Dr. Cheikh Sidy Mouhamed CISSÉ

Contact: sidimouhamed12@gmail.com

cheikhsidy.cisse@univ-thies.sn

Virtual Local Area Network (VLAN)

OBJECTIFS

- Segmentation logique des réseaux
- Contrôle et empêche les dialogues entre équipement interconnectés sur un même commutateur.

INTRODUCTION

- La technique des VLANs (*Virtual Local Area Network*) permet de donner au réseau l'architecture logique souhaitée par l'administrateur, en le libérant de certaines contraintes physiques.
- C'est une technique de segmentation, qui participe donc à la sécurité
- Cependant, les protocoles utilisés ne sont pas spécialement conçus pour être « sécurisés »
- Il faut donc utiliser cette technique quand elle est vraiment utile, et maîtriser les conséquences sur la sécurité du réseau.

INTRODUCTION

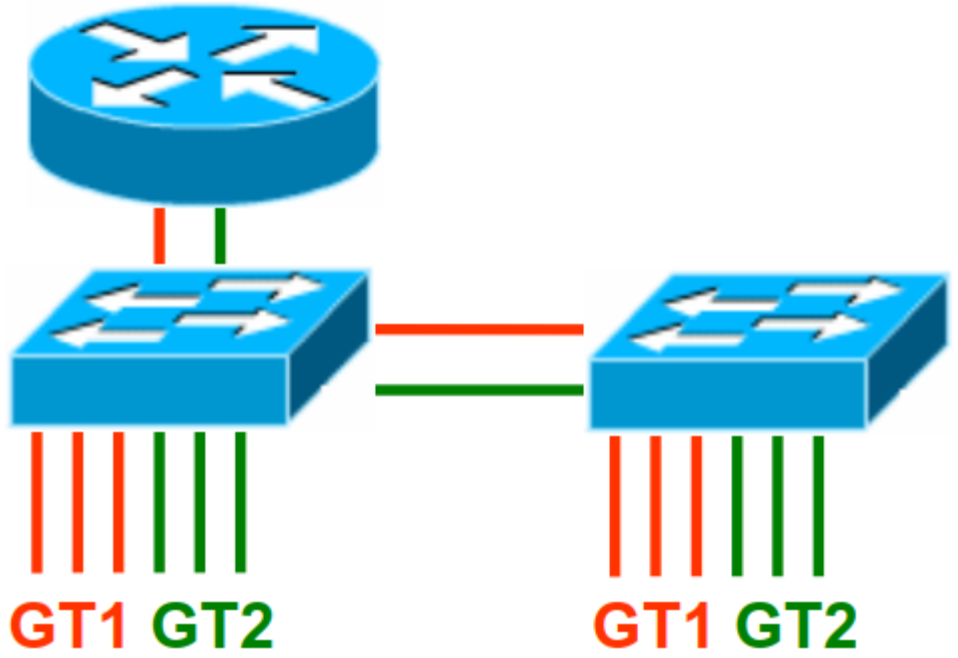
- Les VLANs doivent être utilisés pour :
  - regrouper des postes selon un critère logique et non plus géographique
  - gérer correctement la mobilité des postes
  - contrôler la taille des domaines de *broadcast*

- Leur utilisation n'est pas motivée par des raisons liées à la sécurité, mais à l'architecture

- La conception d'une architecture bien pensée, avec si besoin l'utilisation des VLAN est le prérequis à une bonne gestion de la sécurité

ENSEMBLE LOGIQUE

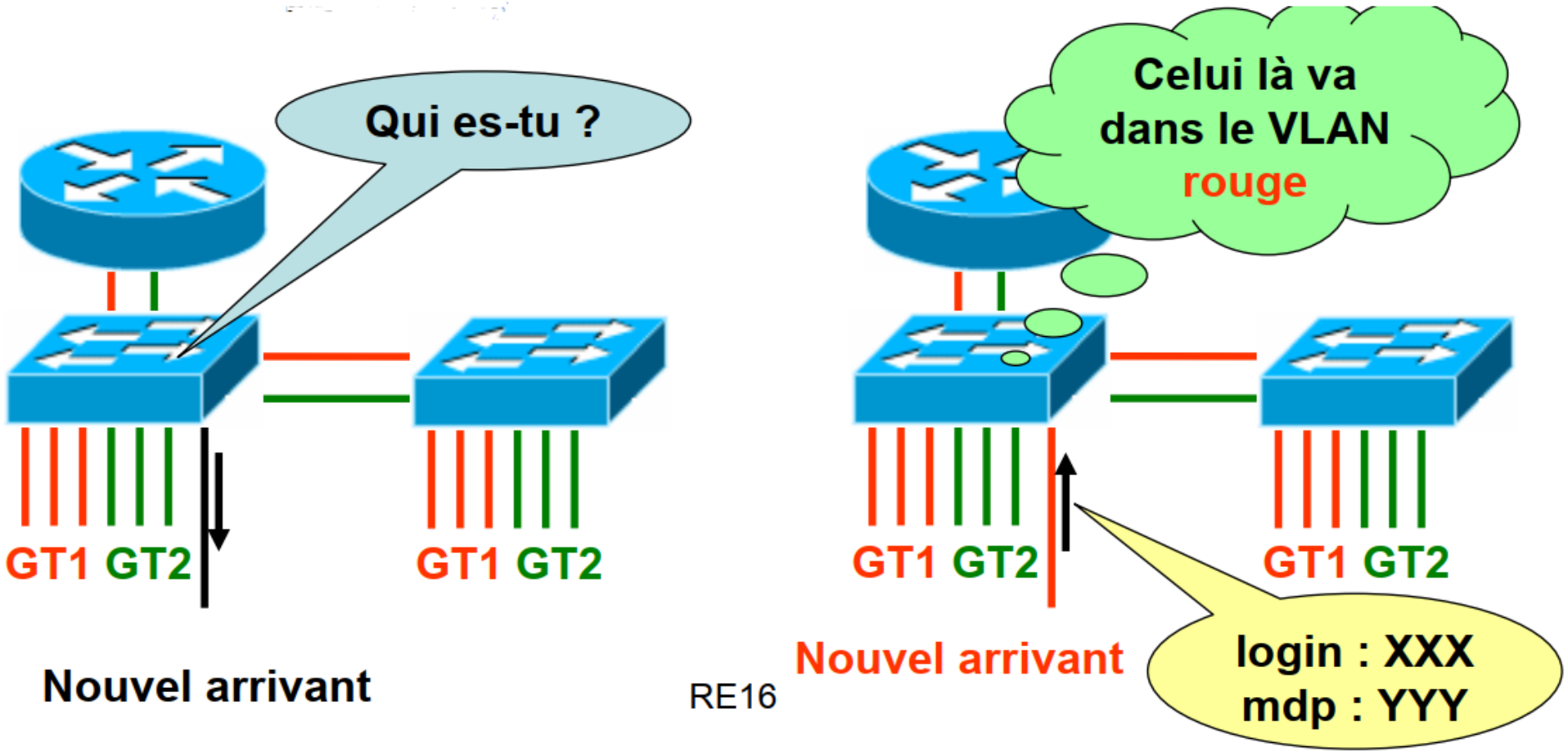
- Les *VLANs* doivent être utilisés pour cloisonner un réseau indépendamment de la répartition géographique des postes.



ENSEMBLE LOGIQUE

- On peut créer des ensembles de machines, cohérents :
  - au sens de la sécurité :
    - ✓ Identification et gestion des droits
    - ✓ On peut utiliser l'@MAC ou le couple login/mdp pour mettre les utilisateurs qui se connectent dans le VLAN qui correspond à leurs droits

ENSEMBLE LOGIQUE

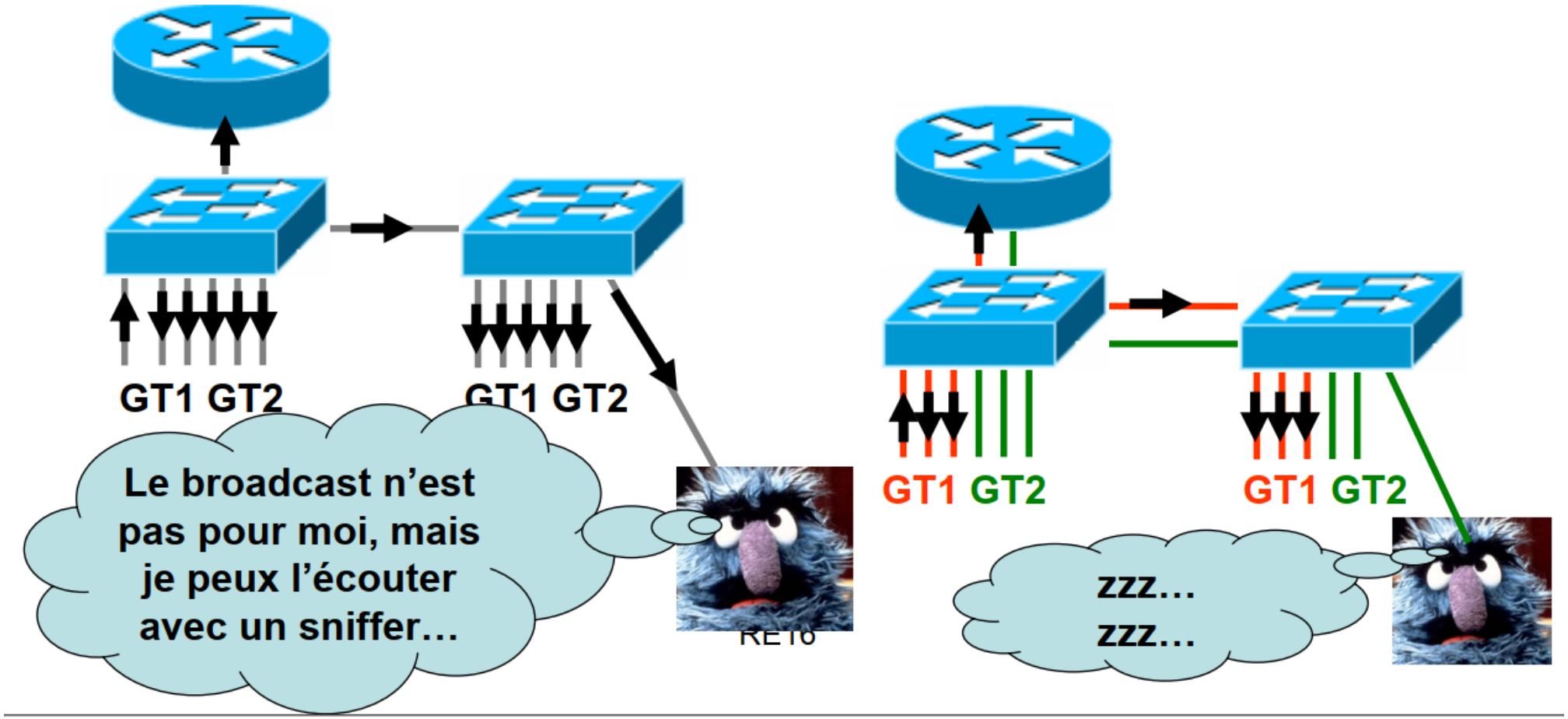


RE16

ENSEMBLE LOGIQUE

- On peut créer des ensembles de machines, cohérents :
  - au sens de la sécurité :
    - ✓ accès aux trames de ***broadcast*** (visibles avec un sniffer)
    - ✓ Un utilisateur malveillant peut utiliser un sniffer pour décode des trames de ***broadcast*** qui ne le concernent pas. Pire encore, un switch peut, si sa table d'adresses MAC lui impose, retransmettre une trame unicast sur toutes ses interfaces

ENSEMBLE LOGIQUE

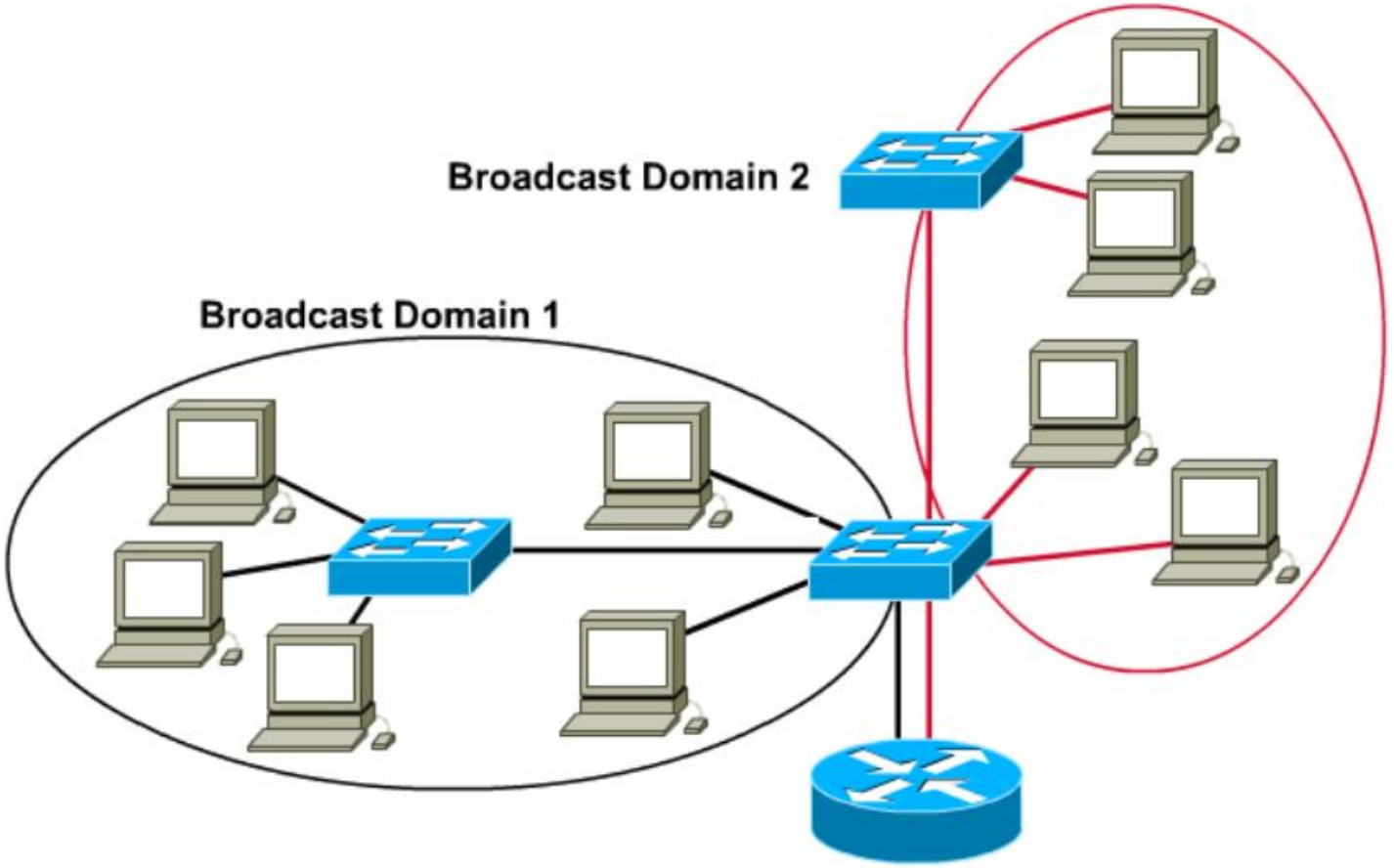


SEGMENTATION / FILTRAGE

- La technique des *VLANs* est une technique de niveau 2

- Elle permet de créer des domaines de *broadcast* qui correspondent aux ensembles logiques définis par l'administrateur.

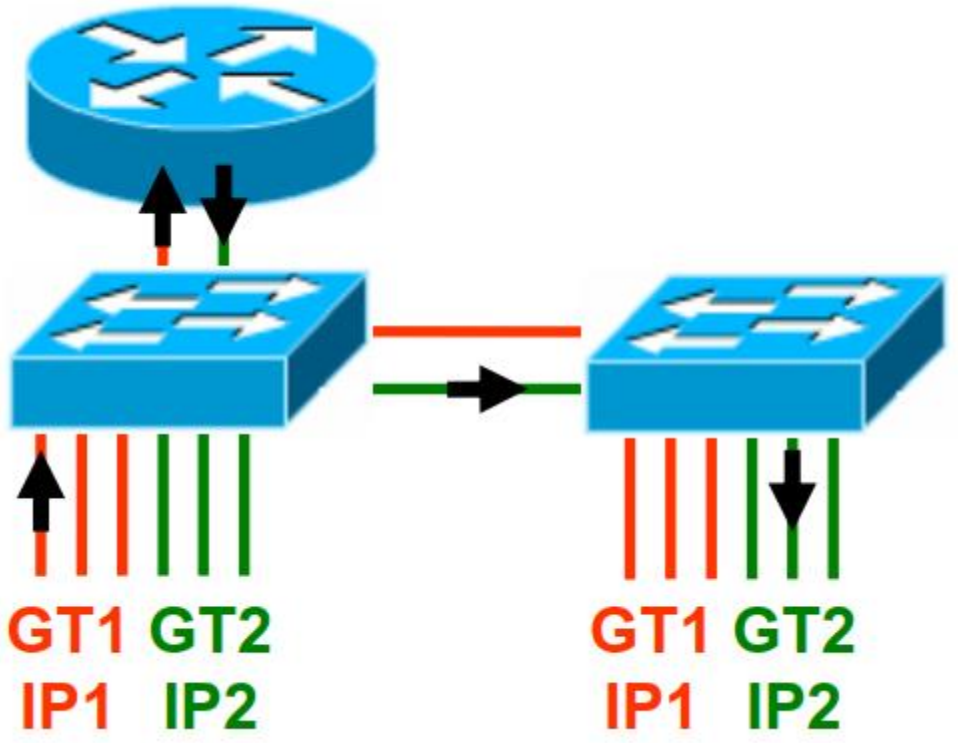
SEGMENTATION / FILTRAGE



SEGMENTATION / FILTRAGE

- La segmentation crée des groupes séparés strictement
- La séparation peut être rendue perméable par l'utilisation d'un routeur
- Ceci qui conduit alors à attribuer des réseaux IP différents pour chaque VLAN

SEGMENTATION / FILTRAGE



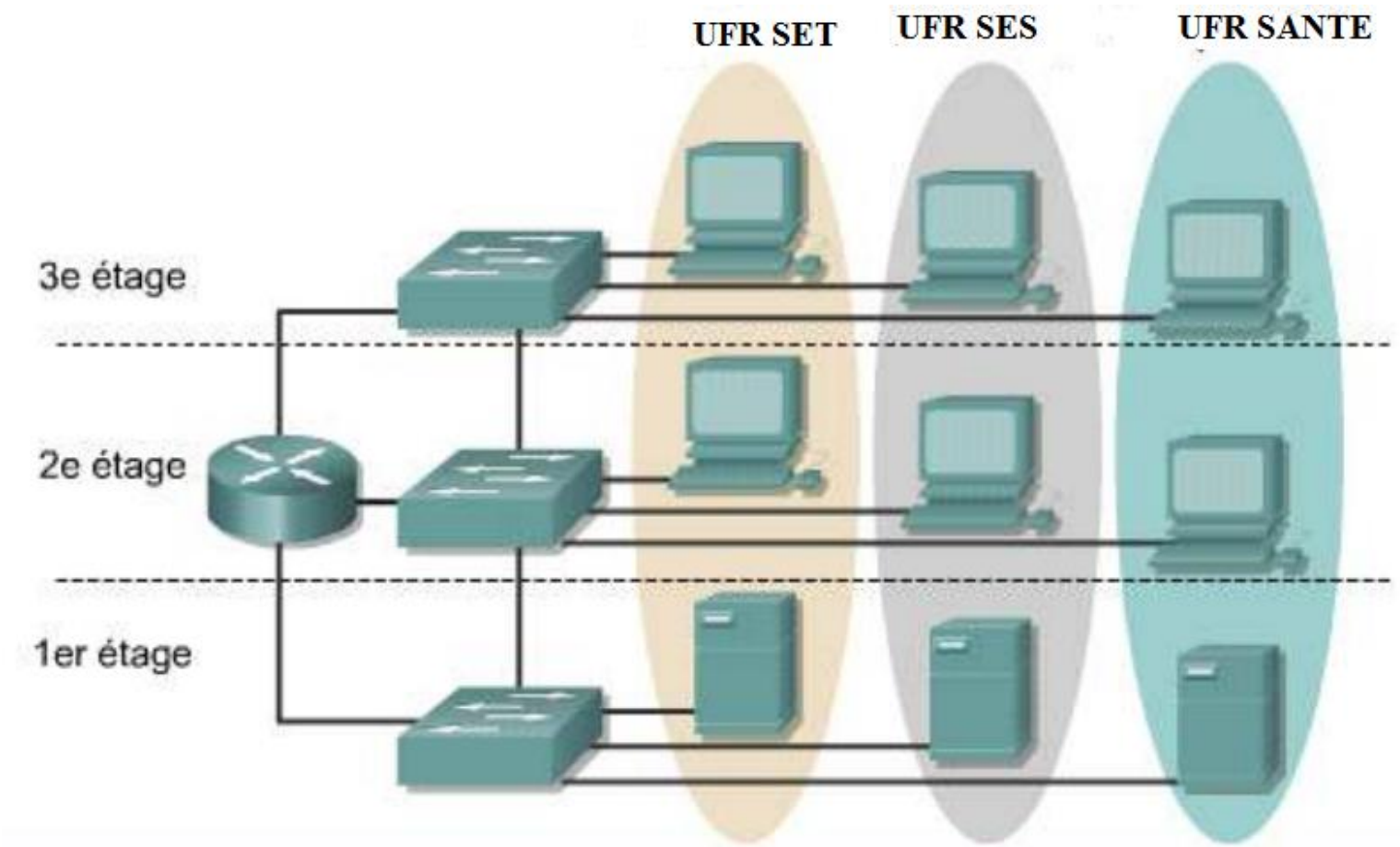
SEGMENTATION / FILTRAGE

- L'utilité de cette technique de segmentation réside dans la possibilité de faire du routage avec filtres entre les segments ainsi créés

- Ainsi, même si il s'agit d'une technique de niveau 2, son utilisation est motivée par des raisons s'attachant au niveau 3.

NB: C'est le switch qui sépare en différents VLANs, c'est le routeur qui autorise les communications utiles entre ces VLANs

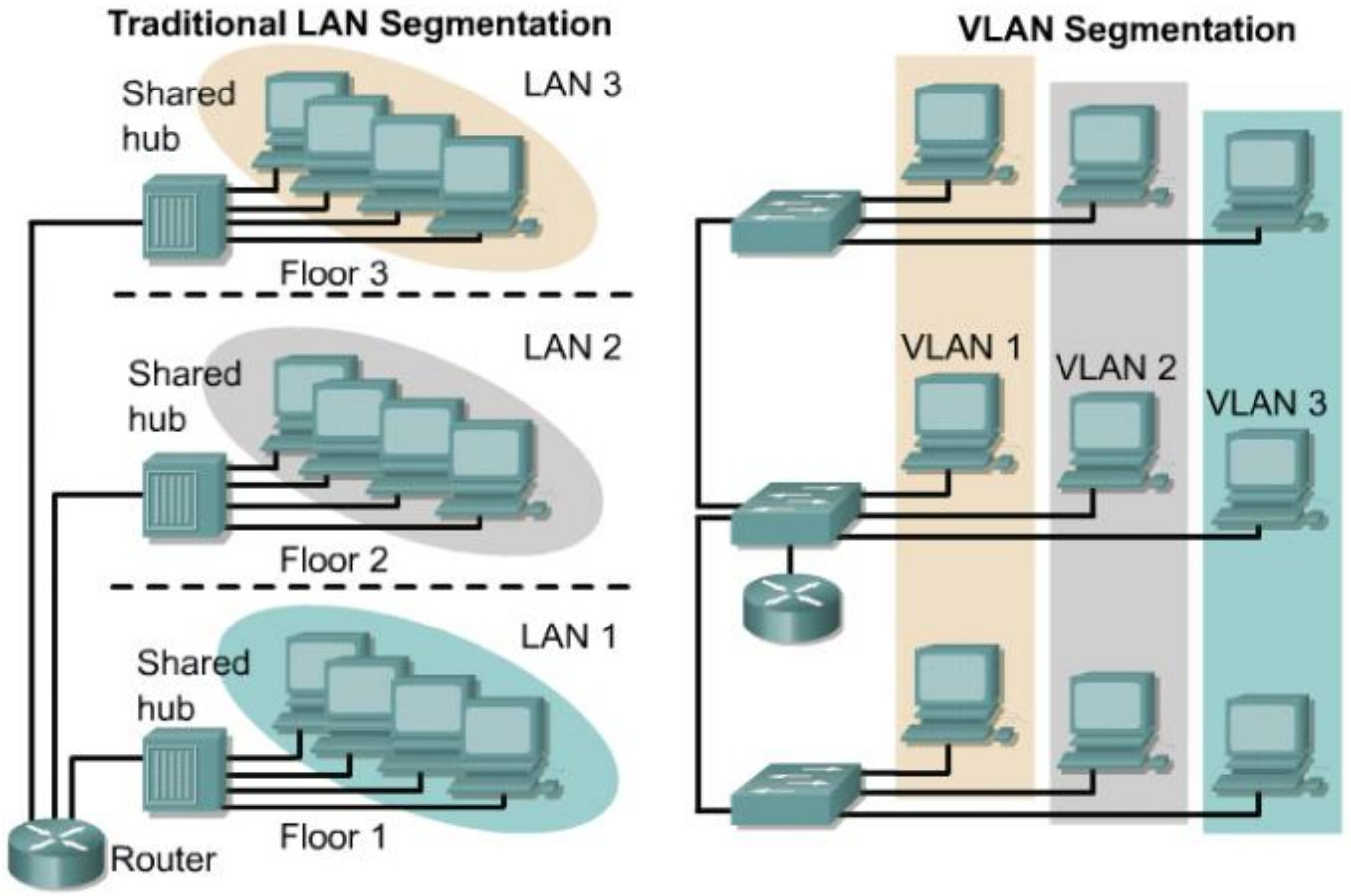
VLAN: à quoi cela sert-il?



VLAN: à quoi cela sert-il?

- Réseau logique, non tributaire de l'emplacement physique
- Les domaines de broadcast sont définis administrativement
- Les utilisateurs sont affectés par logiciel aux différents VLANs
- Un switch contient donc un IOS et une base de données montrant l'appartenance aux VLANs

VLAN: à quoi cela sert-il?



VLAN: mise en œuvre

- La définition des VLANs se fait sur les équipements d'interconnexion de niveau 2 (*switchs*)
- Les équipements terminaux ignorent leur appartenance à un VLAN
- Les *switchs* ont donc un IOS qui permet de mettre à jour une micro base de données
- Cela peut se faire par le branchement d'une console en mode texte directement sur switch
- Certains switch contiennent un mini serveur web qui permet de paramétrer les VLANs (entre autres choses)
- Un switch peut donc avoir une adresse IP !

VLANs statiques dynamiques

- La définition d'un VLAN peut reposer :
  - sur le port de connexion sur le switch (VLAN statique ou par port, ou de niveau 1) ;
  - sur l'adresse MAC (VLAN dynamique, ou de niveau 2) ;
  - sur le résultat MAC, conditionné à l'authentification.

VLANs statiques dynamiques

- Les VLANs statiques sont :
  - simples à mettre en place
  - plus difficiles à maintenir (déplacements)
  - vulnérables à l'utilisation incontrôlée des prises
- Les VLAN dynamiques sont :
  - plus difficiles à mettre en place (création de bases d'@MAC)
  - faciles à maintenir (mobilité)
  - générateurs de trafic sur le réseau (VTP) pour propager les bases
  - moins vulnérables (même si il existe des cartes réseaux pour lesquelles l'@MAC est paramétrable)

VLANs statiques dynamiques

- Deux VLANs propagés sur deux switchs avec lien en mode trunk (étiquetage des trames, 802.1q ou ISL)

VLANs: étiquetage des trames

- C’est une modification de l’en-tête de niveau 2, pour qu’elle puisse porter la mention de l’appartenance à un VLAN
- Cette modification peut être « propriétaire » :
  - ISL de Cisco
  - non compatible avec ce qui n’est pas Cisco
  - les infos relatives au VLAN sont vues comme un protocole supplémentaire, encapsulé entre la trame et le paquet.

Port trunk

- On appelle « port en mode trunk » un port pour lequel l'étiquetage des trames a été activé
- Ils sont utilisés entre deux switchs ou entre un routeur et un switch
- Ils peuvent être configurés pour transporter tous les VLANs, ou une partie d'entre eux seulement.
- Ils n'appartiennent à aucun VLAN, sauf dans le cas où un VLAN particulier a été prévu pour assurer une connectivité minimum au cas où l'étiquetage serait défectueux

Port trunk

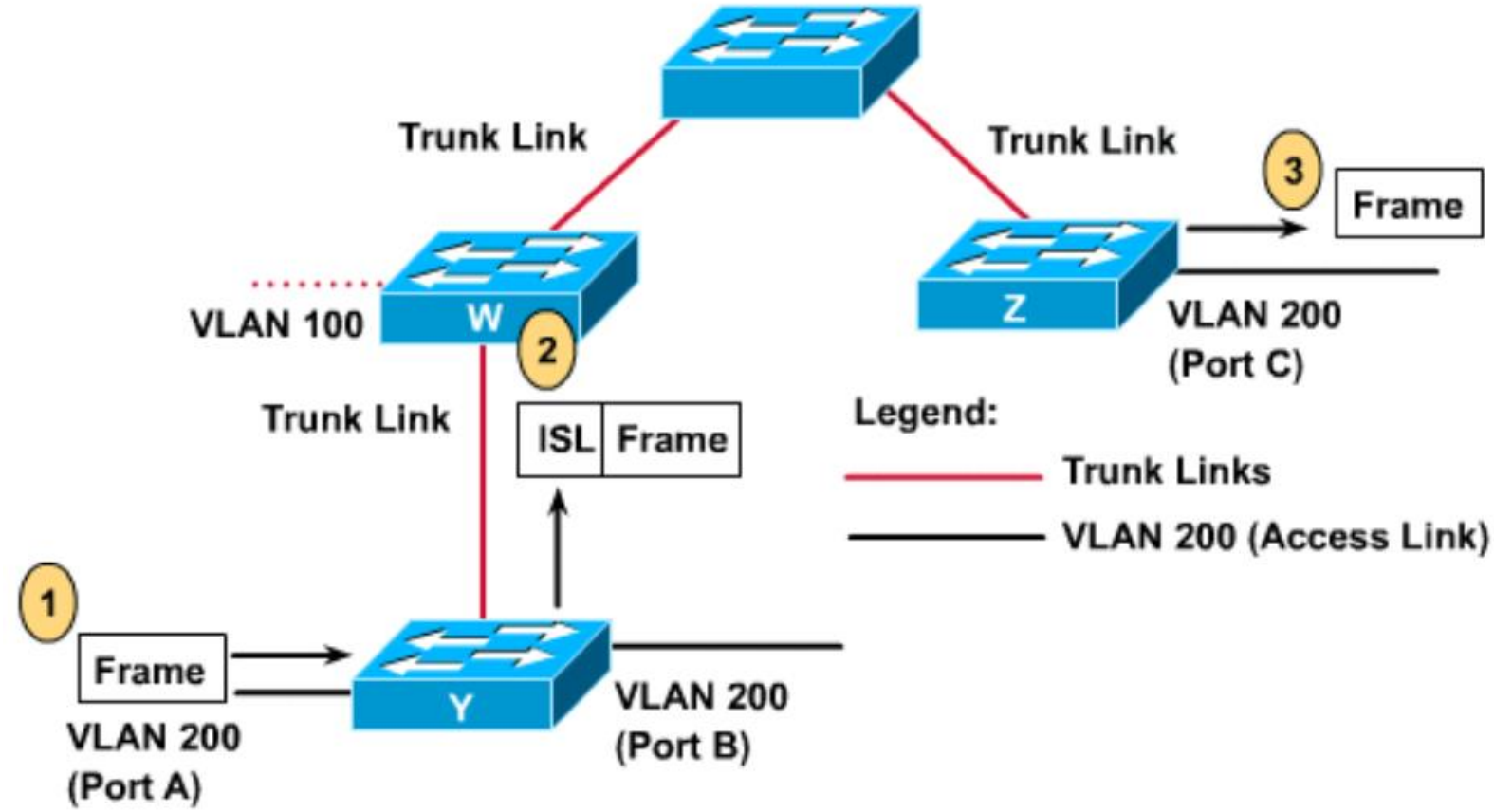
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation ?

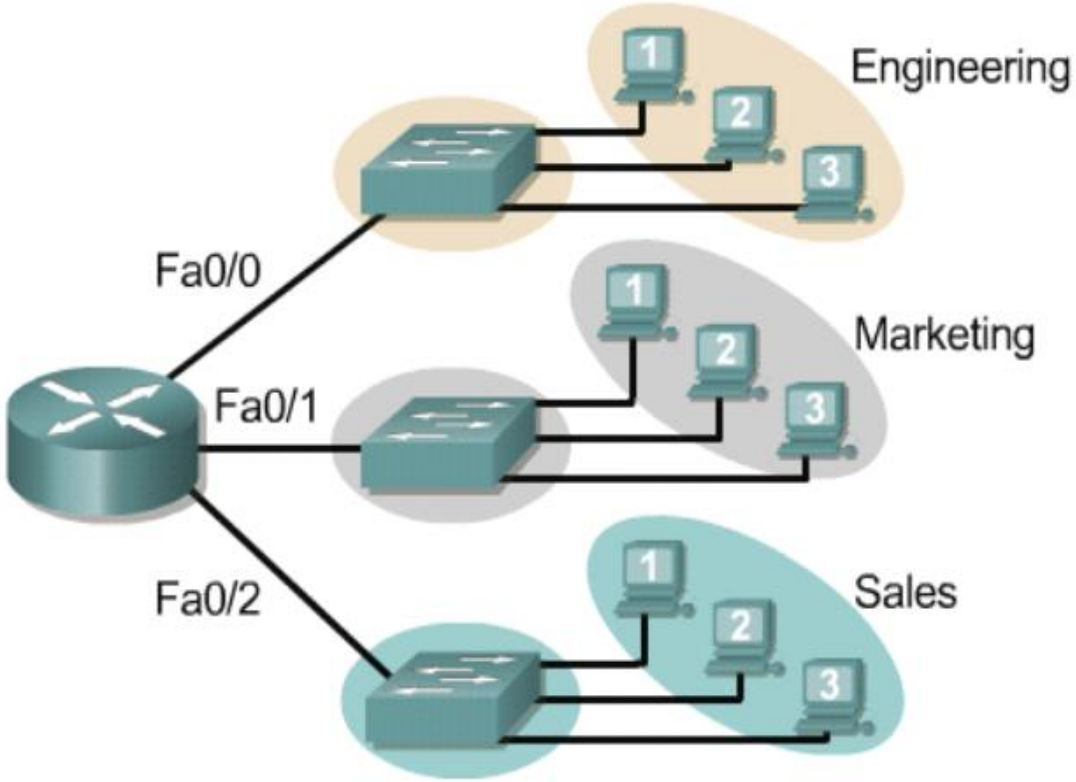
dot1q - interface uses only 802.1q trunking encapsulation when trunking

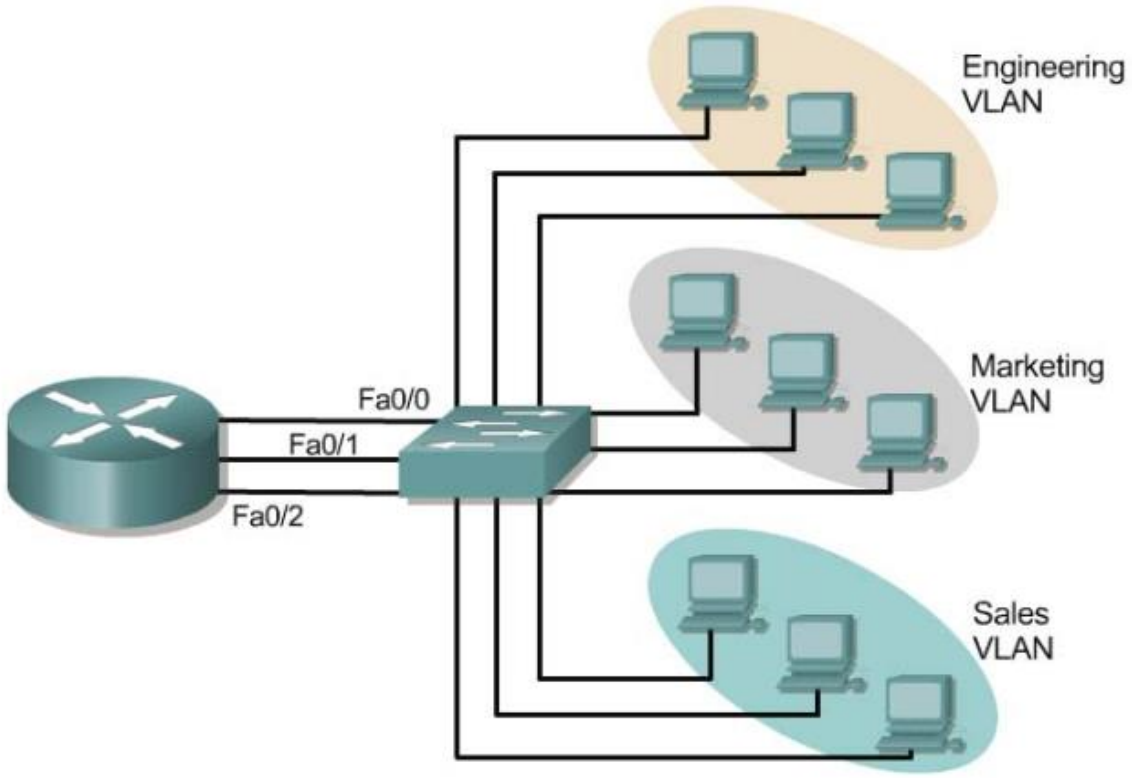
isl - interface uses only ISL trunking encapsulation when trunking

Port trunk


Trunk Link
Trunk Link
3
Frame
VLAN 100
W
2
Z
VLAN 200
(Port C)
Trunk Link
ISL
Frame
Legend:
Trunk Links
VLAN 200 (Access Link)
1
Frame
VLAN 200
(Port A)
Y
VLAN 200
(Port B)

Exemple


Engineering
Marketing
Sales
Fa0/0
Fa0/1
Fa0/2
1
2
3


Engineering
VLAN
Marketing
VLAN
Sales
VLAN
Fa0/0
Fa0/1
Fa0/2

Que fait le Switch?

- Le switch doit maintenir une table pour chaque VLAN (besoin de mémoire)
- L'apprentissage des adresses MAC des machines se fait VLAN par VLAN
- Le routeur a une interface (ou sous-interface) dans chaque VLAN (passerelle pour ce VLAN)
- Le routeur verra :
  - les trames qui lui sont adressées (en tant que passerelle)
  - les trames de broadcast

VMPS / VTP

- Avec l'utilisation d'un VLAN Policy Management Server VMPS, il est possible de centraliser la base @MAC/VLAN
- Au démarrage un switch ainsi configuré télécharge la base @MAC/VLAN par le protocole tftp, sur le serveur VMPS
- La gestion de la base se fait donc de façon centralisée

VMPS / VTP

Switch> (enable) set vmps tftpserver ip_addr [filename]

Switch> (enable) set vmps state enable

Switch> (enable) show vmps

VMPS / VTP

- Pour ajouter un VLAN sur un sur un réseau,
  - Les VLANs doivent être configurés sur chaque commutateur
  - Beaucoup de manipulations

- Solution:
  - La configuration peut être faite sur un seul commutateur
  - La modification sera propagée sur les autres commutateurs via le protocole VTP (Vlan Trunking Protocole) de CISCO.

CONCLUSION

- Grâce à l'utilisation des VLAN, on peut segmenter un réseau, indépendamment de la répartition géographique des machines
- On réalise une économie de matériel
- On facilite la gestion des utilisateurs (ajout, déplacement)
- On améliore la segmentation

CONFIGURATION

- **1 ère étape: création de VLAN**

switch1(config)# vlan ***numéro***

- **2éme étape: attribution de nom au VLAN**

switch1(config-vlan)# name ***nom_vlan***

- **3éme étape: attribution de port au VLAN**

switch1(config)# interface ***NomInterface numéroInterface***

switch1(config-if)# switchport mode access

switch1(config-if)# switchport access vlan ***numéro***