

## CHAPTER 2

Routing yang umum digunakan adalah RIP, OSPF dan BGP. RIP dan OSPF dikategorikan sebagai interior gateway routing protocol (IGP) sedangkan BGP atau bordeway routing protocol termasuk kategori external routing protocol.

IGP menangani routing jaringan internal pada sebuah AS sedangkan EGP antar AS

### Karakteristik RIP

mendukung jaringan Point to point, point to multipoint dan jaringan multiakses. Kelebihan utama dari OSPF adalah dapat dengan cepat mendeteksi perubahan yang terjadi di jaringan dan menjadikan routing kembali konvergen dalam waktu singkat dengan sedikit pertukaran data, lambat mengetahui perubahan jaringan dan menggunakan metrik tunggal.

RIP adalah protocol yang menggunakan algoritma distance vector, kelemahan algoritma distance vector adalah lambat dalam mengetahui perubahan jaringan dan dapat menimbulkan routing loop, routing loop adalah suatu kondisi ketika kedua router bertetangga saling mengira bahwa untuk mencapai suatu alamat, datagram seharusnya dilewatkan ke router tetangganya tersebut.

RIP v 1, Setiap host yang menjalankan RIP v1 ini, memiliki tabel routing yang setidaknya berisi : IP Address tujuan, metrik yang menunjukkan biaya total tujuan, ip address router yang akan dilalui, suatu tanda perubahan route.

Kelebihan RIPv2 adalah tag untuk rute eksternal, subnet mask, alamat hop berikutnya dan autentikasi, mendukung VLSM

## OSPF

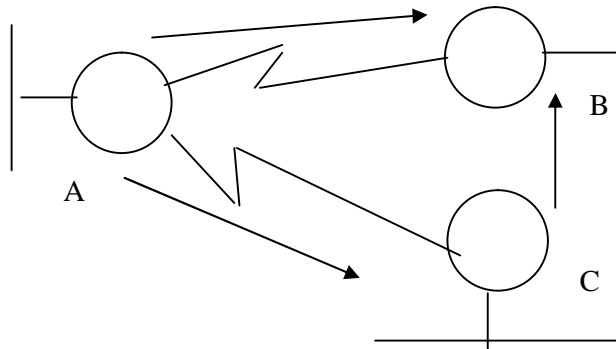
Protocol ini termasuk dalam link-state protocol, kelebihan utama dari protocol ini adalah dapat dengan cepat mendeteksi perubahan dan menjadikan routing kembali konvergen dalam waktu singkat dengan sedikit pertukaran data.

Routing ini membentuk peta jaringan dalam tiga tahap, tahap pertama setiap router mengenali seluruh tetangganya, lalu router saling bertukar informasi dan router akan menghitung jarak terpendek ke setiap tujuan. Peta jaringannya akan disimpan dalam basis data sebagai hasil dari pertukaran informasi antar router

OSPF dapat menangani routing jaringan TCP/IP yang besar dan membuat hirarki routing dengan membagi jaringan menjadi beberapa area. Setiap paket yang dikirim dapat dibungkus dengan autentikasi, namun protocol ini membutuhkan kemampuan CPU dan memori yang besar

Proses dasar routing OSPF adalah menghidupkan adjacency, proses flooding, dan perhitungan table routing. Router-router mengirimkan paket hello ke seluruh jaringan yang terhubung secara periodic, jika paket tidak terdengar maka jaringan dianggap down, defaultnya mengirimkan 4 kali paket hello

Router-router selalu berusaha adjacent dengan router tetangganya berdasarkan paket hello yang diterima. Dalam jaringan multi access, router memilih Designated Router (DR) dan Backup Designated Router (BDR) dan mencoba adjacent dengan kedua router tersebut.



Ket :

Misalkan jaringan baru terkoneksi, maka router A akan membroadcast paket hello ke semua int dengan memberikan informasi tentang router A, dan begitu juga sebaliknya A akan mengetahui informasi tentang tetangganya berdasarkan informasi yang diterima dan mengetahui berapa biaya untuk mencapai router lain. Data-data ini disimpan dalam basis data

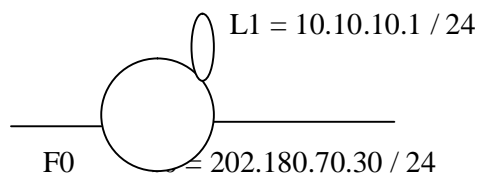
Setelah itu setiap router mengirimkan basis data tersebut dalam satu paket LSA (link state advertisement), dan router yang menerima LSA harus mengirimkan ke semua router yang terhubung dengannya.

Karena router B telah menerima paket LSA dari router A maka jika LSA yang dikirimkan C sama dengan yang ada pada basis data B atau bukan yang baru, maka paket LSA dari C akan di drop.

Antara router satu dengan yang lain akan mengirmkan paket hello dengan interval tertentu misalnya 120 detik , jika tidak terdapat hello paket dari jaringan yang terkoneksi dengannya atau tidak mendapat balasan maka jaringan tersebut dianggap down. Maka jika terjadi NT down maka paket LSA akan disebarkan ke semua jaringan dengan menggunakan floading dan akan menyebabkan basis data LSA berubah untuk mencari jalan yang terbaik dalam paket data

**Router ID**

Router ID didapatkan dari IP address tertinggi yang dimiliki semua interface router, apabila router mempunyai interfaces loopback maka yang digunakan adalah IP address tertinggi dari interface loopback tersebut



Router id router diatas adalah 10.10.10.1 (L 1), apabila tidak memiliki int loopback maka yang menjadi router Id adalah 202.180.70.30 (S 0), router id akan diambil dari int yang di UP sebelum proses OSPF dimulai

Router ID digunakan dalam proses penentuan DR/BDR yang dalam pembentukan hubungan bi-directional

### **Tahapan dalam membentuk adjacency**

Pada saat baru pertama ON, router OSPF tidak tahu apapun tentang tetangganya, router akan mulai mengirimkan paket Hello ke seluruh interface jaringan untuk memperkenalkan dirinya. Jika router yang baru ON ini menerima paket hello yang menyimpan informasi tentang dirinya maka router ini dapat saling berhubungan dua arah dengan router pengirim hello,

Default nilai hello pada broadcast multi-access adalah 10 detik dan 40 detik jika tidak ada respon akan mati, dan pada NBMA hello 30 detik dan akan mati pada 120 detik jika tidak terdapat respon

1. down : router tidak dapat hello packet dari router manapun
2. attempt : router mengirimkan hello packet tetapi belum mendapat respon, hanya ada pada tipe NT *non broadcast multi-access* (NBMA) dan tidak ada respon dari router lain.
3. Init : router mendapatkan hello packet dari router lain, tetapi belum terbentuk hubungan yang bidirectional (2 way)
4. 2 way : pada tahap ini hubungan antar router sudah bi-directional, untuk NT broadcast DR & BDR nya akan melanjutkan ke tahap full, router non DR & BDR akan melanjutkan Full hanya dengan DR & BDR saja
5. Exstart : terjadi pemilihan Master dan Slave, master adalah router yang memiliki router id tertinggi
6. exchange : terjadi pertukaran Database Descriptor (DBD) paket DBD ini digambarkan dari topologi DB router, proses dimulai oleh master
7. loading : router akan memeriksa DBD dari router lain dan apabila ada entry yang tidak diketahui maka router akan mengira **link state request (LSR)** , LSR akan dibales dengan link state state ACK dan link state reply, diakhir tahap ini semua router yang di adjacent memiliki topologi DB yang sama
8. Full : masing-masing router sudah membentuk hubungan yang adjacent.

### **Pemilihan DR & BDR**

Dalam jaringan multi akses router-router akan memilih DR (designated router) dan BDR(Backup designated router) dan berusaha adjacent dengan kedua router tersebut.

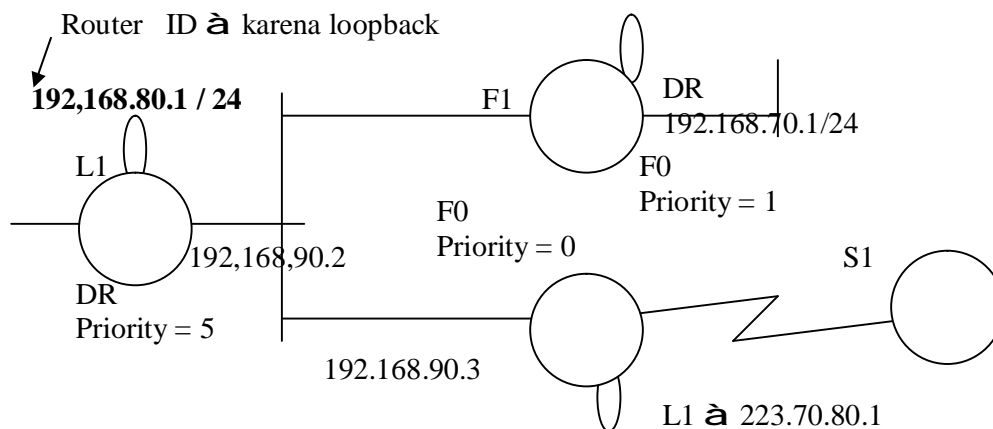
- Pemilihan terhadap tipe network multi access (broadcast & non broadcast)
- Pemilihan dilakukan berdasarkan nilai ;
  - Router Priority
  - Router ID

- Router priority diset per interface nilainya 0-255
  - Router (config-if)# IP OSPF priority [0-255]
- Router mempunyai priority 0 tidak akan menjadi DR/BDR, statusnya DROTHER, semakin besar priority semakin besar kemungkinan dipilih menjadi BR (Priority paling tinggi) dan BDR (kedua paling tinggi / slave)
- Setting nya oleh administratornya, sesuai yang mana dulu routernya UP
- By default nilai router priority untuk semua router adalah ;
  - Apabila priority router sama maka yang digunakan untuk menentukan DR/BDR adalah **Router ID**
  - Pada tiap NT non broadcast (ex : Frame Relay) router yang menjadi DR adalah router yang memiliki link ke semua router yang lain (mutipoint)

Jika terjadi DR & BDR mati maka router-router akan mengadakan pemilihan untuk menggantikan router yang mati tersebut.

Proses flooding adalah router dengan paket LSA harus meneruskan paket ke semua jaringan, dan memasukkan informasi LSA dalam databasenya , jika paket data yang diterima tidak baru maka akan di drop, disebut flooding karena seolah-olah membanjiri jaringan dengan LSA (link state advertisement)

Setiap kali BD linkstate router berubah, router kembali perlu menghitung rute terbaik dan membentuk table routing terbaru, dengan biaya terendah dan shortest path terpendek



Router (config) #router OSPF 1  
 Router (Config-router) # default-information originate à hanya untuk default router  
 Perintah redistribute static metric 100 – semua static routing akan didistribusikan

**Perintah-perintah OSPF**

- Router(config)#router OSPF [process id]
- Router(config-router)#network network id wildcard mask area number
- Router(config-if)#ip OSPF priority [0-255] à bandwidth link
- Router(config-if)#IP OSPF cost [1-65535]
- Rouer(config-if)##bandwidth [1-10.000.000] -> kbps

**Authentikasi**

MD5 : suatu teknik enkapsulation enkripsi password

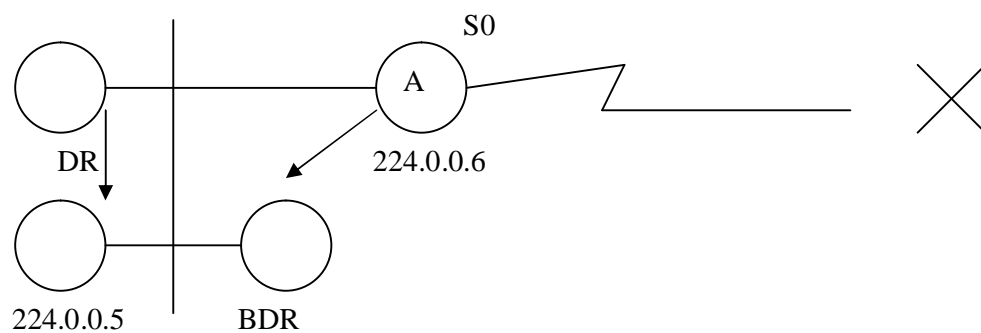
Setting :

router (config-if)#ip ospf authentication-key password (yang dipasang pada INT)

Router(config-router)# area nomer area authentication

Hello interval dan dead interval (sebanyak 4 x) adalah waktu apabila router mendapat hello packet dari neighbour dan setelah waktu habis berarti NT tersebut down dan tidak akan dihubungi

Contoh update jika NT down



224.0.0.6 à DR & BDR

224.0.0.5 à DR ke non DR

## Chapter 3

### IGRP & EIGRP

Perbedaannya :

#### 01. Compatible mode

- IGRP Kompatibel 100 % dengan EIGRP
- Antara router-router yang menjalankan EIGRP & IGRP dengan autonomous system yang sama akan langsung otomatis terdistribusi

#### 02. Metric calculation

- Metric IGRP :  $k1 * \text{bandwidth} / 256 - \text{load} + k3 * \text{delay} * k5 / \text{reliability} + k4$ 
  - Nilai :  $K1, k3 = 1$ , nilai  $k2, k4, k5 = 0$
- Metric IGRP =  $K1 * \text{bandwidth} + k3 + \text{delay}$
- Bandwidth =  $10^7 / \text{bandwidth link} * 256$
- Delay =  $\text{delay} / 10 * 256$
- Dikarenakan metric IGRP = 24 bit. Metric EIGRP = 32bit

#### 03. Hop count

- IGRP support = 255 hop count (MAX)
- EIGRP support = 224 hop count (max)

#### 04. autonomous Protocol redistribution

#### 05. route tagging

- EIGRP akan memberi tagging external route untuk setiap route yang berasal dari ;
  - Routing protocol non eigrp
  - Routing protocol IGRP dengan AS number yang sama

### EIGRP konsep

EIGRP memiliki 3 table untuk proses kerjanya

#### 01. Topologi table

- Merupakan table yang berisi informasi mengenai suatu route lengkap dengan metric
- Topologi table ini dibangun berdasarkan informasi dari route tetangga
- Informasi yang ada di topologi table :
  1. Feasible distance : metric terbaik untuk ke suatu NT hasil perhitungan router
  2. Reported distance : metric ke suatu NT hasil pemberitahuan router tetangganya
  3. Router source : informasi mengenai sumber route berasal dari router mana
  4. Interface information : informasi mengenai interface suatu route berasal
  5. Router status : ada 2 : passive : route bisa dipakai dan operasional dan active : route sedang diproses oleh EIGRP

#### 02. neighbour table : berisikan informasi mengenai router-router neighbour EIGRP dan identik dengan adjacency database OSPF

#### 03. routing table : successors : router yang dipakai untuk menuju ke suatu NT

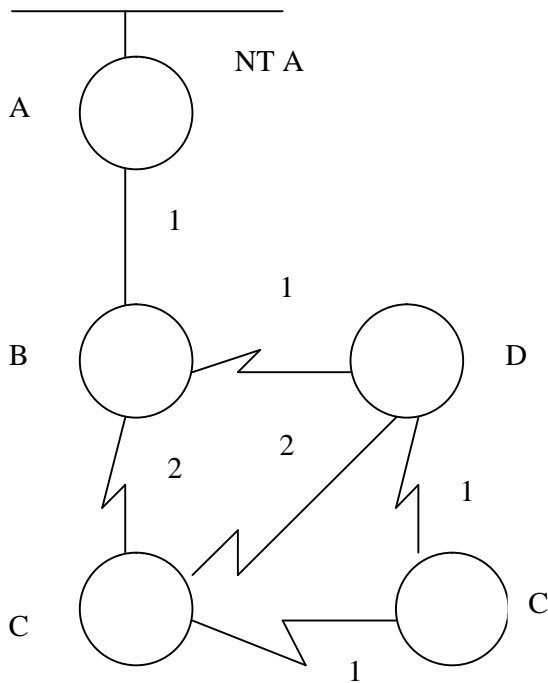
pada saat Hello protocol ke NT lain maka ;

01. neighbour discovery & recovery : mengirim topology table ke neighbour baru
02. reliable transport protocol : TCPnya EIGRP dan memastikan agar packet yang dikirim selalu diterima oleh router lain
03. dual finite-state-algorithm : difusing update algoritma, merupakan algoritma untuk menentukan route terbaik (successor) dan bekerja berdasarkan informasi dari topologi table dan neighbour table
04. protocol dependent modules : protocol yang membuat EIGRP bisa support terhadap multiple NT layer protocol e : ex : untuk IP, IPX dan appletalk

**EIGRP packet Type :**

01. hello : untuk maintenance, mencari neighbour router
02. acknowledgment : hello packet yang data fieldnya 0
03. update : paket yang digunakan untuk memberikan perubahan NT
04. Query : paket yang dikirim oleh router untuk meminta informasi ke routerlain mengenai suatu route / NT
05. reply : balasan dari query packet

ex :



Topologi table

Router D	FD	RD
NT A	2	
Via B	2	1 (successor)
Via C	5	3

Router C	FD	RD
NT A	3	
Via B	3	1 (successor)
Via D	4	2 (feasible successor)
Via E	4	3

Router E	FD	RD
NT A	3	
Via D	3	2 (succsessor)
Via C	4	3 <b>à</b> ngak bisa karena sama

Note : Feasible distance (FR) dan Reported distance (RD)  
 FR : kalkulasi matrik yang paling terpendek ke tujuan  
 RD : laporan Path tujuan yang spesifik oleh adjacent neighbor

Tata cara pemilihan FD, router tersebut harus memiliki RD yang lebih kecil dari FD yang ada sekarang.

**Config EIGRP**

Router (config) #router EIGP [AS number]

Router(config-router)#network network id [wild card]

**Manual summarization**

Yang dipasang pada tiap interface

(config-if) #ip summary-address EIGRP [AS number] network id subnet mask AD  
Administrative distances [optional 5]

## Chapter 4

### Switching Concepts

Teknologi Ethernet yang saat ini banyak digunakan, ada teknologi thick dan thin Ethernet. Dengan menggunakan collision, layer 2 lebih pintar dari layer 1 dimana dapat meforwarding decisions based pada Media Access Control (MAC) addresses.

bridge berada pada layer 2 yang berfungsi untuk membagi-bagi persegment pada network. Begitu juga dengan switch yang berada pada layer 2, cara kerjanya mirip dengan bridge namun memiliki banyak port (multiport bridge).

Kelemahan perangkat pada layer 2 ini adalah melakukan forward frame secara broadcast ke semua device NT, dimana jika terjadi baanyak broadcast pada NT maka akan terjadi sluggish pada waktu respon

Saat ini LAN menggunakan kombinasi perangkat pada Layer 1, 2 dan 3 yang disesuaikan dengan kebutuhan dari perusahaan tersebut

Mengapa perlu Segmentasi, karena untuk membagi sebagian kecil dari jaringan yang disebut sebagai segment. Segmentasi mengikuti congestion NT untuk dapat secara signifikan mengurangi banyak segment, disaat transmisi data antar segment, device pada satu segment akan membagi total bandwidth yang ada. Segmentasi dapat dilakukan dengan menggunakan Bridge, Router dan Switch

Switch menggunakan cara collision domain yang tergantung dari jumlah port, dimana 1 port ada 1 collision domain, sedangkan akan ada 1 broadcast domain jika tidak menggunakan fungsi VLAN

Perangkat router : 1 port 1 collision domain

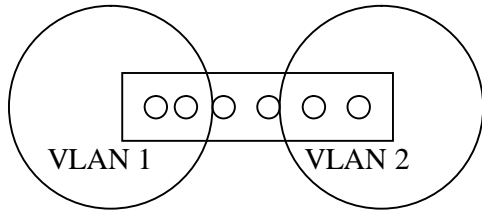
Perangkat hub menggunakan sistem Half duplex sedangkan switch menggunakan mekanisme full duplex

#### **LAN Switching**

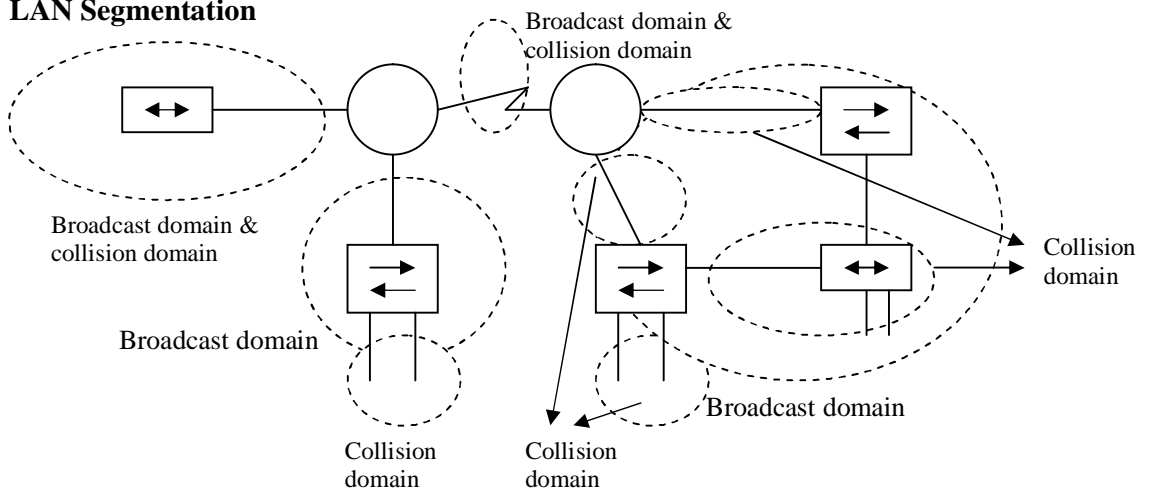
Ada 2 klasifikasi pada alokasi badwidth di switch port yaitu as symmetric or asymmetric based. Asymmetric switch membuat koneksi antara port dengan bandwidth yang sama. Switching Asymmetric memungkinkan bandwidth untuk terhubung dedicated ke server port switch untuk mencegah terjadinya bottleneck. Metode switching ini memerlukan memory buffering, diperlukan buffer untuk menjaga agar tetap kesinambungan frames diantara perbedaan data rate pada ports.

#### **VLAN**

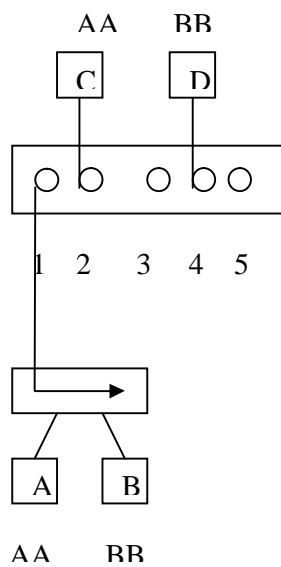
Teknologi VLAN adalah suatu cara yang memisahkan segmen-segmen pada switch dimana antara 1 segmen dengan segmen lain tidak dapat terkoneksi, koneksi dapat dilakukan dengan menggunakan router. dalam satu switch akan berbeda network idnya dan berbeda broadcast domainnya. VLAN dijalankan berdasarkan software pada Switch, misalnya ;



**LAN Segmentation**



**Cara kerja Switch**



MAC	Port
AA	1
BB	1
CC	2

### Metode Switching

- Cut Through = pada metode ini frame diperiksa sampai field destination, fragment free = frame diperiksa sampai 64 byte pertama, collision bisa menjadi pada 64 bytes pertama
- Store & Forward = frame disimpan terlebih dahulu, dicek nilai FCS (Frame check) nya baru di forward, apabila framenya tidak rusak
- Adaptive Cut Through = gabungan dari cut thorough dengan store n forwarf, apabila dirasa ada error maka akan berubah dari cut through menjadi store n forward setelah error berkurang akan kembali lagi

### Perbedaan

<b>Waktu</b>	<b>error checking</b>
Store n forward	store n forward
Fragment free	fragment free
Cut through	cut through

Microsegmentasi : 1 port 1 host

Unicast : hanya 1 yang dikomunikasikan dan diproses

Broadcast : ke semua dan diproses

Multicast : ada 2 dikomunikasikan namun hanya 1 yang diproses.

## Chapter 5

Dalam mendesign LAN kita harus memperhatikan aspek : Fungsional, Skalability, Adapsi dan Manajemen, fungsi dan penempatan pada server seperti enterprise yang melayani hamper semua user dalam organisasi ex : mail, DNS , dll, (MDF) dan Workgroup : yang melayani dari user dalam 1 organisasi (IDF).

Metodelogi dalam design bertujuan untuk melihat kebutuhannya user dan ekspetasinya, analisa kebutuhan data, mendesign strukturnya dan membuat dokumentasi.

MDF terdapat Horizontantal Cross Connect (untuk user) dan Vertical Cross Connect (untuk backbone)

Perancangan NT dengan system hirarki :

1. access layer : paling dekat dengan hirarki
2. distribution layer : policy terhadap traffic
3. core layer : high speed switching, tidak ada policy terhadap data

VLAN : berupa suatu software dari device switch yang berfungsi untuk mengelompokan user berdasarkan fungsional, 1 broacast domain (1 VLAN) dan antar VLAN dapat terkoneksi dengan router

## Chapter 6

### Setting Switch

Switch#show flash

Config.txt → start up config

Vlan.dat → isi info tentang vlan switch

Untuk menghapusnya ;

Switch# delete flash : vlan.dat

Switch# delete flash : config.txt atau erase startup configuration

Switch#reload

Switch# show mac-address-table

Setting security, misalnya hanya MAC address tertentu

Switch(config)# mac-address-table static 0010.7a60.1884 interface fast Ethernet 0/5  
vlan 100

Switch(config)#show mac-address-table aging → setiap 30 detik akan meresh mac  
tablenya (default)

Switch(config)# mac-address-table aging-time 0 → disable aging nilanya 0 – 1000000s

Untuk mengganti IOS Switch ;

Switch# erase flash → seluruh file pada switch akan dihapus

Switch# archive tar/xtract tftp// 10.21.22.200/namafile.tar

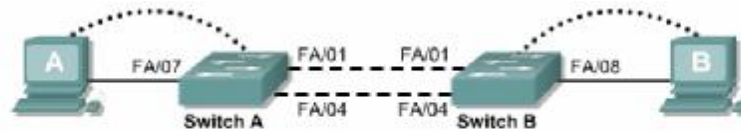
Mengganti password recovery pada switch

1. cabut kabel power switch
2. sambungkan kabel power switch sambil menekan tombol mode
3. tunggu sampai lampu system menjadi oranye
4. ketikan : switch# flash\_init → untuk inialisasi flash
5. rename file konfigurasi switch#rename flash: config.text flash : config.old
6. ketik pada switch#boot
7. masuk ke switch seperti biasa dan jawab 'NO' pada setiap mode
8. masuk ke privileged mode
9. rename flash : config.old flash : config.text
10. copy flash : config.text start-up configuration
11. copy run start
12. ganti password (secret, enable, telnet)
13. copy run start

## Chapter 7

### Spanning Tree Protocol

Tahapan STP ; pilih root bridgenya, root portnya dan designed portnya  
 Contoh kasus STP dengan memilih Root Bridge :



Switch Designation	Switch Name	Enable Secret Password	Enable/VTY/and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0
Switch 2	Switch_B	class	cisco	192.168.1.3	192.168.1.1	255.255.255.0



SwitchA#show spanning-tree **a** untuk melihat konfigurasi root id dan bridge id, interface dan priority

SwitchA#config t

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

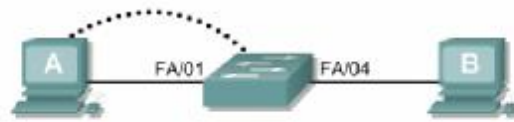
SwitchA(config)#show spanning-tree **a** untuk melihat perubahan pada root id

SwitchA(config)#show running-config

SwitchA(config)# show spanning-tree

## Chapter 8

### Kasus VLAN



Switch Designation	Switch Name	Enable Secret Password	Enable/VTY/and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0



Setelah start up Switch, maka pilih ‘ K ‘ untuk konfigurasi dengan menggunakan command line sedangkan ‘ M ‘ untuk masuk ke menu step by step.

```
Switch> en
Switch> config t
Switch(config)# hostname swithA
SwithA(config)#vlan database
SwithA(vlan)# vlan 2 name VLAN2
SwithA(vlan)# vlan 3 name VLAN3
SwithA(vlan)# exit
SwithA# show vlan  a untuk melihat vlan yang telah dibuat
```

```
Switch#config t
SwitchA(config)#enable secret cisco
SwitchA(config)#line console 0
SwitchA(config-line)#password cisco
SwitchA(config-line)#login
SwitchA(config-line)#exit
```

```
SwitchA(config)#line vty 0 15
SwitchA(config-line)#password cisco
SwitchA(config-line)#login
SwitchA(config-line)#exit
```

```
SwitchA(config)#interface vlan 1
SwitchA(config-if)#ip address 192.168.1.2 255.255.255.0
SwitchA(config-if)#exit
SwitchA(config)#ip default gateway 192.168.1.1
```

```
SwithA# config t
SwithA(config)# int fa 0/1 à memasukkan port 0/1 ke dalam group vlan 2
SwithA(config)# switchport mode access
SwithA(config)# switchport access vlan 2
SwithA(config)# end
```

```
SwithA# config t
SwithA(config)# int fa 0/4 à memasukkan port 0/4 ke dalam group vlan 2
SwithA(config)# switchport mode access
SwithA(config)# switchport access vlan 2
SwithA(config)# end
```

```
SwitchA# show vlan id 2 à melihat status pada config vlan 2
```