**Perancangan Jaringan Cisco Switch**

Implementasi dari perangkat share ke perangkat switch mengalami evolusi selama beberapa tahun. Perancang jaringan awalnya mempunyai keterbatasan dalam pemilihan perangkat untuk membangun sebuah jaringan kampus atau jaringan antar LAN. Pesatnya perkembangan PC dan kebutuhan aplikasi klien-server membutuhkan pipa jaringan yang lebar dan cepat, terutama untuk aplikasi multimedia. Pemenuhan kebutuhan ini berevolusi dari pemakaian perangkat *share-hub* ke switch.



Gambar di atas menunjukkan sebuah strategi untuk mempertahankan infrastruktur kabel dengan pemakaian perangkat yang baru. Bermula dari pemakaian hub, digantikan dengan switch layer 2, switch layer 3, ATM, CDDI (Copper Data Distributed Interface) dan FDDI (Fiber Data Distributed Interface). Strategi dasar perancangan jaringan switch meliputi:

**Switch LAN**

Switch LAN adalah perangkat yang secara tipikal mempunyai beberapa port yang menghubungkan beberapa segmen LAN lain dan port pada switch ini berkecepatan tinggi (kita kenal 100Mbps untuk Ethernet, FDDI dan 155Mbps pada ATM). Sebuah switch mempunyai bandwidth yang dedicated untuk setiap portnya. Untuk kinerja yang tinggi biasanya satu port dipasang untuk satu workstation PC. Contoh sederhana seperti terlihat di gambar.



Ketika switch mulai bekerja maka pada saat yang sama setiap workstation memulai request data ke workstation lain (atau server), setiap request yang diterima ditampung oleh switch dan memfilter MAC address dan port yang tersambung dari masing-masing workstation, lalu disusun ke dalam sebuah tabel. Switch pada saat ini rata-rata mampu menampung tabel MAC address sebanyak 8000.

Ketika host A pada port 1 akan melakukan transfer data ke host B di port 2 switch akan mem-forward bingkai paket dari port 1 ke port 2. Pada saat yang bersamaan host C melakukan transmisi data ke host D maka komunikasi masing-masing tidak akan saling terganggu sebab switch telah menyediakan jalur logik dan fisik secara dedicated.
Ketika perangkat yang terhubung ke switch akan melakukan transmisi data ke sebuah host yang tidak termasuk dalam tabel MAC di atas maka switch akan mengalihkan bingkai data tersebut ke seluruh port dan tidak termasuk port asal data tersebut. Teknik ini disebut dengan *flooding*. Implementasi switch atau beberapa switch jika tanpa pertimbangan dan perancangan bisa menyebabkan jaringan lumpuh karena flooding ini (bayangkan jika flooding ini terjadi di share-hub).

Dalam jaringan TCP/IP setiap workstation juga mempunyai tabel MAC address, tabel ini biasa disebut dengan ARP (Address Resolution Protocol). Tabel ini disusun sebagai pasangan MAC address dengan IP address. Dengan tersambungnya workstation tersebut ke switch, pada saat workstation membroadcast ARP/NetBIOS untuk mencari pasangan MAC address dan IP address workstation lain akan dihadang oleh switch. Kondisi seperti ini menyebabkan nama workstation tidak bisa langsung tampil dalam jaringan Samba atau Windows. Solusi masalah fisik ini ditanggulangi dengan implementasi WINS server, setiap workstation mendaftarkan dirinya langsung ke WINS server dan WINS server akan menjawab setiap query dari broadcast ARP/NetBIOS.

**Virtual LAN**

Sebuah Virtual LAN atau dikenal sebagai VLAN merupakan fungsi logik dari sebuah switch. Fungsi logik ini mampu membagi jaringan LAN ke dalam beberapa jaringan virtual. Jaringan virtual ini tersambung ke dalam perangkat fisik yang sama. Implementasi VLAN dalam jaringan memudahkan seorang administrator jaringan dalam membagi secara logik group-group workstation secara fungsional dan tidak dibatasi oleh batasan lokasi. Generasi pertama VLAN berbasis dari OSI Layer 2 (MAC address) dengan mekanisme bridging dan multiplexing.
Implementasi umum VLAN bisa kita deskripsikan dalam gambar berikut:



Ethernet 10Mbps tersambung ke masing-masing switch A, B, C dan D di tiap-tiap lantai, keempat switch ini tersambung ke sebuah Fast-Ethernet switch E 100Mbps. Dari gambar tersebut bisa kita lihat ada dua VLAN yaitu VLAN 10 dan VLAN 20. Masing-masing VLAN mempunyai jalur yang dedicated antar workstationnya, jalur ini sering disebut sebagai sebuah broadcast domain. Selain secara fisik switch membatasi broadcast data, manajemen VLAN akan membatasi lagi broadcast ini sehingga VLAN 10 dan VLAN 20 sama sekali tidak ada komunikasi langsung.
Implementasi VLAN biasanya digabungkan dengan teknologi routing yang bekerja di lapisan ketiga OSI (lapisan network). Dalam jaringan TCP/IP masing-masing VLAN membutuhkan sebuah gateway (gateway dalam artian logik) untuk bisa berkomunikasi dengan VLAN lainnya.

**Kampus LAN**

Sebuah jaringan yang terdiri dari beberapa segmen dan menggunakan perangkat switch sering disebut sebagai Campus LAN. Selain teknologi switching yang mengendalikan jalur data juga diterapkan teknologi routing untuk mewadahi kebutuhan komunikasi antar VLAN. Kombinasi dua teknologi ini memberikan kelebihan jaringan berupa:

* Jalur data yang dedicated sebagai backbone kecepatan tinggi
* Implementasi VLAN bagi workgroup yang terpisah secara lokasi yang berjauhan
* Teknologi routing antar VLAN untuk komunikasi karena batasan VLAN itu sendiri selain juga sebagai penerapan jaringan TCP/IP untuk bergabung ke network yang lebih besar, internet.

Implementasi firewall pada teknologi routing (berbasis TCP/IP). Implementasi fisik dalam satu Campus LAN didasarkan atas kondisi fisik yang ada, apakah memungkinkan dengan kabel UTP/STP, atau kabel telepon secara *back-to-back* atau harus dengan kabel serat optik.



**Pertimbangan Perancangan dan Implementasi**

Ada beberapa pertimbangan dalam perancangan jaringan dengan penggunaan teknologi switching yaitu perbandingan switch LAN dengan router, kelebihan switch LAN, kelebihan router, dan beberapa prinsip perancangan switch dan VLAN.

**Perbandingan Switch LAN dengan Router**

Perbedaan mendasar switch dan router adalah prinsip kerjanya yang berbeda dilihat dari referensi lapisan OSI. Perbedaan ini menghasilkan cara yang berbeda dalam mengatur lalu lintas jaringan.

* + **Loops**, penggunaan beberapa switch dalam satu jaringan memungkinkan terjadinya loop pada komunikasi antar host/workstation. Switch mempunyai teknologi algoritma *Spanning Tree Protocol* (STP) untuk mencegah loop data seperti ini. Jika dibandingkan dengan router, router menyediakan komunikasi yang bebas loop dengan jalur yang optimal.
	+ **Convergence**, dalam switch yang transparan bisa terjadi jalur data secara switching lebih panjang jika dibandingkan dengan penggunaan router. Protokol routing seperti OSPF (*Open Shortest Path First*) menyediakan komunikasi routing data berdasarkan jalur data terdekat.
	+ **Broadcast**, switch LAN tidak memfilter data *broadcast* dan *multicast* karena switch beroperasi pada lapisan 2 sedangkan broadcast/multicast adalah paket data di lapisan 3, broadcast yang berlebihan bisa menyebabkan kondisi yang disebut *broadcast-storm*. Pada router broadcast dan multicast tidak diforward dan bisa difilter.
	+ **Subnet**, switch dan router mempunyai perbedaan mendasar dalam mengurangi broadcast domain, secara fisik kita bisa merancang segmentasi LAN, dalam teknologi routing perbedaan subnet tidak dibatasi secara fisik harus dalam switch yang sama.
	+ **Security**, kombinasi switch dan router mampu meningkatkan keamanan secara protokol masing-masing. Switch bisa memfilter header paket data berdasarkan MAC address dan router selain memfilter di lapisan 3 network juga mampu memfilter berdasarkan MAC address.
	+ **Media-**Dependence, dua faktor yang harus dipertimbangkan dalam perancangan jaringan heterogen (*mixed-media*), yang pertama adalah faktor *Maximum Transfer Unit* (MTU), tiap topologi mempunyai MTU yang berbeda. Yang kedua adalah proses translasi paket karena perbedaan media di atas. Switch secara transparan akan menerjemahkan paket yang berbeda supaya tetap saling berkomunikasi. Pada router terjadi secara independen karena router bekerja di lapisan network, bukan lapisan data-link.

**Kelebihan Switch**

* + Switch dan Switch VLAN sama-sama bekerja di lapisan kedua lapisan OSI. Implementasi teknologi pada lapisan ini memberikan tiga kelebihan utama:
	+ Bandwidth, switch LAN memberikan bandwidth yang dedicated untuk setiap dan antar portnya. Jika masing-masing port tersambung ke switch lagi atau share-hub maka tiap segmen tersebut mendapat alokasi bandwidth yang sama (contohnya adalah gambar implementasi VLAN di atas). Teknik ini biasa disebut dengan segmentasi mikro (microsegmenting).
	+ **VLAN**, switch VLAN mampu membagi grup port secara fisik menjadi beberapa segmen LAN secara logik, masing-masing broadcast domain yang terjadi tidak akan saling mengganggu antar VLAN. VLAN ini sering juga disebut sebagai switched domains atau autonomous switching domains. Komunikasi antar VLAN membutuhkan router (berfungsi sebagai gateway masing-masing VLAN).
	+ **Otomatisasi** pengenalan dan penerjemahan paket, salah satu teknologi yang dikembangkan oleh Cisco adalah Automatic Paket Recognition and Translation (APaRT) yang berfungsi untuk menyediakan transparansi antara Ethernet dengan CDDI/FDDI.

**Kelebihan Router**

* + **Broadcast/Multicast Control**, router mampu mengendalikan broadcast dan multicast dengan tiga cara yaitu dengan meng-cache alamat host, meng-cache layanan *network-advertise* dan menyediakan protokol khusus seperti *Internet Group Message Protocol* (IGMP) yang biasa dipakai dalam jaringan *Multicast Backbone.*
	+ **Broadcast Segmentation**, untuk mencegah broadcast router juga bertanggungjawab dengan cara yang berlainan tergantung protokol yang dipakai misalnya dalam TCP/IP menggunakan proxy ARP dan protokol *Internet Control Message Protocol* (ICMP).
	+ **Media Transition**, dalam jaringan heterogen router mampu menerjemahkan paket ke dalam media yang berbeda, dalam kondisi ini paket data di-fragmentasi oleh router karena perbedaan MTU.

**Kelebihan VLAN**

Isu utama implementasi VLAN dibandingkan jaringan hub/flat adalah scalability terhadap topologi jaringan dan penyederhanaan manajemen. Kelebihan yang ditawarkan pada VLAN adalah:

* + **Broadcast control**, layaknya switch biasa membatasai broadcast domain VLAN mampu membatasi broadcast dari masing-masing grup-grup VLAN, antar VLAN tidak terjadi broadcast silang.
	+ Security, meskipun secara fisik berada dalam switch yang sama VLAN membentengi sebuah grup dari VLAN lain atau dari akses luar jaringan, selain itu implementasi firewall di routernya bisa dipasang juga.
	+ **Performance**, pengelompokkan secara grup logik ini memberikan jalur data yang dedicated untuk setiap grup, otomatis masing-masing grup mendapat kinerja jalur data yang maksimum.
	+ **Management**, prinsip logik pada VLAN memberikan kemudahan secara manajemen, seorang user dari satu grup VLAN yang berpindah lokasi tidak perlu lagi mengganti koneksi/sambungan ke switch, administrator cukup mengubah anggota grup VLAN tersebut (port baru masuk grup VLAN dan port lama dikeluarkan dari grup VLAN).

**Implementasi VLAN**

Implementasi VLAN pada sebuah switch bisa dibedakan atas:

* + - **port**, cara ini mengatur agar setiap port hanya mendukung satu VLAN, workstation dalam **VLAN** yang sama memperoleh sambungan *switched* dan komunikasi antar VLAN harus *routed*melalui perangkat khusus router atau internal switch itu sendiri jika mendukung teknologi routing (perangkat ini sering disebut sebagai Switch Layer 3). Cara seperti ini sering disebut sebagai *segment-based VLAN*.
		- **protokol**, VLAN berdasarkan alamat network (OSI lapisan ketiga) memungkinkan topologi virtual untuk setiap protokol, dengan setiap protokol mempunyai rule, firewall dll. Routing antar VLAN akan terjadi secara otomatis tanpa tambahan perangkat router eksternal. Dengan kata lain VLAN ini membolehkan satu port menjadi beberapa VLAN. Cara seperti ini sering disebut sebagai *virtual subnet VLAN.*
		- **user defined**, cara ini bisa dianggap paling fleksibel, membolehkan switch membentuk VLAN atas dasar paket data, sebagai contoh VLAN disusun atas dasar MAC address.