

Les réseaux locaux virtuels

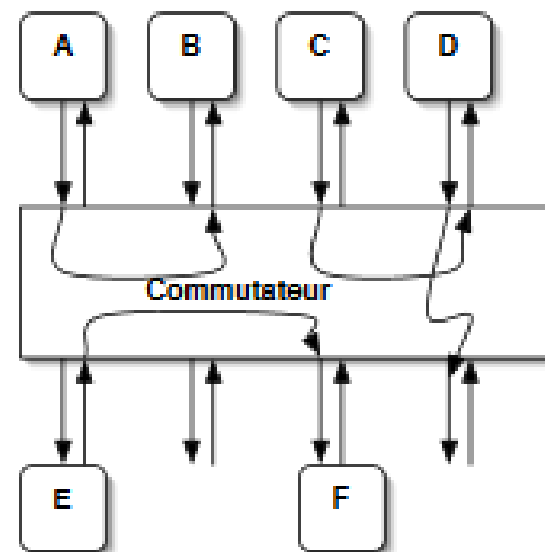
- **VLAN: Virtual LAN**
- A ne pas confondre avec les **VPN: Virtual Private Network** et **WLAN (Wireless LAN)**
- **But :**
 - Découper un réseau local physique en plusieurs réseaux virtuels
 - Les réseaux virtuels sont isolés les uns des autres
 - Limite les domaines de diffusion: les trames en broadcast sont isolées
 - Possible seulement avec un commutateur

Intérêt des VLANs

- Mettre en place plusieurs réseaux locaux virtuels sur un seul LAN physique
- Mise en oeuvre simple et souple contrairement à du vrai câblage
- Isolation des VLANS : sécurité, confidentialité
- Administration plus aisée qu'une administration de niveau 3 (routage)

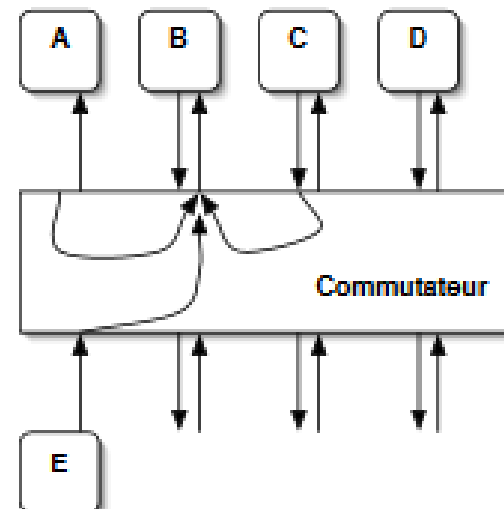
Rappel sur le fonctionnement des commutateurs

- Mémorisation des trames
- Table Port/adresse MAC
 - Rempli à l'aide des premiers paquets
- Les trames ne sont re-émises que vers la destination
- Plus de collisions, fonctionne en full-duplex



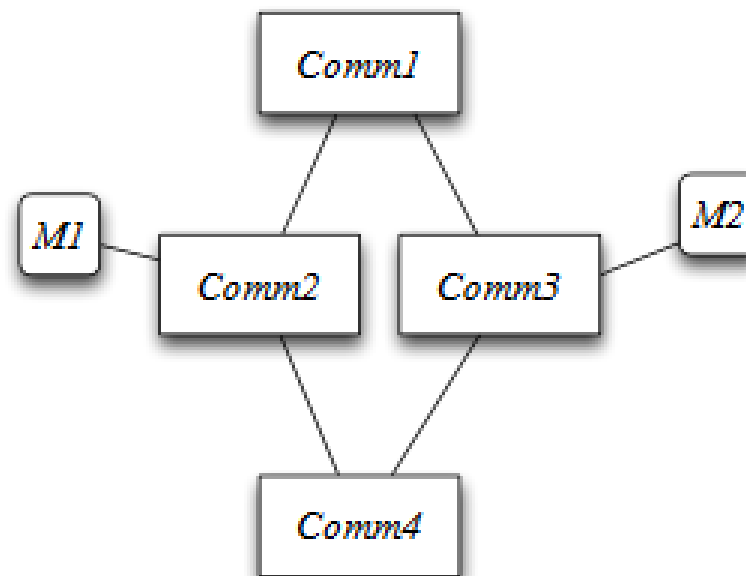
Rappel sur le fonctionnement des commutateurs

- Possibilités de saturation d'un commutateur
 - Qui implique des pertes de trames
- Contrôle de flux (ou plutôt de congestion) au niveau liaison de donnée
- Trame “pause” émises par les commutateurs permettant de limiter les émissions des ordinateurs quand il s'approche de la saturation (remplissage de la mémoire)



Rappel sur le fonctionnement des commutateurs

- Nécessité d'un protocole particulier dans le cas de réseaux possédant plusieurs commutateurs avec des boucles
 - Boucle intéressante pour augmenter la fiabilité
 - Problème lors de l'émission des premiers paquets lorsque les associations *Port/Adresse* ne sont pas encore faites

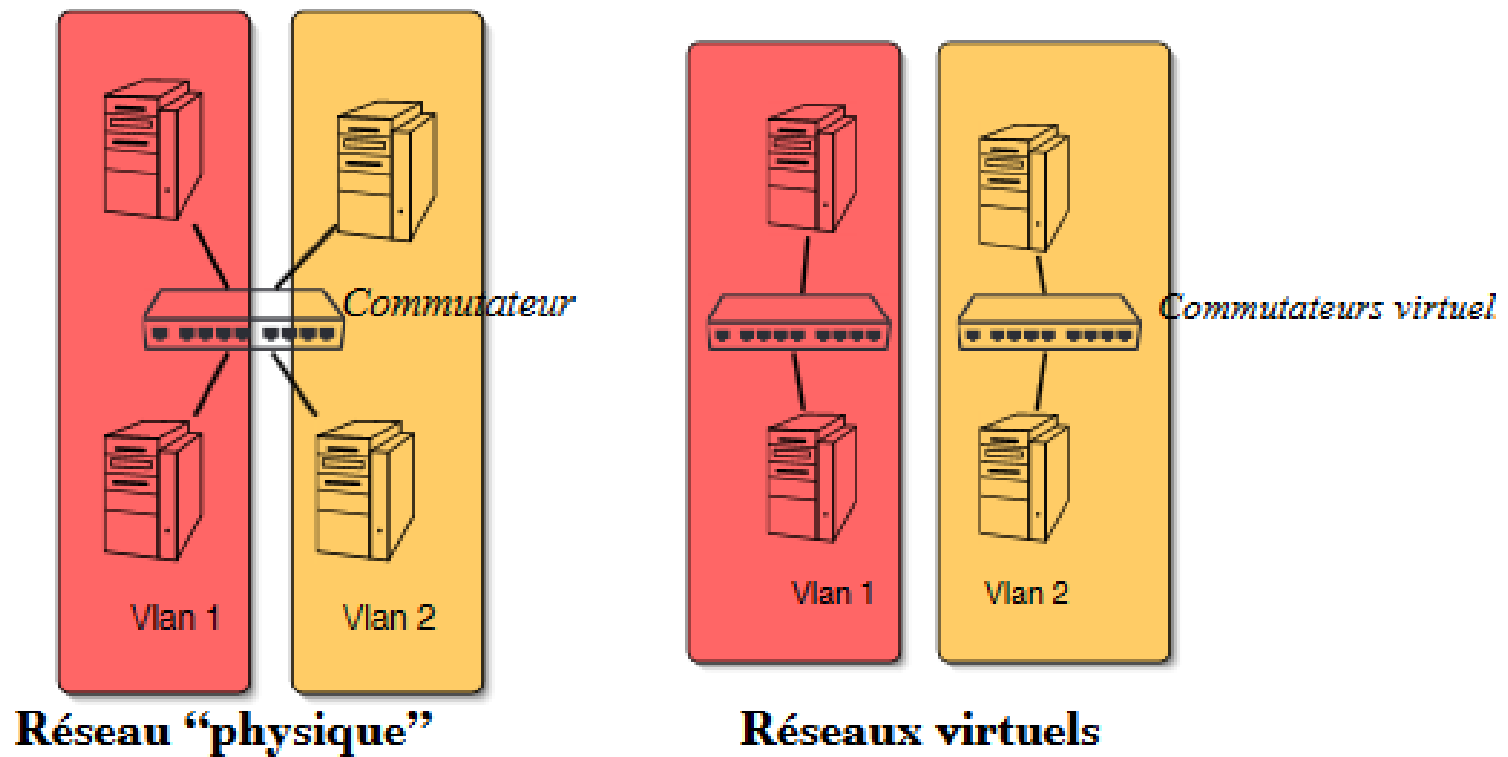


Algorithme de l'arbre recouvrant (spanning tree ou STP ou 802.1d)

- Trouver un arbre recouvrant un graphe quelconque pour éliminer les boucles
- Une fois l'arbre déterminé, les ponts désactivent certains ports
- Construction de l'arbre:
 - Basé sur les identificateurs des ponts (adresse Ethernet ou autres)
 - » Racine : identificateur le plus grand
 - Echange de paquets spéciaux (BGPDU: Bridge Protocol Data Unit) entre les ponts contenant les informations permettant de déterminer la racine et le chemin vers la racine
 - Mise à jour périodique de ces informations pour d'éventuelles modifications de topologie

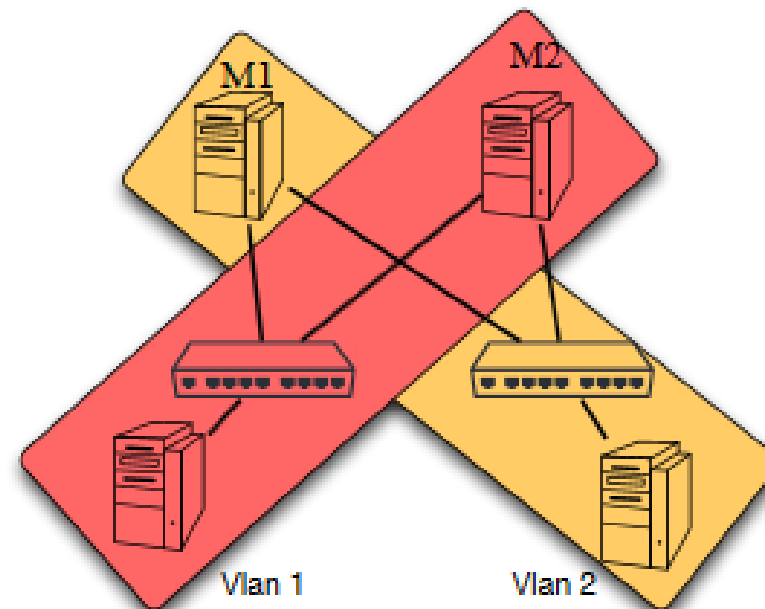
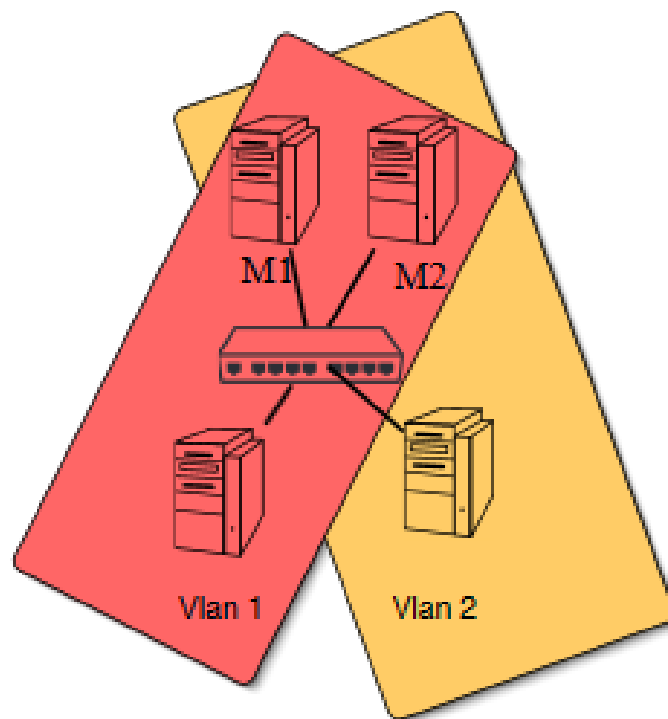
Exemple de VLAN

- Deux VLANs sur un commutateur



Exemple de VLAN

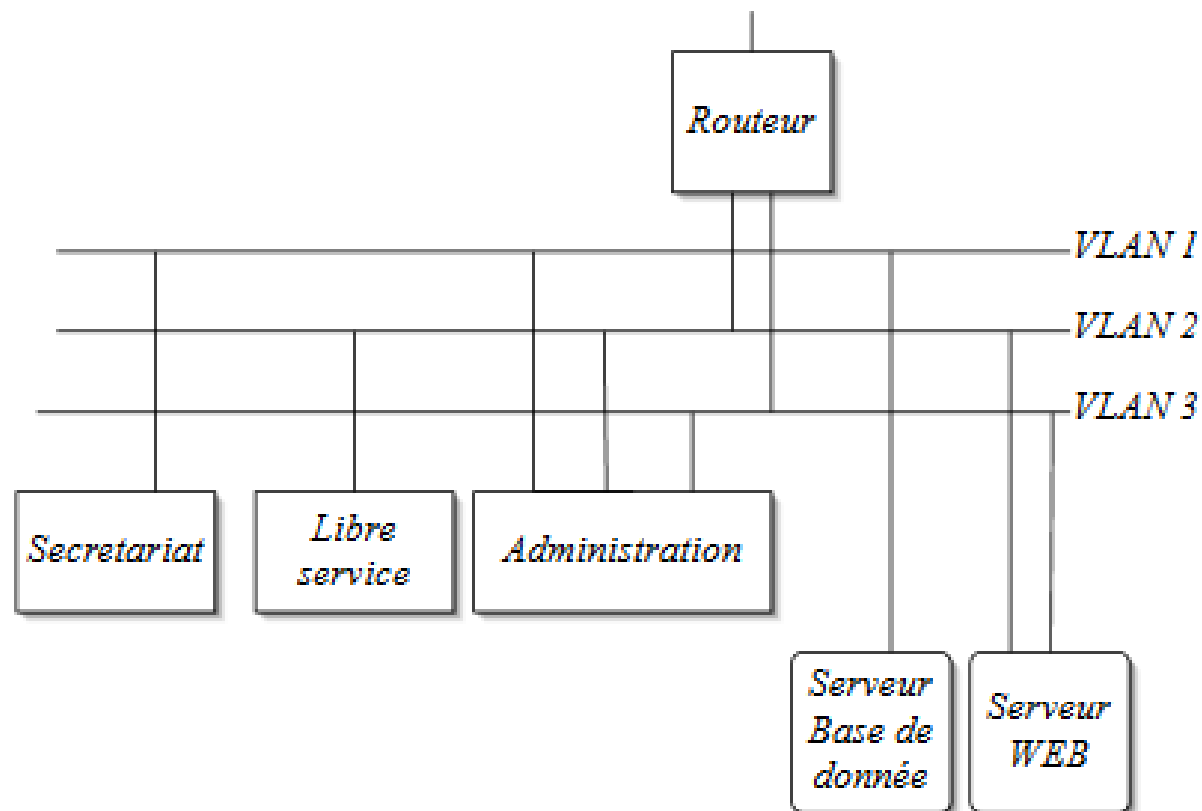
- Une machine peut appartenir à plusieurs VLANs



Réseaux “virtuels”

Exemple d'administration

- Suivant le type d'utilisateur, de l'accès aux serveurs et à l'extérieur

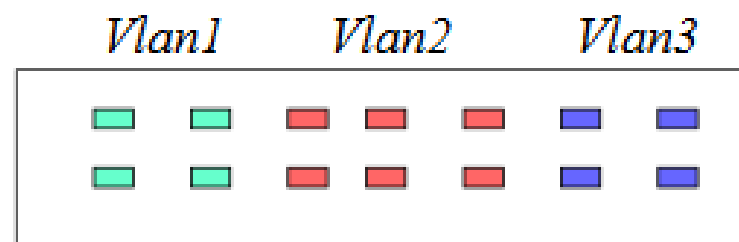


Définitions de VLANs

- Plusieurs techniques pour définir un VLAN:
 - Ports physiques des commutateurs
 - Adresse MAC des ordinateurs
 - Adresse IP des ordinateurs
 - Protocole Réseaux
- Dans tous les cas : cela définit l'appartenance de chaque port du commutateur à un ou plusieurs VLANs (table dans le commutateur)
- A la réception d'une trame sur un port, la trame n'est re-émise que sur le (ou les) port (associé à l'adresse MAC destination) qui appartient au même VLAN
- Dans le cas d'une adresse destination broadcast, la trame est re-émise sur tous les ports appartenant au même VLAN

Définition de VLANs A l'aide des ports du commutateur

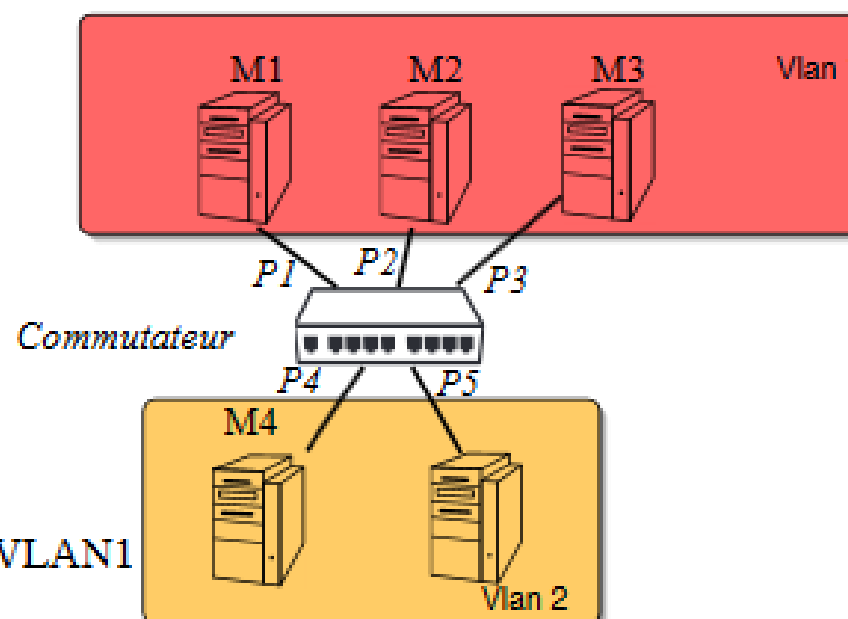
- On associe un numéro de VLAN à chacun des ports du commutateur
- Effectué par l'administrateur sur le commutateur
- Le plus simple et le plus sûr mais "statique"
- La définition du VLAN ne dépend que de la configuration du commutateur (un utilisateur ne peut pas la changer)



Ports du commutateurs

Exemple de configuration de VLANs A l'aide des ports du commutateur

- Dans le commutateur
 - Port VLAN
 - P1 1
 - P2 1
 - P3 1
 - P4 2
 - P5 2
- Sur M1 : ping M4
 - Paquet ARP request diffusé seulement sur VLAN1
 - Donc pas de réponse



Définition de VLANs Par les adresses MAC

- Dans le commutateur il faut remplir une table (Adresse Mac, VLAN)
 - L'association (port,VLAN) se fait à l'aide des premiers paquets portant l'adresse MAC source
- **Plus souple** (nouveaux utilisateurs, portables, changement des branchements)
 - On peut changer la liaison ordinateur/commutateur et appartenir toujours au même VLAN
- **Moins sûr:**
 - L'utilisateur peut changer de VLAN puisque l'on peut changer une adresse MAC sur une machine !
- **Plus lourd** : connaissance des adresses MAC par l'administrateur

Définition de VLANs Par les adresses IP

- Dans le commutateur il faut remplir une table (Adresse IP réseau, VLAN)
 - L'association (port, VLAN) se fait à l'aide des premiers paquets portant l'adresse IP source
- **Moins sûr:**
 - l'utilisateur peut changer d'adresse IP
- **Moins performant:**
 - Analyse des entêtes IP
- Peu conventionnel : indépendance des couches
- Plus simple pour l'administrateur :
 - Peut se faire à partir du plan d'adressage IP
- Souvent appelé VLAN par sous-réseau

Définition de VLANs Par le protocole réseau

- Dans le cas où plusieurs protocole réseau sont utilisés (IPX, IP, Apple Talk ...)
- On associe un VLAN suivant le protocole Réseau

Exemple de configuration de VLANs

- Dans le commutateur 1:

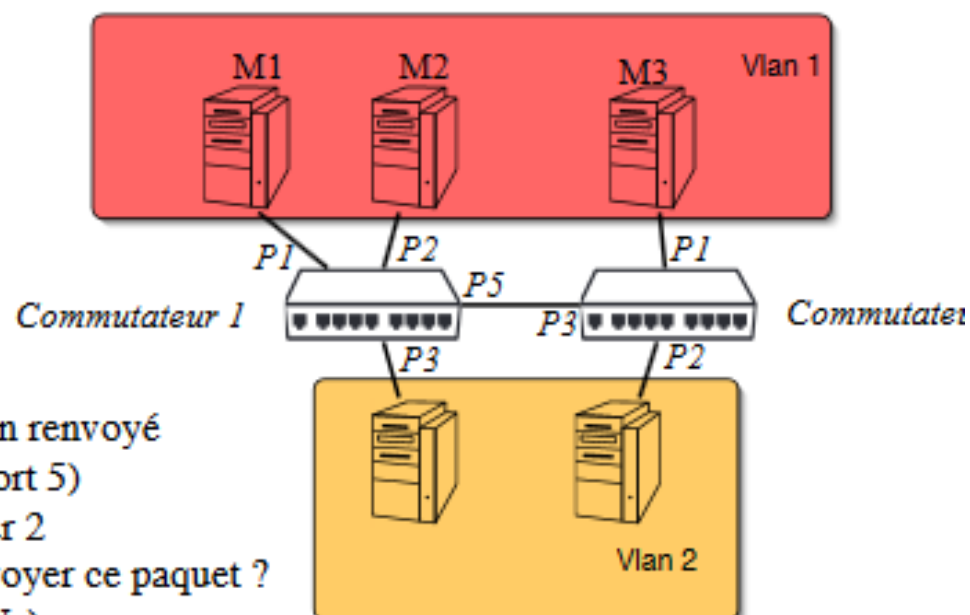
- PORT VLAN
- P1 1
- P2 1
- P3 2
- P5 1, 2

- Dans le commutateur 2:

- PORT VLAN
- P1 1
- P2 2
- P3 1, 2

- Problème :

- Sur M1: ping M3
- Le paquet ARP request est bien renvoyé sur le commutateur 2 (par le port 5)
- Mais comment le commutateur 2 peut il savoir sur quel port renvoyer ce paquet ? (P3 est associé aux deux VLANs)

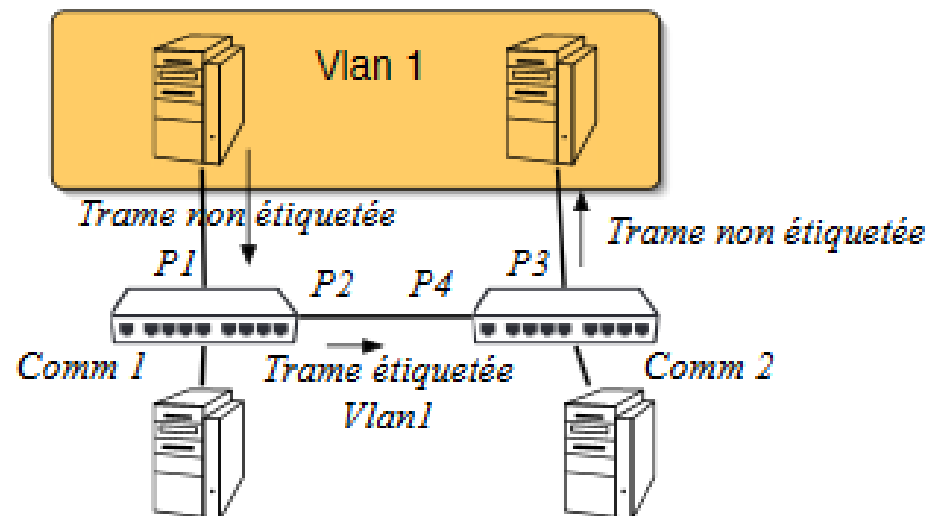


Etiquetage des trames

- Dans le cas précédent on peut résoudre le problème
 - en ajoutant l'association (Adresse MAC, VLAN) dans les commutateurs
 - le commutateur 2 peut savoir ainsi à quel VLAN doit être renvoyé une trame à l'aide de l'adresse MAC source incluse dans l'entête du paquet
 - l'association VLAN/Ports et VLAN/Adresse MAC à faire sur tous les commutateurs devient laborieuse
- On peut aussi mettre deux liaisons physiques entre les deux commutateurs et associés leurs deux ports à un seul des deux VLANs
- Idée d'amélioration : il faut que le paquet porte le numéro de VLAN dans son entête
- On parle alors de VLAN “étiqueté” (tagged) ou “informé”

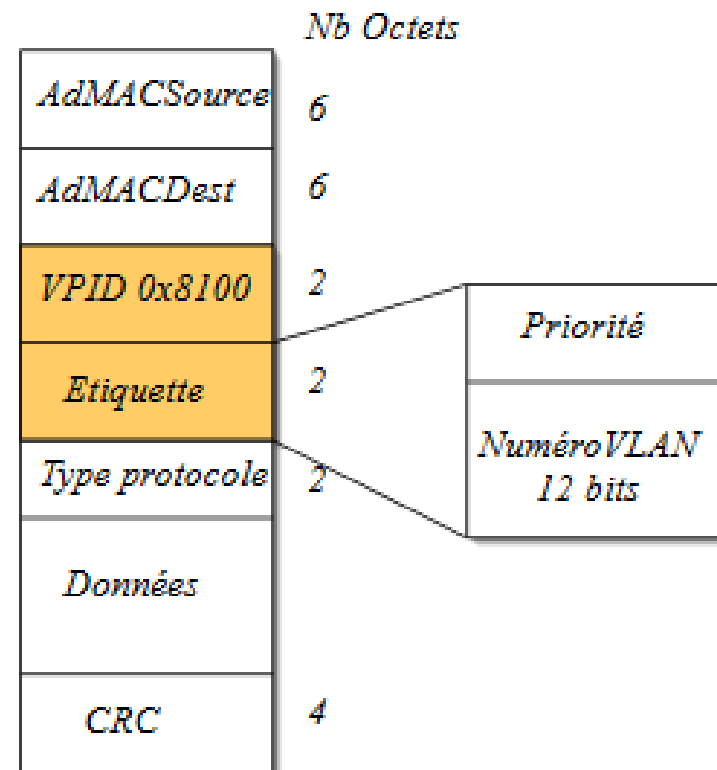
Exemple de VLAN étiqueté

- L'étiquetage des trames indiquant le numéro de VLAN auquel elle appartient peut se faire
 - Dans les machines (carte Ethernet compatible 802.1Q)
 - Seulement dans les commutateurs le cas échéant
- Exemple d'étiquetage des trames dans les commutateurs
 - sur M1 : ping M2



Format frame 802.1Q

- VPID : identifie une trame 802.1Q
- VID(VLAN Identifier): numéro de VLAN
- Gestion de priorités (ou COS Class Of services) : 3 bits possible : norme 802.1p (indépendant des VLAN)

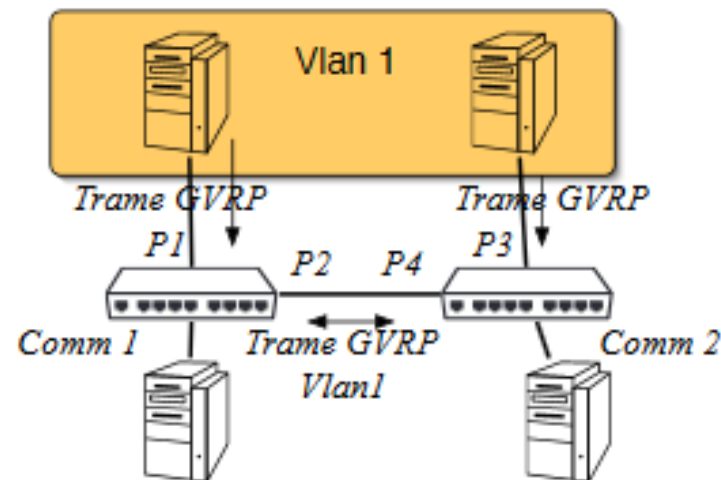


VLAN dynamique

- VLAN “statique”: la définition des VLANs pour tous les ports se fait “à la main” dans les commutateurs (table port/VLAN)
 - Dans le cas de port *multiVLAN*, les commutateurs doivent étiqueter les trames en fonction du port source de la trame
- Possibilités de configuration automatique de certains ports à l’aide de l’étiquetage
 - On parle de VLAN “dynamique”
 - L’association des ports aux VLANs peut être fait à l’aide du protocole GVRP (GARP VLAN Registration Protocol)
 - On peut mélanger les associations statiques (par exemple pour les ports branchés aux machines) et dynamique (pour les ports inter-commutateur)

Exemple de VLAN dynamique

- GVRP tourne sur les deux machines et les deux commutateurs
- On associe aux machines le VLAN 1
- GVRP va propager à l'aide de trame particulière l'appartenance à ce VLAN sur les commutateurs
- L'information sera propagée entre les commutateurs
- Les ports des commutateurs seront ainsi associés automatiquement au VLAN 1



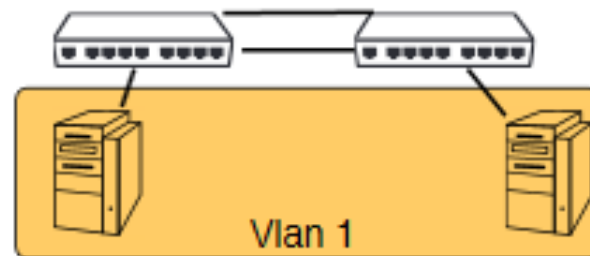
Dans la pratique

- On peut définir sur un commutateur
 - Des ports “non étiquetés” (relié au machines). Ces ports ne peuvent appartenir qu’à un seul VLAN
 - Des ports étiquetés (inter-commutateur ou vers des machines compatibles 802.1Q). Ils peuvent appartenir à plusieurs VLANs
- Certains commutateurs n’autorisent que l’association (port, VLAN)
- L’association automatique port/VLAN (protocole GVRP) peut être implémentée ou pas dans les commutateurs

Autres possibilités dans les commutateurs “administrables”

- Groupement de ports (ports *trunking*)
- On peut augmenter les performances entre 2 commutateurs en groupant plusieurs ports
- Il faut que les ports appartiennent au même VLAN
- Le lien virtuel comportent ainsi plusieurs liens physiques
- L'émission des trames est partagée entre les ports groupés
 - En fonction de l'adresse source des paquets (toujours le même lien)
 - En fonction des adresses source et destination

2 liens groupés et associés au Vlan1



Dans la pratique sur les machines

Exemple de configuration d'une interface virtuelle sous Debian :

Création des VLANs

```
vconfig add eth0 10
```

Activation de l'interface physique et des sous-interfaces réseau

```
ifconfig eth0 up
```

```
ifconfig eth0.10 up
```

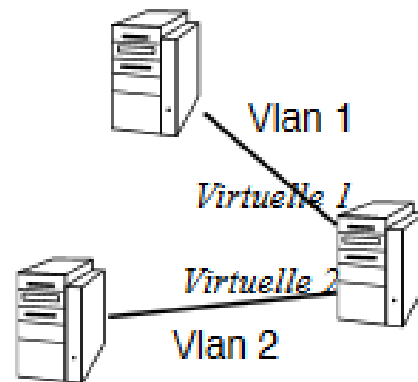
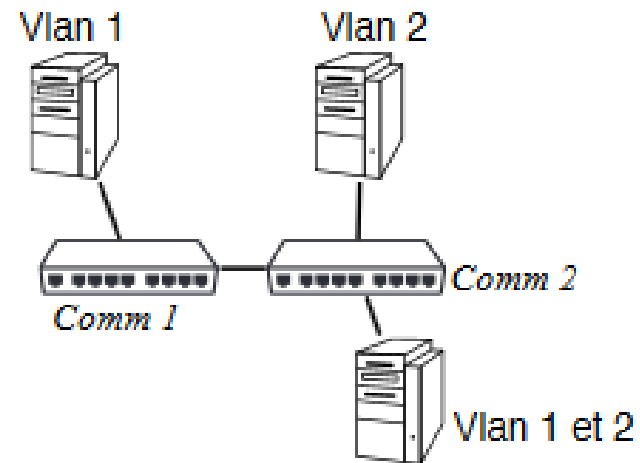
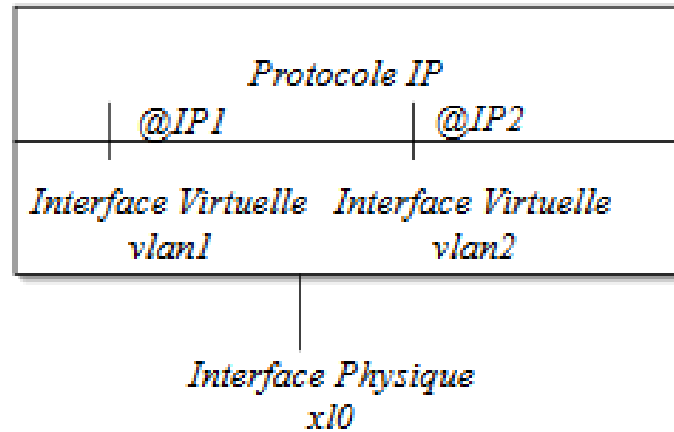
Affectation d'une adresse IP à chaque sous-interface

```
ifconfig eth0.10 172.17.10.254/24
```

Plusieurs d'interfaces virtuelles peuvent être associées à une même interface physique

Chaque interface virtuelle doit avoir une adresse IP différentes

Exemple



Autres possibilités dans les commutateurs “administrables”

- **Port miroir (Mirroring)**
 - On peut définir un port particulier permettant d’observer le trafic passant par un certains nombres d’autres ports
 - Pratique pour l’administration
- **Restriction des adresses MAC**
 - on peut limiter l’accès à un port du commutateur
 - on définit sur pour chaque port l’adresse MAC de la (ou les) machines qui peuvent être branché sur ce port
 - Sécurité faible: changement possible des adresses MAC sur les machines