meng-update keberadaan Laptop0 berdasarkan informasi packet yang diterima paling akhir (antara packet dari Switch1 atau Switch2).
- Dan packet akan terus diputar antar switch sehingga menghasilkan loop

2. Broadcast Storm :

- Ketika Laptop0 ingin mem-broadcast packet, sudah dipastikan terjadi loop sebagaimana dijelaskan pada no. 1

- Kondisi ini bisa makin diperparah ketika *end-device* lain ingin mem-*broadcast packet*.
 - Ketika *traffic* dari *packet-packet* tersebut sudah melampaui ambang batas, maka jika terdapat *end-device* yang mencoba mem-*broadcast packet*, maka *packet* tersebut akan dibuang.
3. *Packet* terduplikasi saat diterima :
- Ketika Laptop0 ingin mengirim *packet* ke PC0, ia terlebih dahulu mengirim *packet* ke Switch0.
 - Switch0 yang tidak mengetahui keberadaan PC0 kemudian mem-*broadcast packet* ke semua *link* yang aktif (kecuali *link* pengirim).
 - Switch2 menerima *packet* dari Switch0 dan mengetahui bahwa PC0 terdapat pada Fa0/1. Switch2 mem-*forward packet* tersebut ke Fa0/1, yang langsung menuju PC0. *Packet* dari Laptop0 diterima oleh PC0.
 - Switch1 yang juga menerima *packet* dari Switch0, mengetahui bahwa PC0 terdapat pada Fa0/1. Switch1 mem-*forward packet* tersebut ke Fa0/1, menuju Switch2.
 - Switch2 menerima *packet* dari Switch1 dan mengetahui bahwa PC0 terdapat pada Fa0/1. Switch2 mem-*forward packet* tersebut ke Fa0/1, yang langsung menuju PC0. *Packet* duplikat pun diterima.

Teknologi STP kemudian hadir sebagai “pelengkap” dari adanya *redundancy* dalam sebuah topologi jaringan. Dengan STP inilah, *redundancy* yang terdapat dalam sebuah jaringan, dapat diatur sedemikian hingga mencegah adanya *loop* pada layer 2. Teknologi STP menggunakan *packet* BPDU (*Bridge Protocol Data Unit*) untuk pertukaran informasi antar *switch* yang menggunakannya. *Packet* BPDU terdiri dari BID (*Bridge ID*) dari *switch* pengirim, RID (*Root ID*) pada topologi tersebut, serta ID sistem STP tambahan yang sifatnya opsional. STP sendiri sebenarnya menggunakan algoritma *spanning tree*, sebuah algoritma yang bertujuan mencegah adanya *loop* dalam sebuah graf. Secara sederhana, algoritma *spanning tree* adalah sebagai berikut :

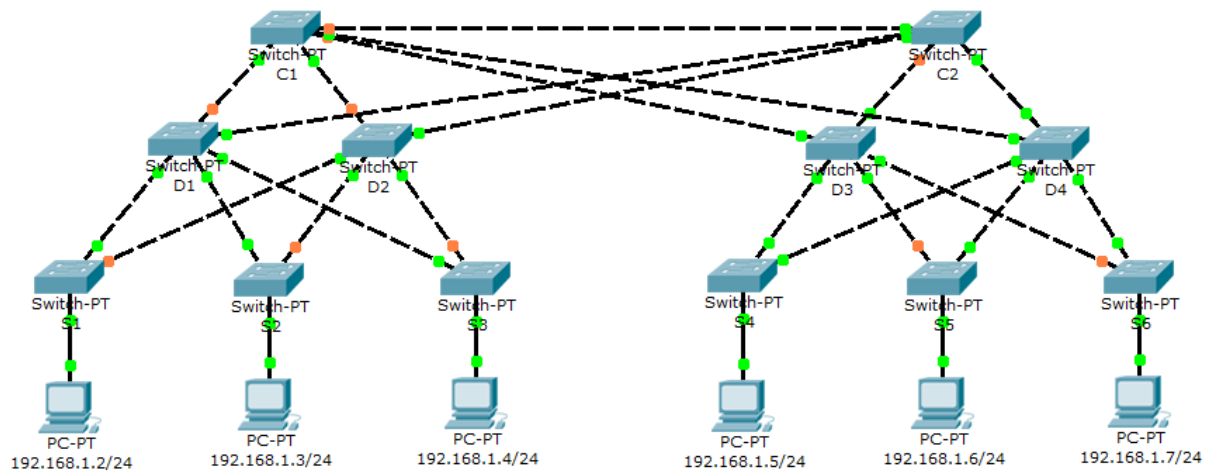


Dalam sebuah topologi yang menggunakan STP, akan diatur terlebih dahulu siapa *switch* yang akan menjadi **root bridge**. Pemilihan didasarkan atas informasi BPDUs yang beredar disekitar topologi, dimana *switch* yang memiliki BID terkecil (informasi BID terdapat pada BPDUs) akan dipilih sebagai *root bridge* (pada gambar, S1 terpilih sebagai *root bridge*). Jika terdapat BID terkecil lebih dari satu, maka penentuan akan dilakukan berdasarkan *MAC address* terkecil. Kemudian dilakukan penentuan jalur terbaik (*best path*), penentuan ini dilakukan oleh masing-masing *switch* untuk menuju ke *root bridge* (kecuali *switch* yang terpilih sebagai *root bridge*). Penentuan jalur terbaik didasarkan atas *cost* yang dibebani pada jalur yang ada dari tiap-tiap *switch* ke *root bridge*, meliputi *bandwidth* yang disediakan, waktu yang dibutuhkan, dan lain-lain yang berkaitan. Hasil dari penentuan jalur tersebut adalah dengan membiarkan jalur yang terpilih agar tetap terbuka, sementara jalur yang tidak terpilih akan “di-block”. Jalur yang terpilih dan yang tidak kemudian dispesifikan atas *root port* (port pada tiap *switch* yang terdekat dengan *root bridge*) dan *designated port* (port pada beberapa *switch* yang tidak tergolong atas *root ports* namun diizinkan untuk mem-forward packet), serta *non-designated port* (port pada beberapa *switch* yang “di-block” untuk mem-forward packet). Pada gambar, *root port* terdapat pada F0/1 milik S3 dan F0/1 milik S2, *designated port* terdapat pada F0/2 dan F0/1 milik S1, serta F0/2 milik S2, dan juga *non-designated port* terdapat pada F0/2 milik S3.

Selama aktivitas diatas berlangsung, setiap *packet* data selain BPDUs yang akan melalui jaringan tersebut akan dibuang.

Hands on : Session 1

Dalam praktik sesi pertama, kita akan mencoba bagaimana mengkonfigurasi STP pada sebuah topologi yang terdapat *redundancy*. Topologi yang akan digunakan adalah sebagai berikut :



Konfigurasi STP pada topologi yang memiliki *redundancy* secara *default* dilakukan secara otomatis segera setelah *switch* terlibat komunikasi dengan *switch* disekitarnya, untuk kemudian ditentukan siapa yang akan menjadi *root bridge*. Namun, *network administrator* juga dapat mengkonfigurasi secara manual untuk menentukan siapa *switch* yang akan menjadi *root bridge*.

Analisis konfigurasi STP secara otomatis :

1. Buatlah topologi seperti gambar diatas, berikut pengaturan IP untuk setiap *end device*-nya.
2. Biarkan sejenak sehingga tidak terdapat lagi perubahan warna indikator setiap *link* yang ada.
3. Disini kita tidak akan mengetahui siapa *switch* yang menjadi *root bridge* secara langsung, namun kita bisa mengetahui tanda-tanda *switch* yang menjadi *root bridge*. Caranya adalah dengan memperhatikan kira-kira *switch* mana yang *link-link* disekitarnya aktif (berwarna hijau). Setelah diperoleh *switch* dengan tanda-tanda tersebut, maka jalankan perintah berikut :

```
#show spanning-tree
```

Switch yang menjadi *root bridge* akan mengeluarkan *output* sebagai berikut (perhatikan teks yang diberi tanda cetak tebal miring) :

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    0000.0CE4.720E
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0000.0CE4.720E
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa1/1	Desg	FWD	19	128.2	P2p
Fa2/1	Desg	FWD	19	128.3	P2p

Harap diperhatikan bahwa setiap percobaan ini dilakukan, adakalanya memperoleh *switch* yang berbeda dalam penentuan *root bridge*. Dalam percobaan ini, yang menjadi *root bridge* adalah *switch* S4. Jika percobaan anda memperoleh hasil yang sama dengan percobaan ini, apakah menurut anda terasa ganjil jika *root bridge* dipegang oleh *switch* S4 yang mana langsung terhubung pada *client*?

Konfigurasi STP secara manual, serta simulasi penggunaan jalur *backup* :

1. Gunakan topologi pada percobaan sebelumnya. Kita akan menentukan secara manual *switch* yang akan menjadi *root bridge*, dalam hal ini *switch* C1. Caranya adalah dengan menggunakan perintah berikut pada *switch* C1 :

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

2. Biarkan sejenak sehingga tidak terdapat lagi perubahan warna indikator setiap *link* yang ada.
3. Verifikasikan bahwa C1 telah menjadi *root bridge* dengan perintah berikut :

```
#show spanning-tree
```

Hasilnya kurang lebih seperti ini :

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    4097
Address     000D.BD18.2C1D
This bridge is the root
Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec

Bridge ID   Priority    4097 (priority 4096 sys-id-ext 1)
Address     000D.BD18.2C1D
Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec
Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa1/1	Desg	FWD	19	128.2	P2p
Fa2/1	Desg	FWD	19	128.3	P2p
Fa3/1	Desg	FWD	19	128.4	P2p
Fa4/1	Desg	FWD	19	128.5	P2p

4. Cobalah untuk mengirim *ping* dari PC 192.168.1.2/24 ke PC 192.168.1.7/24. Lakukan dengan menggunakan *Simple PDU* pada *Simulation Mode*, kemudian perhatikan jalur yang ditempuh oleh *packet*. Pastikan pula pada *event list filter* agar hanya ARP, ICMP, dan STP saja yang terpilih (untuk memudahkan pengamatan).
5. Kemudian, kita akan mencoba membuat *root bridge backup* (sebuah *switch* non-*root bridge* yang secara otomatis menjadi *root bridge* ketika *switch* yang saat itu menjadi *root bridge* mengalami masalah). Sebelumnya, kita tentukan dahulu *switch* yang akan menjadi *root bridge backup*. Dalam percobaan ini, *switch* C2 akan menjadi *root bridge backup*. Jalankan perintah berikut pada *switch* C2 :

```
(config)#spanning-tree vlan 1 priority 8192
```

Kemudian tunggu sejenak, lalu verifikasi dengan perintah :

```
#show spanning-tree
```

6. Cobalah kembali untuk mengirim *ping* dari PC 192.168.1.2/24 ke PC 192.168.1.7/24. Adakah perbedaan jalur dari langkah sebelumnya? Catat jalur tersebut.
7. Hapus kabel yang menghubungkan antara S1 dan D1. Kemudian tunggu sejenak sehingga tidak terdapat lagi perubahan warna pada *link*. Kemudian lakukan *ping* dari PC 192.168.1.2/24 ke PC 192.168.1.7/24. Sekarang, adakah perbedaan jalur dari langkah sebelumnya? Catat jalur tersebut.
8. Ulangi percobaan 7 dengan menghapus secara tahap demi tahap : kabel C1 dan D4, kabel C1 dan D3, *switch* C1.
9. Lakukan *cross-check* untuk memastikan bahwa percobaan sudah benar. Pastikan pula bahwa anda benar-benar memahami STP berdasarkan percobaan ini.

Komunikasi antar VLAN, mungkinkah?

VLAN pada dasarnya merupakan jaringan LAN yang kemudian dikonfigurasi sedemikian rupa sehingga terdapat lebih dari satu jaringan LAN (yang kemudian disebut *Virtual LAN*), yang mana secara *default* masing-masing LAN *virtual* tersebut tidak dapat terhubung satu sama lain. Dalam pembahasan kali ini, kita akan mencoba bagaimana menghubungkan inter-VLAN, sehingga setiap *end-device* pada VLAN yang berbeda (namun LAN yang sama) dapat berkomunikasi satu sama lain.

Ide “menjembatani” antar VLAN sebenarnya berasal dari fungsi utama *router*, yakni menjalankan fungsi OSI layer 3, sebagai pe-rute atau yang merutekan *packet* melalui *interface*/IP spesifik menuju *broadcast domain* tertentu. Oleh karena setiap VLAN adalah sebuah *broadcast domain*, maka fungsi utama *router* tentu saja bisa digunakan untuk menghubungkan antar VLAN tersebut.

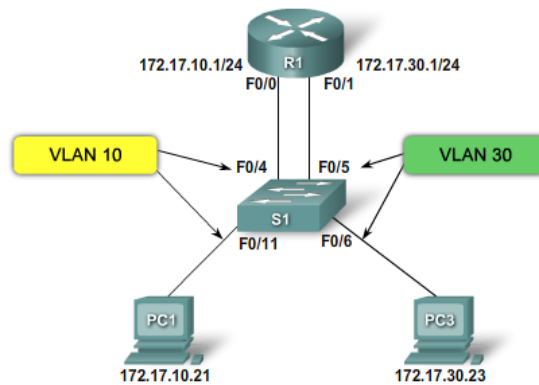
Adapun secara fisik, inter-VLAN *routing* dapat diimplementasikan dengan :

1. Menggunakan *router*

Inter-VLAN *routing* dengan menggunakan perangkat *router* dibagi 2 cara :

- a. Menggunakan *interface* fisik (cara tradisional)

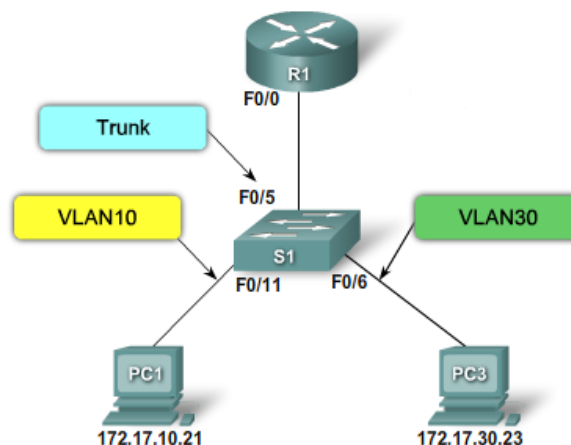
Caranya yakni setiap VLAN memiliki *interface* spesifik yang terhubung pada *router*. Nantinya akan dibutuhkan *resource* berupa *interface* sebanyak jumlah VLAN yang ada. Setiap port *switch* yang terhubung ke *router* harus terkonfigurasi dalam mode *access*. Contohnya adalah sebagai berikut :



Pada contoh diatas, terlihat bahwa VLAN 10 dan VLAN 30 masing-masing menggunakan *interface* spesifik untuk terhubung dengan *router*. Router kemudian membuat tabel *routing* untuk memuat rute VLAN 10 dan VLAN 30.

Menggunakan *subinterface*

Caranya adalah dengan memanfaatkan sebuah *interface* untuk digunakan oleh sejumlah VLAN yang ada. Nantinya, port *switch* yang terhubung ke *router* harus dalam mode *trunk*. Contohnya adalah sebagai berikut :



Pada contoh diatas, terlihat bahwa baik VLAN 10 maupun VLAN 30 menggunakan sebuah *interface* untuk terhubung ke *router*. Router kemudian membuat tabel *routing* untuk memuat rute VLAN 10 dan VLAN 30, yakni melalui rute *subinterface*.

Kedua cara diatas memiliki kelebihan dan kekurangan masing-masing. Berikut merupakan perbandingan kedua cara diatas dengan menggunakan 5 aspek perbandingan :

Aspek\Metode	Menggunakan <i>interface fisik</i>	Menggunakan <i>subinterface</i>
<i>Physical looks</i>	Satu VLAN menggunakan <i>interface</i> , sedangkan port terbatas.	Beberapa VLAN menggunakan sebuah <i>interface</i> saja.

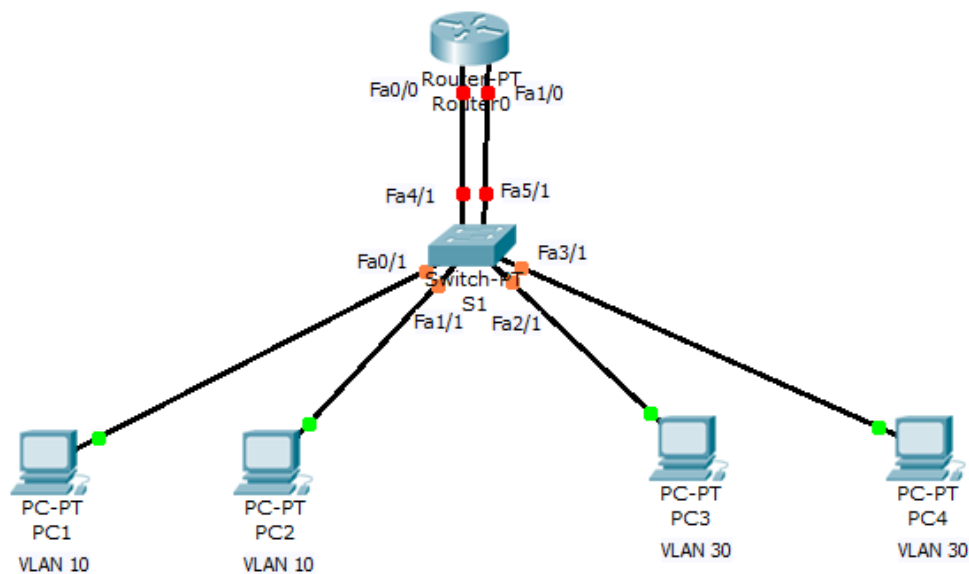
<i>Bandwidth</i>	Setiap VLAN memiliki <i>bandwidth</i> besar karena menggunakan satu <i>interface</i> masing-masing.	<i>Bandwidth</i> dapat tidak terpersir dengan baik ketika beberapa VLAN menggunakan sebuah <i>interface</i> saja.
<i>Port mode</i>	Menggunakan mode <i>access</i> .	Menggunakan mode <i>trunk</i> .
<i>Cost</i>	Banyak <i>interface</i> yang digunakan, berarti <i>cost</i> akan cukup besar.	Dapat dihemat dengan memanfaatkan sebuah <i>interface</i> .
<i>Complexity</i>	Secara <i>physical</i> akan lebih kompleks, namun secara <i>logical</i> cukup sederhana.	Secara <i>physical</i> cukup sederhana, namun secara <i>logical</i> cukup kompleks.

2. Menggunakan *switch* khusus

Switch khusus disini merupakan *switch* yang memiliki kemampuan menjalankan fungsi OSI layer 3 (meskipun tidak sama persis dengan *router*). Tidak dicakup pada percobaan ini.

Hands on : Session 2

Dalam praktik sesi ini, kita akan mencoba mengkonfigurasi inter-VLAN *routing* dengan menggunakan *router*. Percobaan akan menggunakan 2 cara yang sebelumnya dibahas (menggunakan *interface* dan *subinterface*). Untuk cara pertama, topologi yang digunakan adalah sebagai berikut :



Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN Association
--------	-----------	------------	-------------	-----------------	------------------

R1	Fa0/0	192.168.10.1	255.255.255.128	N/A	10
	Fa1/0	192.168.10.129	255.255.255.128	N/A	30
PC1	NIC	192.168.10.10	255.255.255.128	192.168.10.1	10
PC2	NIC	192.168.10.20	255.255.255.128	192.168.10.1	10
PC3	NIC	192.168.10.140	255.255.255.128	192.168.30.1	30
PC4	NIC	192.168.10.150	255.255.255.128	192.168.30.1	30
S1	Fa0/1	-	-	-	10
	Fa1/1	-	-	-	10
	Fa4/1	-	-	-	10
	Fa2/1	-	-	-	30
	Fa3/1	-	-	-	30
	Fa5/1	-	-	-	30

Konfigurasi inter-VLAN *routing* dengan cara pertama (*interface* fisik) :

1. Buat topologi sesuai gambar diatas. Sesuaikan IP *end device* dengan yang terdapat pada tabel.
2. Kita akan membuat VLAN 10 dan VLAN 30. Jalankan perintah berikut pada S1 :

```
(config)#vlan 10
(config-vlan)#vlan 30
```

Verifikasikan dengan perintah :

```
#show vlan brief
```

Contoh output yang sudah benar :

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa1/1, Fa2/1, Fa3/1 Fa4/1, Fa5/1
10	VLAN0010	active	
30	VLAN0030	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

3. Petakan *interface-interface* pada S1 dengan VLAN-id sesuai pada tabel. Prosedur perintahnya adalah sebagai berikut :

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

Perintah diatas merupakan contoh untuk fa0/1 yang diset untuk VLAN 10. Ulangi prosedur diatas untuk *interface* lainnya sesuai VLAN-id-nya. Jangan lupa untuk selalu melakukan verifikasi.

4. Atur *interface* pada *router* agar memiliki IP sesuai pada tabel. Prosedur perintahnya adalah sebagai berikut :

```
(config)#interface fa0/0
(config-if)#ip address 192.168.10.1 255.255.255.128
(config-if)#no shutdown
```

Perintah diatas merupakan contoh untuk fa0/0 untuk diset agar memiliki IP 192.168.10.1/25. Ulangi prosedur diatas untuk *interface* lainnya. Lakukan verifikasi dengan perintah :

```
#show ip route
```

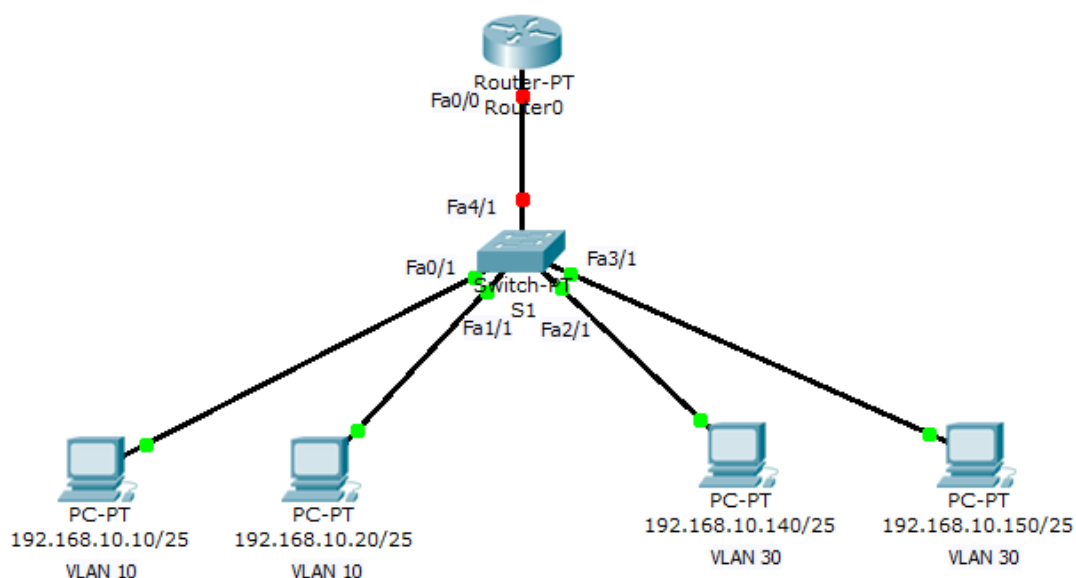
Contoh output yang sudah benar :

```
<output omitted>
Gateway of last resort is not set

192.168.10.0/25 is subnetted, 2 subnets
C      192.168.10.0 is directly connected, FastEthernet0/0
C      192.168.10.128 is directly connected, FastEthernet1/0
```

5. Tunggu sejenak hingga semua *link* berwarna hijau. Cobalah mengirim *packet* antar *enddevice* yang berbeda VLAN. Lakukan *cross-check* untuk memastikan bahwa percobaan sudah benar. Pastikan pula bahwa anda benar-benar memahami konfigurasi inter-VLAN *routing* dengan cara pertama berdasarkan percobaan ini.

Selanjutnya adalah dengan menggunakan cara kedua, topologinya adalah sebagai berikut :



Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN Association
R1	Fa0/0.10	192.168.10.1	255.255.255.128	N/A	10
	Fa0/0.30	192.168.10.129	255.255.255.128	N/A	30
PC1	NIC	192.168.10.10	255.255.255.128	192.168.10.1	10
PC2	NIC	192.168.10.20	255.255.255.128	192.168.10.1	10
PC3	NIC	192.168.10.140	255.255.255.128	192.168.30.1	30
PC4	NIC	192.168.10.150	255.255.255.128	192.168.30.1	30
S1	Fa0/1	-	-	-	10
	Fa1/1	-	-	-	10
	Fa4/1	-	-	-	None (Trunk mode)
	Fa2/1	-	-	-	30
	Fa3/1	-	-	-	30

Konfigurasi inter-VLAN *routing* dengan cara kedua (*subinterface*) :

- Ikuti langkah konfigurasi inter-VLAN *routing* dengan cara pertama mulai dari no. 1-3.
- Masih pada konfigurasi S1, atur untuk *interface* fa4/1 agar menggunakan mode *trunk*. Caranya adalah dengan perintah :

```
(config)#interface fa4/1
(config-if)#switchport mode trunk
```

- Berikutnya, kita akan “memecah” *interface* fa0/0 menjadi *subinterface* fa0/0.10 dan fa0/0.30 agar dapat memuat masing-masing VLAN 10 dan VLAN 30. Jalankan perintah berikut pada R1:

```
(config)#interface fa0/0.10
(config-subif)#encapsulation dot1Q 10
(config-subif)#ip address 192.168.10.1 255.255.255.128
(config-subif)#interface fa0/0.30
(config-subif)#encapsulation dot1Q 30
(config-subif)#ip address 192.168.10.129 255.255.255.128
(config-subif)#interface fa0/0
(config-if)#no shutdown
```

Jangan lupa untuk melakukan verifikasikannya.

- Tunggu sejenak hingga semua *link* berwarna hijau. Cobalah mengirim *packet* antar *enddevice* yang berbeda VLAN. Lakukan *cross-check* untuk memastikan bahwa percobaan sudah benar. Pastikan pula bahwa anda benar-benar memahami konfigurasi inter-VLAN *routing* dengan cara kedua berdasarkan percobaan ini.

MODULE 6

Basic Wireless LAN Concepts and Configuration

Tujuan :

- Memahami konsep Wireless LAN
- Memahami konsep Wireless LAN Roaming
- Memahami konsep keamanan jaringan pada Wireless LAN
- Memahami konsep VLAN dalam kaitannya dengan Wireless LAN
- Dapat mengkonfigurasi Wireless LAN yang terhubung dengan jaringan VLAN
- Melakukan *troubleshoot* pada permasalahan Wireless LAN

Alat & Bahan :

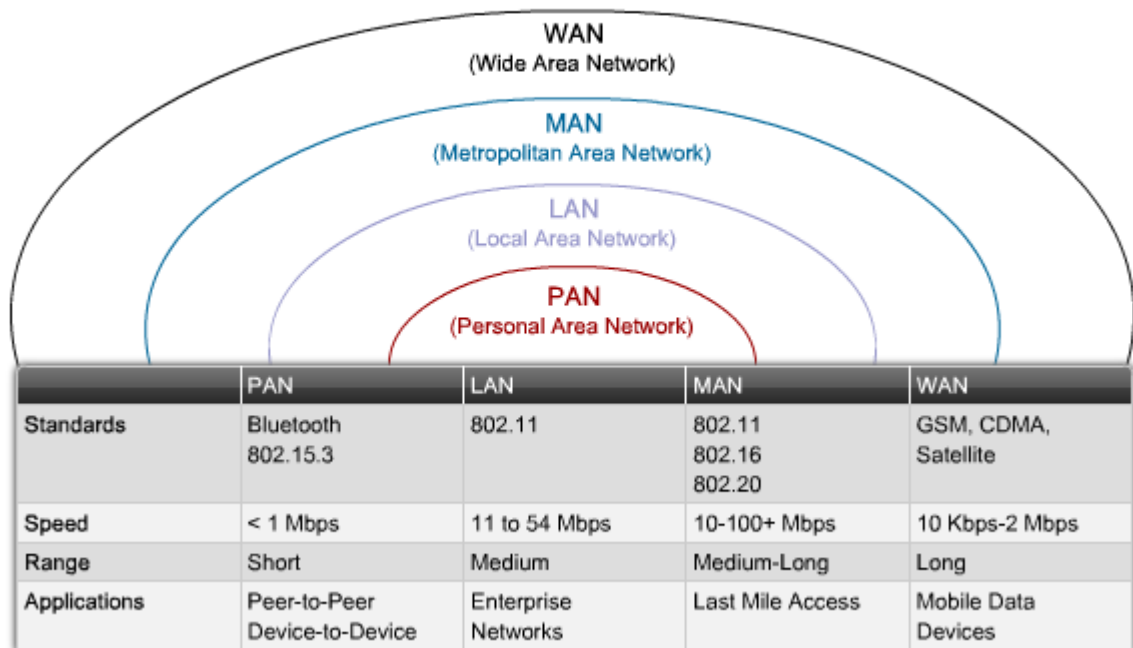
- ✓ Komputer/Laptop yang terinstal aplikasi Packet Tracer.

Wireless LAN

Aktifitas manusia yang begitu dinamis telah membuat evolusi dari teknologi yang begitu dramatis. Karyawan dan pengusaha, mahasiswa dan fakultas, agen pemerintah dan orang-orang di dunia ini telah merasakan konvergensi yang amat tinggi dalam berkomunikasi. Hal ini terjadi pada berbagai perangkat komunikasi mobile yang mendukung mobilitas penggunanya. Bisa terwujudnya komunikasi yang mobile adalah karena adanya jaringan yang tersambung ke perangkat-perangkat tersebut.

Saat ini ada banyak infrastruktur yang berbeda yang memungkinkan mobilitas yang tinggi bisa terjadi. Akan tetapi dalam lingkungan bisnis yang konvensional, infrastruktur yang paling penting adalah WLAN. Wireless adalah suatu koneksi satu perangkat dengan perangkat lainnya dengan tanpa menggunakan media kabel. WLAN atau Wireless LAN adalah jaringan yang menghubungkan dua atau lebih perangkat menggunakan metode-metode wireless atau tanpa kabel dan biasanya memberikan konektivitas yang meliputi daerah tertentu.

Wireless LANs



Bagian-bagian dari Wireless LAN

WLAN Roaming

Seringkali perusahaan atau institusi yang membutuhkan layanan WLAN yang memiliki jangkauan dan bandwidth yang tinggi, memilih untuk menggunakan beberapa access point dengan jangkauan yang terbatas tetapi bisa meningkatkan throughput yang dihasilkan. Untuk kebutuhan yang satu ini, maka diperlukanlah teknik yang dinamakan Roaming. Roaming adalah sebuah kondisi dimana digunakan untuk mendeskripsikan perpindahan switching dari wilayah kontrol sebuah Access Point ke Access Point yang lainnya.

Access Point seharusnya diletakkan pada posisi dimana mencegah terjadinya daerah tanpa sinyal WLAN. Dimana begitu user menjauhi satu AP, maka kekuatan dan kualitas sinyal WLAN akan berkurang. Perencanaan roaming yang baik adalah dimana ketika hal itu terjadi, maka akan ada AP lain yang mengambil alih koneksi wireless yang ada. Pengambilalihan ini terjadi melalui koordinasi sedemikian rupa yang terlihat oleh klien, mirip seperti koneksi pada telepon seluler. Hal ini bisa terjadi pada koneksi VLAN yang sama. Apabila VLAN-nya berbeda, maka koneksi bisa terputus sampai perangkat user terkoneksi dengan jaringan yang baru.

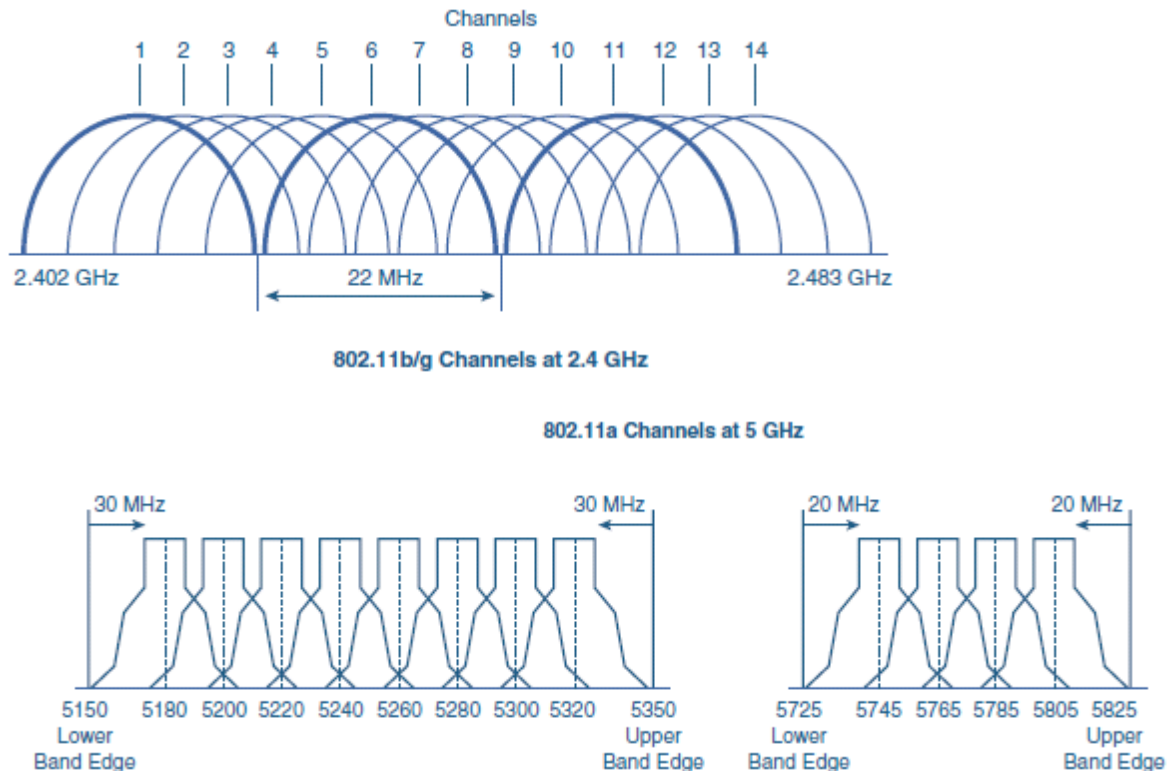
Desain Jaringan Wireless

Karena jaringan wireless digunakan untuk mengatasi berbagai keterbatasan yang ada pada jaringan kabel (seperti fleksibilitas, jumlah user, dan lainnya) maka diperlukan perencanaan yang matang dalam implementasinya.

Jaringan wireless sendiri memiliki beberapa standar yang berbeda, seperti a, b, g, dan n. Pada umumnya standar wireless yang digunakan adalah b, g, dan n. Karena standar-standar ini

memiliki 14 channel yang kompatibel di frekuensi 2,4 GHz. Tapi kebanyakan standar yang dipakai hanya 11 channel.

Dari semua channel yang ada hanya channel 1, 6, dan 11 yang tidak overlapping. Channel-channel inilah yang biasanya disetting pada access point yang ada.



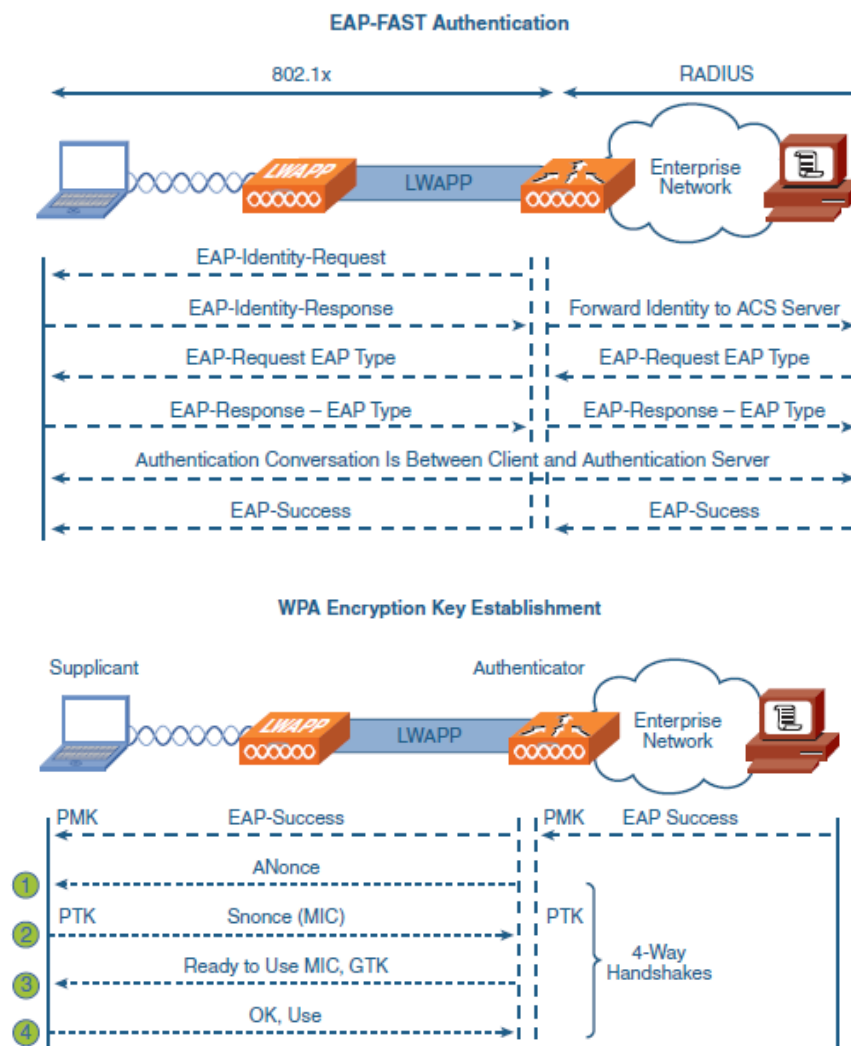
Dari gambar di atas bisa dilihat bahwaspektrum gelombang standar 802.11a sangat berbeda dengan standar 802.11b/g/n. Sehingga standar a tidaklah kompatibel dengan standar lainnya.

Keamanan Jaringan

Suatu jaringan kabel bisa lebih aman daripada jaringan wireless sebab dalam kenyataannya seorang penyerang untuk masuk ke jaringan haruslah memiliki media kabel dan portnya. Berbeda dengan jaringan wireless yang dimana penyerang hanya perlu melihat sinyal yang ia bisa tangkap dengan wireless adaptornya dan tinggal mengkoneksikan ke jaringan yang diinginkan. Oleh sebab itu, dalam jaringan wireless sangat diperlukan adanya keamanan jaringan yang bisa memastikan bahwa pengguna di areanya memang berhak untuk mendapat hak akses atas jaringan tersebut.

Langkah penting pertama dalam pengamanan jaringan WLAN adalah dengan mengautentikasi dan mengenkripsi paket data dari klien. Hal pertama yang dilakukan jaringan adalah melakukan autentikasi klien dengan metode Extensible Authentication Protocol (EAP) dan Flexible Authentication via Secure Tunnel (FAST) dimana user yang terautentikasi benarlah yang berhak lanjut ke fase berikutnya. Setelah terautentikasi maka dilanjutkan dengan enkripsi komunikasi data untuk penyerahan kunci enkripsi dengan metode WPA atau WPA2 (tergantung dari metode enkripsi yang dipilih). Setelah EAP-FAST berhasil maka sepasang master key akan dihasilkan(PMK/Pairwise

Master Key). WPA2 lebih dianjurkan untuk digunakan karena memiliki algoritma AES (Advanced Encryption Standard) yang menambahkan keamanan diatas WPA.

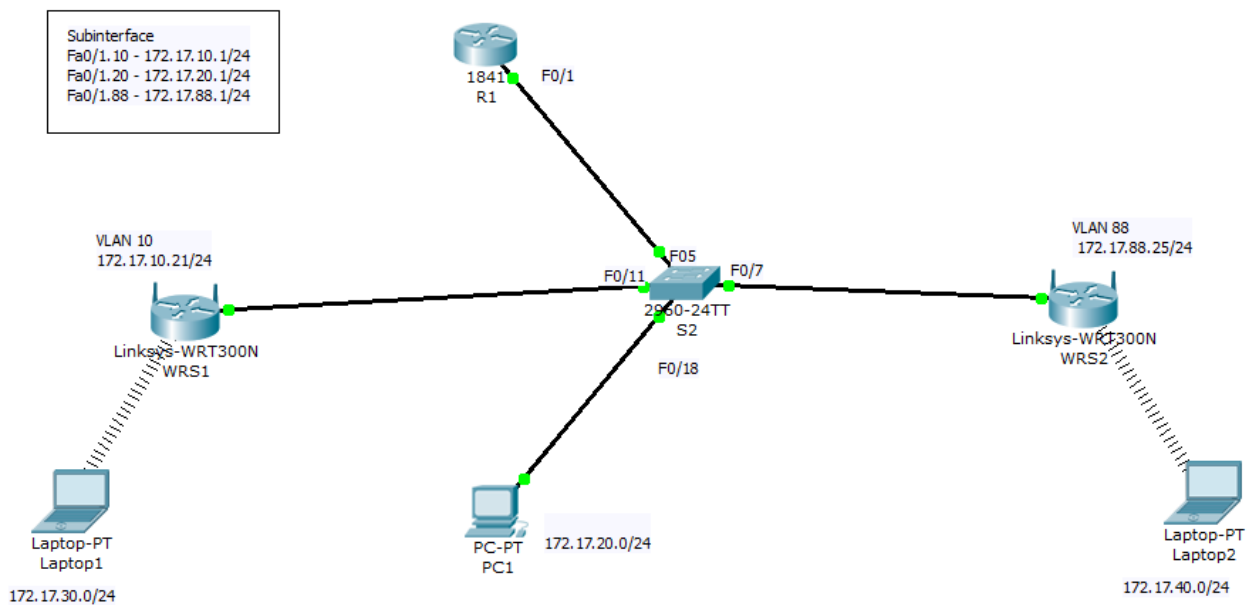


SSID (Service Set Identifier)

SSID adalah nama daripada sebuah jaringan WLAN. Semua perangkat wireless yang ada pada jaringan tersebut harus menerapkan nama jaringan atau SSID yang sama untuk berkomunikasi satu sama lain dalam jaringan tersebut. Karakter dalam SSID maksimal berjumlah 32 karakter alpanumerik yang case-sensitive.

Pada komputer klien, SSID bisa disetting secara manual pada konfigurasi daripada networknya. Akan tetapi biasanya administrator dari jaringan WLAN akan menerapkan sebuah public SSID yang diset di Access Point dan nantinya akan di-broadcast ke semua perangkat wireless yang ada. Fitur ini bisa dinonaktifkan sehingga hanya user tertentu yang mengetahui adanya jaringan SSID ini yang bisa mengaksesnya.

Langkah-Langkah Praktikum



1. Hidupkan port dan konfigurasi Router R1

Beri nama R1 pada router tersebut

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

Beri IP Address dan hidupkan portnya pada interface dan subinterfacenya

```
R1(config)#interface fastEthernet 0/0
```

```
R1(config-if)#ip address 172.17.50.1 255.255.255.0
```

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

```
R1(config-if)#exit
```

```
R1(config)#interface fastEthernet 0/1
```

```
R1(config-if)#no ip address
```

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

```
R1(config-if)#exit
```

```
R1(config)#interface FastEthernet0/1.10
```

```
R1(config-subif)#encapsulation dot1Q 10
```

```
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
```

```
R1(config-subif)#exit
```

```
R1(config)#interface FastEthernet0/1.20
```

```
R1(config-subif)#encapsulation dot1Q 20
```

```
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
```

```
R1(config-subif)#exit
```

```
R1(config)#interface FastEthernet0/1.88
```

```
R1(config-subif)#encapsulation dot1Q 88
```

```
R1(config-subif)#ip address 172.17.88.1 255.255.255.0
```

```
R1(config-subif)#exit
```

2. Konfigurasi Switch S2

Beri nama S2 pada switch tersebut

```
Switch(config)#hostname S2
```

Aktifkan VLAN pada switch

```
S2(config)#interface fastEthernet 0/5
```

```
S2(config-if)#switchport trunk allowed vlan all
```

```
S2(config-if)#switchport mode trunk
```

```
S2(config-if)#no shutdown
```

```
S2(config-if)#exit
```

```
S2(config-if)#interface FastEthernet0/7
```

```
S2(config-if)#switchport access vlan 88
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#no shutdown
```

```
S2(config-if)#exit
```

```
S2(config)#interface FastEthernet0/11
```

```
S2(config-if)#switchport access vlan 10
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#no shutdown
```

```
S2(config-if)#exit
```

```
S2(config)#interface FastEthernet0/18
```

```
S2(config-if)#switchport access vlan 20
```

```
S2(config-if)#switchport mode access
```

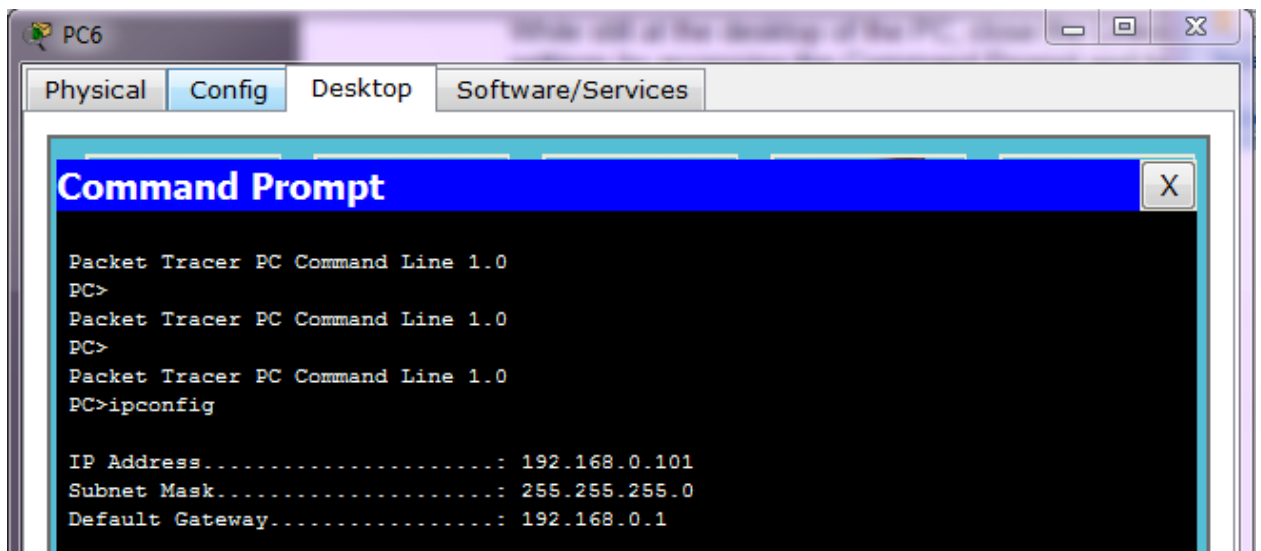
```
S2(config-if)#no shutdown
```

```
S2(config-if)#exit
```

3. Konfigurasi Laptop 1

Pastikan **laptop1** secara fisik sudah terpasang modul wireless Linksys-WPM300N. Klik tab Desktop dan pilih PC Wireless. Modul Linksys akan terbuka dan mengkoneksikan PC secara default ke jaringan wireless di dekatnya. Atau klik tab **Connect**. Pilih jaringan yang ada.

Lihat IP yang didapatkan dari Access Point. Buka command prompt dan ketik perintah ipconfig.



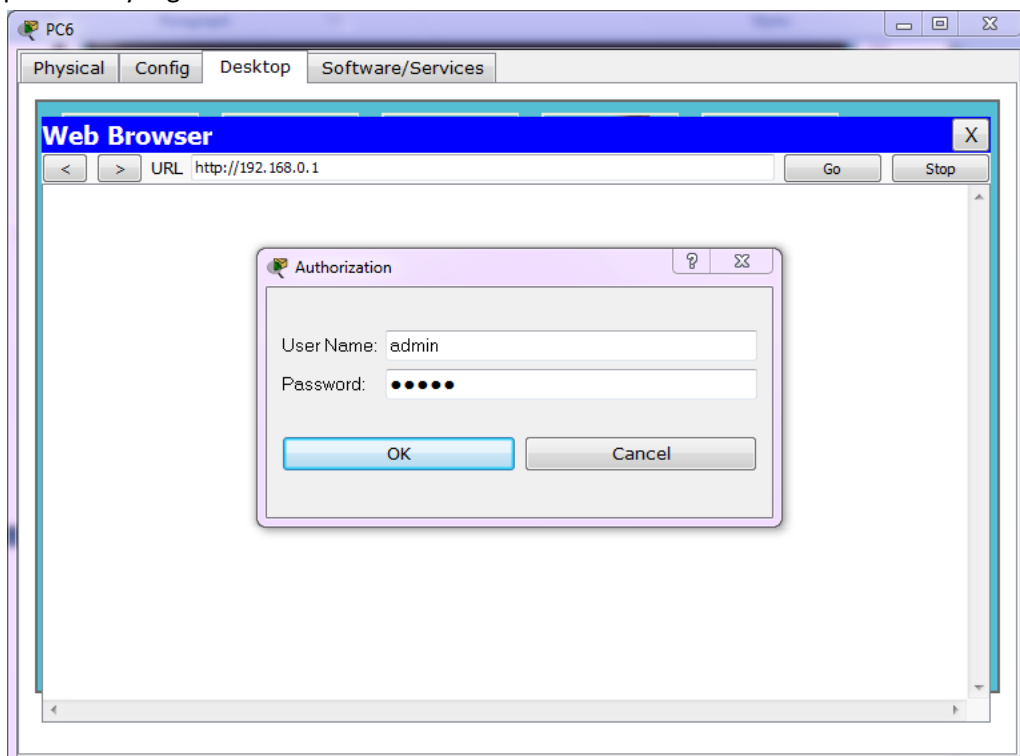
4. Mengakses menu admin WRS1

Akses WRS1 dengan web browser

Buka web browser yang ada pada tab Destop di **laptop1**. Pada URL ketik default gateway yang didapatkan **laptop1**.

Masukkan password WRS1

Akan muncul prompt yang meminta username dan password. Secara default username dan password yang ada adalah **admin**. Klik **Ok**.



5. Konfigurasi IP Address untuk WRS1

Perlu diketahui bahwa kita akan mensetting Access Point yang bertindak seperti router dengan dua interface yang berbeda. Yang pertama adalah interface yang bertindak sebagai

Internet atau jaringan luar dari wireless(dalam hal ini adalah jaringan ke switch). Yang kedua adalah interface yang menghubungkan klien dari jaringan wireless kita.

Mengeset koneksi Internet menjadi IP statik

Pilih halaman Setup. Pada Internet Setup pilih Internet Connection Type : Static IP.

Mengeset IP address untuk Internet Setup

Masukkan Internet IP address ke **172.17.10.25**

Masukkan subnet mask **255.255.255.0**

Masukkan default gateway ke IP address VLAN 10, **172.17.10.1**

The screenshot shows the Linksys WRT300N web interface. The top header includes the Linksys logo, 'A Division of Cisco Systems, Inc.', and 'Firmware Version: v0.93.3'. The main navigation bar has tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Setup' tab is active, and the 'Internet Setup' sub-tab is selected. On the left, a sidebar shows 'Internet Setup' and 'Internet Connection type'. The main content area shows a dropdown menu set to 'Static IP'. Below this, fields for 'Internet IP Address', 'Subnet Mask', 'Default Gateway', 'DNS 1', 'DNS 2 (Optional)', and 'DNS 3 (Optional)' are displayed with input boxes. The values entered are: Internet IP Address: 172.17.10.21, Subnet Mask: 255.255.255.0, Default Gateway: 172.17.10.1, and all DNS fields are set to 0.0.0.0. A 'Help...' link is visible on the right side of the form.

6. Konfigurasi DHCP Access Point

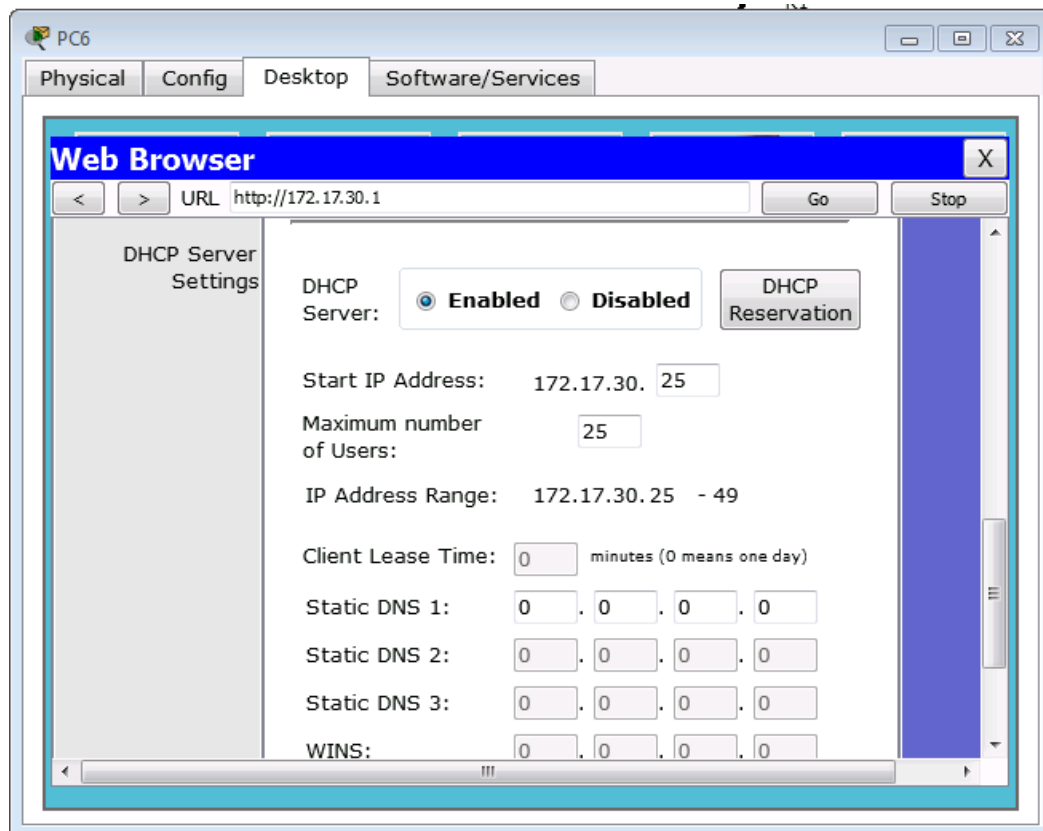
Menset IP address untuk Network Setup

Masukkan IP address **172.17.30.1** netmask **255.255.255.0**

Setting DHCP

Pada DHCP Server Settings set **Start address** ke **25** dan **Maximum number of users** menjadi **25**. Nantinya akan didapatkan range dari IP address DHCP yaitu **172.17.30.25 - 172.17.30.39**

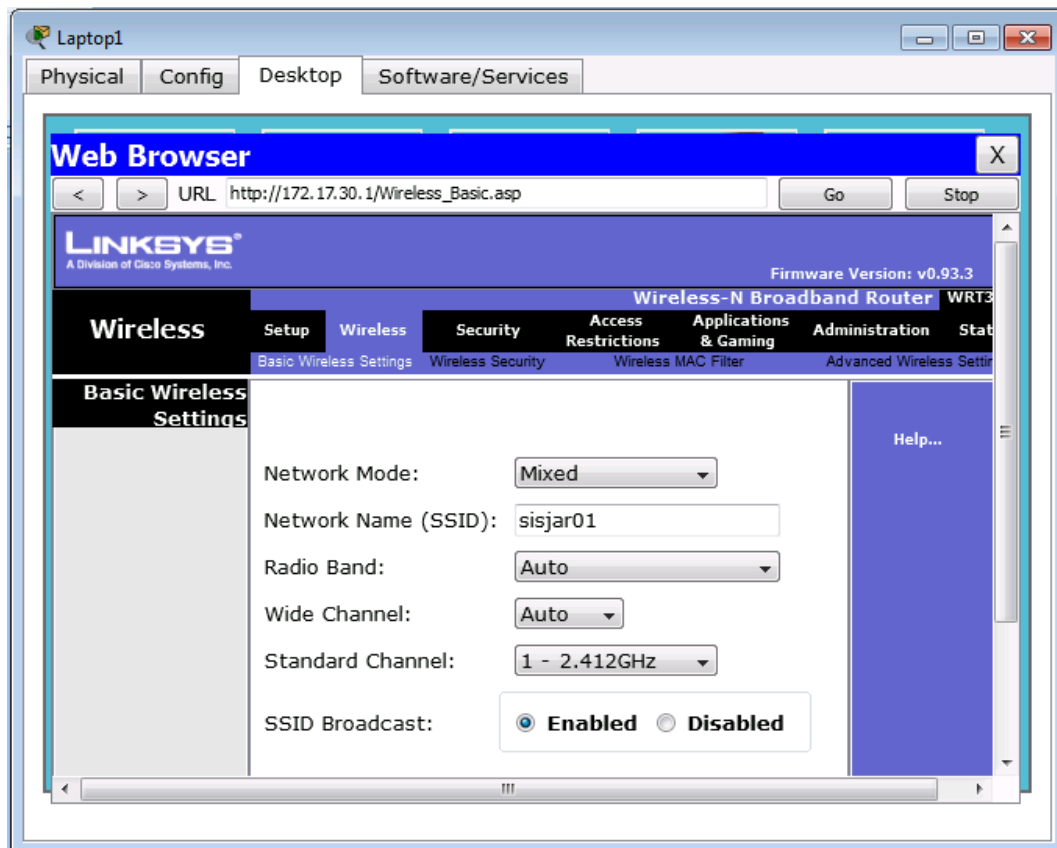
Klik **Save Settings** untuk menyimpan konfigurasi.



7. Setting SSID

Mengatur SSID

Akses web untuk router wirelessnya. Pilih menu Wireless dan ganti Network Name SSID menjadi "sisjar01".



Simpan perubahan yang ada

Koneksi ulang wirelessnya

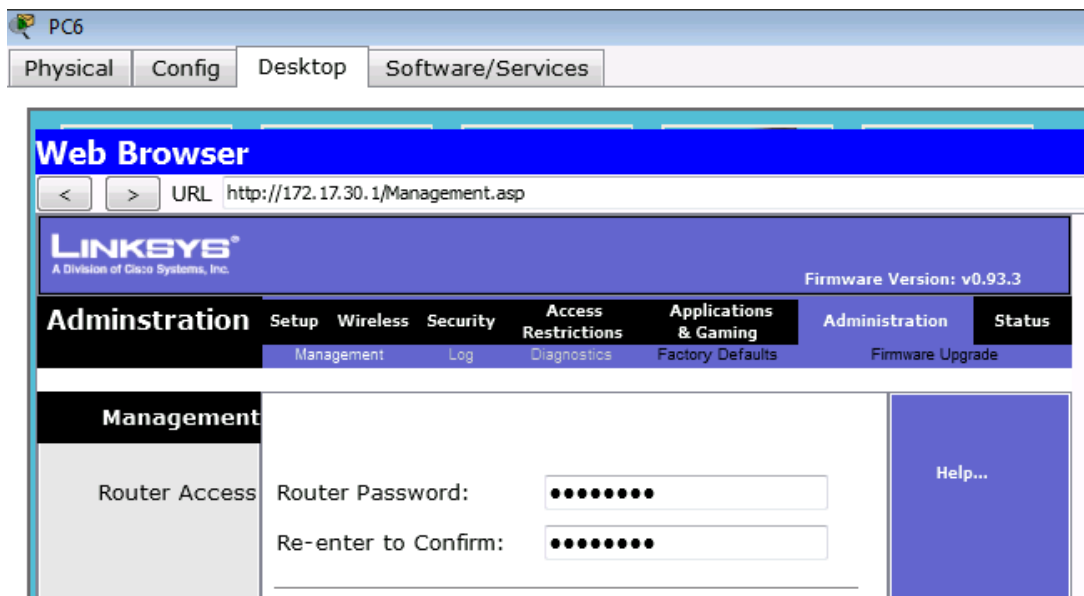
Karena sudah bergantinya nama jaringan yang ada maka diperlukan koneksi ulang pada **laptop1**. Pada Desktop buka lagi PC Wireless dan pilih tab Connect. Pilih "**sisjar01**".

8. Mengatur dan Mengamankan Web Setup pada Wireless Router

Oleh karena username dan password yang terset secara default yaitu "admin", maka ini menimbulkan lubang keamanan yang besar. Sistem Web Setup bisa diakses dan dikontrol orang yang tidak bertanggung jawab. Setingan default ini semestinya dirubah.

Masuk ke web setup

Pilih tab **Administration**, di **Router Access** ganti passwordnya menjadi "**sisjar01**".



Simpan perubahan yang ada

Kembali ke halaman web setup

Masukkan password

Pada web router ketika diprompt untuk meminta username maka isi dengan admin dan password "sisjar01"

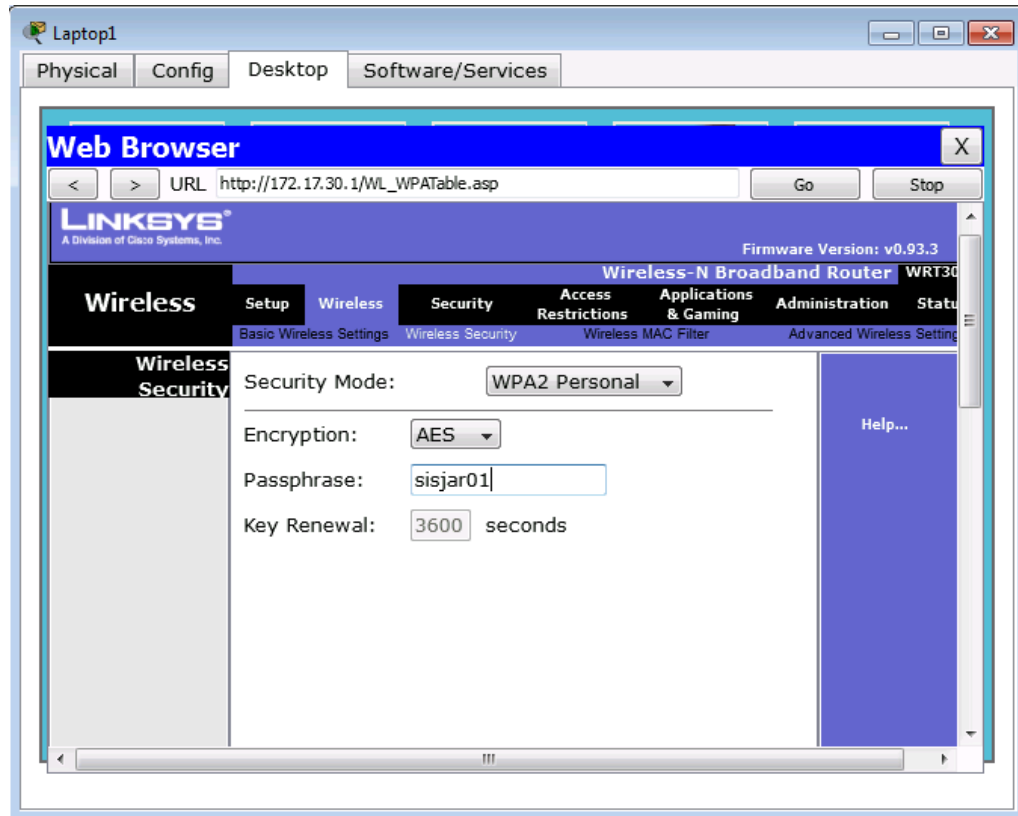


Refresh interface pada laptop1 dengan IP yang baru didapatkan

Ketik pada command prompt `ipconfig /renew`

9. Mengaktifkan Keamanan Jaringan Wireless

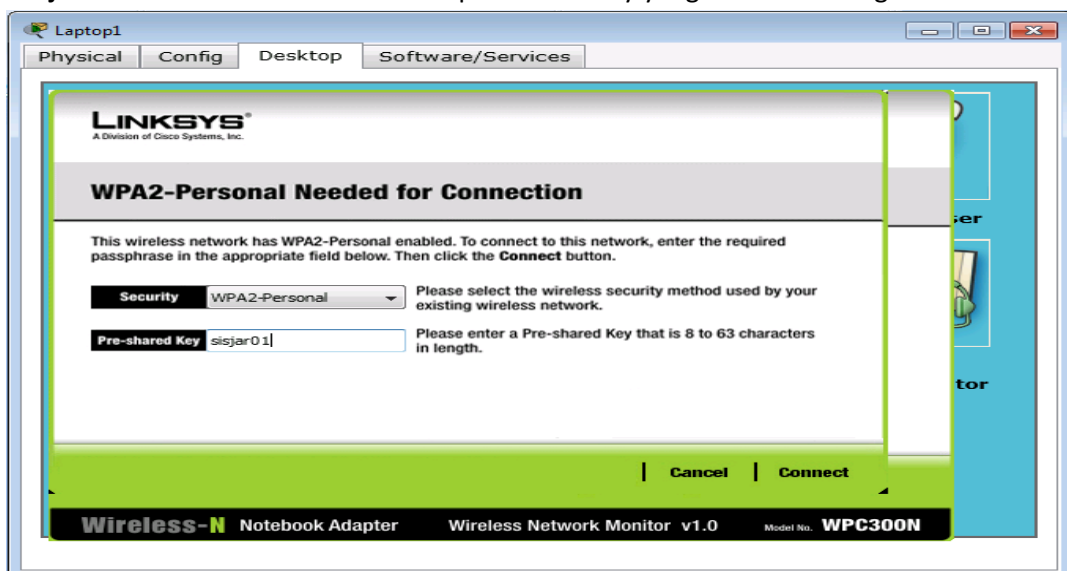
Akses web untuk router. Pilih menu **Wireless** dan klik tab **Wireless Security**. Pada pilihan **Security Mode**, pilih **WPA2 Personal** dan masukkan key “sisjar01”. Dengan menggunakan **Security Mode** maka jaringan akan menjadi lebih aman dari penyadapan yang bisa terjadi apabila paket yang dilewatkan tidak disertai jenis enkripsi apapun.



Simpan perubahan yang ada

Koneksi ulang wirelessnya

Kembali ke **Desktop** pada PC6, klik **PC Wireless**. Pilih tab **Profiles** dan klik **Edit**. Pilih jaringan “sisjar01”. Tekan **Connect**. Masukkan pre-shared key yang sudah disetting. Klik **Connect**.

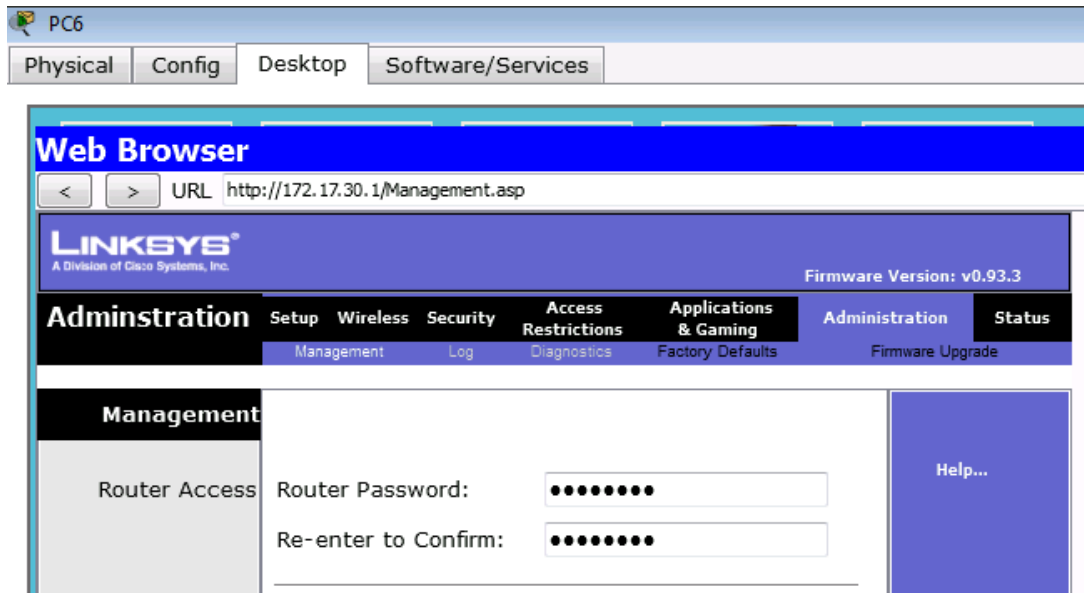


10. Mengatur dan Mengamankan Web Setup pada Wireless Router

Oleh karena username dan password yang teraset secara default yaitu “admin”, maka ini menimbulkan lubang keamanan yang besar. Sistem Web Setup bisa diakses dan dikontrol orang yang tidak bertanggung jawab. Setingan default ini semestinya dirubah.

Masuk ke web setup

Pilih tab **Administration**, di **Router Access** ganti passwordnya menjadi “sisjar01”.



Simpan perubahan yang ada

Kembali ke halaman web setup

Masukkan password

Pada web router ketika diprompt untuk meminta username maka isi dengan admin dan password “sisjar01”