Académie Cisco
Reims
Champagne-Ardenne

UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

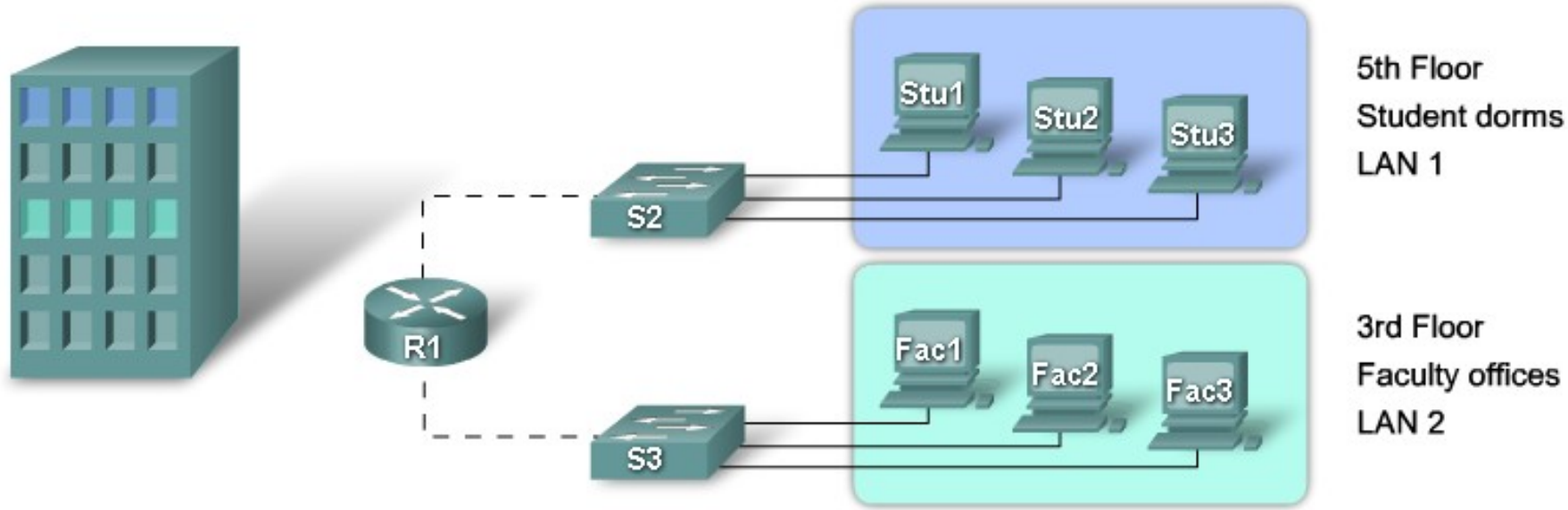
Les Virtual LAN

Les Virtual LAN

Introduction

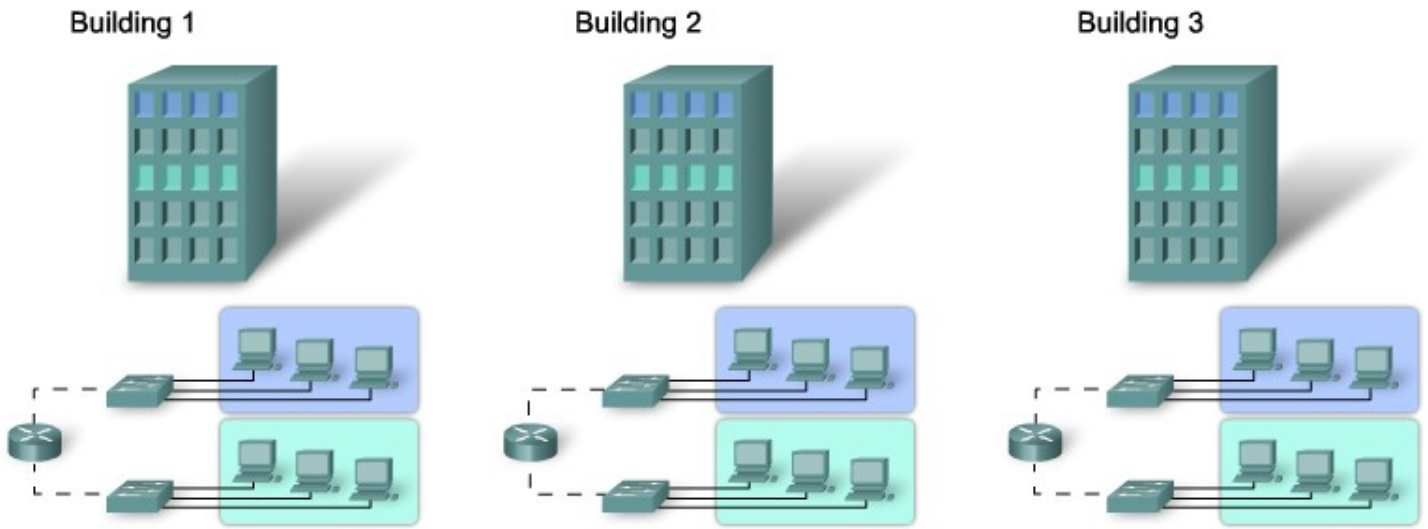
Architecture d'un réseau

- Pour séparer, sur un réseau global, les rôles de chacun
  - Solution classique : utilisation de sous-réseaux différents



Problème !

- Et si nous devons attribuer les mêmes rôles à des utilisateurs, mais répartie sur des bâtiments différents ?
  - Obligation de faire de multiples sous-réseaux !



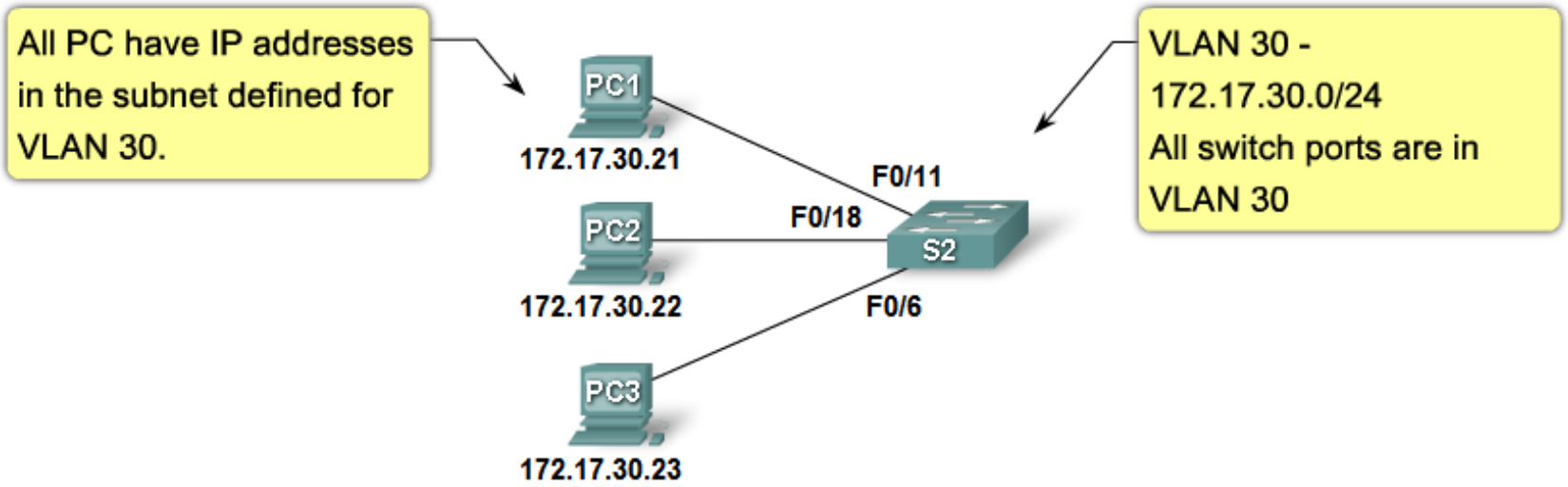
Same network in each building:

5th Floor Student dorms LAN 1	3rd Floor Faculty offices LAN 2

Une solution : Les Réseaux Locaux Virtuels (VLAN)

- Objectifs des VLAN
  - Avoir des fonctions de la couche 3 avec la vitesse de la couche 2
  - Faciliter la gestion de la mobilité des postes
  - Supprimer la possibilité de communication entre certaines parties du réseau, sécurisé des domaines
  - Pouvoir facilement attribuer des autorisations différentes, en fonction des droits et rôles de chaque groupe de personnes

Exemple



- A VLAN = Subnet (in modern switched LANs)
- On the switch
  - Configure the VLAN
  - Assign the port to the VLAN
- On the PC assign an IP address in the VLAN subnet

Les VLAN IDs

- Les identifiants des VLAN font parti de 2 plages
  - Les normal-range ID
  - Les extended-range ID
- Les normal-range ID
  - De 1 à 1005
  - Utilisé dans les réseaux des petites et moyennes entreprises
  - Les identifiants 1002 à 1005 sont réservés aux protocoles Token Ring et FDDI
  - Les VLAN 1, 1002 et 1005 sont créés par défaut, ils ne peuvent être supprimés
  - Les configurations des VLAN sont stockées dans un fichier, appelé vlan.dat en mémoire flash du switch

Les VLAN IDs

- Les extended VLANs
  - Plage comprise entre 1006 et 4094
  - Supporte moins de fonctionnalité que le normal range VLAN
- Les switch Catalyst 2950 et 2960 supportent un maximum de 255 VLAN normal et extétendu, simultané.
- Par contre, l'augmentation du nombre de VLAN sur un switch dégrade les performances de celui-ci

Définitions

- Un réseau local (LAN)
  - est défini par un domaine de diffusion
  - Limité par des équipements fonctionnant au niveau 3 du modèle OSI : la couche réseau
- Un **réseau local virtuel** (VLAN) est un **LAN distribué** sur des équipements fonctionnant au **niveau 2** du modèle OSI : la couche liaison (Ethernet)
- A priori, nous n'avons plus besoin d'avoir recours à un équipement de niveau 3 pour délimiter le LAN
- Les VLAN sont distribués sur différents équipements via des liaisons dédiées appelées **trunk**
- Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels

Les types de VLAN

- Actuellement, sur un réseau, plusieurs VLAN sont distingués (3.1.2.3 Lan Switching)
  - Les Data VLAN
    - Ne véhiculent que des données utilisateurs
  - Le Default VLAN
    - Le VLAN dans lequel un switch, à la livraison se trouve
    - Chez Cisco, c'est le VLAN 1 et il ne peut pas être changé
    - Les protocoles CDP et les spanning tree sont associés à ce VLAN
  - Le Native VLAN
    - C'est le VLAN associé au port trunk 802.1Q qui a la capacité de véhiculer les données marquées ou pas par un identifiant de VLAN
  - Le Management VLAN
    - C'est le VLAN qui est utilisé pour configurer les swicths.
- Maintenant, il existe le Voice VLAN

Le Voice VLAN

- La VoIP nécessite des impératifs afin de pouvoir assurer une qualité suffisante sur le trafic vocal
  - Garantir une bande passante suffisante
  - Transmettre en priorité ces flux
  - Etre capable de router ces flux vers des zones congestionnées du réseau
  - Avoir un délai inférieur à 150 ms à travers le réseau

Les différents modes

- A un VLAN est associé un ID
- Chaque port d'un switch appartient à un VLAN
- Cette affectation peut être
  - Statique
    - Cf 3.1.3.1 CCNA 4.0 LAN Switching
  - Dynamique
    - Peut utilisé dans les réseaux
    - Nécessite un VLAN Membership Policy Server (VMPS)
    - L'affectation à un VLAN se fait en fonction de l'adresse MAC d'une machine
- Dans le cas d'un Voice VLAN, il ne faut pas oublier que tout le réseau doit le supporter
  - Gestion de la priorité de ces flux sur les autres

Utilisation des trunks

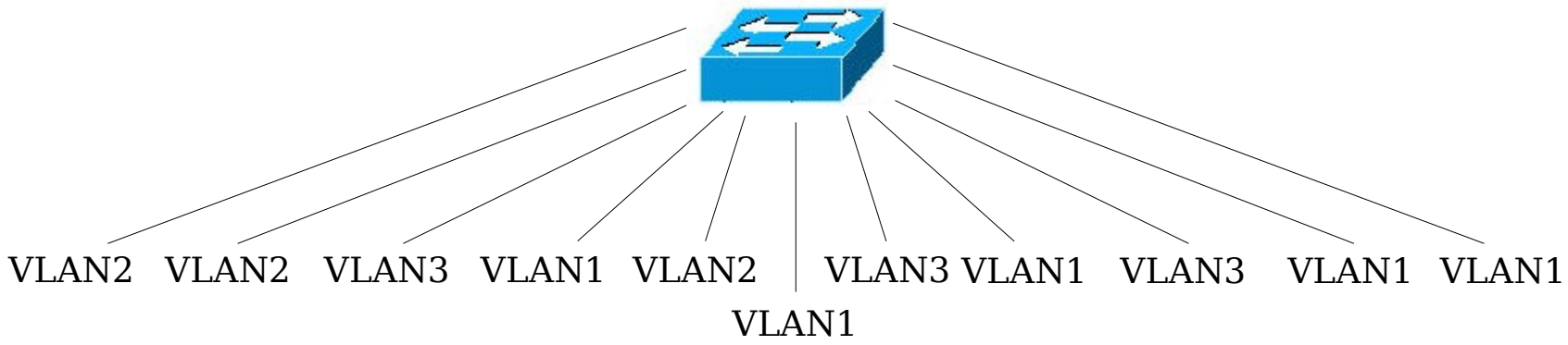
- Les trunk peuvent être utilisés
  - Entre 2 commutateurs
    - C'est le mode de distribution des réseaux locaux le plus courant
  - Entre un commutateur et un hôte
    - Si un hôte supporte le trunking, il a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels
  - Entre un commutateur et un routeur
    - Permet d'accéder aux fonctionnalités de routage entre des VLAN

Les Virtual LAN

Les solutions classiques

VLAN par ports

- Permet de faire une division d'un équipement de niveau 2 (un commutateur) en plusieurs domaines de diffusion
- Obligation de gérer manuellement sur chaque équipement la distribution des réseaux locaux
- Problème : une station ne peut pas changer de VLAN ou appartenir à plusieurs VLAN. Le commutateur assure une isolation complète entre la station et le VLAN auquel il appartient

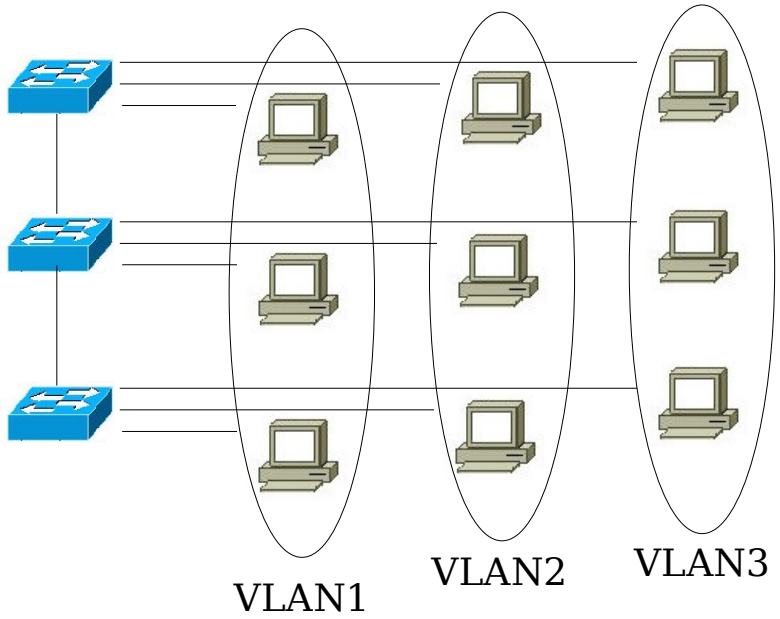


VLAN type Cisco Inter-Switch Link (ISL VLAN)

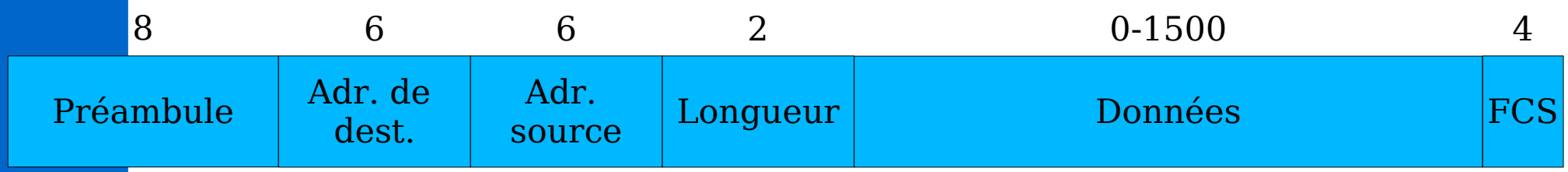
- Technique développée pour les équipements Cisco. Chaque en-tête de trames en complétée de 30 octets répartis en 13 champs
- Solution surtout utilisée dans le Voice over IP des équipements Cisco
- Technique non compatible avec les standards IEEE 802.1Q

VLAN IEEE 802.1Q

- Standard qui fournit un mécanisme d'encapsulation très répandu, implanté dans de nombreux équipements de marques différentes
- Comme dans l'encapsulation ISL, l'en-tête de la trame est complétée par une balise de 4 octets

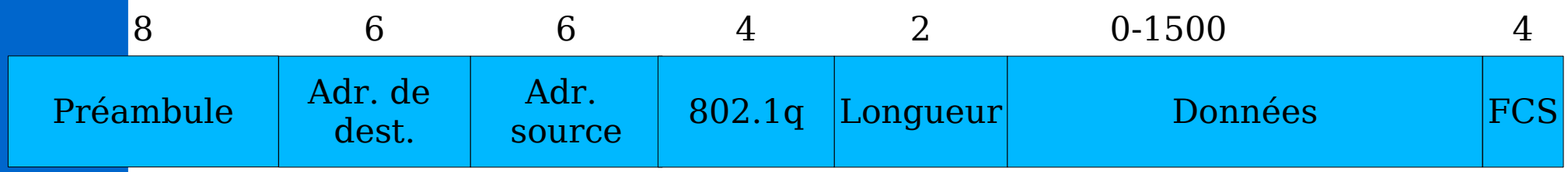


La trame Ethernet 802.3



- Le champ Type est remplacé par le champ longueur
- Pour éviter des problèmes de compatibilité, IEEE a décidé de considérer ce champ comme indiquant une longueur si la valeur est <= 1500 sinon c'est le type de données transportées

La trame IEEE 802.1Q

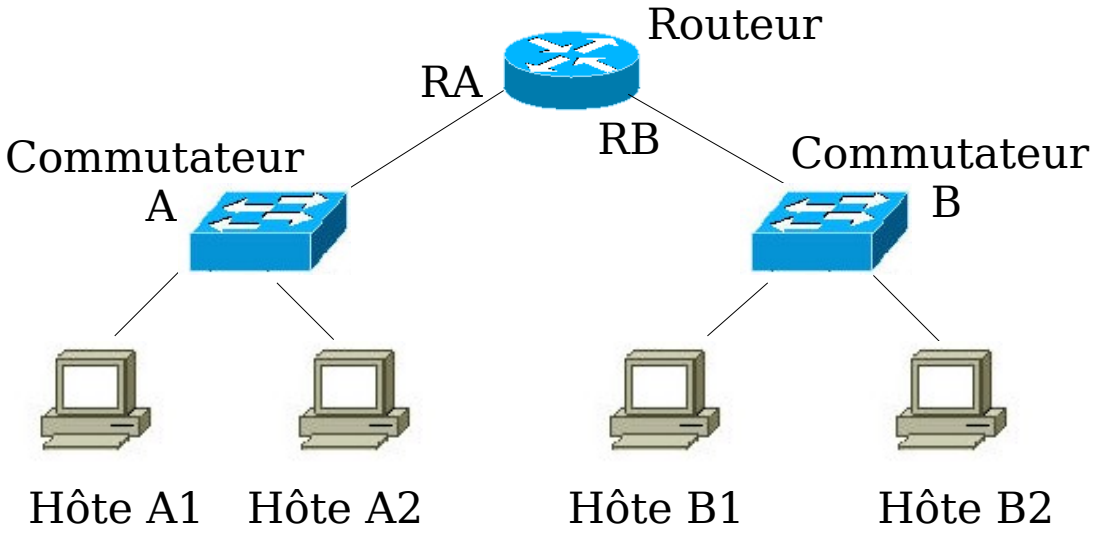


- 4 octets du 802.1q découpés de la façon suivante :
  - EtherType ou Tag Protocol IDentifier (TPID)
    - 12 bits utilisés pour identifier le protocole de la balise insérée. Pour une balise 802.1q, la valeur est fixée à 0x8100
  - Priority
    - 3 bits pour coder 8 niveaux de priorité. Aucun rapport avec les priorités sur IP. Uniquement pour mettre des priorités entre les trames de certains VLAN par rapport à d'autres
  - Canonical Format Identifier
    - 1 bit pour la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe toujours cette valeur à 0. Si une trame avec la valeur 1 pour ce champ arrive, celle-ci ne sera pas propagée
  - VLAN Identifier
    - 12 bits qui permettent de définir l'appartenance de la trame à un VLAN, au maximum 4094 VLAN possibles

Les Virtual LAN

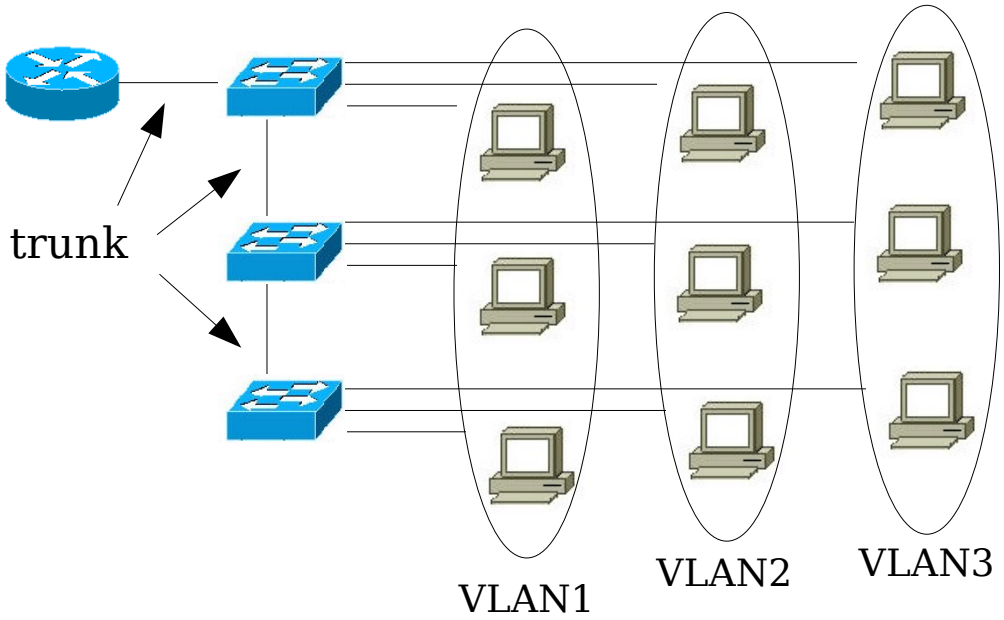
Le routage inter-VLAN

Sans le routage inter-VLAN



- Si le comm. A possède un VLAN pour A1 et un VLAN pour A2, A1 et A2 ne peuvent pas communiquer entre-eux. Si l'un d'entre-eux veut communiquer avec un autre VLAN, il faut que l'interface RA appartiennent aux 2 VLAN
- Si la machine A1 déménage dans un autre endroit !
  - Installation d'un nouveau switch et connecter celui-ci vers le VLAN A1

Avec le routage inter-VLAN



- Le contrôle d'accès est centralisé au niveau du routeur
- Gestion optimisée des ports de commutation. Tous les VLAN peuvent être accessible sur n'importe quel port. L'administration est donc concentré sur un nombre minimum de matériel, contrairement à la solution sans routage inter-VLAN

La commutation niveau 3 ?

- Les switchs niveau 3 sont capables de faire du routage inter-vlan
- Ils utilisent une Switch Virtual Interface
  - C'est une interface logique qui doit être configuré pour chaque VLAN à router