



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE



Administration réseau et sécurité : *Les VLAN*

Denis Pugnère

CNRS / IN2P3 / IPNL

d.pugnere @ ipnl.in2p3.fr



Les principes

- Longtemps on a introduit des routeurs pour séparer domaines logiques des réseaux :
 - Diminution du domaine de « broadcast »
 - Filtrage de niveau 3 entre les stations : complexité du routage, affectation d'adresses de niveau 3
 - Coûts assez élevé en matériels
 - Câblage complexe, brassage des prises réseau
 - Problématique de l'interconnexion d'utilisateurs éloignés
 - Charge d'administration importante
 - Problème de mobilité des postes
- Idée : construire un réseau logique sur un réseau physique, mais indépendant de l'architecture du réseau physique
- Notion de réseau virtuel





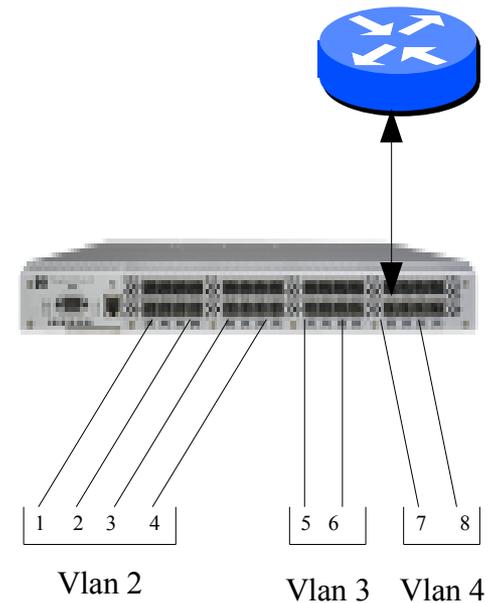
Le fonctionnement

- Utilisation commutateur manageable (pas hub, ni switch non manageable) pour segmenter (créer des sous-réseaux) :
 - Ces sous-réseaux ne peuvent pas communiquer entre eux
 - Chaque élément de chaque sous-réseau peut avoir une adresse de niveau 3.
 - Chaque élément de chaque sous-réseau DOIT avoir une adresse de niveau 3 pour communiquer en dehors de son sous-réseau
 - Passage obligatoire par un élément de routage pour sortir
 - Possibilité de filtrage des flux entre sous-réseaux
- Principes de segmentation
 - VLAN par ports
 - VLAN par adresse MAC
 - VLAN de niveau 3
 - VLAN par utilisateurs



VLAN par port

- 1 port = 1 VLAN
- 1 table de correspondance dans le commutateur entre les ports et les VLAN
- Configuration simple, mais statique
- Implémentation la plus répandue



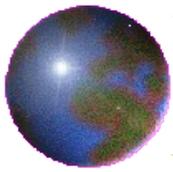
Forwarding Database

VLAN	Port
2	1,2,3,4
3	5,6
4	7,8



VLAN par adresse MAC

- Appartenance à un VLAN en fonction de l'adresse MAC de l'élément
- Le commutateur consulte une table de correspondance entre les Adresses MAC et le VLAN
- Plusieurs VLAN possibles par port du commutateur
- Nécessité de gérer une table d'adresses MAC (peut devenir complexe)
- Degré de confiance limité dans les adresses MAC des machines. NB = il est possible de modifier l'adresse MAC de chaque PC (windows, Linux) ou MacOS...
- Implémentation assez peu répandue : exemple VMPS pour Cisco



VLAN de niveau 3

- Analyse dans les trames de niveau 2 d'informations de niveau 3 (adresses IP, type de protocole...)
- Correspondance dans le commutateur des informations de niveau 3 et les VLAN
- Plusieurs VLAN possibles par port du commutateur
- Gestion intéressante pour les postes nomades
- Mise en oeuvre pas très répandue
- Degré de confiance TRÈS limité dans les adresses IP des machines.



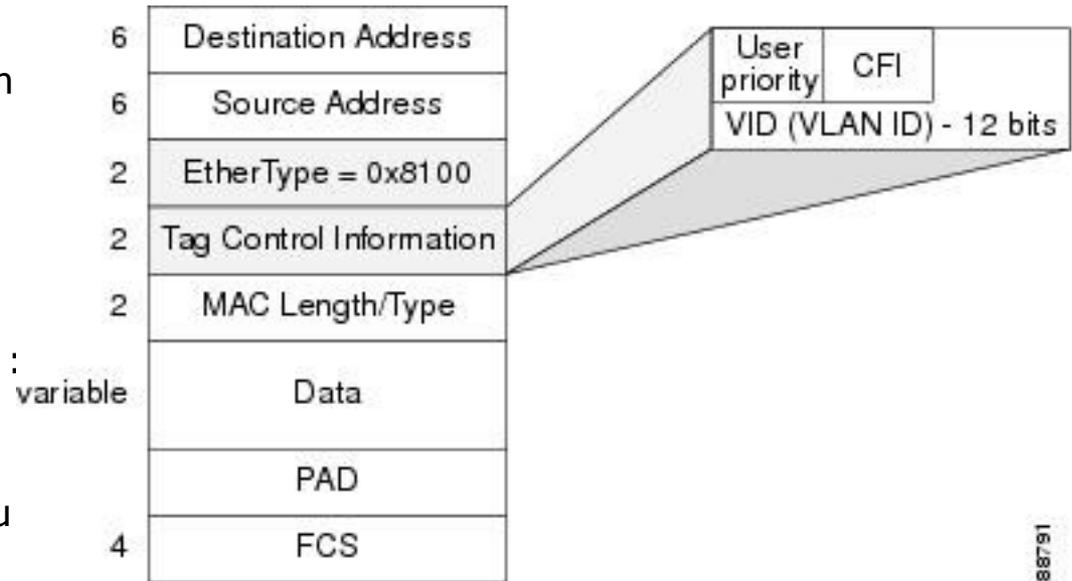
VLAN par utilisateur

- Norme 802.1X : port based network access control
- Utilisation du protocole EAP (Extensible Authentication Protocol) pour transmettre les échanges d'authentification
- Utilisation de serveurs RADIUS et de commutateurs supportant 802.1X : Nécessite que le client supporte le 802.1X
- Modification du poste utilisateur : demande d'authentification réseau lors du démarrage du poste
- Gestion idéale pour les nomades
- On peut utiliser une authentification forte
- Mise en oeuvre peu répandue
- Le degré de confiance repose sur l'utilisateur (identifiants et/ou certificats utilisateurs), couple possible avec le poste (certificat machine).

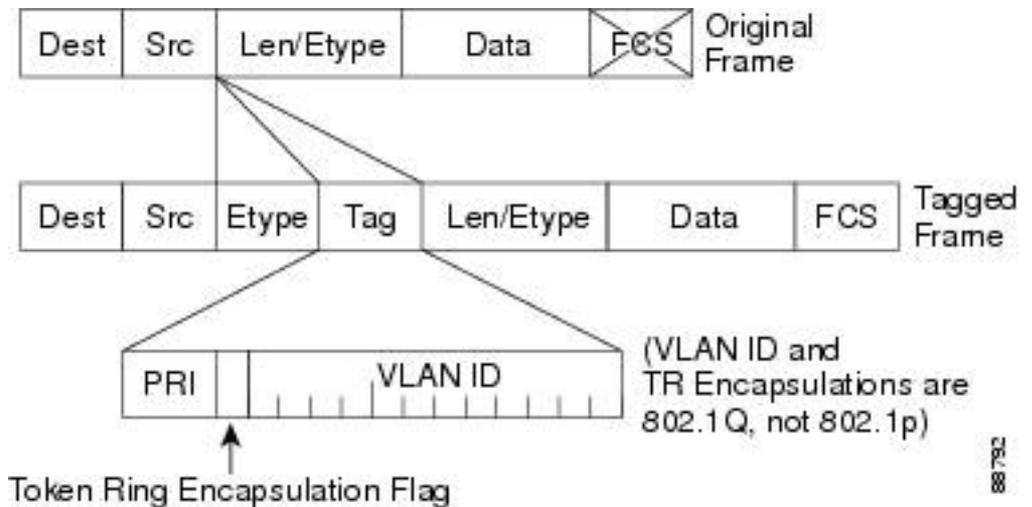


Les standards IEEE 802.1Q et IEEE 802.1p

- Marquage (tagging) des trames : insertion de 4 octets supplémentaires dans la trame Ethernet avec un EtherType spécifique
- Utilisation d'un EtherType = 0x8100
- User priority (802.1p) : 3 bits
- 1 bit de Canonical Format Identifier (CFI) : compatibilité entre les réseaux de type Ethernet et Token Ring.
- 12 bits of VLAN ID (VID) : identification du numéro de VLAN : 4096 VLANs



88791



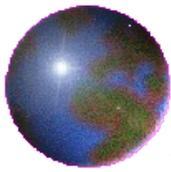
88792



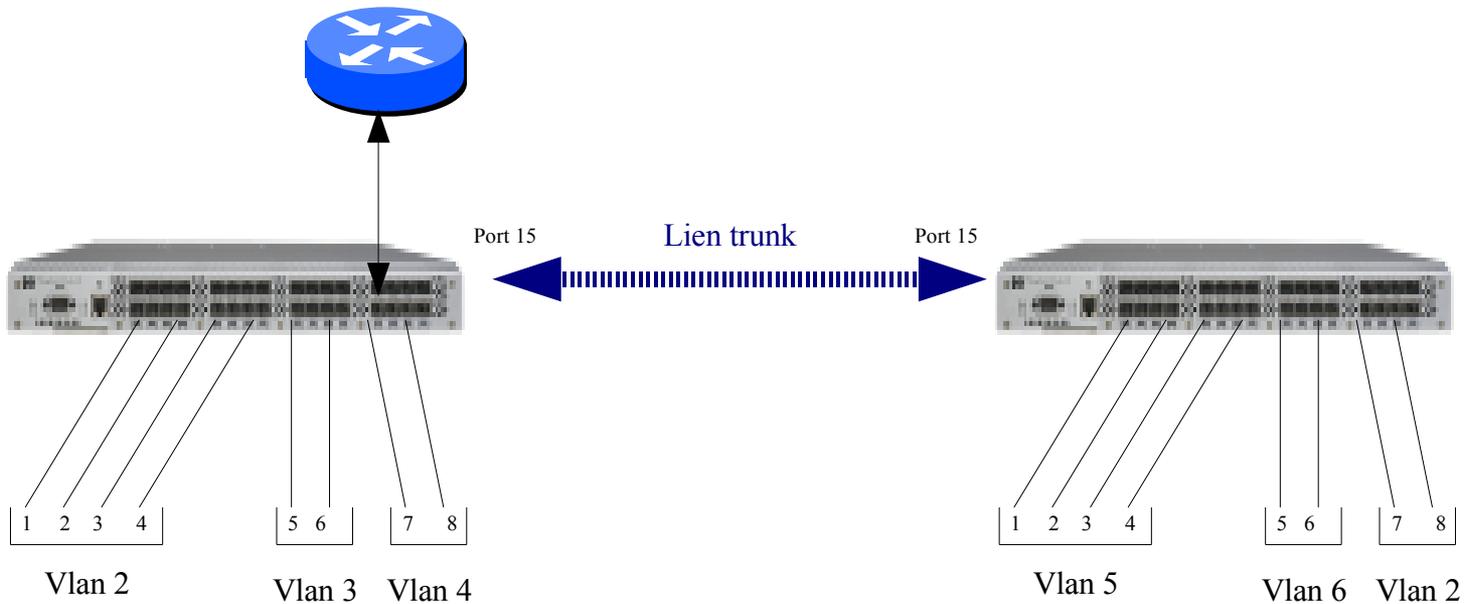


VLAN : les types de liens

- Liens simples : typiquement utilisés par les éléments qui ne supportent pas les VLAN
- Liens Trunk : liens inter-commutateurs transportant des VLAN eux mêmes
- Liens hybrides : liens qui peuvent reconnaître si la connexion distante est de type simple ou de type trunk



Implémentation des VLAN

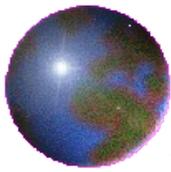


Forwarding Database

VLAN	Port
2	1,2,3,4
3	5,6
4	7,8

Forwarding Database

VLAN	Port
5	1,2,3,4
6	5,6
2	7,8



Conclusion

- Les VLAN proposent une réponse intéressante à la problématique de la séparation de flux sur un réseau
- Mise en oeuvre relativement simple
- Facilite la tâche d'administration (câblage, intervention, évolution du réseau)
- Bien choisir la mise en oeuvre du type de VLAN
- Attention au choix du numéro de VLAN quand on interconnecte des entités administratives différentes
- Le choix de la technologie de VLAN n'est pas neutre sur la sécurité. Chaque implémentation a ses avantages et ses inconvénients. Attribution du numéro de vlan au port ou au client