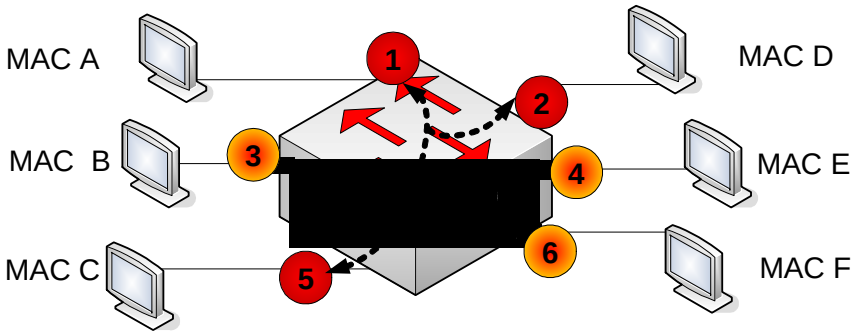
18.4.1 Principes généraux des VLAN[1]

Avec l'accroissement des réseaux, les messages de diffusion (ARP, annonces de service ...) occupent une part de plus en plus importante de la bande passante. En définissant, indépendamment de la situation géographique des systèmes, des domaines de diffusion (domaine de *broadcast),* les VLAN autorisent une répartition et un partage optimal des ressources de l'entreprise. Application directe de la commutation statique, les VLAN associent un port à un identifiant.

Ne peuvent communiquer que les machines raccordées à des ports de même identifiant. Ainsi, sur le commutateur de la figure 18.26 deux VLAN sont déclarés. La communication entre stations n'est possible qu'entre les stations A. C et D d'une part et les stations B. E et F d'autre part. Il en est de même pour les *broadcast* qui ne sont diffusés qu'au sein de leur VLAN respectif (domaine de diffusion),

Figure 18.26 Principe des VLAN.



PORT	VLAN
1	1
3	2
5	1
2	1
4	2
6	2

[1] D'après *Réseaux & Télécoms* de Claude Servin aux éditions DUNOD

La communication n'est autorisée qu'entre machines d'un même VLAN. Les communications inter VLAN doivent transiter par un routeur (figure 18.27). Ainsi les réseaux virtuels permettent de réaliser des réseaux axés sur l'organisation de l'entreprise tout en s'affranchissant de certaines contraintes techniques, notamment celles liées à la localisation géographique des équipements.

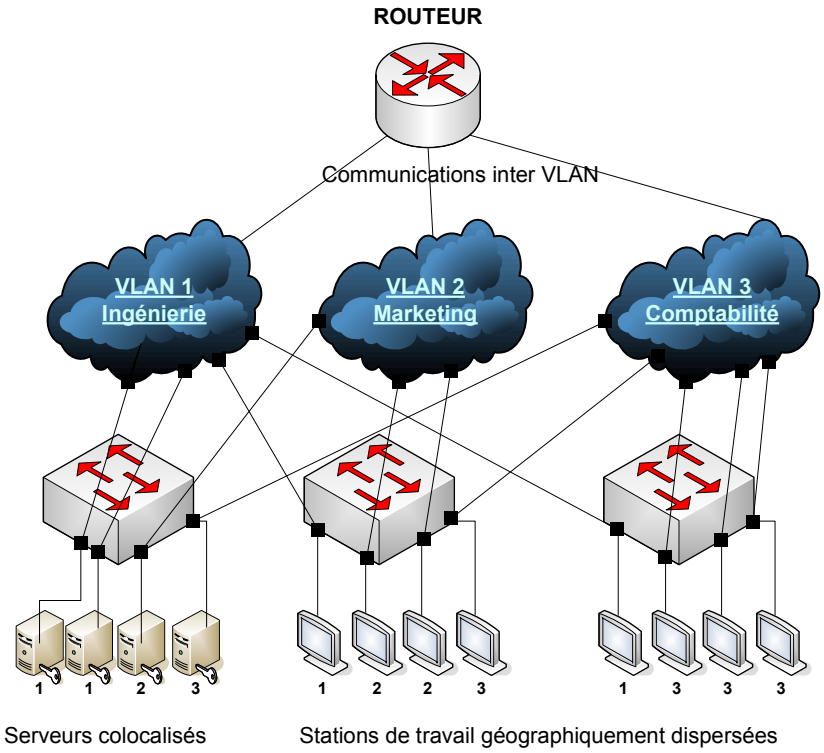


Figure 18.27 La communication inter-VLAN.

En fait, les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critères prédéfinis (ports, adresses MAC, adresses réseau ...).
Un logiciel d'administration permet d'affecter chaque système raccordé à un commutateur à un réseau logique d'appartenance. L'affectation peut être introduite manuellement par l'administrateur station par station (VLAN statique) ou automatiquement par rapport à un identifiant propre à la station comme l'adresse MAC, IP. ..).

18.4.2 Les différents niveaux de VLAN

Les échanges à l'intérieur d'un domaine sont sécurisés et les communications inter domaines sont autorisées et peuvent être contrôlées par les filtres configurés dans le routeur. L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue:

- les VLAN de niveau 1 ou VLAN par port *(Port-based VLAN)* : ces VLAN associent chaque port d'un commutateur à un VLAN. Une station raccordée à 1 port est automatiquement affectée au

VLAN du port. Si le port est raccordé à un hub, toutes les stations de ce hub appartiennent au même VLAN (VLAN par segment). La configuration est statique (VLAN statique), le déplacement d'une station implique son changement de VLAN. C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN. Un port, donc les stations qui lui sont raccordées, ne peut appartenir qu'à un seul VLAN.

- les VLAN de niveau 2 ou VLAN MAC *(MAC Address-based VLAN)* : ces VLAN associent les stations par leur adresse MAC. De ce fait, deux stations raccordées à un même port (segment) peuvent appartenir à deux VLAN différents. Les relations adresses MAC/VLAN sont introduites par l'administrateur. En fonction du critère d'appartenance à un VLAN, ici l'adresse MAC, les ports déterminent automatiquement leur VLAN d'appartenance (VLAN dynamique). Il existe des mécanismes d'apprentissage automatique d'adresses (lecture des adresses MAC des stations raccordées), l'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration *(Drag&Drop).* Une station peut appartenir à plusieurs VLAN. Les VLAN de niveau 2 sont indépendants des protocoles supérieurs. La commutation, s'effectuant au niveau MAC autorise un faible temps de latence.
- les VLAN de niveau 3 ou VLAN d'adresses réseaux *(Network Address-based VLAN)* : ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau *(Subnet* d'IP). Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN. Une station peut appartenir à plusieurs VLAN par affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, **il** s'agit bien de commutation et non de routage. L'en-tête n'est pas modifiée.

Il est aussi envisageable de réaliser des VLAN par :

- protocole (IP, IPX ...), la communication ne pouvant s'établir qu'entre stations utilisant le même protocole.
- par application (N°de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application qu'il utilise.
- par mot de passe (constitution dynamique des VLAN au login de l'utilisateur).

La figure 18.28 illustre ces différentes approches. Les VLAN peuvent être définis sur un ou plusieurs commutateurs, que ceux-ci soient locaux ou distants. Cependant, il devra y avoir, entre chaque commutateur, autant de liens (physiques ou virtuels) que de VLAN interconnectés.

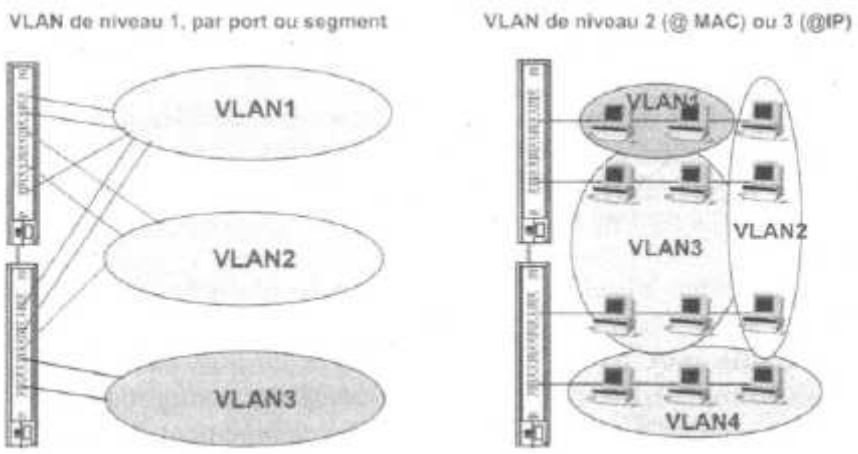


Figure 18.28 Les différents niveaux de VLAN.

18.4.3 L'identification des VLAN (802.1Q)

Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines *(table d'acheminement)* et connaître le VLAN d'appartenance de la source et du destinataire *(filtrage de trafic)*. Lorsque le réseau est important, les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames. L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées. Ainsi. on distingue deux types d'équipement, ceux qui savent gérer l'étiquetage et qui ont donc connaissance des VLAN (les VLAN *aware)* et ceux qui ignorent cette appartenance (VLAN *unaware).*

Dans le réseau de la figure 18.29 cohabitent des équipements *awares* et *unawares.* Les trames émises par les équipements *Awares* sont marquées *(tagged),* celles émises par les équipements *unawares* ne sont pas marquées *(Untagged).* La mixité des équipements nécessite que soit défini un VLAN par défaut : le VLAN auquel sont rattachés les équipements *Unawares* (VLAN C de la figure 18.29). Lorsqu'un équipement *aware* reçoit une trame marquée à destination d'un équipement *Unaware ,* il en extrait le *tag.*

La norme IEEE 802. 1plQ

Marquage des trames

Un VLAN correspond à un domaine de *broadcast.* Cependant, lorsque plusieurs VLAN sont définis sur un même segment, cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le *broadcast* en une rafale *d'unicasts.* La solution adoptée par l'IEEE est toute

différente: un seul VLAN peut être déclaré par port[2], sauf pour les liaisons inter commutateur supportant le trafic de VLAN différents (liens dits: *trunk link,* figure 18.29).

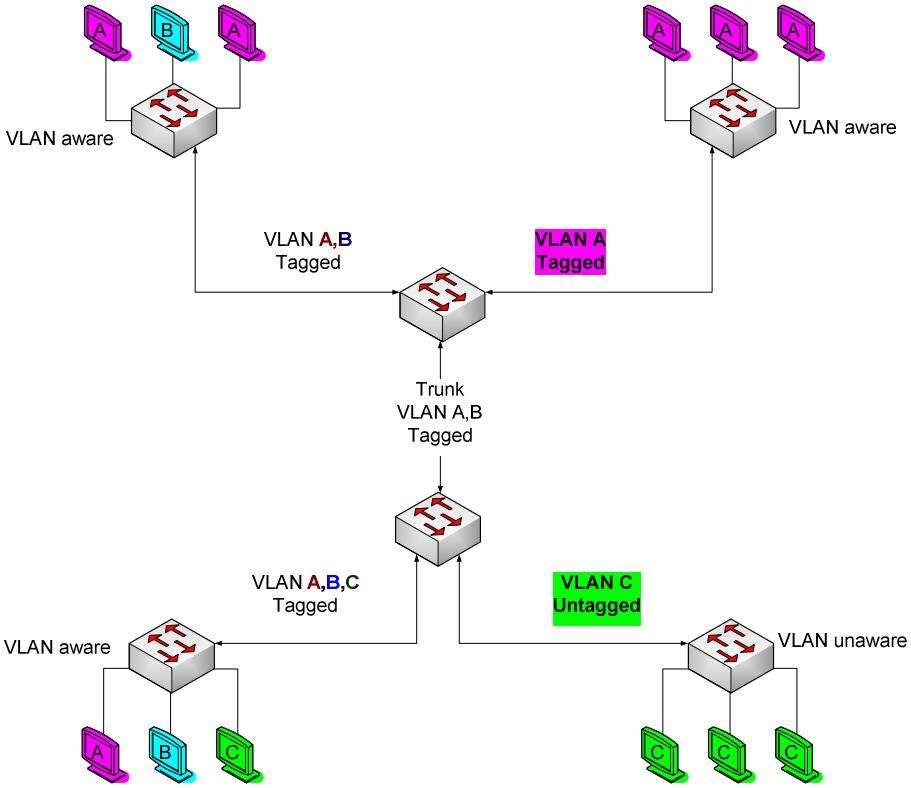


Figure 18.29 Principe de l'étiquetage des trames dans les VLAN.

Les VLAN sont définis dans les normes 802.1 Q et 802.1 p (802.1p/Q[3]) qui introduisent quatre octets supplémentaires dans la trame MAC. Ces quatre octets permettent d'identifier les VLAN *(VLAN tagging)* et de gérer huit niveaux de priorité *(Qualité of Service, QoS).* La figure 18.30 illustre l'étiquetage d'une trame MAC des réseaux de type 802.3.

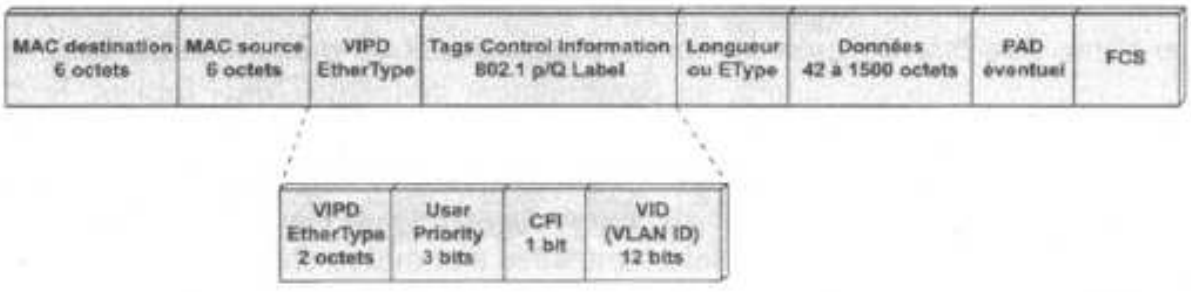


Figure 18.30 Le format de la trame 802.1 p/Q.

[2] Certaines implémentations autorisent le raccordement de périphériques partagés par plusieurs VLAN (superposition de ports).
[3] 802.1Q concerne les VLAN. 802.1p la qualité de service.

La trame 802.1 p/Q augmente la taille de la trame 802.3, la taille maximale passe ainsi de 1 518 à 1 522 octets. Cet accroissement de la taille des trames limite l'usage des trames marquées aux équipements *awares.* En particulier, la plupart des équipements terminaux (station, périphérique) sont encore de type *unaware,* en conséquence, sur les liens d'accès aux commutateurs *(Access link)* ne circulent que des trames non marquées. Les trames sont identifiées par le port d'entrée et le *tag* est extrait par le port de sortie (figure 18.31). Lorsqu'un port d'un équipement *aware* reçoit une trame non marquée, le commutateur affecte le numéro du VLAN du port d'arrivée ou le numéro du VLAN par défaut si ce port n'a pas été configuré.

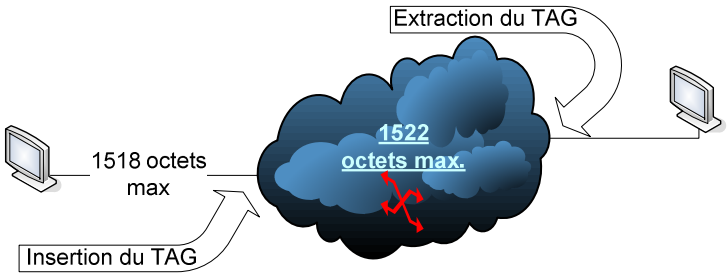


Figure 18.31 L'identification des VLAN internes au réseau.

Pour garantir la compatibilité avec l'existant. le marquage des trames est vu comme une encapsulation supplémentaire. Ainsi, le champ **VPID** *(VLAN ProtocolID)* est similaire au champ Ethertype de la trame 802.3. Il identifie le format 802.1p/Q, sa valeur est fixée à Ox8100 (figure 18.30). Les 2 octets suivants permettent de définir 8 niveaux de priorité *(User Priority).* Les commutateurs de dernière génération disposent de plusieurs files d'attente. Les trames sont affectées à telle ou telle file suivant leur niveau de priorité.
Le bit **CFI** *(Canonicall Format Identifier)* est en principe inutilisé dans les réseaux 802.3, il doit être mis à O. Dans les réseaux Token Ring, à 1. il indique que les données du champ Routage par la source sont au format non canonique. Le champ **VID** *(VLAN IDentifier)* identifie, sur 12 bits, le VLAN destination.
L'introduction de 4 octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS.

Communication intra et inter-VLAN

Lorsqu'une trame doit être diffusée sur un port appartenant au même commutateur que le port d'origine. La communication est réduite au commutateur concerné. Mais lorsque le destinataire n'est pas situé sur le même commutateur, la trame doit être diffusée sur le réseau. Pour limiter la diffusion aux seuls équipements appartenant au VLAN concerné, les équipements *awares* annoncent périodiquement les VLAN qu'ils gèrent (figure 18.32). Le protocole **GVRP** *(GARD VLAN Registrat;on Protocol)* permet de faire connaître aux autres éléments du réseau les VLAN gérés.

Les communications entre VLAN doivent, en principe, transiter par un routeur. Ce dernier doit posséder un attachement sur chaque VLAN routé. La notion d'interfaces virtuelles évite la multiplication des interfaces physiques sur le routeur. Celui-ci possède une seule interface physique reliée à 1 seul port du commutateur (lien et port *trunk).* Sur le routeur plusieurs interfaces virtuelles peuvent être définies (figure 18.33). Lorsque le routeur reçoit une trame marquée, il retire le *tag,* consulte la table de routage et les filtres de trafic associés il détermine alors l'interface virtuelle de sortie. Chaque interface virtuelle est associée à un VLAN et marque la trame sortante. L'acheminement peut aussi être réalisé directement par un commutateur enrichi de fonctions de routage (commutation de niveau 3).

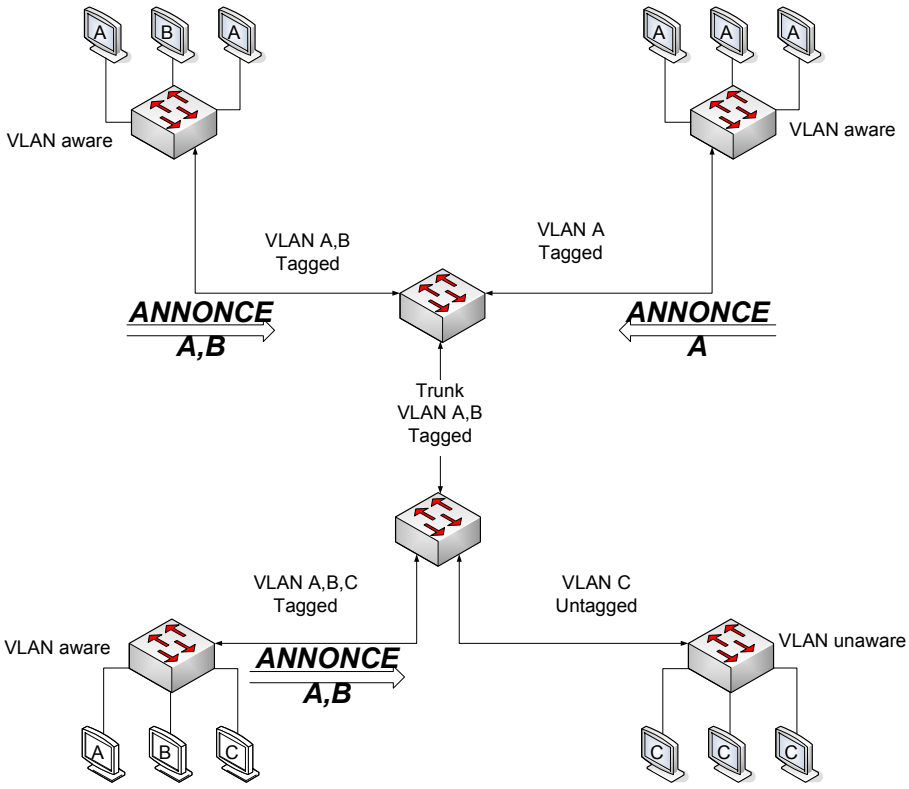


Figure 18.32 Les annonces des VLAN (GVRP).

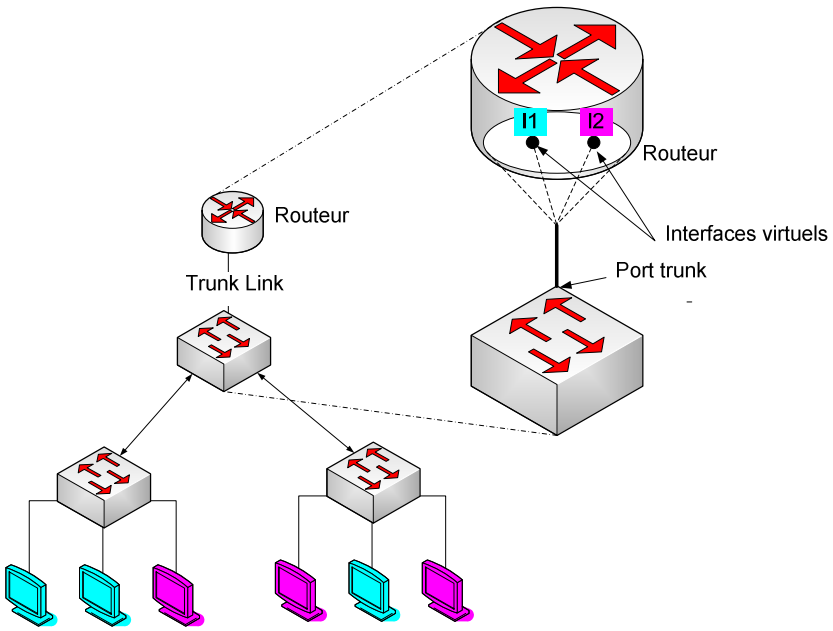


Figure 18.33 Notion d'interfaces virtuelles.

18.5 CONCLUSION

À l'origine imaginés pour des raisons essentiellement de performance, les ponts puis les commutateurs permettent aujourd'hui, non seulement d'améliorer les performances par segmentation des réseaux mais surtout apportent un niveau de sécurité supérieur en isolant les trafics des différents utilisateurs (VLAN).