

Les VLAN

L'objectif de ce cours est de découvrir le fonctionnement et l'utilité d'un **VLAN** (**Virtual LAN**).

Le contexte

Vous êtes à nouveau contacté(e) par la société de services dont vous avez accompagné le développement.

Les besoins

La SSII occupe toujours deux bâtiments voisins. Plusieurs catégories de personnels (développeurs, commerciaux, comptables...) cohabitent à l'intérieur des bâtiments, éventuellement aux mêmes étages. La SSII souhaiterait pouvoir :

- Segmenter son réseau pour que ses employés aient uniquement accès aux ressources nécessaires. Par exemple, les développeurs n'auraient accès qu'aux ressources techniques (code source, documentation...), et pas aux ressources administratives (appels d'offre, fiches de paye...).
- Faire en sorte que des employés appartenant à la même catégorie de personnel mais travaillant dans des étages ou des bâtiments distincts aient accès aux mêmes ressources et puissent collaborer.

Elle vous sollicite pour proposer une solution technique à ses besoins.

Les solutions possibles

Les machines d'un LAN Ethernet sont traditionnellement reliées au moyen de concentrateurs (*hubs*) ou de commutateurs (*switchs*).

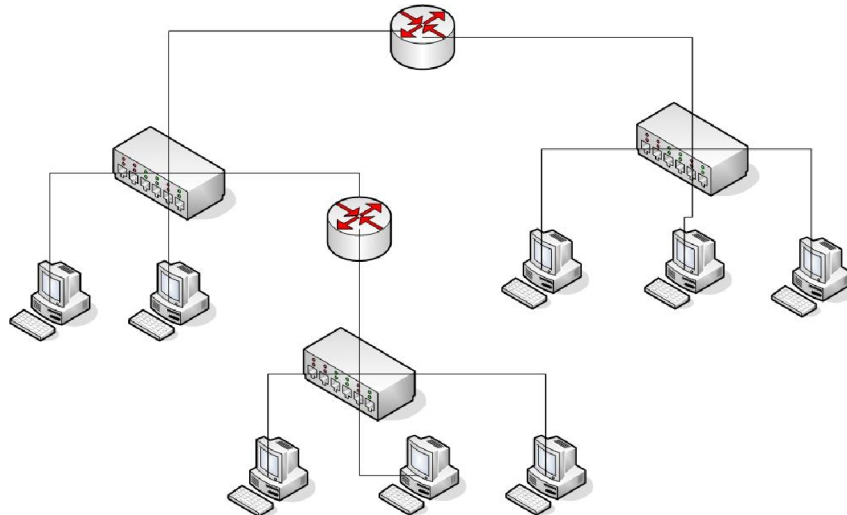
Rappelez les principaux inconvénients d'un concentrateur.

- **Gaspillage de bande passante (diffusion systématique).**
- **Nombre de collisions important qui augmente avec la taille du réseau.**

L'apparition des commutateurs a permis d'améliorer sensiblement le fonctionnement des LAN :

- Commutation des trames en fonction de leur adresse **MAC**.
- Création d'un domaine de **collision** par port.
- Mode **full-duplex** qui augmente les performances.
- Gestion des boucles et de la redondance (protocole **spanning tree**).

Malgré tout, les commutateurs classiques délimitent un seul domaine de **diffusion**. Toutes les machines interconnectées reçoivent donc le trafic de diffusion (ARP, DHCP, NetBios...), ce qui peut poser des problèmes de performance ou de sécurité. Comment faire pour segmenter un LAN en plusieurs réseaux indépendants ? Une solution possible est d'utiliser des **routeurs**. Cependant, ces matériels entraînent une gestion lourde et obligent à regrouper les postes en fonction de leur disposition physique, comme dans l'exemple ci-dessous.



Ces solutions répondent-elles aux besoins exprimés par la SSII ?

Non, elles ne permettent pas une segmentation du réseau indépendante de sa disposition physique.

Les besoins exprimés nécessitent donc de mettre en oeuvre une autre technologie : les **VLAN** ou réseaux locaux virtuels.

Découverte des VLAN

Les VLAN par port

Dans un VLAN par port (également appelé VLAN de niveau **1**), chaque port du commutateur est affecté statiquement à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par le port du commutateur auquel la carte réseau est connectée.

Lorsque le commutateur reçoit une trame sur un port, il parcourt sa table **port / VLAN** pour associer la trame à un VLAN. Il analyse ensuite l'adresse du destinataire et parcourt sa table **MAC / port** pour retrouver le port associé à cette adresse :

- Si le port est trouvé et qu'il appartient au VLAN de la trame, elle est **émise sur ce port**.
- Si le port est trouvé mais qu'il n'appartient pas au VLAN, la trame est **ignorée**.
- Si le port n'est pas trouvé, la trame est **diffusée sur tous les ports associés au VLAN**.

Que faire quand on désire déplacer physiquement une machine (la brancher sur un autre port du commutateur) ?

Il faut désaffecter son port du VLAN puis affecter le nouveau port au bon VLAN.

Que faire quand on désire déplacer logiquement une machine (la changer de VLAN) ?

Il faut modifier l'affectation du port au VLAN.

Il est possible de répartir des VLAN de niveau 1 sur plusieurs commutateurs. Dans ce cas, les trames qui circulent entre les commutateurs sont **marquées** afin d'identifier le VLAN auquel elles appartiennent. Les commutateurs sont reliés par des ports particuliers (ports **802.1q**) qui leur permettent d'ajouter et de retirer les "marques". Le lien entre les commutateurs sur lequel les trames circulent marquées est parfois appelé lien "trunk" (*trunk link*).

Les VLAN par adresse MAC

Dans un VLAN par adresse MAC (également appelé VLAN de niveau **2**), chaque adresse MAC est affectée à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par son **adresse MAC source**. Après une phase d'apprentissage, chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse MAC de la carte réseau qui y est connectée.

Lorsque le commutateur reçoit une trame sur un port, il parcourt sa table **MAC / VLAN** pour associer la trame à un VLAN en fonction de l'adresse MAC de l'expéditeur. Il met ensuite à jour sa table **MAC / port** pour cette adresse puis, si l'association **port / VLAN** n'existe pas, il la crée. Le commutateur analyse aussi l'adresse destinataire de la trame :

- Si l'adresse MAC appartient au même VLAN que l'émetteur et que l'association MAC / port **existe**, il transmet la trame sur le port.
- Si l'adresse MAC appartient au même VLAN que l'émetteur et que l'association MAC / port **n'existe pas**, il diffuse la trame sur tous les ports associés au VLAN.
- Si l'adresse destinataire n'appartient pas au même VLAN que l'émetteur, il ne transmet pas la trame.

Remarque : une fois la table port / VLAN constituée, un VLAN de niveau 2 fonctionne exactement de la même manière qu'un VLAN de niveau 1.

Que faire quand on désire déplacer physiquement une machine ?

Son adresse MAC ne changeant pas, elle appartient toujours au même VLAN après son déplacement.

Que faire quand on désire déplacer logiquement une machine ?

Il faut modifier l'association MAC / VLAN.

Comme pour les VLAN de niveau 1, la répartition de VLAN de niveau 2 sur plusieurs commutateurs se fait grâce à l'utilisation de ports 802.1q pour marquer les trames qui circulent entre les commutateurs. Le partage des tables MAC / VLAN de chaque commutateur n'est pas nécessaire.

Les VLAN par adresse IP

Dans un VLAN par adresse IP (également appelé VLAN de niveau **3**), chaque carte réseau est affectée à un VLAN en fonction de son adresse IP. L'appartenance d'une trame à un VLAN est déterminée par l'**adresse IP** du paquet véhiculé (le commutateur doit donc accéder à ces informations au niveau **3** du modèle OSI). **Après une phase d'apprentissage**, chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse IP de la carte réseau qui y est connectée.

Que faire quand on désire déplacer physiquement une machine ?

Sa configuration IP ne changeant pas, elle appartient toujours au même VLAN après son déplacement.

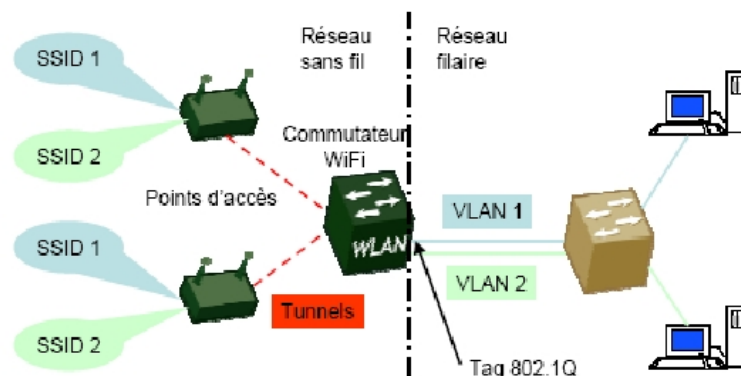
Que faire quand on désire déplacer logiquement une machine ?

Il faut modifier sa configuration IP.

Avec cette méthode, on crée souvent un VLAN par sous-réseau IP en définissant les masques de sous-réseau adaptés. Elle permet d'utiliser des **commutateurs** à la place des **routeurs** comme éléments d'interconnexion.

Autres types de VLAN

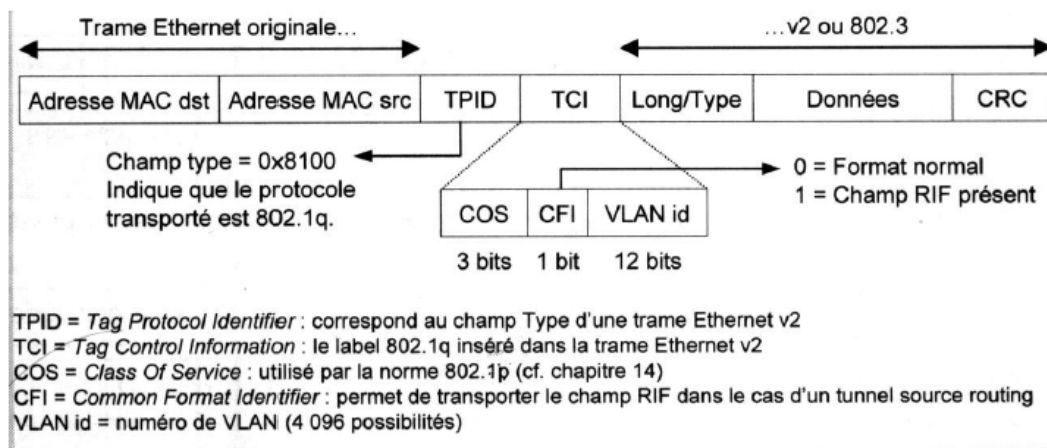
Il est également possible (quoique moins fréquent) définir des VLAN par protocole. Avec cette méthode, une trame est affectée à un VLAN en fonction du protocole qu'elle transporte (IP, IPX, AppleTalk...). L'explosion du sans-fil a conduit à l'apparition de VLAN par **SSID** (identifiant de réseau Wifi).



Fonctionnement d'un VLAN

Marquage des trames

Tous les types de VLAN reposent sur l'utilisation d'un protocole commun, nommé **802.1q**. Ce protocole permet d'identifier le VLAN auquel appartient une trame. Il attribue à chaque trame un code d'identification VLAN (TCI, *Tag Control Information*), parfois appelé étiquette. L'en-tête de la trame est donc modifié par rapport au format Ethernet classique.



Une trame n'a qu'un seul identifiant de VLAN (VLAN id ou VID) et ne peut donc appartenir qu'à un seul VLAN. Sauf cas particulier, une carte réseau est associée à un VLAN et ne communique qu'avec les machines de ce VLAN.

Un commutateur interconnecte plusieurs machines éventuellement situées dans des VLAN différents. Il identifie le VLAN auquel appartient une trame grâce au protocole 802.1q. Il échange les trames avec d'autres commutateurs via des ports d'interconnexion (parfois appelés ports *trunk*). Un port de commutateur n'est associé qu'à un seul VLAN, à l'exception des ports d'interconnexion.

Communication entre VLAN

Le principe d'un VLAN est de segmenter un réseau local en plusieurs domaines de diffusion étanches, ce qui rend impossible la communication entre machines situées sur des VLAN différents.

Il existe deux solutions pour partager des ressources ou échanger des données entre VLAN :

- Ajouter un **routeur** (comme entre deux LAN classiques).
- Utiliser une machine dotée de plusieurs cartes réseau, chacune située sur un VLAN différent.

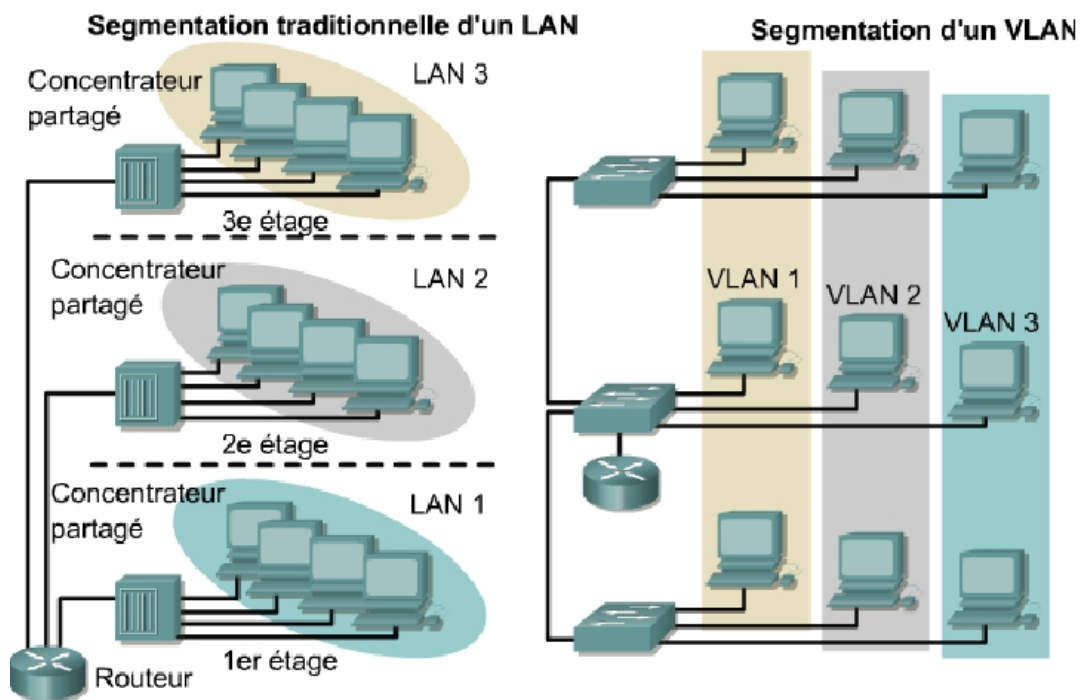
Conclusion

Rôle des VLAN

Un VLAN permet de segmenter un réseau local en plusieurs réseaux isolés correspondant à des domaines de **diffusion** différents.. Ces réseaux sont indépendants de l'emplacement physique des noeuds du réseau, c'est pourquoi on parle de LAN **virtuel**. On peut affecter une machine d'un VLAN à l'autre sans pour autant devoir la déplacer physiquement.

Intérêts des VLAN

Imaginons une entreprise installée dans un immeuble de trois étages. Le 1er étage gère le marché français, le deuxième le marché européen et le 3ème le reste du monde. En utilisant des VLAN, cette entreprise pourrait définir plusieurs LAN virtuels regroupant des postes appartenant à plusieurs étages. Exemple : un VLAN pour la production, un VLAN pour le marketing et un VLAN pour la comptabilité.



Quels sont les intérêts des VLAN ?

- **Segmentation d'un LAN indépendamment de la disposition physique des machines.**
- **Diminution du trafic de diffusion.**
- **Meilleure sécurité.**

Choix du type de VLAN

Les méthodes de construction des VLAN doivent donc déterminer la façon dont le commutateur va associer une trame à un VLAN. Il existe trois grandes méthodes de construction d'un VLAN qui travaillent à des niveaux différents du modèle OSI :

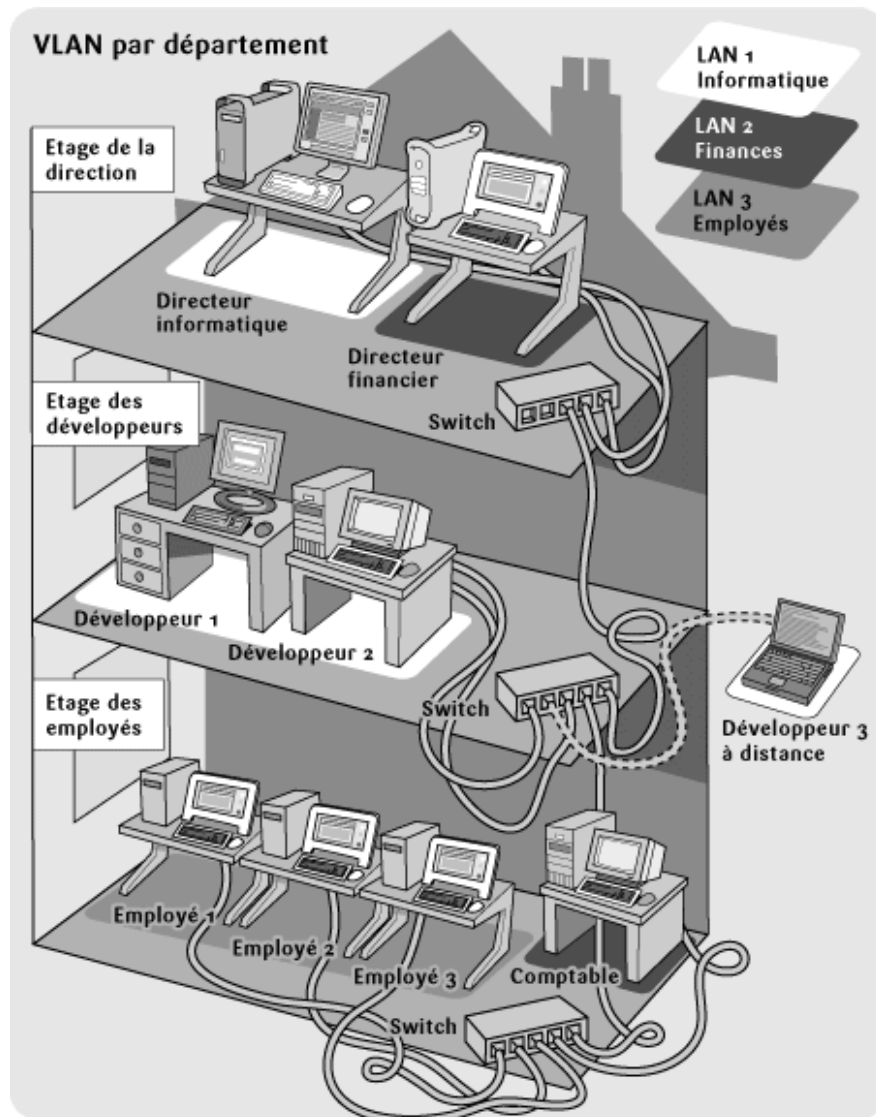
- Les VLAN par **port**, ou de niveau 1.
- Les VLAN par **adresse MAC**, ou de niveau 2.
- Les VLAN par **adresse IP**, ou de niveau 3.

Chaque technique a ses avantages et ses inconvénients. Par exemple, les VLAN de niveau 2 sont bien adaptés aux machines nomades (ordinateurs portables).

Application

La mise en place de VLAN est une solution efficace aux besoins de la SSII.

- L'utilisation de commutateurs gérant les VLAN lui permettra de segmenter son réseau par catégorie d'utilisateurs.



- Le regroupements d'utilisateurs entre plusieurs bâtiments est possible en utilisant des commutateurs VLAN reliés par des liens *trunk*.

