

Sécurité au niveau de la commutation

I) Utilité

Les informations qui transitent sur les réseaux peuvent être sensibles. L'espionnage industriel peut être un problème qu'il faut anticiper. C'est pourquoi il faut s'assurer que les ressources ne soient pas accessibles par des personnes non autorisées sans empêcher les employés de travailler. Il existe des techniques qui permettent d'augmenter la sécurité sur tous les niveaux des modèles OSI et TCP/IP. Au niveau de la commutation les techniques sont :

- Désactivation de port
- Réserveation d'adresse MAC
- Vlan
- Radius

II) Désactivation de port

Pour éviter les intrusions, la première règle consiste à désactiver les ports non utilisés. De ce fait il y a juste le nombre de port suffisant d'activé pour chacune des connections.

III) Réserveation d'adresse MAC

a) Fonctionnement

Nous avons vu que les switchs utilisent les adresses MAC pour choisir sur quel port envoyer les trames. Avec la réserveation d'adresse MAC, la table de commutation n'est plus dynamique comme nous l'avons vu précédemment. C'est l'administrateur qui renseigne cette table. Si le switch reçoit une trame qui n'est pas déjà dans la table de commutation, le port sera bloqué et une alerte peut être envoyée à l'administrateur.

Pour renseigner la table de commutation, il existe deux méthodes : la méthode statique et la méthode dynamique.

b) Réserveation statique

Avec la réserveation statique, l'administrateur doit relever toutes les adresses MAC des postes de son réseau. Il ajoute une par une les adresses MAC aux tables de commutation de tous les switchs. Cette méthode est longue est fastidieuse, mais elle offre un maximum de contrôle.

c) Réserveation dynamique

Avec la réserveation dynamique, l'administrateur n'est pas obligé de relever toutes les adresses MAC de son réseau. Il lui suffit de spécifier pour chaque port, le nombre d'adresse MAC que le switch devra retenir.

Par exemple : le switch apprendra les 10 premières adresses MAC sur le port 1. A partir de la 11^{ème} adresse, le switch bloquera le port.



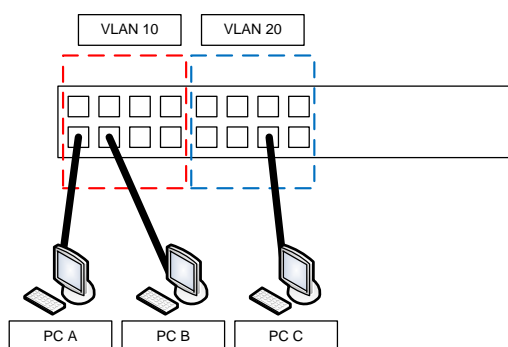
IV) Vlan

a) Fonctionnement

Vlan veut dire Virtual LAN, c'est-à-dire que les ports d'un switch vont être séparés de façon logique. C'est comme s'il y avait plusieurs switches logiques dans un seul switch physique. Seuls les équipements se trouvant dans le même Vlan peuvent communiquer ensemble.

a) Exemple

Sur le schéma suivant les PC A et PC B peuvent communiquer ensemble. En revanche les PC A et B ne peuvent pas communiquer avec le PC C, car ils sont dans des Vlan différents.



b) Utilité

Le fait de séparer logiquement les équipements permet de regrouper les stations par fonction, service, partage de ressource. En séparant logiquement les équipements :

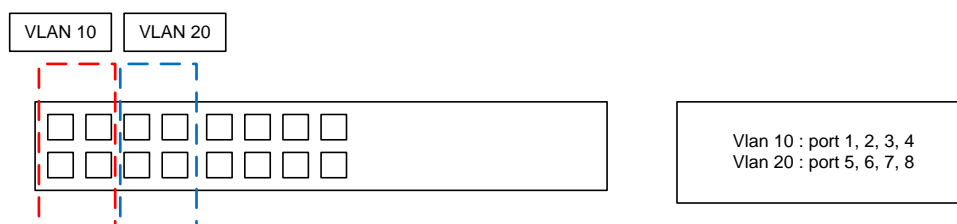
- le réseau est plus sûr car on peut plus facilement contrôler qui accède à quoi.
- cela permet aussi de faire de la segmentation de domaine de Broadcast. Les broadcasts sont cloisonnés dans leurs Vlan.

c) Les différents modes

Il existe différents modes pour l'affectation des Vlan. On peut regrouper ces modes en deux catégories : l'affectation statique et dynamique. L'affectation statique (Vlan de niveau 1) est la plus utilisée car elle apporte un haut niveau de sécurité et une administration simple. L'affectation dynamique (Vlan de niveau 2 et 3) est moins utilisée car elle demande de lourdes configurations.

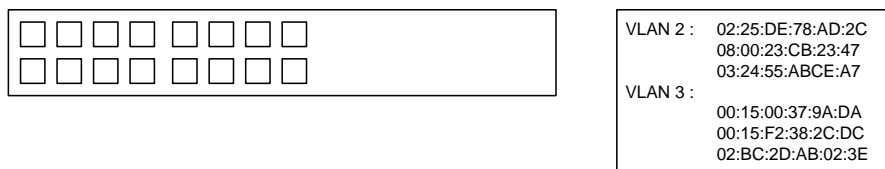
1) Vlan de niveau 1 (Vlan par port)

Les Vlan de niveau 1 sont également appelés VLAN par port ; en anglais *Port-Based VLAN*. Dans ce mode, les vlan sont affectés en fonction du numéro de port.



2) Vlan de niveau 2 (Vlan MAC)

Les Vlan de niveau 2 sont également appelés VLAN MAC, *VLAN par adresse IEEE* ou en anglais *MAC Address-Based VLAN*. Dans ce mode les Vlan sont affectés de manière dynamique en fonction des adresses MAC.



3) Vlan de niveau 3 (Vlan par sous réseau ou Vlan par protocole)

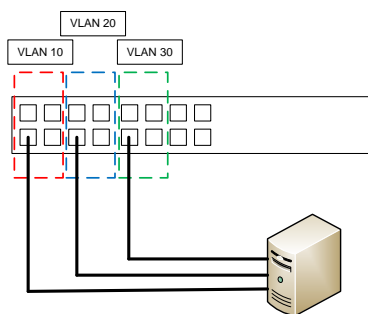
Le **VLAN par sous-réseau** (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce mode augmente la latence, car le switch doit analyser la trame jusque à la couche réseau (couche 3 de OSI).

Le **VLAN par protocole** (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau virtuel.



V) Port Trunk (802.1q)

Nous avons vu qu'avec les Vlan le réseau est segmenté et la communication entre les équipements est impossible. Cela pose des problèmes pour les ressources communes. Les équipements comme les serveurs, routeurs, doivent être joignables par tous les Vlan. La méthode la plus simple consiste à ajouter, sur un serveur par exemple, plusieurs cartes réseaux et câbler chaque carte réseau dans un Vlan différent.

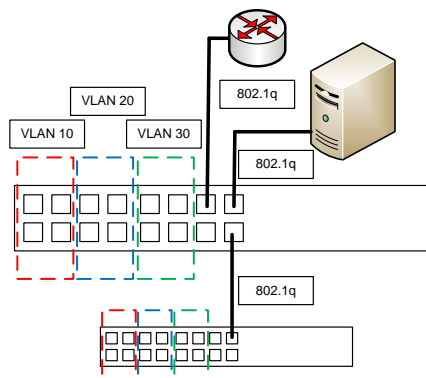


Cette méthode n'est pas envisageable, les coups de câblage seraient exorbitants. C'est pourquoi un protocole a été créé. Ce protocole est le 802.1q, il permet de communiquer avec tous les Vlan. Le 802.1q permet d'ajouter à la trame une information indiquant de quel Vlan elle provient.



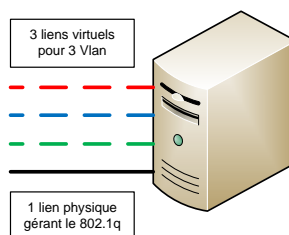
a) Utilisation du 802.1q

Le protocole 802.1q est utilisé à chaque fois qu'une ressource doit être accessible à partir de tous les Vlan.



b) 802.1q sur les serveurs ou les routeurs

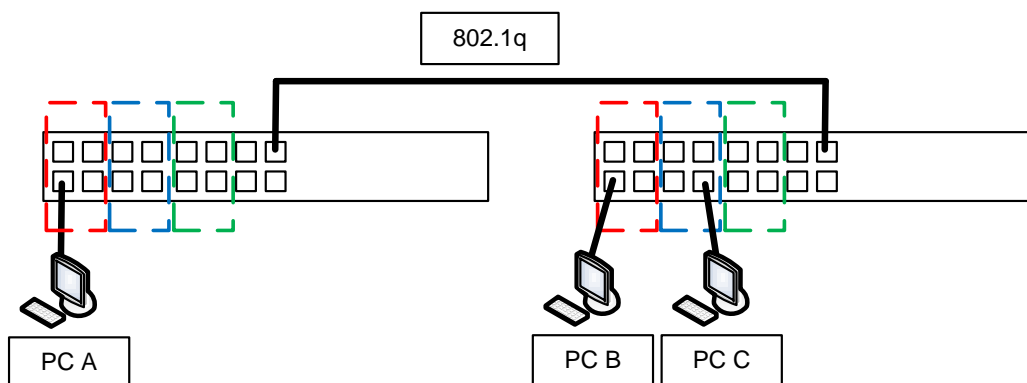
Quand on utilise le 802.1q sur une ressource commune comme un serveur ou un routeur, il faut créer sur ces équipements des cartes virtuelles. Chaque carte virtuelle est associée à un seul Vlan.



Grâce au 802.1q, le serveur est branché sur le réseau avec un seul câble. Mais le serveur est capable de communiquer avec les ressources de tous les Vlan.

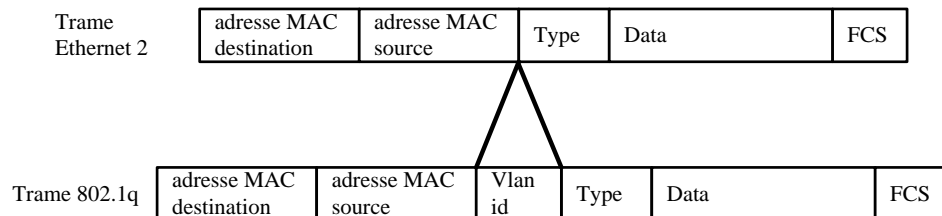
c) Le 801.q sur les switch

On peut également utiliser le protocole 802.1q pour la communication entre plusieurs switches. Dans l'exemple suivant le PC A peut communiquer avec le PC B, mais il ne peut pas communiquer avec le PC C.



d) Constitution d'une trame 802.1q

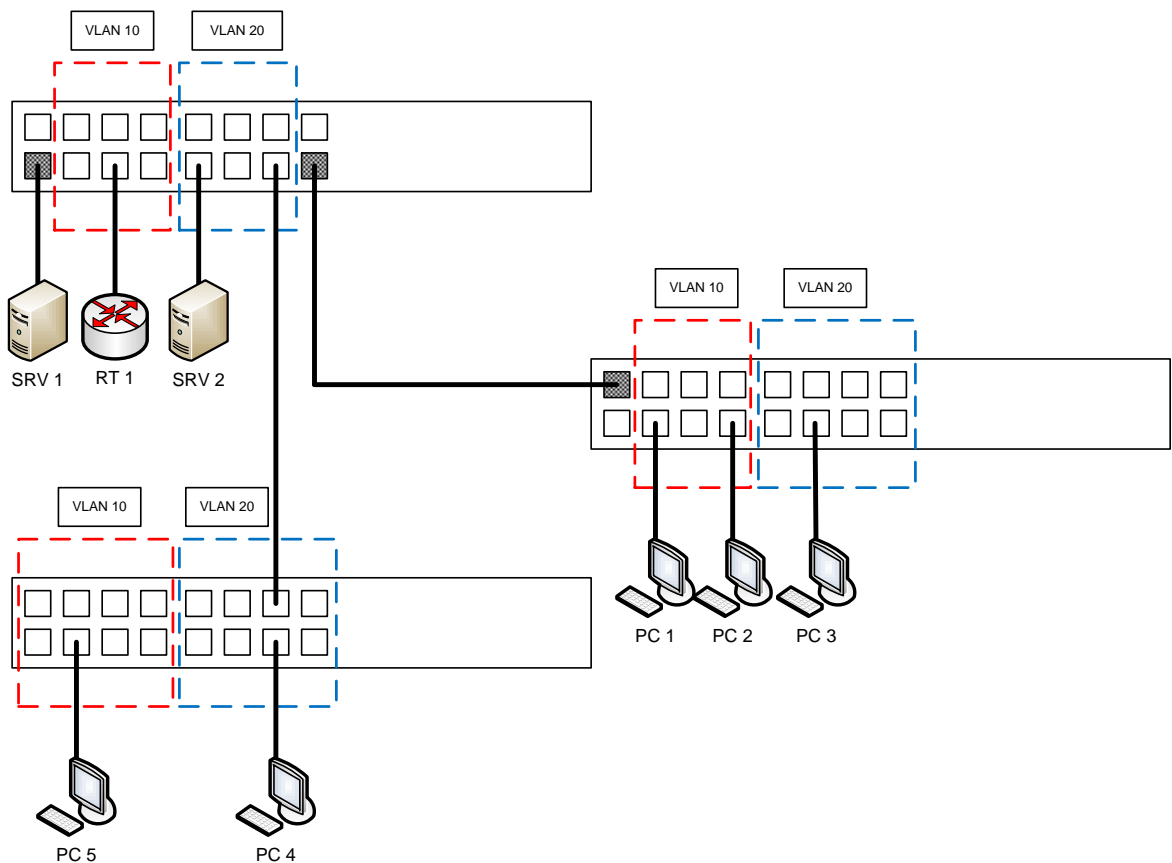
Une trame 802.1q est très semblable à une trame Ethernet 2. Elle comporte aussi les adresses MAC source et destination, le type de protocole de la couche supérieure, les données, et le contrôle appelé FCS. La trame 802.1q comporte un champ supplémentaire. Ce champ est appelé « Vlan id ». Il est de 12 bits et sert à identifier le Vlan auquel appartient la trame. Il est possible de coder 4096 Vlan avec ce champ.



VI) Exercice

a) Schéma

Remarque : sur le schéma, les ports grisés sont Taggé (802.1q)



b) Question

D'après le schéma précédent, placez une croix quand la communication est possible entre deux équipements réseau. Exemple : Le PC 1 peut communiquer avec le serveur SRV 1

	RT 1	SRV 2	SRV 1	PC 5	PC 4	PC 3	PC 2
PC 1			X				
PC 2							
PC 3							
PC 4							
PC 5							
SRV 1							
SRV 2							

