CCNA 3

CHAPTER 1
Introduction to Classless Routing

Perbedaan classfull & classless

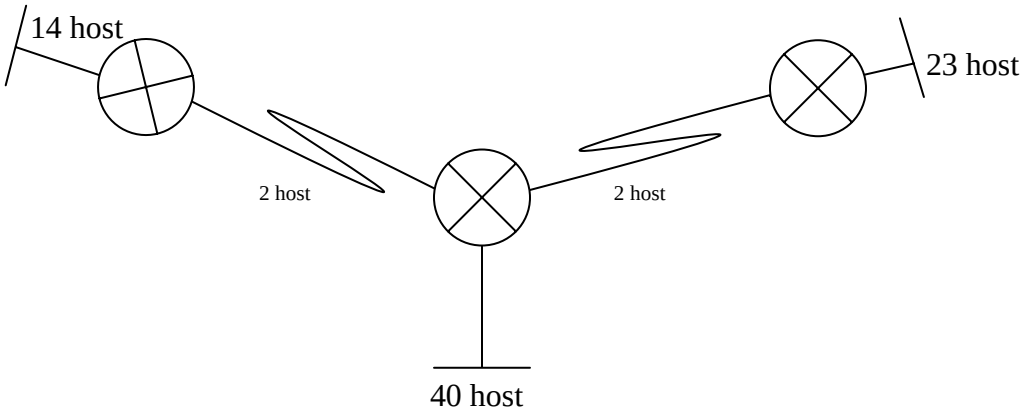
Classfull : Subnet mask yang digunakan adalah sama, misalkan default ataupun subnetting.

Classless : Subnet mask berbeda-beda, disesuaikan dengan kebutuhan, misalnya dilakukan VLSM.

VLSM (Variable Length Subnet Mask)

VLSM digunakan guna penghematan pembagian alamat ip agar tidak boros dalam pemakaian.
Biasanya dibagi mulai dari network yang jumlah hostnya paling banyak.

Contoh :

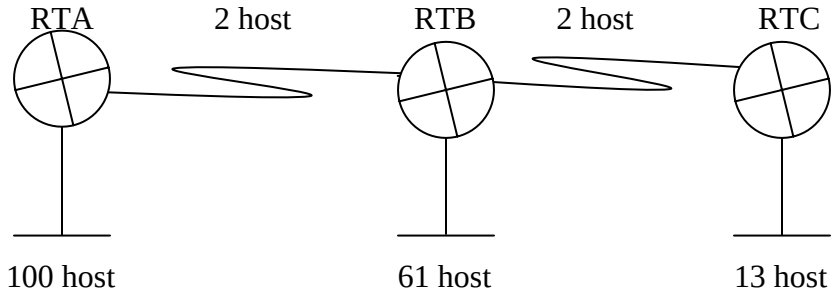


Bila diberikan ip 192.168.10.0/24, maka pembagian VLSM adalah sebagai berikut :

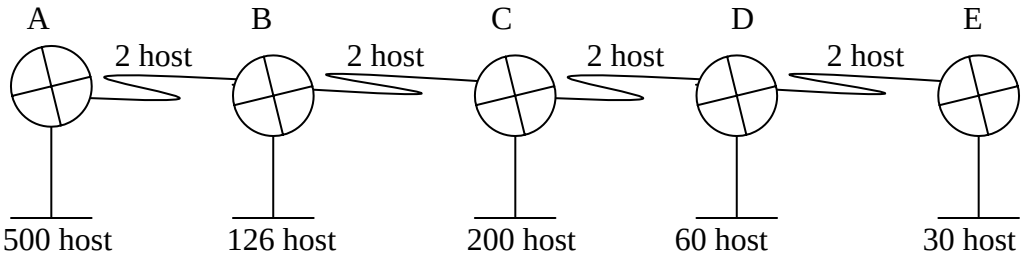
192.168.10.0/26	->	40 host
192.168.10.64/27	->	23 host
192.168.10.96/28	->	14 host
192.168.10.112/30	->	2 host

Latihan :

1) 172.16.0.0/16



2) 10.0.0.0/8



Jawab :

1) 172.16.0.0/25 > 100 host
   172.16.0.128/26 > 61 host
   172.16.0.192/28 > 13 host
   172.16.0.208/30 > 2 host
   172.16.0.212/30 > 2 host

2) 10.0.0.0/23 > 500 host
   10.0.2.0/24 > 200 host
   10.0.3.0/25 > 126 host
   10.0.3.128/26 > 60 host
   10.0.3.192/27 > 30 host
   10.0.3.224/30 > 2 host
   10.0.3.228/30 > 2 host
   10.0.3.232/30 > 2 host
   10.0.3.236/30 > 2 host

Classless didukung oleh routing protocol :

a) RIP v.2
b) OSPF
c) EIGRP

Pada VLSM maupun subnetting, terdapat istilah ip subnet zero yang aktif secara default pada router, untuk memastikannya :

Router(config)#no ip subnet-zero

Setelah dimatikan, maka tidak bisa menulis alamat ip dari subnet-zero (subnet pertama). Menghidupkan kembali dengan :

Router(config)#ip subnet-zero

Penggunaan VLSM dapat menghemat ip, contoh :
WAN link pada serial dapat ditulis /30 sebab hanya perlu 2 host untuk point-to-point, tidak mubazir seperti /24.

Routing Information Protocol Version 2

RIP v.2 mendukung classless routing, pada dasarnya sifatnya mirip dengan RIP v.1 yaitu hop count sebagai metric, maximal hop count yaitu 15 Administrative Distance 20.

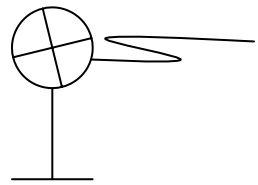
Perbedaannya :

RIP v.1	RIP v.2
- Subnetting	- Subnetting & VLSM
- Tidak mengirim informasi subnet mask	- Mengirim informasi subnet mask
- Broadcast 255.255.255.255	- Multicast 224.0.0.9
- No authentication	- Support Authentication
- Classfull	- Classless

Settingan :

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network network directly connected

Contoh :



200.20.10.0/30

192.168.10.0/27

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 200.10.10.0

Command show :

a) **Melihat routing table :**
   Router#show ip route
b) **Melihat routing protocol, AD, routing update :**
   Router#show ip protocol

Command debug :

a) debug ip rip
b) debug ip rip events
c) debug ip rip database

Authentication

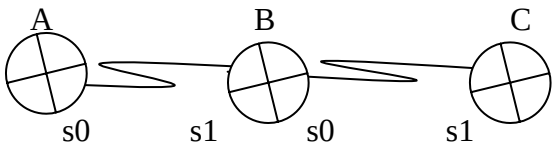
Router(config)#key chain name
Router(config-keychain)#key key number
Router(config-keychain-key)#key-string keyword

Router(config-if)#ip rip authentication key-chain name
Router(config-if)#ip rip authentication authentication mode mode

NB : Mode dapat berubah : a) Text : tanpa enkripsi
b) Md5 : dengan enkripsi

Dalam authentication, antara serial yang berpasangan harus sama key, key-string, & mode-nya.

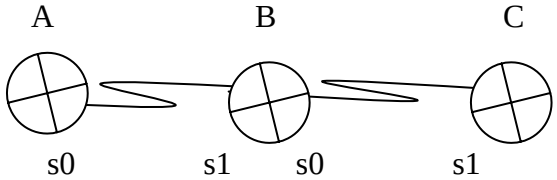
Contoh :



key chain : a	key chain : b	key chain :c
key : 1	key : 1	key : 1
key-string : rt	key-string : rt	key-string : rt

Untuk nama key chain boleh berbeda.

Bisa juga disusun demikian :



key chain : a	key chain : b	key chain :c	key chain : d
key : 1	key : 1	key : 2	key : 2
key-string : rt	key-string : rt	key-string : rt2	key-string : rt2

Jadi pada router B daoat dibuat 2 key chain.

CHAPTER 2
Single Area OSPF

Routing yang umum digunakan adalah RIP, OSPF dan BGP. RIP dan OSPF dikategorikan sebagai interior gateway routing protocol (IGP) sedangkan BGP atau border gateway routing protocol termasuk kategori external routing protocol.
IGP menangani routing jaringan internal pada sebuah AS sedangkan EGP antar AS.

Single area berarti hanya mempunyai area backbone, multi area berarti mempunyai area backbone dan area lain yang terhubung dengannya

Perbandingan Link State & Distance Vector

Distance Vector	**Link State**
-Update frequently	-trigered update
-Routing loop	-tidak rentan routing loop
-Hanya tahu routing tetangga	- tahu seluruh jaringan
-Mudah disetting	-lebih sulit disetting
-Slow convergence	-Fast convergence

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

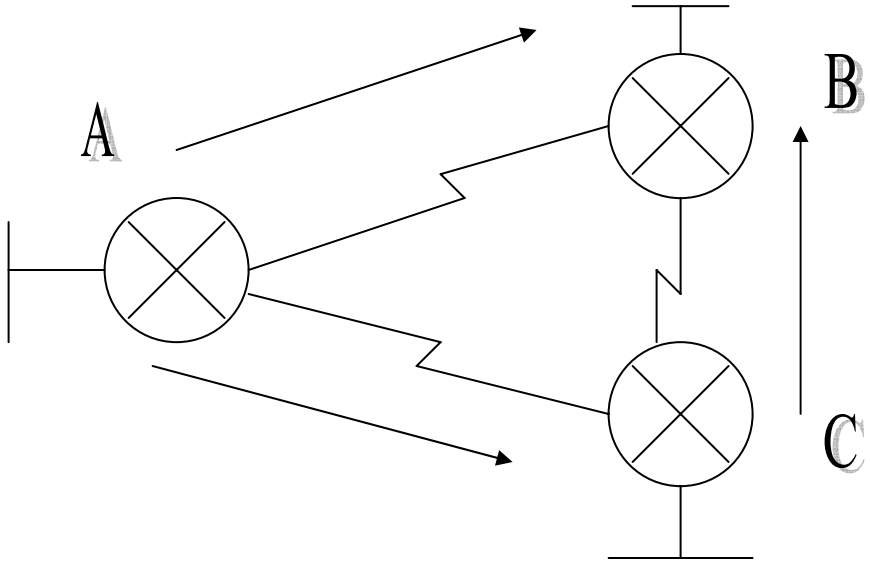
Routing ini membentuk peta jaringan dalam tiga tahap, tahap pertama setiap router mengenali seluruh tetangganya, lalu router saling bertukar informasi dan router akan menghitung jarak terpendek ke setiap tujuan. Peta jaringanya akan disimpan dalam basis data sebagai hasil dari pertukaran informasi antar 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 authentikasi, namun protocol ini membutuhkan kemampuan CPU dan memori yang besar.

Proses dasar routing OSPF adalah menghidupkan adjency, 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, defaultya 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 diangap down. Maka jika terjadi network 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.

Command-command konfigurasi OSPF

Router(config)#router ospf process id
Router(config-router)#network network id wildcard mask area area number

Mengubah hello&dead message
Router(config-if)#ip ospf hello-interval time
Router(config-if)#ip ospf dead-interval time
Mengubah bandwithlink
Router(config-if)#bandwidth bandwith[1-10.000.000] –> kbps
Mengubah cost
Router(config-if)#ip ospf cost cost [1-65535]

Command-command Show
Melihat routing table
Router#show ip route

Melihat process ID,LSA authentication
Router# show ip ospf

Melihat cost,hello,dead interval,state, process ID
Router#show ip ospf interface interface

Melihat router tetangga secara OSPF
Router#show ip ospf neighbor

Melihat protocol
Router#show ip protocol

Command-command debug
Router#debug ip ospf events
Router#debug ip ospf adjacency

OSPF Authentication

Dengan MD5
Router(config-if)#ip ospf message-digest-key 1 md5 7 password
Router(config-if)#exit
Router(config)#router ospf process id
Router(config-router)#area 0 authentication message-digest
Router(config-router)#end

Dengan plain text
Router(config-if)#ip ospf authentication-key password
Router(config)#router ospf process id
Router(config-router)#area 0 authentication

Settingan untuk menyebarkan Loopback: (ip 180.10.10.1)

Router(config)#interface loopback 0
Router(config-if)#ip address 180.10.10.1 255.255.0.0
Router(config)#ip route 0.0.0.0 0.0.0.0 lo 0
Router(config)#router ospf 10
Router(config-router)#default-information originate

Pemilihan DR & BDR

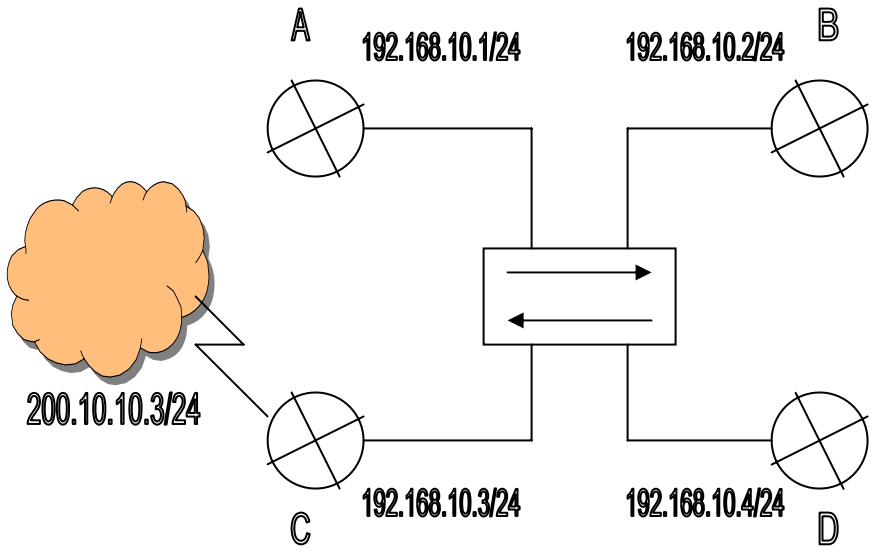
OSPF sifatnya fast confergence, pada broadcast&non broadcast multi access, terdapat pemilihan DR(designated Router) & BDR(Backup designated router) ini tidak berlaku bagi point to point link, missal serial to serial.

DR digunakan sebagai pusat penyebaran informasi bagi router-router lain., alamat multicast 224.0.0.5

Sedangkan BDR memiliki alamat 224.0.0.6 , BDR akan menjadi DR apabila DR down, Router-router lain yang bukan DR atau BDR akan bertindak sebagai DROTHER

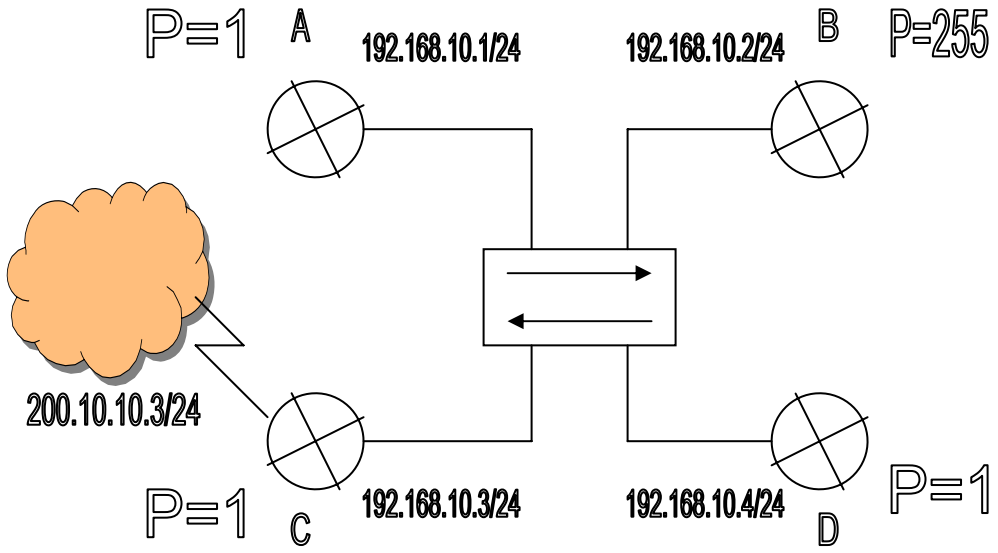
Penentuan DR,BDR dan DROTHER ditentukan oleh:

- **Router ID**
  Yang merupakan IP tertinggi pada interface router. IP tertinggi akan menjadi DR, router id ke dua tertinggi menjadi BDR dan sisanya DROTHER
- Pemberian **Loopback address** akan membuat router tsb mempunyai router id dari alamat loopback itu.



Ket: Router C skrng menjadi DR sebab router id nya menjadi 200.10.10.3/24 Router D menjadi BDR sebab memiliki router id 192.168.10.4, router A & B menjadi DROTHE

- **Router Priority**
  Default nilai router priority untuk semua router adalah 1, semakin tinggi nilai priority maka
  semakin besar kemungkinan untuk menjadi DR
- Apabila priority router sama maka yang digunakan untuk menentukan DR/BDR adalah **Router ID**



Ket: Router B akan menjadi DR sebab prioritas nya tertinggi yaitu 255, meski router id nya 192.160.10.2. Router C akan menjadi BDR sebab memiliki Router id tertinggi dari Loopback yaitu 200.10.10.3 dalam keadaan nilai priority yang sama dngan A & D, router A & D akan menjadi DROTHER

Urutan pemilihan:

Priority

↓

Router ID based on **Loopback**

↓

Router ID based on **Physical address**

CHAPTER 3
EIGRP

EIGRP mirip dengan IGRP sebagai Cisco Properietary routing protocol, tetapi lebih fast convergence & dapat menangani scability network.

- gabungan dari distance vektor & link state (tidak mengenal hop count)

Metric yang digunakan sama dengan IGRP namun dikali 256 sebab memakai metric 32 bit, sedangkan IGRP 24 bit.
Metric = BW + delay

BW → (10 ^ 7 / BW) x 256
Delay → (delay / 10) x 256
Komposisi metric seperti ini dinamakan composite metric. (path bandwidth value dan cumulative delay)

Perbandingan EIGRP dan IGRP terletak pada:

a. compability mode
b. hop count
c. route tagging
d. automatic protocol distribution

Route tagging
Penandaan route external yang dapat dilakukan EIGRP tapi tidak oleh IGRP.
Sama seperti IGRP, EIGRP juga memakai Autonomous System (AS) yang harus sama.

Table pada EIGRP:

a. topology table
b. neighbor table
c. routing table

Info pada topology & neighbor digunakan untuk menentukan jarak ke tujuan.

Proses convergence
Router-router EIGRP membentuk adjacency dengan router tetangga melalui hello & dead message, dilakukan multicast 224.0.0.10, router lain membalas dengan ACK secara unicast.
Bila tidak membalas maka route dinyatakan down, info ini disimpan pada neighbor & topology table.

Diffusing Update Algortihm (DUAL)
DUAL digunakan untuk menghitung jalur ke tujuan, istilah yang penting:

- feasible distance (fd)
- reported distance (rd)
- feasible successor (fs)
- successor (s)

Feasible distance → jarak ke tujuan yang dilihat dari sisi diri sendiri.
Reported distance → jarak ke tujuan yang dilihat dari sisi tetangga.

Pemilihan successor & feasible dilakukan berdasarkan feasible & reported distance.

Pententuan successor yaitu berdasarkan jalur yang feasible distancenya paling kecil ke tujuan.

Diffuse Update Algorithm (DUAL) pada EIGRP memiliki successor dan feasible successor ke network tujuan berdasarkan reported distance dan feasible distance.
Pada saat DUAL bekerja, status router EIGRP dalam keadaan aktif, bila route telah convergence, barulah berubah menjadi pasif kembali.

Proses lengkap pemilihan atau sampai convergence pada EIGRP:

a. hello message dikirim dengan 224.0.0.10
b. neighbor dan topology table didapatkan
c. info pada topology table (feasible dan reported distance) didapat lalu digunakan untuk menghitung successor dan feasible successor.
d. Perhitungan dilakukan oleh DUAL
e. Convergence didapatkan

Info yang terdapat pada topology table:

a. feasible distance
b. reported distance
c. route status
d. interface information
e. copyan dari successor

Successor yang asli disimpan dalam routing table yang menjadi metric terbaik ke destination network.

Info yang terdapat pada neighbor table:

a. neighbor address
b. hold time (berapa kali dikirim tidak menerima ACK)
c. SRTT (Smooth Rand Trip Time): waktu untuk hello packet bolak balik → send dan ACK
d. sequence number
e. queue count

Karakteristik EIGRP:

a. Efisien dalam bandwidth
b. Mendukung VLSM dan subnetting
c. Independent dalam routed protocol

Independent reouted protocol berarti protocol Dependent Module (PDM), routed protocol yang digunakan tidak hanya IP, tapi dapat juga IPX, dll.

EIGRP technologies:

a. Network discovery dan recovery
b. DUAL
c. Protocol Dependent Module (PDM)
d. Reliablity Transport Protocol (RTP)

EIGRP juga memiliki packet-packet sebagai berikut:

a. hello → saat membentuk koneksi awal → 224.0.0.10
b. ACK → balasan dari hello packet
c. update → untuk update
d. reply → balasan query packet
e. query → bila ada perubahan topology, query packet dikirim

EIGRP adalah hybrid routing protocol, yang memiliki sisi:

a. Distance Vector: maksimal top count 224 berbeda dengan IGRP yang maksimal top count 255
b. Link State: mengirim hello message dan punya topology table yang menggambarkan keseluruhan network.

Administrative Distance (AD) nya:

a. internal EIGRP: semua menjalankan EIGRP, ADnya 90
b. eksternal EIGRP: ada router yang tidak memakai IGRP, dikenali dengan route tagging, nilai AD route ini 170

Command-command EIGRP

a. Setting routing protocol:

Router(config)# router eigrp AS number
Router(config-router)# network network directly connected
Router(config-router)# no auto-summary
Rotuer(config-router)# eigrp log-neighbor-changes

b. Command show:

- Melihat routing table
Routing# show ip route
- Melihat routing protocol spesifik
Routing# show ip protocol
- Melihat neighbor eigrp:
Routing# show ip eigrp neighbor
- Melihat topology eigrp:
Routing# show eigrp topology

c. Command debug:

Router# debug eigrp fsm → melihat aktivitas FUAL
Router# eigrp packet

Manual summary pada EIGRP

Secara default EIGRP menjalakan auto summary, ini tidak baik bagi discontigous network → network yang disubnetting atau di VLSM tapi dipisahkan oleh network lain.

CHAPTER 4
Switching Concepts

Switching adalah proses meneruskan frame ke tujuan berdasarkan destination MAC address, ini yang dilakukan oleh Switch.

Switch adalah device layer 2, memisahkan collision domain, tapi tidak memisahkan broadcast domain.

Local Area Network itu sendiri terdiri dari 3 layer pada OSI model:

1. **Layer 1 :** repeater dan hub (tidak memisahkan collision domain, dan tidak memisahkan broadcast domain)
2. **Layer 2 :** switch dan bridge (memisahkan collision domain, dan tidak memisahkan broadcast domain)
3. **Layer 3 :** router (tidak memisahkan collision domain, dan memisahkan broadcast domain)

Memisahkan collision domain artinya melakukan microsegmentasi yang memberikan keuntungan yaitu dapat mengisolasi traffic dan meningkatkan bandwidth pada tiap host yang terhubung di port masing-masing switch.

Selain collision domain, faktor lain yang mempengaruhi perform network yaitu:

a.) multitasking :environment pada jaringan
b.) pemakaian aplikasi seperti browser yang melibatkan jaringan
c.) pengaturan client-server pada jaringan

Bentuk jaringan LAN yang umum yaitu ethernet, tujuan dan fungsi utamanya :

a.) best effort delivery ke tujuan
b.) memastikan semua hos jaringan dapat berbagi media yang sama

Ethernet mempunyai standard IEEE 802.3 yang memiliki kelemahan:

- shared media
- bila tidak dibantu device layer 2, tidak memisahkan collision domain

CSMA/ CD digunakan oleh ethernet untuk mengatasi collision pada collision domain yang sama, tapi sifatnya mendeteksi setelah collision domain terjadi pertama kalinya, bukan mencegahnya.

Faktor-faktor lainnya yaitu:

- penggunaan bandwidth yang besar untuk multimedia, graphic, file, dll
- latency pada jaringan

Latency atau delay adalah waktu yang diperlukan oleh frame dari source menuju destination, contohnya:

a.) **NIC delay :** berapa lama waktu sampai titik menerjemahkan data menjadi layer-layer data untuk dikirim oleh layer 1
b.) **Propagation delay :** waktu yang diperlukan dikur dari delay media misal UTP, dll
c.) **Network device delay :** delay yang dihasilkan network device

Perbandingan ketiga layer:

1.) Layer 1 :
Hub maupun repeater tidak melakukan microsegmentation berdasarkan apapun

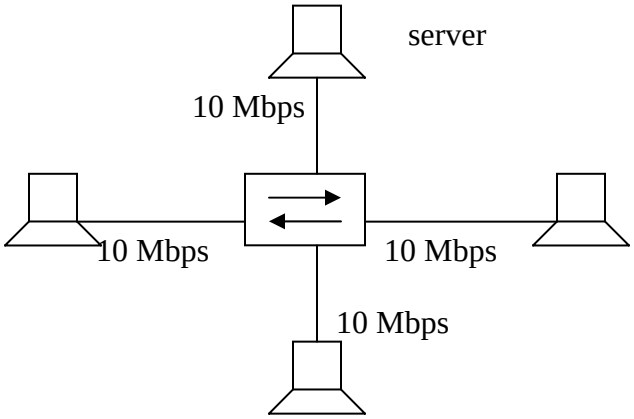
2.) Layer 2 :
Switch maupun bridge melakukan microsegmentation berdasarkan MAC address, dalam mengirim data ke tujuan

3.) Layer 3 :
Router mengirim data berdasarkan destination ip address, malekukan pemisahan broadcast dan collision domain

Switch terdiri dari dua jenis berdasarkan kesamaan bandwidth port-portnya:

a.) symetric switching
Switch yang semua portnya memiliki besar bandwidth yang sama misalnya bila 10 Mbps, maka semua port 10 Mbps

b.) asymetic swtiching
Switch yang port-portnya tidak memiliki bandwidth yang sama besar, ada beberapa port yang uplink atau lebih besar bandwidthnya, biasanya digunakan oleh konektivitas ke server



Berdasarkan sistem antrian data frame ke tujuan, witch juga dibedakan menjadi dua:

a.) port-based memory buffer
Pada saat melakukan antrian di dalam switch, maka frame dimasukkan dalam incoming port yang spesifik barulah diforward ke tujuannya. Penyimpanan dilakukan pada port

b.) shared memory buffer

Frame tidak disimpan dalam incoming port yang spesifik, tapi disimpan dalam memory switch. Besar frame data yang disimpan dipengruhi oleh besarnya memory pada switch.

Kedua sistem penyimpanan dilakukan saat destination sibuk atau ada frame yang belum sampai ke tujuannya sehingga pengiriman berikut ke tujuan yang sama harus mengantri dibelakangnya.

Tujuan dari microsegmentation:

a.) mengisolasi traffisc pada network
b.) meningkatkan bandwidth

Tambahan

Bila CAM table pada switch telah lengkap maka switch setelah membentuk Virtual Circuit (VC) yang artinya dapat langsung memforward frame ke tujuan dengan membuat jalur khusus (dari MAC address dalam hal ini)

CHAPTER 5
Switches

Pedoman dalam membangun LAN :

a) Functionality : Harus mampu memenuhi kebutuhan user
b) Manageability : Harus dapat di manage
c) Scalability : Dapat dikembangkan
d) Adaptability : Mampu beradaptasi dengan teknologi baru.

Macam-macam server :

a) Enterprise Server :
Server Seperti Domain Name System (DNS) & memainkan peranan penting bagi jaringan.

b) Workgroup Server :
Server seperti file server & sifatnya tidak krusial bagi jaringan hanya pelengkap saja.

Enterprise server sebaiknya diletakkan pada Main Distribution Facilities (MDF), sedangkan Workgroup Server diletakkan pada Intermediate Distribution Facilities (IDF)

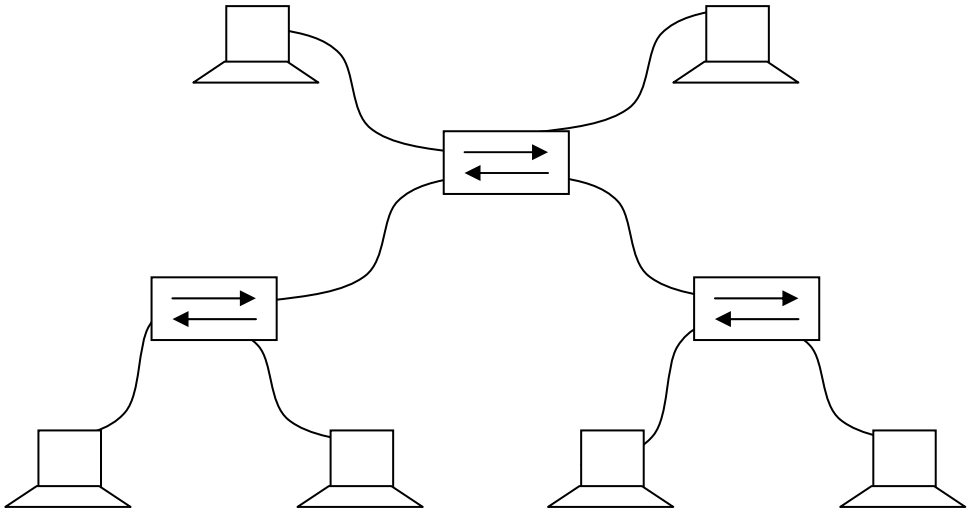
Istilah-istilah lain :

a) Horizontal Cross Connect (HCC) :
Disebut juga horizontal cabling, berfungsi menghubugnkan host pada MDF maupun host pada IDF. Biasanya menggunakan UTP cable dan maksimal 100m.

b) Vertical Cross Connect (VCC) :
Disebut juga vertical cabling, berfungsi menghubungkan MDF & IDF biasanya memakai fiber optic.

c) Main Distribution Facilities (MDF) :
Ruang yang digunakan untuk menyimpan enterprise server, merupakan tempat penyimpanan utama.

d) Intermediate Distribution Facilities (IDF) :
Ruang penyimpanan tambahan untuk menyimpan workgroup server.



Verical Cabling dengan fiber optic menghubungkan MDF dengan IDF, sedangkan antar MDF maupun antar IDF dihubungkan dengan Horizontal Cabling.

Switching mengenal hierachical layer yaitu :

a) Access Layer
b) Distribution Layer
c) Core Layer

Masing-masing layer mempunyai fungsi tersendiri.

Access Layer

Layer yang berkaitan dengan akses ke network resources, direpresentasikan dengan penggunaan hub atau switch.
Hub untuk shared network, sedangkan switc dapat melakukan Microsegmentation.
Contoh alat :

- Catalyst 2900
- Catalyst 2950

Distribution Layer

Layer ini berkaitan dengan security, pembagian broadcast domain, dan VLAN routing, VLAN routing adalah pengelompokan network secara logical.
Contoh alat :

- Catalist 4000
- Catalist 5000
- Catalist 2926

Core Layer

Core layer berkaitan dengan high-speed connection dan tidak ada paket manipulation pada layer ini.
Contoh alat :

- Switch tipe 5000 & 6000
- IGX
- Lightstream

Chapter 6
Switch Configuration

Switch tidak menggunakan shared network, tapi tiap port memiliki dedicated bandwith sendiri, dengan dedicated bandwith menyebabkan Switch lebih cepat dalam speed dibandingkan dengan Hub.

Sistem lampu led (indikator)pada switch berdasarkan mode dibedakan atas:
a. STAT :

- Solid green : link operational
- Flashing green : mengirim data
- Alternated green/amber : link fault
- Solid amber : port di blok oleh STP

b.UTL:

- Off : Penggunaan bandwith, bila lampu mati 1 dari sebelah kanan, maka bandwith ber kurang 50%. Jika lampu mati 2 dari sebelah kanan maka bandwith berkurang 25%

- Green : Jika semua lampu menyala hijau , switch menggunakan 50% atau lebih dari total bandwith

c.FDUP:

- Off : mode half duplex
- Green : mode full duplex.

d.100

- Off : speed 10 Mbps aktif
- Green : speed 100 Mbps aktif

Command-command Setting Switch:
Seting password console
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login

Seting password telnet
Switch(config)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login

Seting password previledge
Switch(config)#enable password password
atau dengan enskripsi
Switch(config)#enable secret password
Pass word yang diambil yaitu password enable secret

Urutan langkah sebelum mereload switch:
Hapus info Vlan ;
Switch# delete flash : vlan.dat
Switch#erase startup configuration
Switch#reload

Switch menyimpan MAC Address dalam CAM table, untuk melihatnya
Switch# show mac-address-table

Syarat agar switch dapat di telnet/ping yaitu: harus dipasang IP address atau IP default gateway, caranya:
Switch (config)#interface vlan1
Switch(config-if)#ip address ip subnetmask
Switch(config-if)#no shut

Pasang default gateway
Switch(config)#ip default-gateway ip

Setting hostname
Switch(config)#hostname name

Mac address terbagi atas 3 jenis:
a. Static MAC
diseting manual pada port tertentu di switch, MAC ini tidak akan di remote oleh switch.
Cara setingnya:
Switch(config)mac-address-table static mac add interface int vlan1

Cara melihatnya:
Switch#show mac-address-table static

b.Dynamic MAC
Mac yang dimiliki oleh host yang dicolokan ke switch, dapat dilihat dengan:
Switch#show mac-address-table dynamic

c.Secure MAC
Mac yang dipasang pada port security, bila dideteksi ada Mac lain yang dipasang pada port Ini maka akan terkena violation, missal di shutdown.

Port Security
Sistem security pada port di switch, bila aturan ini dilanggar akan terkena violation,
Cara setingnya:
Switch(config)# interface int
Switch(config-if)#switch port mode access
Switch(config-if)#switch port port-security
Switch(config-if)#switch port port-security maximum max

Switch(config-if)#switch port port-security mac address mac add
Switch(config-if)#switch port port-security violation violation

Contoh penerapan:
Switch(config-if)#switch port port-security maximum 5
Switch(config-if)#switch port port-security mac address d5ef.1240.abcd
Switch(config-if)#switch port port-security violation shutdown

Bila pada port tersebut di hubungkan ke switch lain yang memiliki 5 port lebih terhubung host, maka port akan shutdown.
Port shutdown juga bila MAC address yang di hubungkan bukan d5ef.1240.abcd.
Ini yang disebut sebagai MAC address secure
Cara melihat port security:
Switch#show port-security

Command-command show lainnya:
Melihat setingan secara global
Switch#show running-config
Melihat isi nvram
Switch#show startup-config
Melihat keterangan interface
Swith#show interface interface

Untuk mengganti IOS Switch
Switch# erase flash (seluruh file pada switch akan dihapus)
Switch# archive tar/xtract tftp// 10.21.22.200/namafile.tar

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 (masuk ke Rommon mode)
4. ketik : flash_init (untuk inisialisasi flash)
5. ketik : dir_flash (untuk melihat isi file)
6. ketik: rename flash: config.text flash: config.old
7. ketik: boot
8. masuk ke switch seperti biasa dan jawab 'NO' pada setiap mode
9. masuk ke privileged mode
   Switch#rename flash: config.old flash: config.text
10. lakukan :
    Switch#copy flash: config.text system: running-config
11. ganti password (secret, enable, telnet)
12. copy run start

Setingan agar switch dapat di HTTP:
Switch(config)#ip http server
Switch(config)#ip http port 80

CHAPTER 7
Spanning-Tree Protocol

Pemasangan redundant link pada switch ke switch lain dapat meningkatkan fault tolerance, namun disisi lain, hal ini dapat menyebabkan terjadinya broadcast storm STP memblok port-port yang dapat menyebabkan broadcast storm, multiple frame transmission & MAC address database inconstancy.

Broadcast storm disebabkan oleh pengiriman frame yang berulang-ulang pada device layer 2, dalam hal ini switch. Device layer 2 tidak mempunya time to live (TTL) seperti device layer 3. Sehingga frame yang berulang-ulang tidak di discard.

Spanning tree protocol (STP) mempunyai standart IEEE 802.1d dapat mengatasi masalah ini. STP aktif secara default pada setiap switch cisco. STP memblok port-port yang dapat menyebabkan broadcast storm.

Pemilihan root bridge menjadi acuan dalam konsep ini, root bridge adalah switch yang memilih MAC address yang paling rendah dalam topologi.

Switch mengirim bridge protocol data unit (BPDU) setiap 2 detik untuk menginformasikan tentang bridge ID (BID) BID berisi MAC Address & priority, priority lebih diutamakan dibandign MAC address, defaultnya 32768.

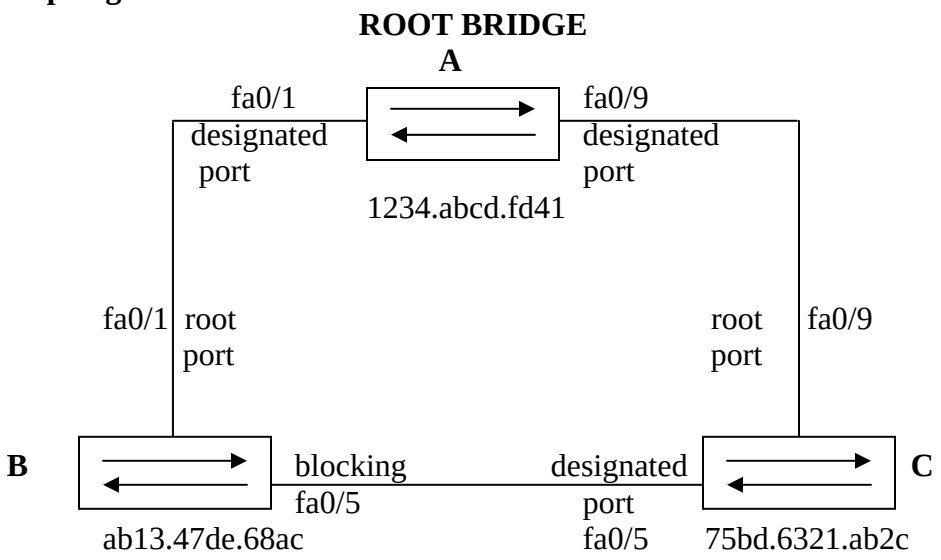
Saat switch dinyalakan proses :

- **Blocking** : tidak ada port yang dapat mengirim data, berlangsung selama 20 detik.
- **Listening** : Mencari path ke root bridge, belum mempelajari MAC address & belum memforward data, berlangsung selama 15 detik.
- **Learning** : Mempelajari MAC address, tapi belum memforward data, berlangsung selama 15 detik.

  Total keadaan ini dinamakan forward delay.

- **Forward :** data telah dapat diforward, keadaan dimana topologi, switch telah selesai dipelajari.
- **Disable :** port yang tidak diijinkan mengirim data, tidak aktif karena spanning-tree protocol (STP).

Contoh topologi :



Priority yang digunakan secara default yaitu 32768 sehingga MAC address yang paling rendah digunakan dalam penentuan root bridge.
Port fa0/5 pada switch B akan diblok untuk menghindari redundant link yang menyebabkan broadcast storm.

Istilah-istilah penting :

a) **Bridge ID (BID) :** dikirimkan dalam BPDU, isinya adalah MAC address dan priority, BID terendah lah yang diambil.
b) **Bridge Protocol Data Unit (BPDU) :** dikirimkan oleh switch tiap 2 detik, isinya adalah BID.
c) **Designated port :** Port yang sifatnya forwarding, dapat mengirimkan data.
d) **Blocking port :** Port yang diblok oleh spanning-tree protocol.
e) **Root port :** Port pada non-root bridge yang tepat langsung mengarah ke root bridge, sifatnya selalu forwarding.
f) **Root bridge :** Switch pada topologi yang menjadi acuan dalam menentukan suatu port lain, dipilih berdasarkan BID yang terendah.
g) **Non-root bridge :** Switch yang BID-nya bukan yang terendah, non-root bridge yang BID-nya paling tinggi, salah satu portnya akan diblok.

Command-command Spanning-tree :

a) Mematikan spanning-tree :
Switch(config)#no spanning-tree vlan 1
b) Mengganti priority :
Switch(config)#spanning-tree vlan 1 priority priority
c) Melihat spanning-tree :
Switch#show spanning-tree
d) Melihat MAC address switch :
Switch#show interface vlan 1

NB : perhatikan not bridge, priority, status port pada swicth, MAC address.

CHAPTER 8
Virtual LAN

Virtual LAN (VLAN) merupakan pengelompokan jaringan yang tidak tergantung dari lokasi fisik, pengelompokan dilakuakn secara logikal.

Biasanya dibagi berdasarkan fungsionalitas atau department tertentu misalnya :

a.) vlan untuk finance
b.) vlan untuk HRD
c.) vlan untuk marketing
dan sebagainya.

Setiap vlan adalah broadcast domainnya masing-masing dan antar vlan yang berbeda tidak dapat saling berhubungan kecuali menggunakan router.

Penghubung vlan yang berbeda dengan menggunakan router disebut inter-vlan routing.
Switch memiliki tabel-tabel yang terpisah untuk tiap vlan dan informasi vlan disimpan pada vlan database dalam bentuk vlan.dat.

Jenis-jenis vlan:

a.) static vlan
dikonfigurasi manual pada switch dengan perintah-perintah kemudian diassign ke dalam port.

b.) dynamic vlan
dikonfigurasi dengan menggunakan software, misalnya Ciscoworks for Switched Internetwork

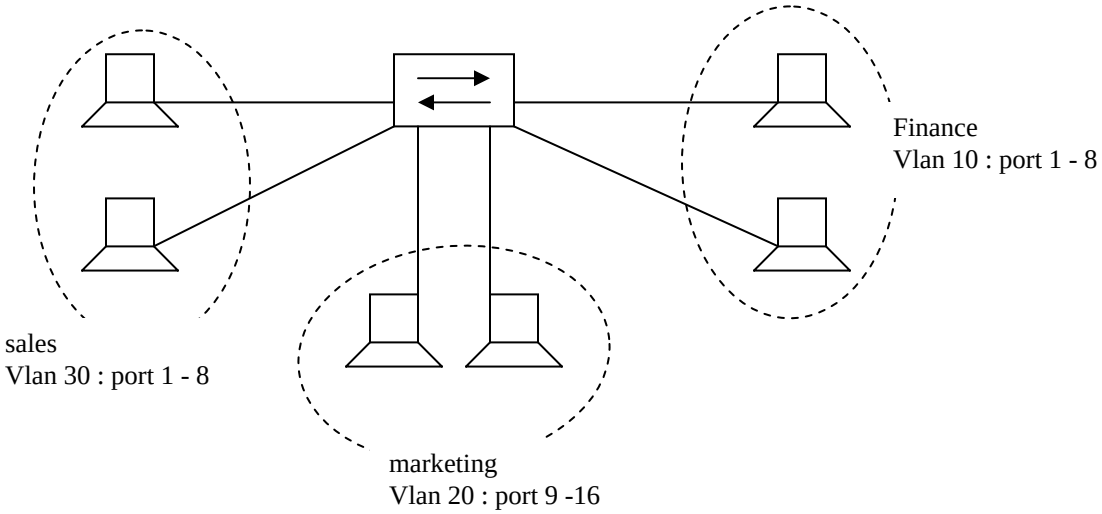
Selain static dan dynamic, vlan juga dapat diassign berdasrkan port, MAC address, atau subnet (jaringan).

Assigning Based on Port
Menciptakan vlan kemudian memasukan port-port ke dalam masing-masing vlan.

Assigning Based on MAC address
Pengelompokan MAC address tertentu dimasukkan ke vlan tertentu, contoh:
Vlan 2 untuk MAC:
ff 3d : 4321 : abcd
cef4 : 5967 : 128

Assigning Based on Subnet
Pengelompokan berdasarkan subnet, subnet tertentu dimasukkan dalam vlan tertentu.
Contoh:
192.168.10.0/24 ke vlan 3
192.168.30.0/24 ke vlan 10
dan sebagainya

VLAN yang paling umum digunakan adalah vlan assigning based on port.
Biasanya dibuat per fungsionalitas, contoh:



Frame tagging digunakan oleh switch dalam mengenali suatu frame milk vlan berapa, farem tagging yang utama ada 2 yaitu:

a.) **Inter Switch Link (ISL):**
Proprietary cisco, menambahkan header pada frame dimana pada header terdapat vlan id.

b.) **IEEE 802.1q :**
Open standard, memodifikasi header frame agar dapat dikenali milik vlan berapa

Satu lagi frame tagging yaitu LANE (LAN Emulator), tapi jarang digunakan.
Biasanya ISL pada switch-swtich cisco lama, switch terbaru mengikuti open standard (IEEE 802.1q)

Keuntungan-keuntungan menggunakan vlan:

a.) mudah menambah host
b.) mudah mengurangi host
c.) security

Command-command dalam membuat vlan
Membuat vlan:
Switch#vlan database
Switch(vlan)#vlan number name name
Switch(vlan)#exit

Pada akhir pembuatan vlan ada 3 perintah yang dapat digunnakan:

- exit : apply + exit
- apply : apply without exit
- abort : exit without apply

contoh:
Switch#vlan database
Switch(vlan)#vlan 10 name finance
Switch(vlan)#vlan 20 name marketing
Switch(vlan)#exit

Memasukkan port pada switch ke dalam vlan :
Switch(config)#interface interface number
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan vlan number

Contoh:
Switch(config)# interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

Secara default, semua port dalam switch adalah vlan 1 (default administrative vlan).
Selain satu per satu, dapat juga memasukkan vlan dalam port sekaligus banyak dengan:
Switch(config)#interface range interface number – number

Contoh:
Switch(config)#interface range fa0/5 – 10

Command-command show

a.) **Melihat vlan(complete)**
switch#show vlan
b.) **Melihat ringkasan info vlan**
switch#show vlan brief
c.) **Melihat vlan berdasarkan nomor vlan**
switch#show vlan id number
d.) **Melihat vlan berdasarkan nama vlan**
switch#show vlan name name
e.) **Menghapus semua vlan**
switch#delete flash:vlan.dat

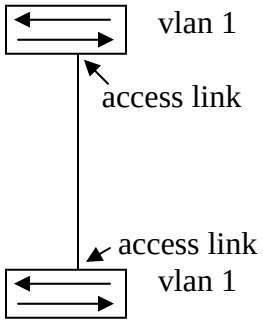
CHAPTER 9
VLAN Trunking Protocol

VLAN Trunking Protocol menggunakan frame tagged untuk menandai suatu frame milik VLAN berapa.

Pada dasarnya trunking mengijinkan komunikasi antar VLAN yang sama pada switch-switch yang berbeda.

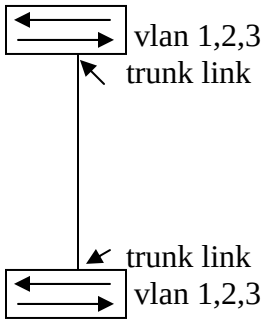
Perbedaan stocking dengan trunking

Stocking : Penghubung antar switch yang berbeda dimana hanya terdapat satu VLAN pada switch-switch tersebut.



Misalnya dua switch dihubungkan dimana switch-switch itu hanya memiliki satu VLAN, yaitu VLAN, secara default.

Trunking : penghubung antar switch yang berbeda dimana terdapat lebih dari satu VLAN pada switch-switch tersebut.



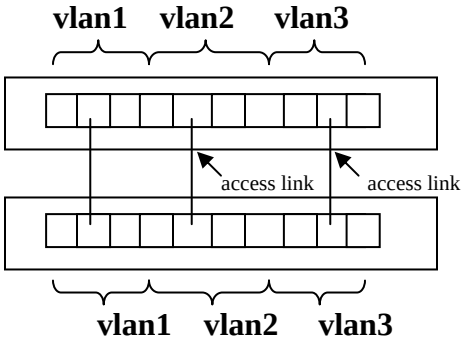
Stocking menggunakan access link sebagai penghubung, sedangkan trunking memakai trunk link.

Secara default, semua port pada switch adalah access link.
Access link : hanya dapat mengirim frame pada VLAN yang sama antar switch, untuk satu VLAN.

Trunk link : dapat mengirim frame yang ditujukan untuk VLAN yang sama antar switch, bila terdapat beberapa VLAN pada switch-switch itu.
Untuk menghubungkan VLAN yang berbeda tetap harus memakai inter VLAN Routing.

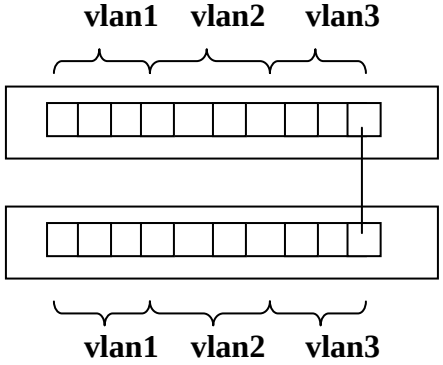
<u>Perbedaan lainnya antara stocking dan trunking</u>
Contoh :

a) **Stocking :**



bisa terdapat beberapa VLAN, namun harus dihubungkan satu per satu VLAN yang ada.

b) **Trunking :**



Dari gambar, terlihat bahwa satu kabel, trunk link dapat membawa info banyak VLAN sekaligus.

VTP digunakan dalam mengontrol VLAN dan mengelompokkan banyak VLAN ke dalam network.

VTP dan VLAN adalah layer 2 OSI (data link).

Frame tangging juga digunakan dalam VTP, ada 2 yang utama :

a) **Interswitch-Link (ISL)**
   Proprietory Cisco, memodifikasi header untuk menandai keanggotaan suatu VLAN.

b) IEEE 802.1q

Open standard, menambahkan tangged berupa VLAN ID untuk menandai keanggotaan VLAN.

Keduanya untuk ethernet dan fast ethernet.
Selain ISL dan IEEE 801.1q, terdapat pula 802.10 untuk FDDI dan LANE untuk ATM.

Fungsi utama VTP yaitu menyederhanakan pembuatan VLAN pada banyak switch. Pada VTP, ada yang bertindak sebagai server, transparant, maupun client.

VTP Server

Dapat create, add, dan delete VLAN, kemudian mengirim informasi VLAN keluar dari trunk port.

VLAN Transparant

Tidak menyimpan informasi VLAN pada NVRAM, hanya meneruskan info VLAN yang diterima dari VTP server ke VTP client.

VTP Client

Menerima dan menyimpan informasi VLAN pada NVRAM, info VLAN disimpan pada NVRAM tersebut berasal dari server.

VTP server, transparant, dan client harus berada dalam domain yang sama dan memiliki password yang sama.

Langkah pemilihan VTP server, transparant, dan client, dilakukan berdasarkan configuration revision number yang saat switch dihidupkan makan bertambah jumlahnya mulai dari 0 sampai 2.147.483.648, walaupun sudah disetting ke mode VTP client, switch harus di reload dulu agar revision number kembali ke 0 sebab angka yang tinggi akan menimpa angka yang lebih rendah. Angka lebih tinggi akan menjadi VTP server.

Pengiriman info dari VTP server ke VTP client melibatkan VTP message berikut :

a) Advertisement Request
b) Summary advertisement
c) Subset advertisement

Advertisement Request

Info request VLAN yang dikirim oleh VTP client pada VTP server.

Summary Advertisement

Digunakan pada saat switch dinyalakan pertama kali untuk menentukan siapa switch yang menjadi VTP server, dikirim setiap 5 menit sekali. Isinya terdapat configuration revision number dimana angka tertinggi akan menimpa angka yang lebih rendah, angka tertinggi akan menjadi server.

Subset Advertisement

Info tentang VLAN yang dikirimkan oleh VTP server kepada VTP client.

Ketiga VTP Message itu dikirimkan keluar melalui trunk port.

Command-command VTP :

Menyetting domain, mode, dan password VTP :

Switch#vlan database
Switch(vlan)#vtp domain name
Switch(vlan)#vtp mode
Switch(vlan)#vtp password password

Mengubah access link port ke trunk link port :

Switch(config)#interface interface number
Switch(config-if)#switchport mode trunk

Perintah show :

a) **Melihat domain dan mode vtp :**
   Switch#show vtp start

b) **Melihat password vtp :**
   Switch#show vtp password

c) **Melihat advertisement request, summary advertisement, subnet advertisement :**
   Switch#show vtp counter

d) **Melihat port yang di trunk :**
   Switch#sshow interface trunk

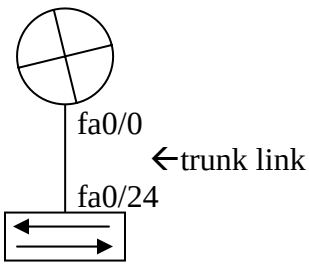
InterVLAN Routing

Konsep interVLAN Routing yaitu menghubungkan VLAN yang berbeda dengan router. Default gateaway tiap VLAN disetting pada router, sering disebut juga "Router on a stick". Command untuk default gateaway tiap VLAN dipasang ke dalam subinterface.

Settingan Command

Router(config)#interface interface number
Router(config-if)#no shutdown
Router(config-if)#interface interface number sub interface
Router(config-subif)#encapsulation dot1q vlan id
Router(config-subif)#ip address ip subnetwork
Router(config-subif)#no shutdown
Contoh :

vlan 1 : port 1-8
vlan 2 : port 9-16
vlan 3 : port 17-23



Pada switch, terdapat :
Vlan 1 192.168.10.0/27, Default Gateaway : 192.168.10.1
Vlan 2 192.168.10.32/27, Default Gateaway : 192.168.10.33
Vlan 3 192.168.10.64/27, Deafult Gateawat : 192.168.10.65

Pada Router, Setting :
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.10.1 255.255.255.224
Router(config-subif)#no shutdown

Router(config-if)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.33 255.255.255.224
Router(config-subif)#no shutdown

Router(config-if)#interface fa0/0.3
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.10.65 255.255.255.224
Router(config-subif)#no shutdown

Pada switch, port fa0/24 setting :
Router(config)#int fa0/24
Router(config-if)#switchport mode trunk

VLAN yang berbeda dapat saling berhubungan, misal host pada vlan 1 dapat connect dengan host pada vlan 10.