Badji Mokhtar University Annaba
Electronics Department

Chapter 2: VLAN (1)

Contact:
seifallah.nasri@univ-annaba.org

November 06, 2018 Annaba, Algeria

Lecture Purposes

L’objectif de ce chapitre est de présenter les réseaux locaux virtuels (Virtual Local Area Network –VLAN). C’est à dire la segmentation des réseaux permise par les commutateurs, une segmentation qui n’est plus physique mais uniquement logique

Principes d’un Vlan et leur méthode de construction

Présenter la norme 802.1q qui définit les principaux concepts mis en œuvre.

Introduction

- Les réseaux Ethernet sont sujets à divers problèmes affectant les performances du réseau, à savoir :

- Les collisions
- La latence des équipements réseaux
- La remise de données de type broadcast

- Le but de la segmentation sur un LAN est d'obtenir:

- Une réduction de la taille des domaines de collision afin d'économiser la bande passante disponible,
- Une réduction de la taille des domaines de diffusion afin d'améliorer la sécurité et de diminuer la taille des réseaux (notion de sous-réseaux

Introduction

Il est possible de recourir à trois types de segmentation des domaines de collisions:

✓ Segmentation par pont

Segmentation du domaine de collision en 2 grâce au pont, dispositif de couche 2 permettant un filtrage des trames en fonction des adresses MAC des hôtes

✓ Segmentation par routeur

Segmentation du domaine de broadcast en fonction des adresses réseau de couche 3

✓ Segmentation par commutateur:

Segmentation du domaine de collision par la mise en place de chemins commuté entre l'hôte et le destinataire (micro segmentation)

Pour quoi les VLANs

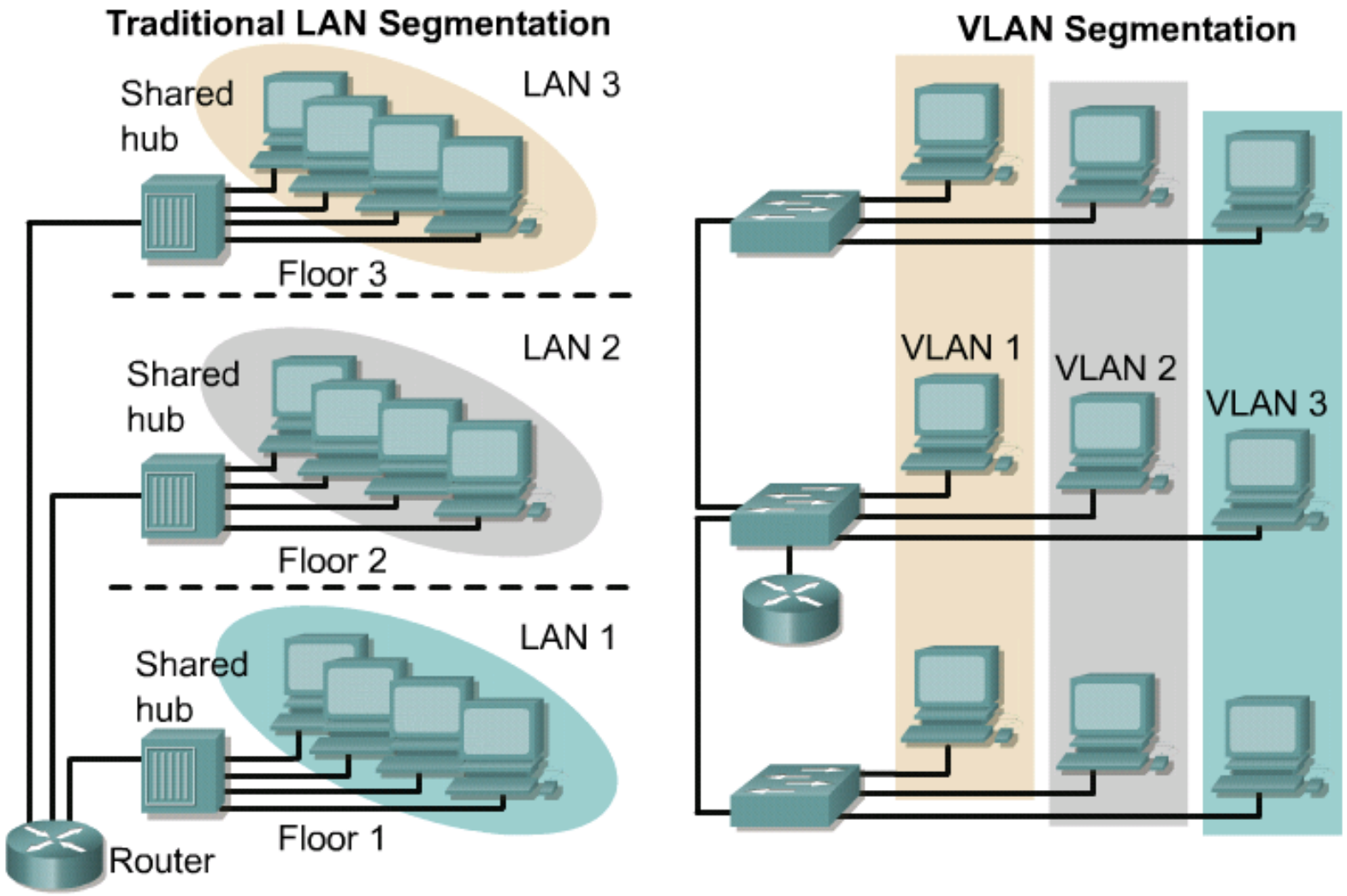
- Avec les concentrateurs et les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion.

- Si l'interconnexion du réseau repose sur les commutateurs et non sur les routeurs (ce qui est de plus en plus le cas) cela pose deux problèmes :

les trames de diffusion sont propagées sur tout le réseau, or ces trames sont nombreuses (ARP, DHCP, .etc.).

En mettant une carte réseau en 'mode promiscuité ' (Promiscuous mode) on peut capturer ces trames (Ce mode est une fonctionnalité généralement utilisée pour écouter le trafic réseau)

- La séparation et la sécurité des domaines de diffusion exigeaient, avant l'apparition des Vlans, une séparation géographique des domaines de diffusion et une interconnexion par routeur


Traditional LAN Segmentation
Shared hub
LAN 3
Floor 3
LAN 2
Shared hub
Floor 2
LAN 1
Shared hub
Floor 1
Router
VLAN Segmentation
VLAN 1
VLAN 2
VLAN 3

Principe

- Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.
- Les VLAN améliorent les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits.
- Si un périphérique d'un VLAN envoie une trame Ethernet de diffusion, tous les périphériques du VLAN la reçoivent, mais pas les périphériques d'autres VLAN.

- Les VLAN n'ont été réalisables qu'avec l'apparition des commutateurs (switchs). Avant, pour réaliser des domaines de diffusion, il était nécessaire de créer des réseaux physiques.

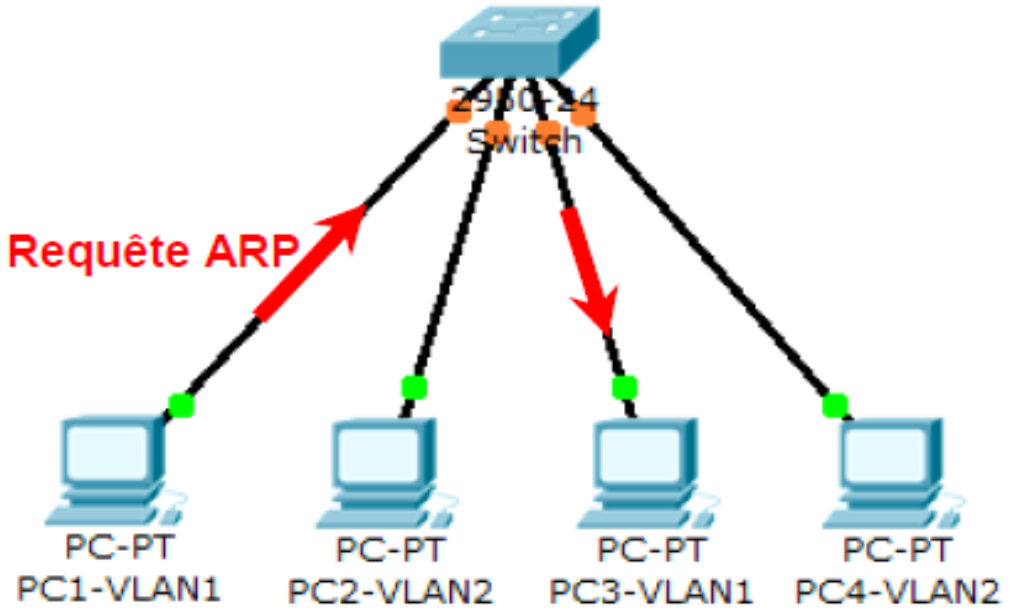
- Les VLAN permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.

- Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique qui prend en charge le routage.

Dans l'exemple ci-dessous, les machines « PC1 à PC4 » sont connectées au même switch sur lequel sont définis deux VLANs : VLAN1 contenant PC1 et PC3, et VLAN2 contenant PC2 et PC4.

Lorsque PC1 émet une trame de diffusion, requête ARP par exemple, celle-ci est transmise uniquement vers les machines du VLAN1, donc ici à PC3.

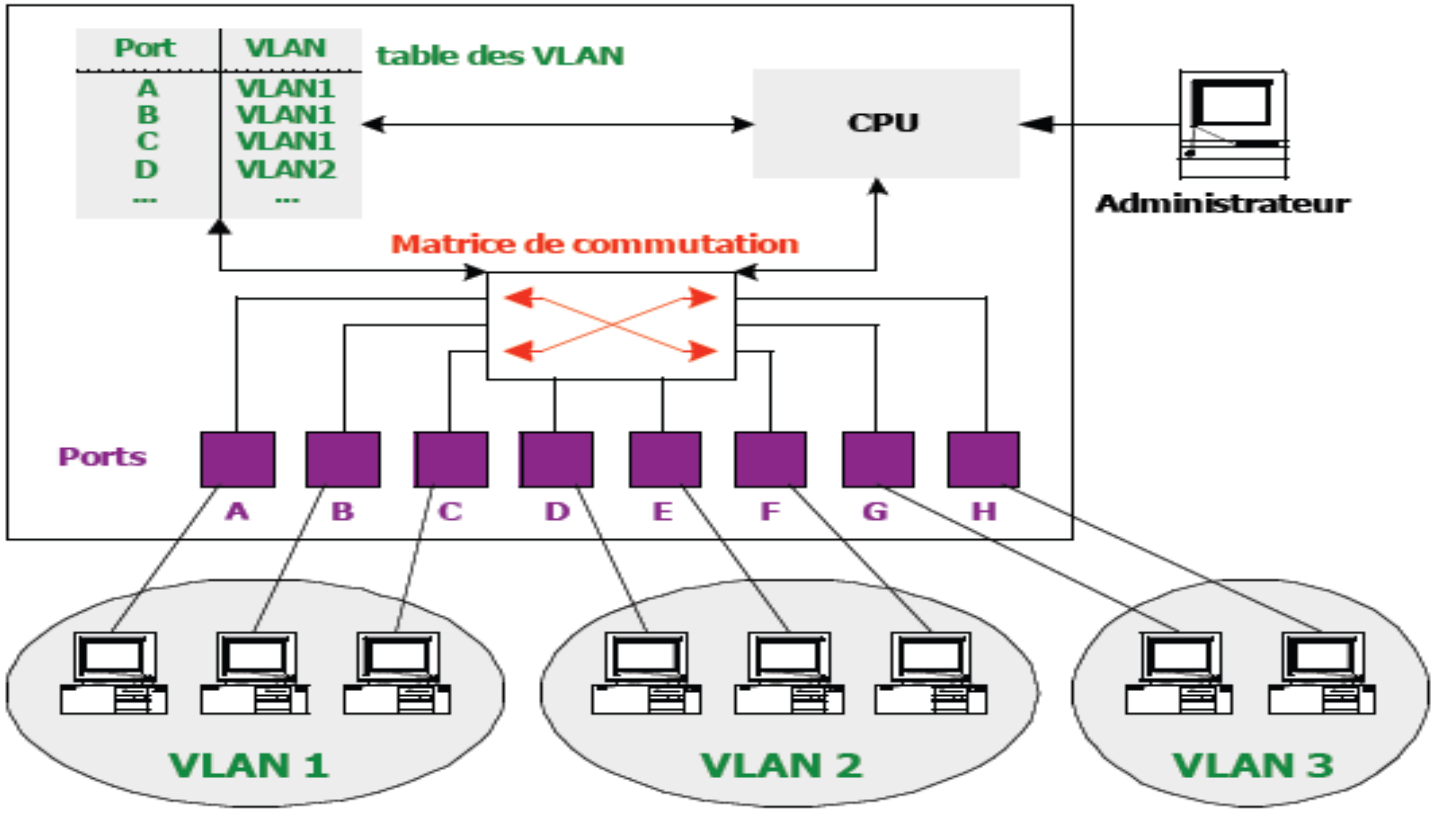
Les machines PC2 et PC4 ignorent le trafic du VLAN1.



Principe VLAN (2)

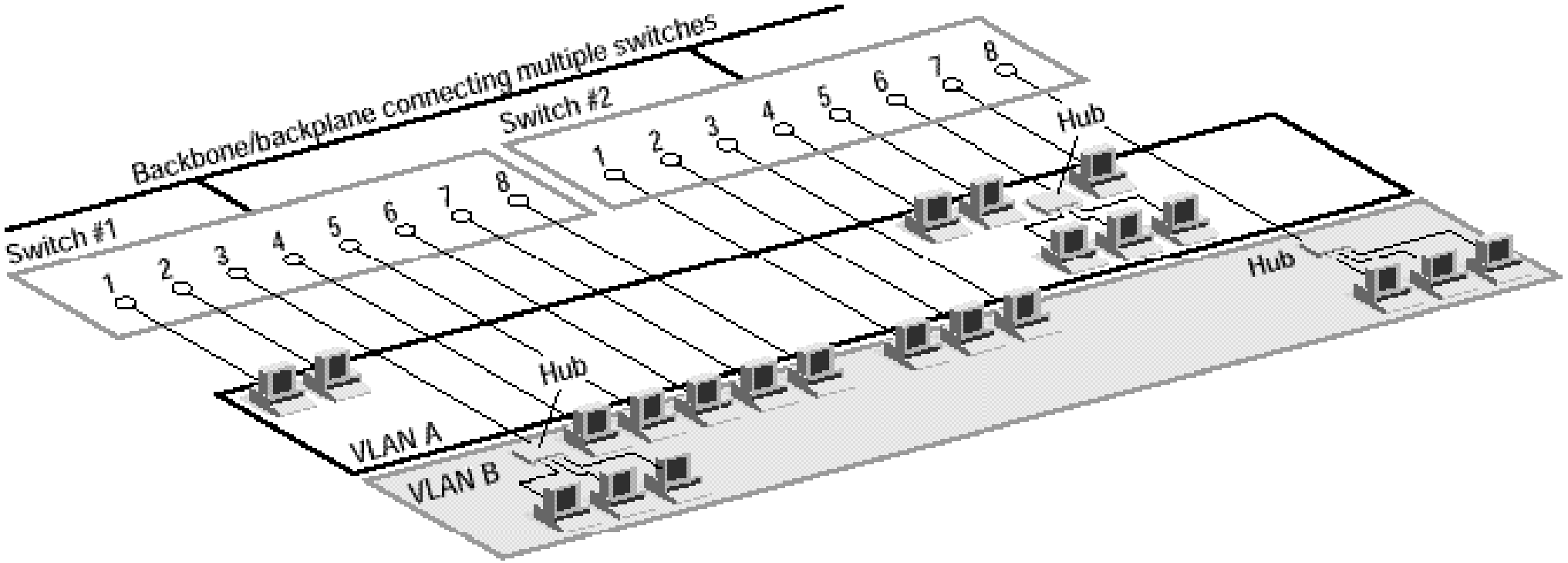
- Il est donc adapté dans ce cas-là de diviser le LAN en unité logique appelés LAN virtuels; cela revient à avoir différent LAN à l'intérieur d'un même LAN physique
- Chaque LAN est identifié par un numéro unique
- Les appareils d'un même VLAN peuvent tous communiquer entre eux, mais pas avec ceux-en-dehors.(L'appartenance à un VLAN étant définie logiquement et non géographiquement)

✓ Une diffusion provenant d'une station du VLAN2 ne sera répercutée que sur les ports D, E, F



Principe VLAN (3)

- L'administrateur configure statiquement la table des VLAN
- Les communications inter-VLAN ne sont possibles qu'à travers un routeur
- L'appartenance à un VLAN est indépendante de la localisation géographique - un VLAN peut s'étendre sur plusieurs commutateurs
- Un segment Ethernet est un domaine de collision
- Un VLAN est un domaine de diffusion



Intérêts des VLANs

- ✓ Confidentialité et sécurité
  - le trafic entre les réseaux virtuels est isolé
  - permet de limiter l'accès à certains équipements ou services (VLAN des machines en libre service, VLAN des accès à Internet, …)
  - Les VLAN permettent la mise en œuvre des stratégies d'accès et de sécurité en fonction de groupes d'utilisateurs précis. Chaque port de commutateur peut être attribué à un seul VLAN
  - Sécurité du réseau améliorée: Un VLAN est une frontière virtuelle, franchissable avec un routeur

- ✓ Performance
  - limite la portée des broadcast (Limiter l'effet des inondations de broadcasts)
  - répartition de la charge du réseau
  - Efficacité de bande passante / utilisation des serveurs: Partage possible d'une même ressource par plusieurs VLAN

Intérêts des VLANs

- ✓ Facilité de mise en œuvre et souplesse
  - logiciel d'administration du commutateur : Modifications logiques ou géographiques facilitées et gérées via une console d'administration plutôt que changer des câbles dans une armoire de brassage
  - on peut retirer ou donner l'accès à un VLAN sans modifier le câblage dans les armoires de brassage, voir sans déplacer la station
  - une station peut appartenir à plusieurs VLANs

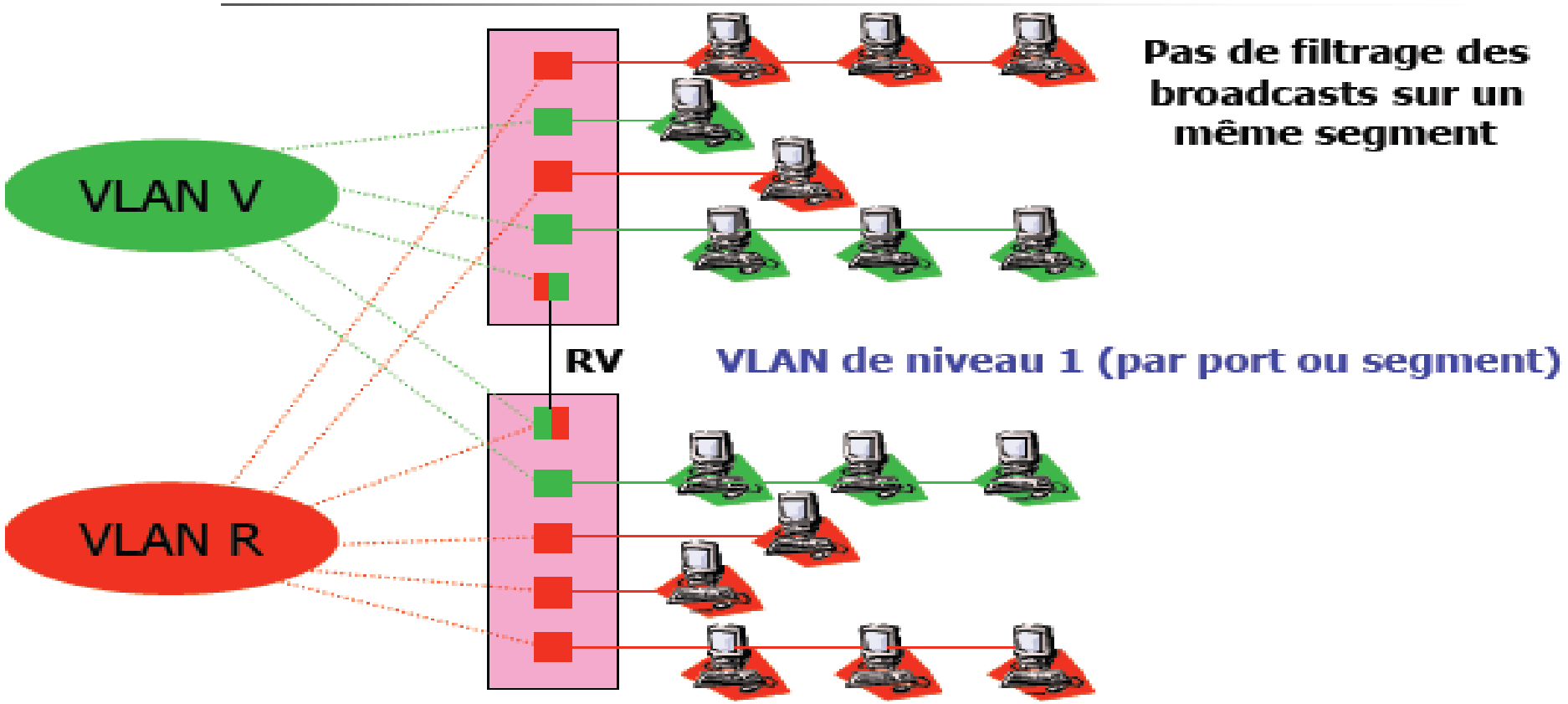
- ✓ Réduction des coûts : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons montantes existantes.

- ✓ Efficacité accrue du personnel informatique : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN.

- ✓ Gestion simplifiée de projets et d'applications : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée.

Appartenance à un VLAN

- ✓ Définie par le port physique du commutateur (niveau 1 :VLAN par Port)
  - chaque port est associé à 1 VLAN
  - configuration statique fixée par l'administrateur
  - sécurisé : un utilisateur ne peut pas changer de VLAN
  - le déplacement d'une station implique son changement de VLAN



Pas d'analyse de la trame pour déterminer l'appartenance à un VLAN

Appartenance à un VLAN

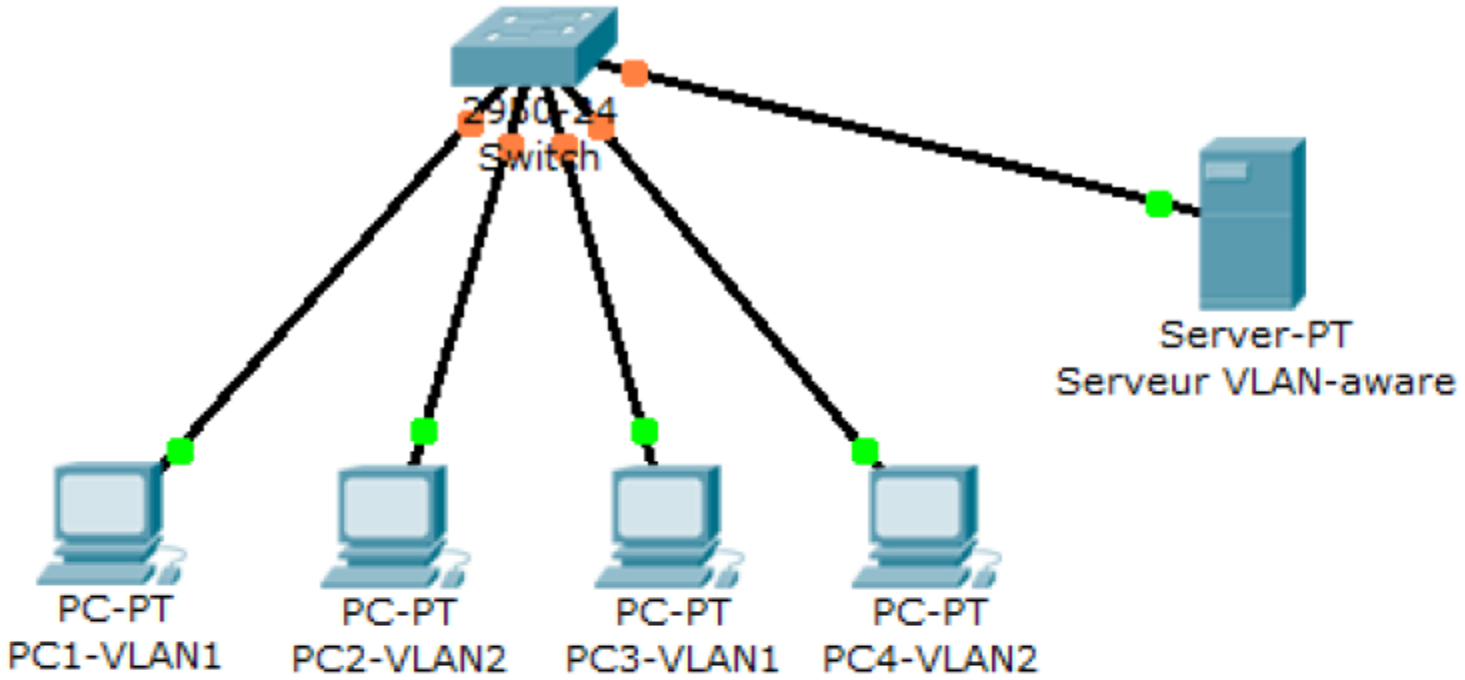


Table	
Port	**VLAN**
1	1
2	2
3	1
4	2
5	1 ; 2

Vlan de niveau 2

- ✓ Définie par l'adresse MAC (niveau2: VLAN MAC) : En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

- Plus souple : permet la mobilité des machines sans reconfigurer les VLAN. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).

- L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

- L'administrateur doit connaître les @ MAC…

- Deux stations du même segment Ethernet peuvent appartenir à des VLAN distincts

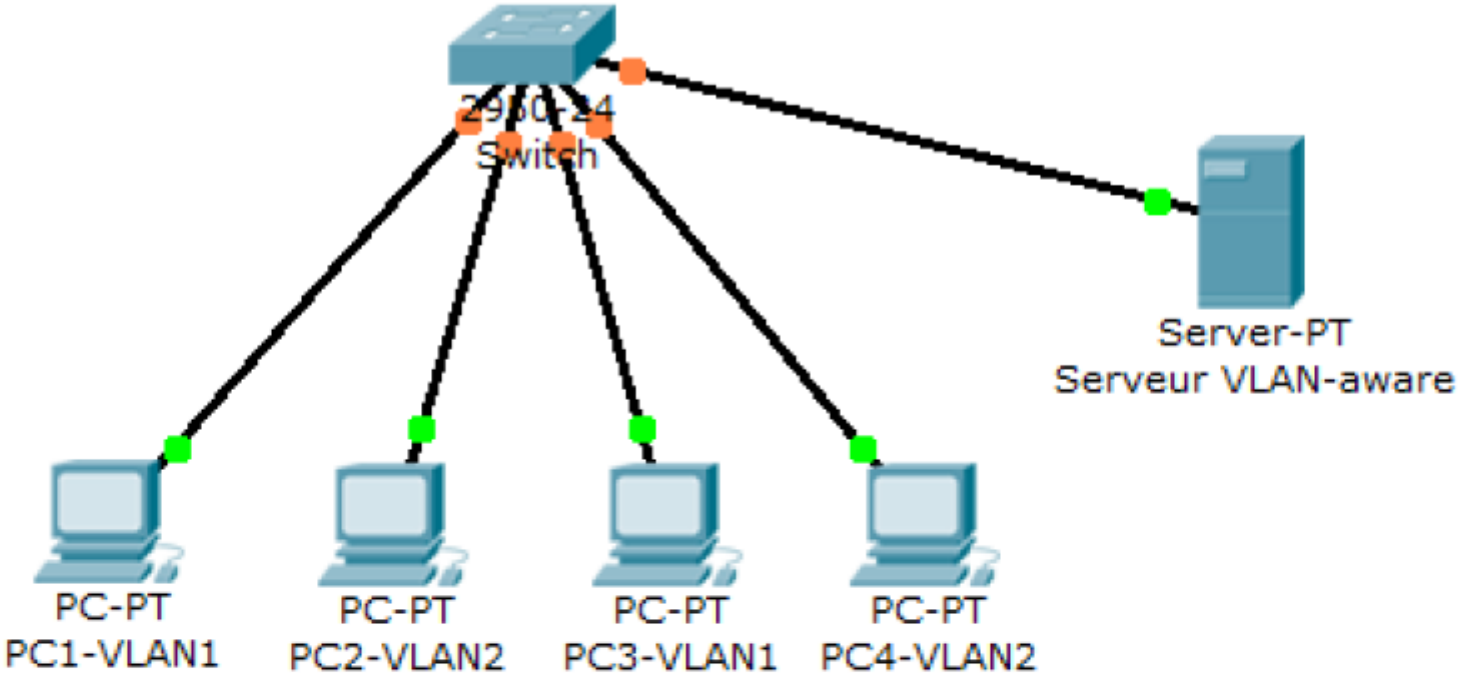
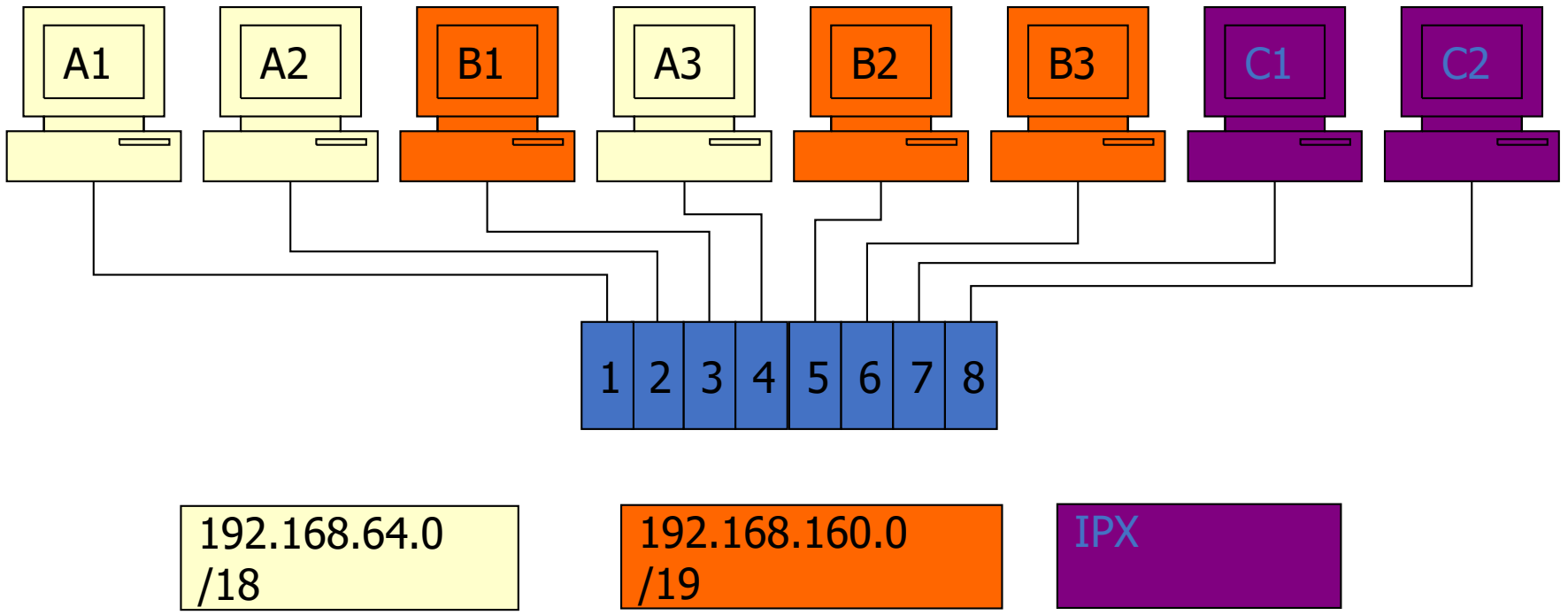


Table créée dynamiquement	
Port	**VLAN**
1	1
2	2
3	1
4	2
5	1 ; 2

Table construite par l'administrateur	
VLAN1	**VLAN2**
@ MAC PC1	@ MAC PC2
@ MAC PC3	@ MAC PC4

- Définie par les adresses de niveau 3 (IP)
  - Très souple : association d'un préfixe IP (@ de sous-réseau ou plages d'@) et d'un numéro de VLAN : On affecte une adresse de niveau 3 à un VLAN.
  - Un routeur permet de passer d'un VLAN à l'autre
  - Perte de performance : il faut analyser les trames au niveau 3 pour déterminer l'appartenance à un VLAN
  - Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.
  - Non sécurisé : l'utilisateur peut facilement changer son @ IP

VLAN de niveau 3



(IEEE 802.1Q) Protocol d'étiquitage

- Il faut transporter l'information d'appartenance à un VLAN (chaque commutateur doit connaître le VLAN associé à la source et au destinataire)

- Deux possibilités

▪ chargement des tables de VLAN dans tous les équipements.(Lorsque le réseau est important les tables peuvent devenir très grandes et pénaliser les performances.)

▪ ajout d'une étiquette aux trames transportées entre les commutateurs uniquement (côté émetteur)

  - l'étiquette identifie le VLAN de la station source

  - norme IEEE 802.1p/Q : format des étiquettes indépendant du constructeur de l'équipement

Thank you for your attention