Setelah memahami [konsep](http://junisco.blogspot.com/2013/04/apa-itu-vlan-virtual-lan.html) dan [konfigurasi VLAN](http://junisco.blogspot.com/2013/06/konfigurasi-vlan-pada-switch-cisco.html), pada artikel ini akan di jelaskan tentang **VLAN Trunking**.

**Konsep Trunk.**
Jika suatu port pada switch di set ke **switchport mode access**, maka port tersebut hanya akan bisa dilewati oleh 1 VLAN, yaitu VLAN yang di assign ke port tersebut karena tidak mungkin satu port dengan mode access di assign ke lebih dari 1 VLAN.

Jika jumlah port pada switch sudah tidak mencukupi untuk jumlah PC, maka mau tidak mau anda harus menambah switch baru untuk tambahan port. Lalu bagaimana jika switch-switch yang akan anda hubungkan itu masing-masing berisi lebih dari 1 VLAN? sementara dengan port mode access hanya bisa membawa 1 VLAN? Nah, disini lah anda membutuhkan Trunk.

Dalam *VLAN trunking* ada beberapa poin yang harus diperhatikan :
- Port mode
- Trunk Encapsulation
- Native VLAN

**Switch Port Mode.**

Berikut mode-mode port pada layer 2 switching :

- **Mode access.**

Port dengan mode ini hanya akan bisa membawa 1 VLAN. Itulah mengapa mode ini biasanya hanya di set di port switch yang terhubung ke Endpoint (PC, Server , dll). Port mode access bisa saja di gunakan untuk menghubungkan switch ke switch lain jika port tersebut memang benar-benar hanya digunakan untuk membawa 1 VLAN.



Pada gambar di atas terlihat bahwa semua port pada switch yang terhubung ke PC maupun ke switch lain terdaftar di VLAN 20. Artinya hanya traffic dari VLAN 20 yang dibolehkan melewati port fa0/1.

- **Mode Trunk.**

Port switch pada mode trunk bisa untuk membawa banyak VLAN. Port mode ini akan menjadi trunk jika port pada switch lawan di set ke mode trunk atau *Dynamic Trunking Protocol.*



Pada gambar di atas terlihat ada beberapa VLAN yaitu VLAN 10, 20, 30, 40, dan 50. Secara default, trunk port (fa0/1) bisa di lewati oleh traffic dari semua VLAN tersebut, namun bisa di setting juga agar beberapa VLAN saja yang boleh melewati port tersebut.

Mode trunk akan membuat port switch menjadi trunk port secara permanen dan akan memaksa port switch lawan nya untuk membentuk trunk link.

***Dynamic Trunking Protocol (DTP).***
Untuk negosiasi pembentukan *trunk* port secara dinamis, bisa menggunakan **DTP (Dynamic Trunking Protocol)** yang akan secara dinamik mengirimkan atau hanya menerima *DTP advertisement*.
DTP merupakan protokol Cisco proprietary artinya protokol ini di kembangkan oleh Cisco dan hanya bisa digunakan di switch Cisco.
Berikut adalah port mode pada DTP :

**- Mode Dynamic Auto.**

Ini adalah mode **default**untuk port switch Cisco. Port mode ini bersifat *passive* dalam negosiasi trunk, artinya port ini hanya akan memerima DTP advertisement dari port switch lawannya.
Port ini akan menjadi trunk hanya jika port switch lawan nya adalah mode *Trunk*atau *Dynamic Desirable.*

**- Mode Dynamic Desirable.**

Mode ini adalah kebalikan dari mode *dynamic auto*, jika pada *dynamic auto* bersifat passive dalam negosiasi trunk, maka mode *dynamic desirable* adalah bersifat active. Port mode ini akan secara aktif mengirimkan DTP advertisement ke port switch lawannya.
Port ini akan menjadi trunk port hanya jika port lawan nya adalah *dynamic auto*, *trunk*, atau *dynamic desirable* itu sendiri.

Pada kenyataannya, menggunakan DTP untuk negosiasi trunk port akan berdampak pada masalah *network security*karena jika ada switch asing yang terkoneksi ke switch di jaringan internal anda maka switch asing tersebut bisa membentuk trunk port dengan switch anda dan bisa mengakes semua VLAN di jaringan anda, tentu hal ini akan menjadi masalah security. Untuk mengatasi hal tersebut anda bisa nonaktifkan DTP secara total dengan menggunakan **Switchport Nonegotiate**yang kompatibel dengan *mode trunk* dan *mode access*.

Port **nonegotiate**ini akan mengabaikan DTP advertisement, jadi untuk membentuk trunk di port ini maka interface pada swtich lawan juga harus di set ke **mode trunk** secara manual.

**Trunk Encapsulation.**

Perhatikan *ethernet frame* berikut :



Gambar di atas merupakan isi dari ethernet frame pada *ethernet switching* (Layer 2) traffic.
*Trunk*beroperasi pada layer 2 switching, sementara di ethernet frame tersebut tidak ada field untuk VLAN. Jika ada traffic yang masuk ke sebuah switch dan akan dilewatkan ke trunk port, lalu bagaimana switch ini mengetahui traffic tersebut milik VLAN mana?sementara pada ethernet frame tidak field VLAN?

Maka dari itu di perlukan yang namanya **trunk encapsulation**. Ada 2 trunk encapsulation yang digunakan di swtich Cisco yaitu **ISL** (Cisco Propriatery) dan **IEEE 802.1q** (open standard). Trunk encapsulation default pada switch Cisco adalah 802.1q. ISL hanya support di beberapa switch Cisco dan ISL sudah sangat jarang digunakan lagi, oleh karena itu kita hanya akan membahas **802.1q**



Pada gambar di atas, terlihat bahwa*ethernet frame* di modifikasi dengan menyisipkan field "**Tag**" yang berisi **VLAN ID**. Anggap saja misalnya port pada switch di set ke mode access untuk VLAN 10, maka semua packet yang datang dari PC yang masuk ke port tersebut akan di tag dengan VLAN 10. Dari sini lah switch akan tahu dari VLAN mana packet tersebut berasal.
 **CATATAN :**
- Pada access port, semua frame nya adalah *untagged*. Artinya tidak akan ada penambahan *VLAN tag* pada ethernet frame jika masuk dan keluar melalui port ini. Hal ini dikarenakan jika ethernet frame masuk dan keluar melalui port di switch yang kedua-duanya adalah access port ,yang pastinya kedua port tersebut di assign ke vlan yang sama, maka switch tidak perlu tahu ethernet frame tersebut datang dari VLAN berapa. Dalam VLAN trunking, hal ini dikenal sebagai **untagged frames** atau **untagged VLAN.**
- Pada trunk port, frame nya adalah *tagged*. Artinya akan ada penambahan *VLAN tag*pada ethernet frame jika keluar melalui port ini. Hal ini dikarenakan pada umumnya trunk port di switch terhubung ke perangkat layer 3 (router, firewall, dll), yang dimana port pada router tersebut menggunakan sub-interface yang berisi informasi tag vlan, jadi ethernet frame yang keluar lewat trunk port di switch dan mengarah ke router akan di tag agar router tahu traffic tersebut datang dari VLAN berapa. Dalam VLAN trunking, hal ini dikenal sebagai **tagged frames** atau **tagged VLAN.**

**Native VLAN.**
Pada trunk port, memang semua traffic yang lewat adalah *tagged frames*. Namun agar trunk port dapat beroperasi, harus ada 1 VLAN yang digunakan untuk memproses *untagged frames* yang masuk ke trunk port. Nah, *untagged frames* inilah yang merupakan *untagged VLAN* pada trunk port yang disebut dengan **Native VLAN**.
*Untagged frames* ini biasanya berasal dari hub yang dimana traffic nya tidak di *tagged* sebelum masuk ke trunk port di switch. Begitu masuk ke trunk port, switch akan *tag* traffic tersebut sebagai native VLAN.
Suatu trunk link hanya bisa mempunyai 1 native VLAN. VLAN ID yang akan dijadikan *native VLAN* ini harus sama pada kedua port switch yang akan membentuk trunk. Jika berbeda, maka untagged frames tidak akan bisa di forward melewati trunk link

Artikel selanjutnya : [Konfigurasi Trunk](http://junisco.blogspot.com/2015/06/konfigurasi-trunk-pada-switch-cisco.html)