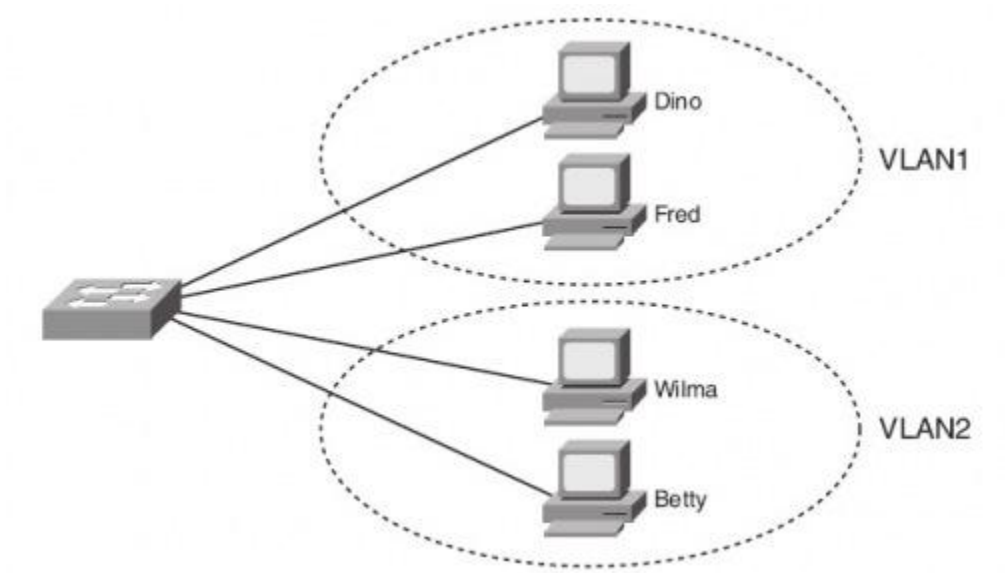
Konsep Virtual LAN (VLAN)

Prinsip utama sebuah LAN adalah, semua device yang berada pada satu LAN berarti berada pada satu broadcast domain.

Sebuah broadcast domain mencakup semua device yang terhubung pada satu LAN dimana jika salah satu device mengirimkan frame broadcast maka semua device yang lain akan menerima kopi dari frame tersebut. Jadi pada dasarnya kita bisa menganggap LAN dan broadcast domain adalah hal yang sama.

Tanpa VLAN, sebuah switch akan menganggap semua interface (port) nya berada pada satu broadcast domain; dengan kata lain, semua komputer yang terhubung ke switch tersebut berada pada satu LAN yang sama. Dengan VLAN, switch bisa meletakkan beberapa interface ke dalam satu broadcast domain dan beberapa interface yang lain ke dalam broadcast domain lain yang berbeda, sehingga tercipta multiple broadcast domain. Masing-masing broadcast domain yang dibuat oleh switch inilah yang kita sebut sebagai Virtual LAN (VLAN).

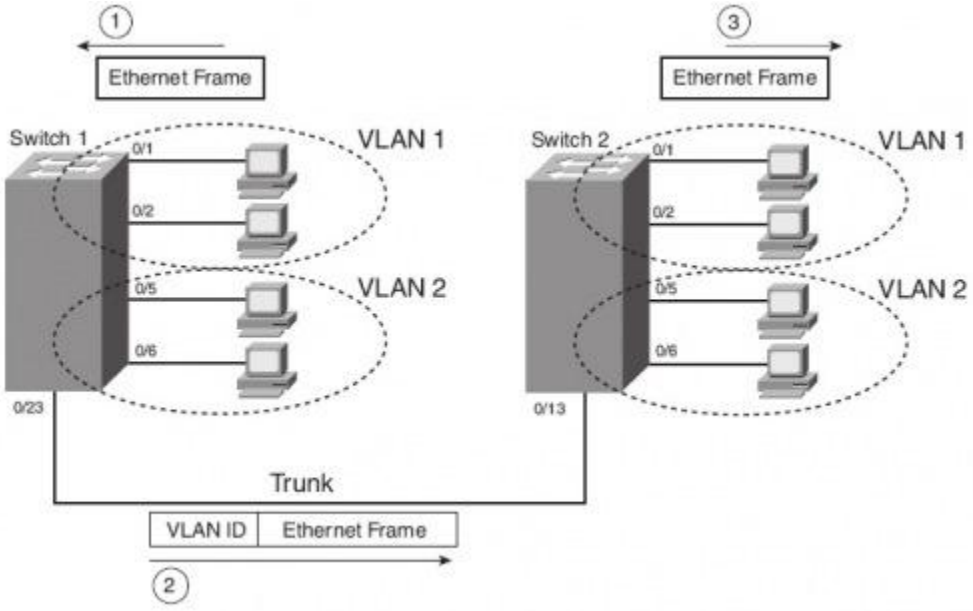


Berikut beberapa alasan untuk memisahkan beberapa komputer pada VLAN yang berbeda :

- Agar design jaringan yang lebih flexible, pengelompokan user tidak berdasarkan lokasi fisik tapi bisa dilakukan dengan berdasarkan kesamaan departemen/ divisi/ pekerjaan.
- Untuk melakukan segmentasi LAN menjadi LAN-LAN yang lebih kecil sehingga mengurangi traffik jaringan.
- Untuk mengurangi beban kerja STP.
- Untuk alasan keamanan yang lebih baik dengan memisahkan user-user yang bekerja menggunakan data-data yang sensitif pada 1 VLAN yang terpisah.
- Untuk memisahkan trafik IP Phone dengan trafik PC yang terhubung dengan phone.

Trunking dengan ISL and 802.1Q

Saat menggunakan beberapa VLAN pada network yang memiliki beberapa switch yang terhubung, maka switch-switch tersebut harus menerapkan VLAN trunking pada segment yang menghubungkan switch dengan switch lainnya. VLAN trunking mengakibatkan switch menggunakan proses yang dinamakan VLAN tagging, dimana switch yang mengirimkan data ke switch lain menambahkan header pada frame sebelum dikirimkan via trunk. Header tambahan ini berisi VLAN identifier (VLAN ID) sehingga switch pengirim bisa mencantumkan VLAN ID dari frame yang dikirimkan dan switch penerima akan mengetahui frame yang diterima ditujukan untuk VLAN yang mana.

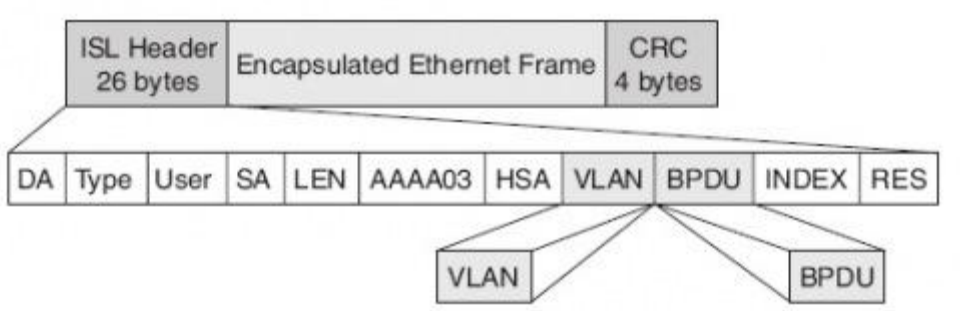


Penggunaan trunking memungkinkan switch untuk mengirimkan frame dari satu VLAN ke VLAN yang berbeda melalui satu koneksi fisik (trunk link).

Cisco switch men-support 2 jenis protokol trunking : Inter-Switch Link (ISL) dan IEEE 802.1Q.

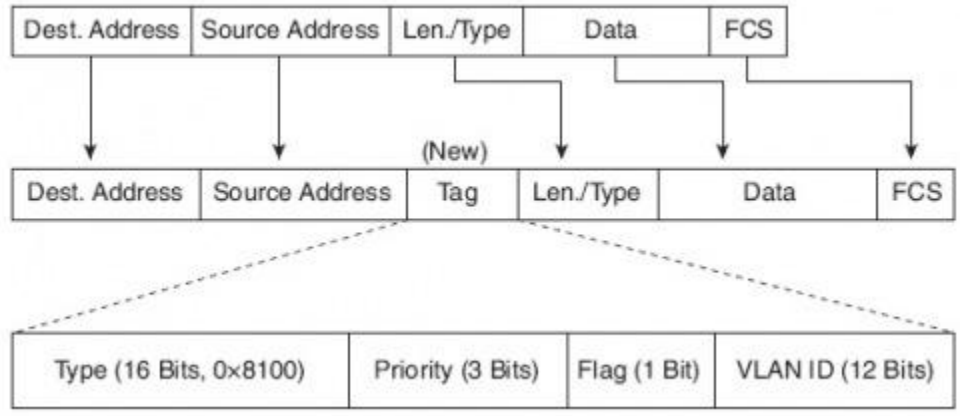
ISL

Cisco menciptakan ISL beberapa tahun sebelum IEEE menciptakan standard 802.1Q untuk protokol VLAN trunking. Karena ISL adalah proprietari Cisco, maka ISL hanya bisa digunakan antar-switch buatan Cisco yang mendukung ISL. ISL meng-enkapsulasi (membungkus) keseluruhan frame ethernet dengan ISL header dan trailer. Frame ethernet original dalam ISL tetap tidak berubah.



IEEE 802.1Q

IEEE melakukan standardisasi beberapa protokol yang berhubungan dengan LAN, termasuk protokol VLAN trunking. 802.1Q menggunakan header yang berbeda dari ISL untuk menyematkan angka VLAN pada frame. Sebenarnya 802.1Q tidak melakukan enkapsulasi penuh seperti halnya ISL. Sebagai gantinya, 802.1Q menyisipkan 4-byte VLAN header pada header original dari ethernet frame. Hasilnya, tidak seperti ISL, frame yang dikirimkan masih memiliki source dan destination MAC address yang original. Dan juga, karena headernya berubah, maka enkapsulasi 802.1Q terpaksa menghitung ulang frame check sequence (FCS) yang asli yang berada pada ethernet trailer.



802.1Q mendefinisikan satu VLAN untuk setiap trunk sebagai native VLAN, sedangkan ISL tidak. Defaultnya, 802.1Q native VLAN adalah VLAN 1. Singkatnya 802.1Q tidak menambahkan header pada frame yang berada dalam native VLAN. Saat switch diujung yang lain menerima frame yang tidak memiliki header 802.1Q, maka switch tersebut menganggap bahwa frame tersebut adalah termasuk frame dari native VLAN. Karena itu, kedua switch yang berhubungan harus menyepakati VLAN mana yang diperlakukan sebagai native VLAN.

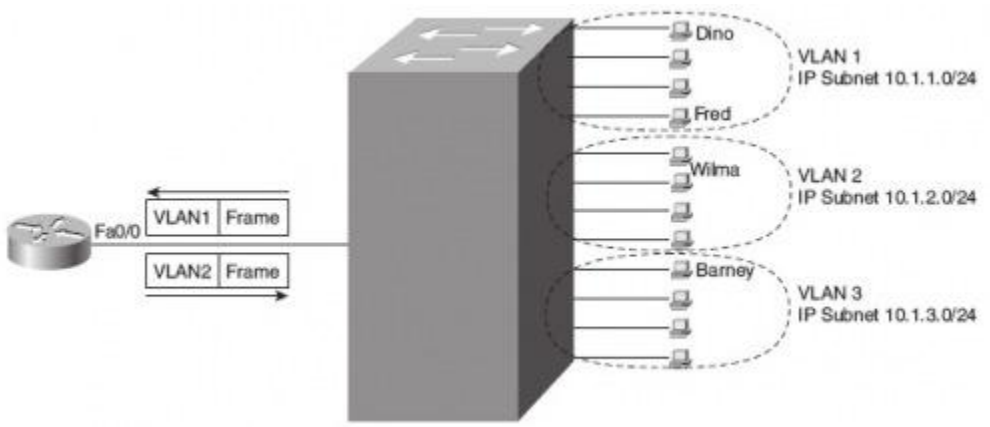
IP Subnets dan VLAN

Saat menyertakan konsep VLAN dalam mendesain sebuah network, perlu diingat bahwa komputer-komputer yang berada dalam satu VLAN haruslah berada pada subnet yang sama.

Dengan demikian, komputer-komputer yang berada pada VLAN yang berbeda haruslah berada pada subnet yang berbeda pula.

Karena aturan inilah, banyak orang yang beranggapan bahwa VLAN adalah subnet dan subnet adalah VLAN. Meski tidak sepenuhnya benar, karena VLAN adalah konsep layer 2 (Data Link) sedangkan subnet adalah konsep layer 3 (Network), namun ide ini cukup beralasan, karena device/komputer-komputer yang berada pada satu VLAN akan berada pada subnet yang sama pula.

Dibutuhkan minimal satu router agar sebuah komputer bisa mengirimkan paket ke komputer lain pada subnet yang lain.



VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) adalah proprietari Cisco yang memungkinkan switch-switch Cisco yang terhubung bisa saling bertukar informasi konfigurasi. Bayangkan, jika sebuah network memiliki 10 switch yang saling terhubung menggunakan VLAN trunk, dan setiap switch memiliki minimal satu port yang ditempatkan pada satu VLAN dengan VLAN ID 3 dengan nama *Accounting*. Tanpa VTP, enginer harus login satu persatu ke semua 10 switch dan melakukan konfigurasi yang sama untuk membuat sebuah VLAN dan memberikan nama pada VLAN tersebut. Dengan VTP, user dapat membuat VLAN 3 dan memberikan namanya pada salah satu switch, dan ke-sembilan switch yang lain akan otomatis membuat VLAN 3 sekaligus namanya.

VTP mendefinisikan protokol pertukaran informasi pada layer 2 yang dipakai switch untuk saling bertukar informasi konfigurasi VLAN. Saat salah satu switch merubah konfigurasi VLAN nya, dengan kata lain, menambah, mengedit, atau menghapus salah satu VLAN, VTP akan membuat switch-switch yang lain melakukan sinkronisasi pada VLAN konfigurasinya.

Setiap switch akan menggunakan salah satu dari 3 mode VTP: server mode, client mode, or transparent mode. Untuk memanfaatkan fitur VTP, engineer harus menge-*set* salah satu switch-nya menjadi server mode dan switch sisanya yang lain sebagai client mode. Kemudian, Konfigurasi VLAN dilakukan pada switch server dan switch-switch lain yang berada pada client mode akan menyesuaikan konfigurasinya dengan server. Switch yang berada pada client mode tidak bisa merubah konfigurasi VLAN nya. Sedangkan transparent mode, memungkinkan switch untuk tetap saling bertukar informasi konfigurasi VLAN, namun switch pada transparent mode itu sendiri tidak ikut melakukan sinkronisasi.

Agar fitur VTP berjalan, Cisco IOS membutuhkan 3 hal berikut :

- Link yang digunakan antar switch harus diset sebagai VLAN trunk (ISL atau 802.1Q).
- Switch-switch tersebut harus memiliki VTP domain name yang sama.
- Jika dikonfigur pada lebih dari 1 switch, maka switch-switch tersebut harus memiliki password yang sama.