VLAN (*Virtual LAN*)

Un VLAN ou **réseau local virtuel** est un réseau informatique logique indépendant. En configurant un **commutateur** (*switch*), il est possible de créer des réseaux dits « virtuels » au sein d'un LAN.

Plusieurs VLANs peuvent coexister sur un même commutateur réseau. Pour *Ethernet*, un VLAN est un **domaine de diffusion** (*broadcast domain*).

Les VLANs permettent la **segmentation des réseaux** ce qui permettra d'augmenter ou d'améliorer les performances (débit, bande passante, sécurité...).

Un **domaine de collision** est une zone logique d'un réseau informatique où les trames peuvent entrer en collision, ce qui est le cas des réseaux locaux *Ethernet*. Cela est lié à la topologie logique en **bus** et à la méthode d'accès **CSMA/CD** des réseaux Ethernet. Un concentrateur (*hub*) forme un seul domaine de collision alors qu'un commutateur (*switch*) en crée un par port, ce qui réduit les risques de collision. Lorsque *Ethernet* est utilisé en mode ***full-duplex***, il n'y a plus de domaine de collision, car aucune collision n'est possible.

Un **domaine de diffusion** (*broadcast domain*) est une aire logique d'un réseau informatique où n'importe quel hôte connecté au réseau peut directement transmettre à tous les autres hôtes du même domaine en envoyant une trame à l'adresse de diffusion.

Construction des VLANs

VLAN par port (*Port-based VLAN*)
On affecte chaque port du commutateur à un VLAN. En cas de déplacement d'une machine, il suffit d'affecter (manuellement) son VLAN au nouveau port.

VLAN par adresse MAC (*MAC address-based VLAN*)
Chaque commutateur maintient une table @ MAC ←→ VLAN. Il faut les initialiser (solution : VLAN par défaut). Le commutateur détermine le VLAN de chaque trame à partir de l'adresse MAC source ou destination. Le déplacement d'une machine est possible et transparent.

VLAN par adresse de niveau 3
On affecte une adresse de niveau 3 à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de couche 3 (IP par exemple) qu'elle contient (le commutateur doit donc accéder à ces informations). Cela provoque un fonctionnement moins rapide que les VLANs par port ou par MAC. Quand on utilise le protocole IP on parle souvent de VLAN par sous-réseau.

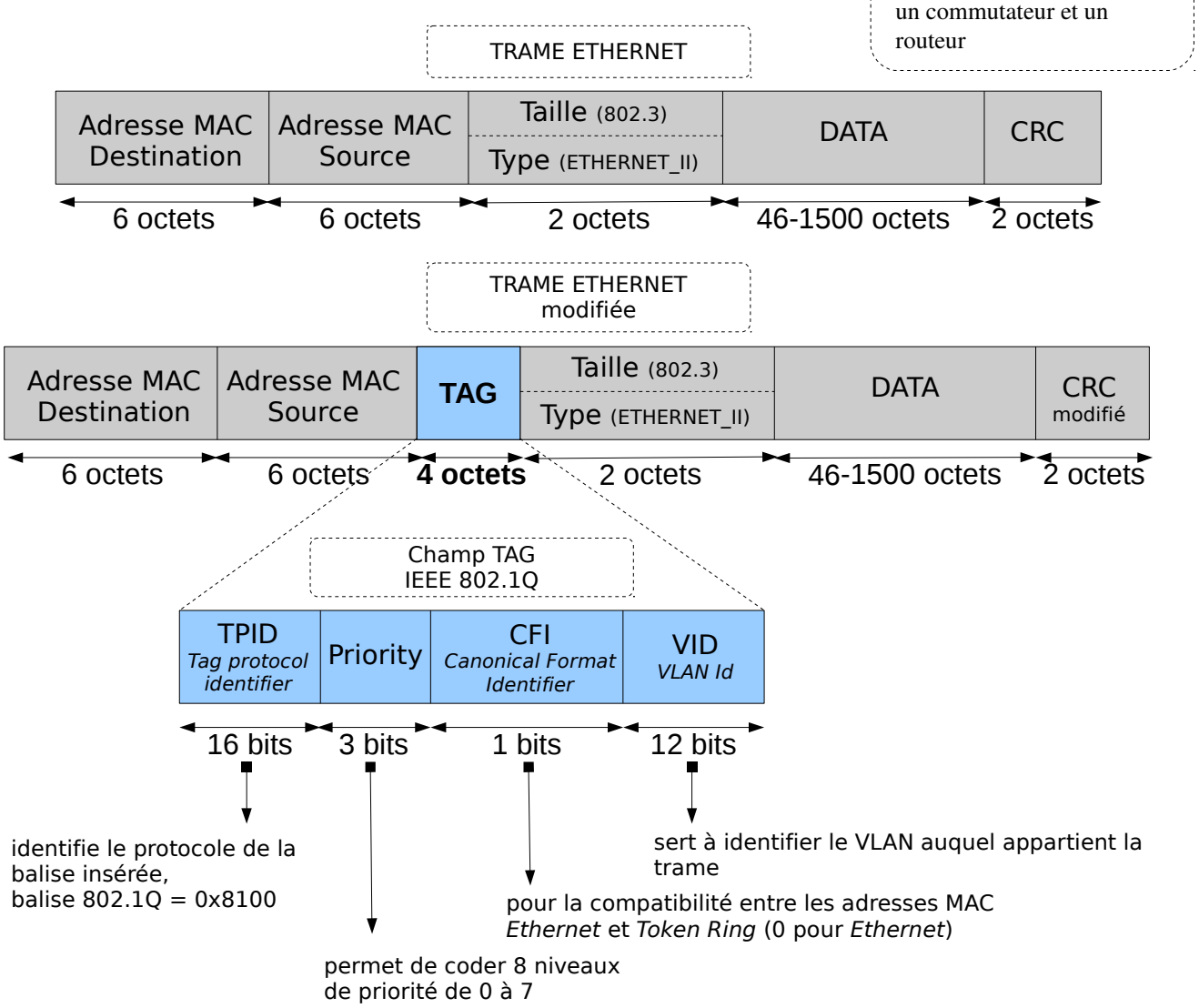
Dans les commutateurs (*switch*), on utilisera la commande **`vlan`**. Sous Linux, Les commandes permettant leur configuration sont : **`vconfig`** ou **`iproute`**.

Le standard IEEE 802.1Q

Il permet de modifier la trame *Ethernet* au niveau de la sous-couche MAC (la couche 2 du modèle OSI) afin de fournir un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. Il permet de propager plusieurs VLAN sur un même lien physique (*trunk*).

802.1Q définit le contenu de la balise de VLAN (*VLAN tag*) avec laquelle on complète l'en-tête de la trame *Ethernet*.

Le terme *trunk* indique un lien de réseau supportant des VLAN multiples entre 2 commutateurs ou entre un commutateur et un routeur



Capture

```
    15 200.521815  192.168.1.2          192.168.1.3          ICMP     Echo (ping) request
    16 200.521917  192.168.1.3          192.168.1.2          ICMP     Echo (ping) reply

▷ Frame 15 (102 bytes on wire, 102 bytes captured)
▷ Ethernet II, Src: 2e:fe:a2:81:23:ce (2e:fe:a2:81:23:ce), Dst: ce:53:0c:0c:ef:61 (ce:53:0c:0c:ef:61)
▽ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 200
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 1100 1000 = ID: 200
    Type: IP (0x0800)
▷ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.3 (192.168.1.3)
▷ Internet Control Message Protocol

0000  ce 53 0c 0c ef 61 2e fe  a2 81 23 ce 81 00 00 c8   .S...a.. ..#.....
0010  08 00 45 00 00 54 00 00  40 00 40 01 b7 53 c0 a8   ..E..T.. @.@..S..
0020  01 02 c0 a8 01 03 08 00  f5 75 e6 01 00 01 fb a2   ........ .u......
0030  57 5a d5 86 09 00 08 09  0a 0b 0c 0d 0e 0f 10 11   WZ...... ........
```