Pertemuan 7

Pengenalan Virtual Local Area Network (VLAN)

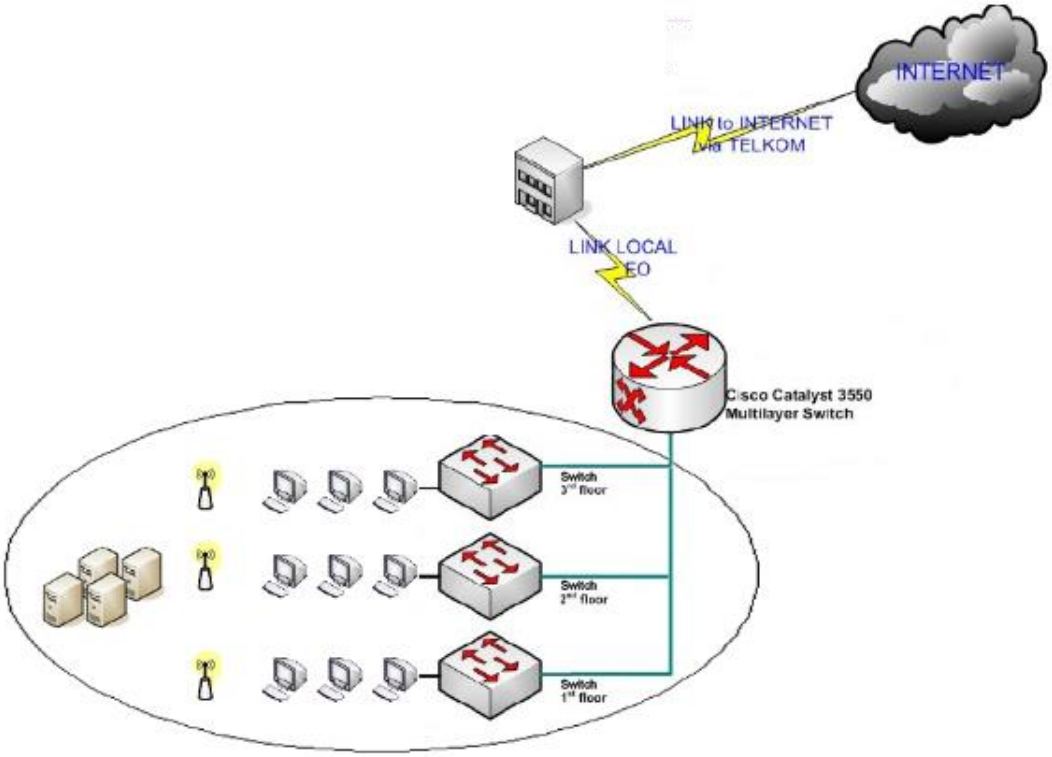
Objektif :

1. Mahasiswa dapat memahami tentang Virtual Local Area Network (VLAN)
2. Mahasiswa dapat mengenal Tipe-tipe VLAN
3. Mahasiswa dapat memahami tentang Identitas yang terdapat pada VLAN

7.1. Pengantar VLAN

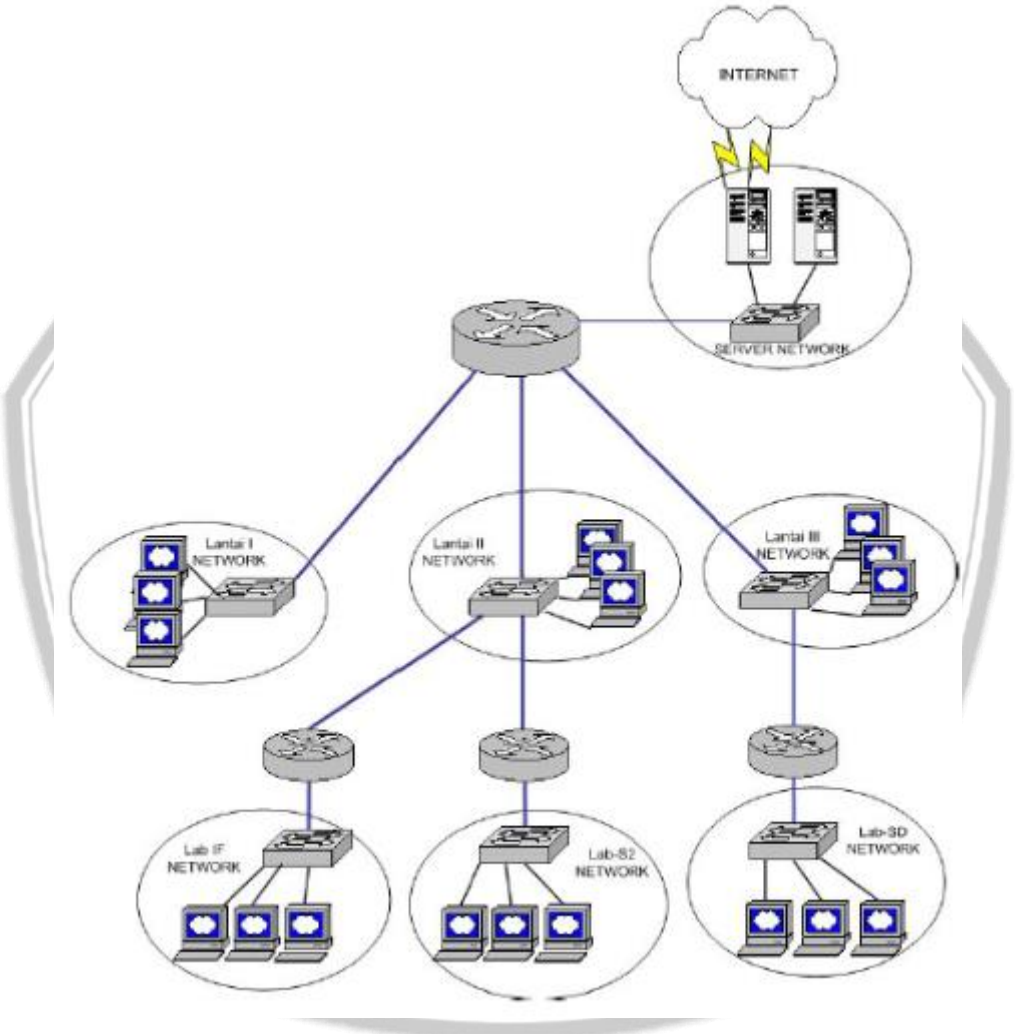
Salah satu permasalahan pada komponen jaringan yang hanya bekerja pada layer 2 (data link) seperti HUB, bridge dan switch unmanageable adalah bahwa alat tersebut akan menimbulkan broadcast dan multicast. Hal ini akan mempengaruhi seluruh mesin atau komputer yang terhubung de ngan alat tersebut, baik proses yang dilakukan CPU maupun bandwidth pada segmen yang memiliki broadcast yang sama.

Pada komponen gambar dibawah adalah solusi yang sering digunakan umumnya memisah broadcast domain dengan memberi router pada setiap segmen yang akan dipisah. Masalahnya adalah bahwa jika pada setiap segmen harus dipasang router maka tentu saja akan membutuhkan biaya yang cukup besar. Karena semakin banyak segmen yang dibutuhkan, maka semakin banyak pula port router yang harus disediakan.



Gambar 1. Sebuah jaringan flat menggunakan 4 buah switch

Saat ini solusi yang terbaik dan relatif lebih murah adalah menggunakan switch manageable yang sudah mendukung VLAN (Virtual Local Area Network). Dengan switch tersebut, dapat dibuat banyak VLAN tanpa membutuhkan router yang banyak. Untuk menghubungkan antar VLAN, cukup digunakan sebuah router yang mendukung VLAN atau switch multilayer (mampu melakukan routing)



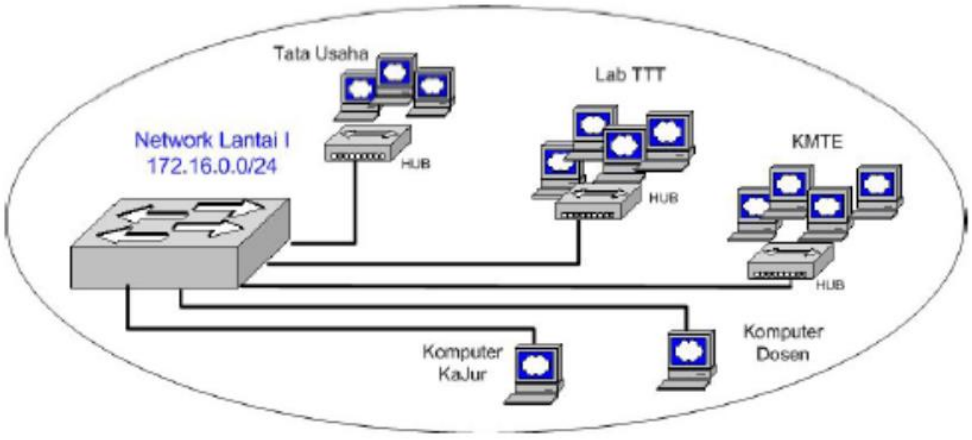
Gambar 2. Jaringan dengan 7 segmen dengan 4 buah PC router

7.2. Pengertian dan Keuntungan VLAN

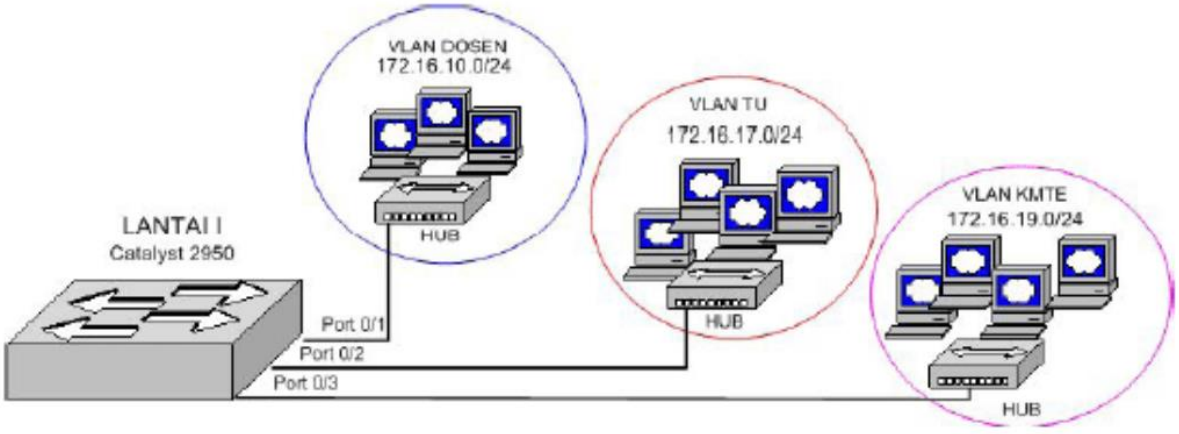
Yang dimaksud dengan sebuah VLAN (Virtual Local Area Network) adalah sekelompok komponen jaringan yang saling terhubung dan memiliki broadcast domain yang sama. Pada umumnya koneksi antar komponen jaringan

ini menggunakan Hub atau switch . Dengan adanya dukungan VLAN pada switch maka dapat dilakukan pemisahan broadcast domain yang terjadi berdasarkan kelompok VLAN.

Pada gambar 4 dapat dilihat bahwa jaringan pada lantai satu terdiri dari 3 buah VLAN yakni VLAN Dosen, VLAN TU dan VLAN KMTE. Implementasi VLAN pada switch catalyst akan membatasi broadcast yang dilakukan oleh komputer-komputer di KMTE sehingga ha nyatertuju kepada komputer lainnya yang tergolong pada VLAN yang sama (VLAN KMTE), sedang komputer yang termasuk VLAN Dosen dan Tata Usaha (TU) tidak terganggu atas broadcast yang dilakukan oleh jaringan KMTE.



Gambar 3. Sebuah VLAN dengan jaringan flat menggunakan sebuah switch dan 3 buah HUB



Gambar 4. Tiga buah VLAN pada sebuah switch dan 3 HUB

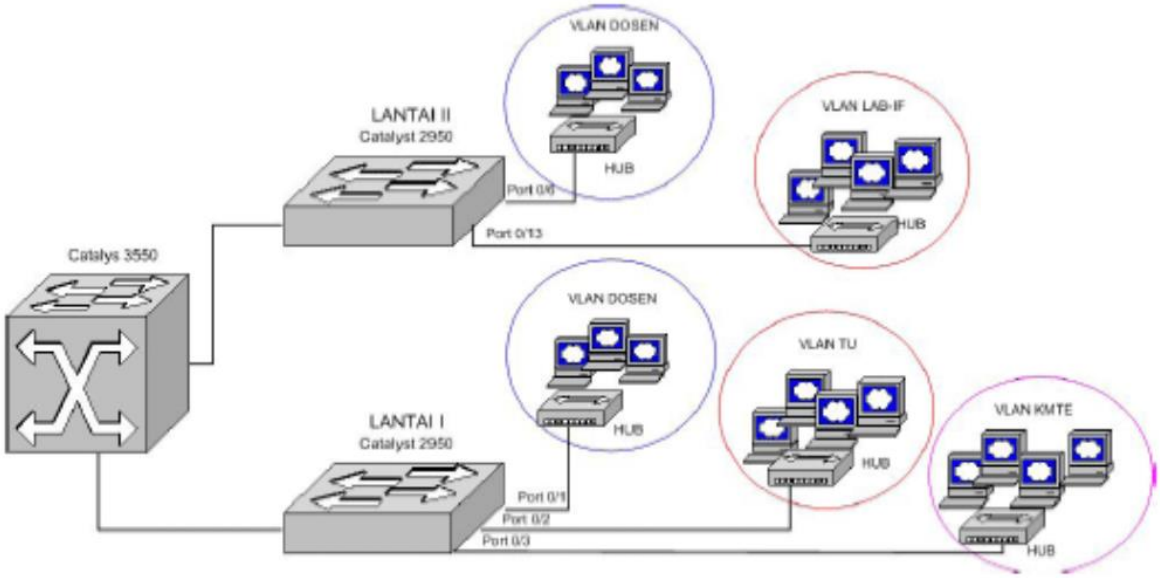
Saat ini, hampir semua switch manageable sudah mendukung VLAN di setiap port-port yang disediakan. Dengan adanya VLAN maka banyak keuntungan dan kemudahan yang akan diperoleh antara lain : broadcast control , keamanan (security) dan fleksibilitas.

a) Broadcast Control

Broadcast terjadi pada setiap protokol komunikasi, tetapi berapa banyak broadcast terjadi tergantung dari jenis protokol tersebut, aplikasi yang berjalan pada jaringan tersebut dan bagaimana layanan tersebut digunakan. Semua komponen jaringan yang menjadi anggota sebuah VLAN berada pada broadcast domain yang sama akan menerima semua broadcast jika terjadi komunikasi didalam VLAN tersebut. Setiap membuat VLAN baru, maka kita akan otomatis membuat broadcast domain yang baru pula. Dalam bahasa sehari-hari kita sering menyebutkan broadcast domain ini sebagai sebuah subnet. Untuk menghubungkan broadcast domain yang berbeda dibutuhkan sebuah router atau device yang bekerja pada layer 3 (network layer) .

b) Keamanan (Security)

Pada jaringan yang bersifat flat network, sistem keamanan pada umumnya dengan cara menambah router yang sekaligus berfungsi sebagai firewall diantara hub atau switch tersebut. Jadi sistem keamanan akan ditangani oleh router, hal ini memiliki beberapa kelemahan yakni setiap orang yang terhubung ke hub atau switch tersebut akan dengan mudah mendapatkan akses terhadap resource yang ada pada jaringan fisik (Hub atau switch) tersebut. Pada jaringan tersebut juga setiap orang bisa menjalankan network analyzer atau program sniffing untuk melihat trafik yang terjadi pada jaringan. Dengan VLAN dan membuat kelompok kelompok broadcast domain , administrator akan dapat mengendalikan setiap port, resource dan pengguna yang ada pada jaringan tersebut.



Gambar 5 Jaringan VLAN dosen berbeda lokasi fisik

c) Fleksibilitas

VLAN juga memiliki fleksibilitas yang tinggi dalam jaringan, sebab user pada broadcast domain yang sama tidak tergantung letak atau lokasi fisik user tersebut terhubung. Pada gambar 5 dapat dilihat bahwa lokasi fisik tidak menjadi kendala dalam segmentasi ataupun pembagian broadcast dengan VLAN. Dengan demikian switch bisa ditempatkan dilokasi yang berbeda tanpa mempengaruhi jaringan logikalnya.

7.3. Tipe VLAN

Ada dua tipe koneksi atau interface pada switch yang digunakan untuk implementasi VLAN yakni access-links dan trunk-links. Tipe koneksi ini akan ditentukan pada port-port sebuah switch melalui konfigurasi melalui sistem yang ada pada switch tersebut.

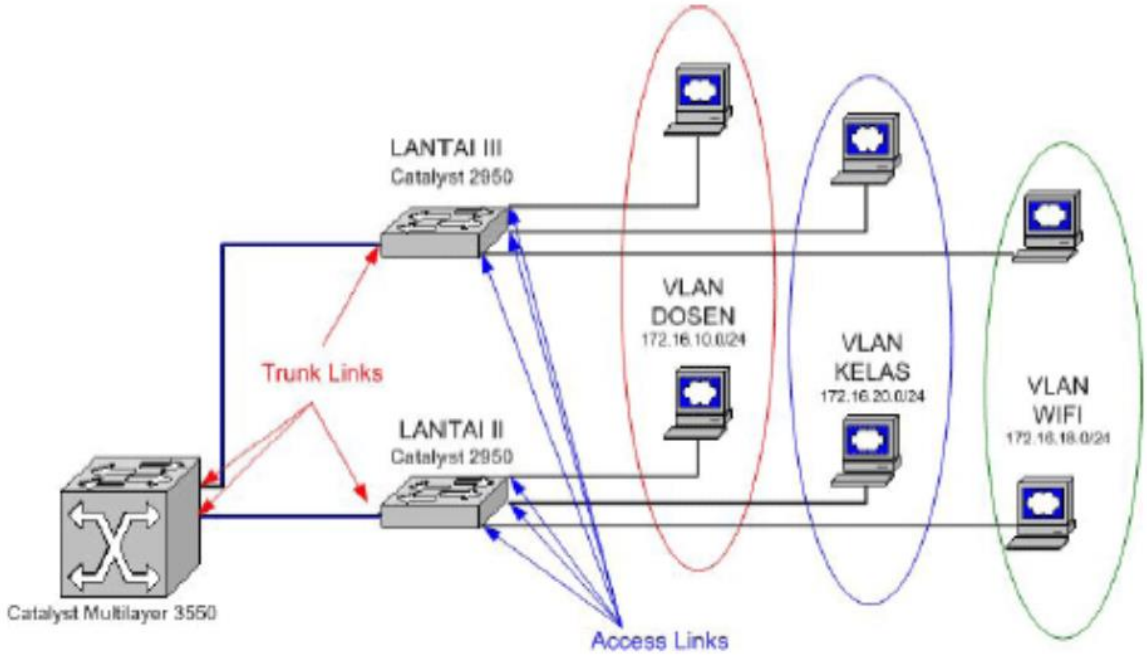
a) Access-links

Access-links adalah sebuah koneksi atau interface pada switch menuju peralatan jaringan seperti personal komputer, file server, dan router. Sebuah access-link hanya dapat terhubung dengan sebuah VLAN, contohnya pada gambar

6 terdapat beberapa PC yang terhubung ke jaringan melalui access-link dan menjadi anggota VLAN tertentu.

b) Trunk-links

Sebuah trunk-links dapat membawa trafik dari beberapa VLAN sekaligus melalui satu koneksi. Untuk membawa trafik beberapa VLAN melalui sebuah koneksi, misalnya antara dua switch , maka dibutuhkan koneksi trunk. Pada gambar 5 dapat dilihat sebuah koneksi trunk 3 buah switch . Koneksi antar komponen jaringan yang berbeda lokasi fisik tetapi tetap dalam satu VLAN terjadi melalui koneksi trunk. Seperti gambar 6, trunking yang terjadi antara switch lantai II ke switch distribusi (catalyst 3550) kemudian dari switch distribusi ke access switch di lantai III sehingga mampu melewatkan beberapa VLAN sekaligus.



Gambar 6 Access-links dan trunk-links

7.4. VLAN Tagging

VLAN tagging disebut juga dengan frame tagging, yaitu suatu metoda yang dikembangkan oleh Cisco untuk membantu mengidentifikasi perjalanan paket data melalui trunk links. Ketika sebuah ethernet frames berubah menjadi

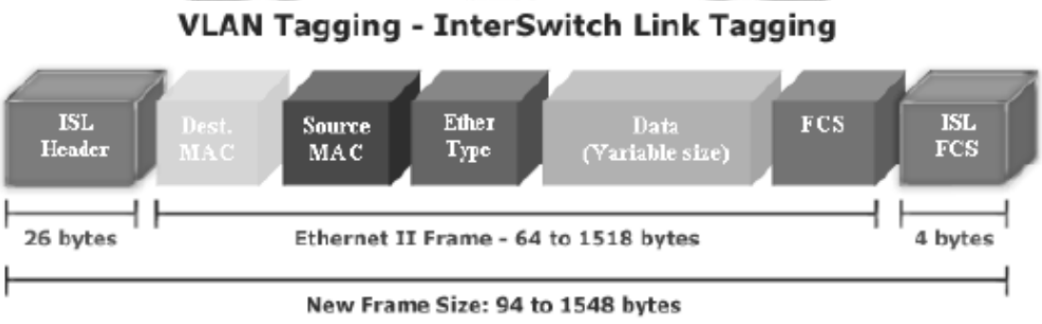
sebuah trunk link, sebuah tag VLAN khusus ditambahkan pada frame tersebut kemudian dikirimkan melalui trunk link . Setelah frame tersebut sampai di ujung trunk link kemudian tag khusus tersebut akan dilepaskan dan frame tersebut akan dikirimkan pada port access link yang sesuai dengan tabel pada switch .

a) VLAN Tagging Protocol

Ada dua jenis VLAN tagging yang sering digunakan pada jaringan berbasis VLAN dengan produk cisco yakni ISL (InterSwitch Link) dan IEEE 802.1q. ISL merupakan protokol proprietary Cisco yang digunakan hanya untuk koneksi pada FastEthernet dan Gigabit Ethernet . Protokol ini bersifat proprietary membuat dukungan terhadap protokol ISL hanya ada pada produk-produk Cisco saja. Sedangkan IEEE 802.1q merupakan protokol standar yang diciptakan oleh group IEEE dan menjadi pilihan lain selain protokol ISL dalam mempermudah manajemen jaringan yang luas berbasis VLAN.

b) ISL (InterSwitch Link)

Proses tagging pada protokol ISL sering disebut dengan external tangging process. Artinya adalah bahwa protokol tersebut tidak merubah struktur frame ethernet melainkan membungkus frame ethernet tersebut, pada bagian awal menambahkan 26 byte ISL header dan 4 byte frame check sequence (FCS) pada bagian akhir frame ethernet. Pada gambar 7 dapat dilihat sebuah ISL frame membungkus ethernet frame . Frame baru tersebut yang akan dilewatkan melalui sebuah trunk links antara dua buah peralatan cisco, jika dikonfigurasi menggunakan ISL sebagai protokol tangging. ISL memiliki kemampuan untuk mendukung sebanyak 1000 VLAN. Jadi dalam koneksi trunk links jumlah VLAN yang mungkin dilewatkan mencapai 1000 VLAN.

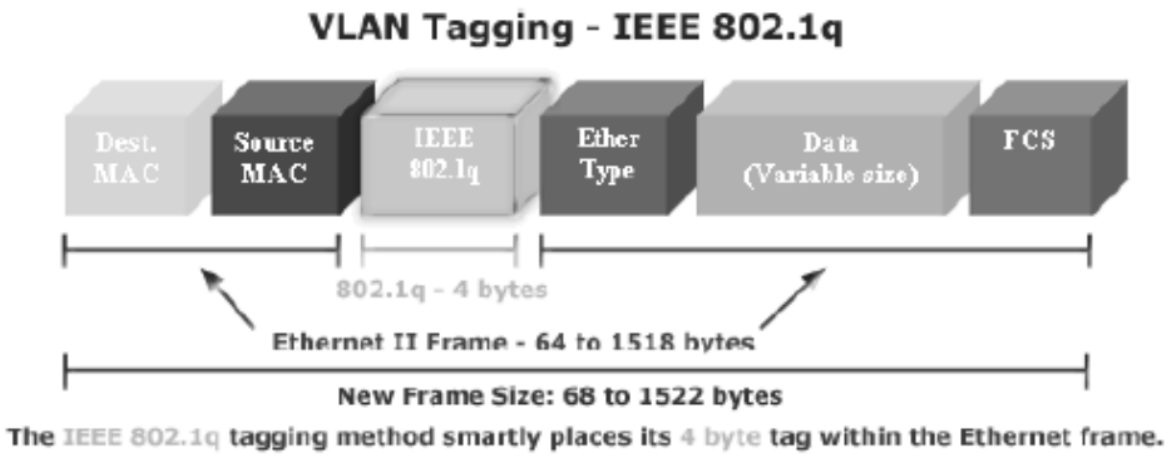


Gambar 7 ISL tagging

c) IEEE 802.1q

Protokol standar IEEE 802.1q merupakan protokol tagging yang paling banyak digunakan pada implementasi VLAN bahkan digunakan pada jaringan meskipun semua peralatannya menggunakan produk cisco. Hal ini disebabkan karena IEEE 802.1q memiliki kompatibilitas dengan peralatan lain, sehingga jika suatu saat melakukan upgrade menggunakan produk vendor lain tidak akan menemukan masalah. Selain karena kompatibilitas, ada beberapa alasan lain yakni:

- IEEE 802.1q mendukung hingga 4096 VLAN
- Proses tagging pada protokol ini dengan cara melakukan tanpa melakukan pembungkusan tetapi hanya penyisipan VLAN tagging sebesar 4 byte.
- Proses tagging menghasilkan ukuran frame yang lebih kecil dibanding frame akhir pada VLAN tagging menggunakan ISL.



Gambar 8 IEEE 802.1q tagging

7.5. Identitas VLAN

Untuk memberi identitas sebuah VLAN digunakan nomor identitas VLAN yang dinamakan VLAN ID. Digunakan untuk menandai VLAN yang terkait. Dua range VLAN ID adalah:

a. Normal Range VLAN (1 – 1005)
   - digunakan untuk jaringan skala kecil dan menengah.
   - Nomor ID 1002 s.d. 1005 dicadangkan untuk Token Ring dan FDDI VLAN.
   - ID 1, 1002 - 1005 secara default sudah ada dan tidak dapat dihilangkan.
   - Konfigurasi disimpan di dalam file database VLAN, file ini disimpan dalam memori flash milik switch.
   - VLAN trunking protocol (VTP), yang membantu manajemen VLAN, hanya dapat bekerja pada normal range VLAN dan menyimpannya dalam file database VLAN.

b. Extended Range VLANs (1006 – 4094)
   - memampukan para service provider untuk memperluas infrastrukturnya kepada konsumen yang lebih banyak. Dibutuhkan untuk perusahaan skala besar yang membutuhkan jumlah VLAN lebih dari normal.
   - Memiliki fitur yang lebih sedikit dibandingakn VLAN normal range.
   - Disimpan dalam NVRAM (file running configuration).

Beberapa terminologi di dalam VLAN.

a. VLAN Data

   VLAN Data adalah VLAN yang dikonfigurasi hanya untuk membawa data-data yang digunakan oleh user. Dipisahkan dengan lalu lintas data suara atau pun manajemen switch. Seringkali disebut dengan VLAN pengguna, User VLAN.

b. VLAN Default

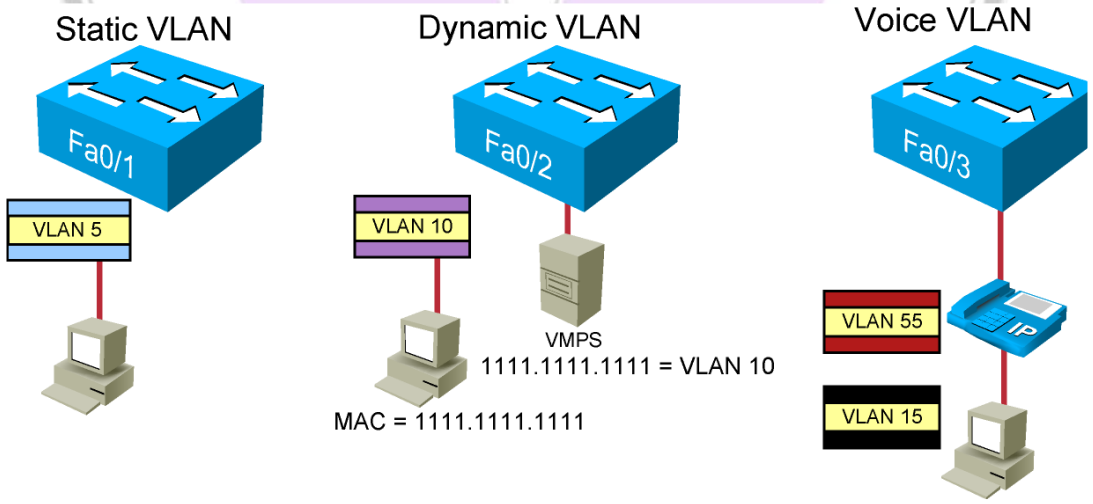
   Semua port switch pada awalnya menjadi anggota VLAN Default. VLAN Default untuk Switch Cisco adalah VLAN 1. VLAN 1 tidak dapat diberi nama dan tidak dapat dihapus.

c. Native VLAN

Native VLAN dikeluarkan untuk port trunking 802.1Q. port trunking 802.1Q mendukung lalu lintas jaringan yang datang dari banyak VLAN (*tagged traffic*)

Terdapat 3 tipe VLAN berdasarkan konfigurasinya, yaitu:

a. Static VLAN – Mode ini biasa digunakan dijaringan kecil dan menengah. Ciri utama pada static VLAN ini adalah port switch yang dikonfigurasi secara manual.
b. Dynamic VLAN – Mode ini digunakan secara luas di jaringan skala besar. Keanggotaan port Dynamic VLAN dibuat dengan menggunakan server khusus yang disebut VLAN Membership Policy Server (VMPS). Dengan menggunakan VMPS, kita dapat menandai port switch dengan VLAN. secara dinamis berdasar pada MAC Address sumber yang terhubung dengan port.
c. Voice VLAN - port dikonfigurasi dalam mode voice sehingga dapat mendukung IP phone yang terhubung.



Gambar 9. Tipe VLAN