

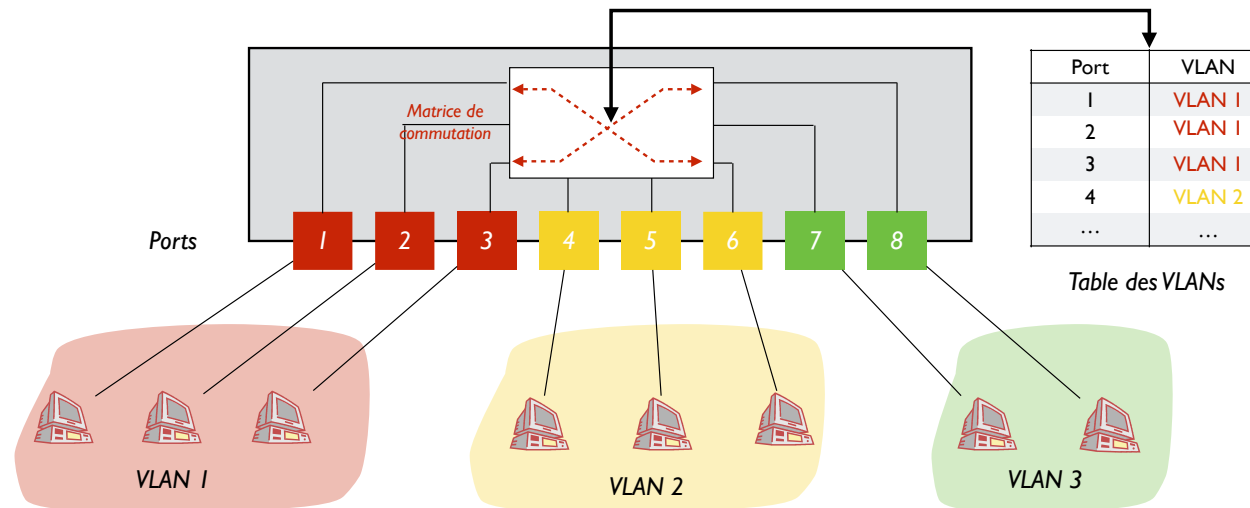
VLANs

Introduction

- Problèmes d'un grand réseau avec seulement des commutateurs
 - Un seul domaine de diffusion
 - problème de performances
 - Sécurité
 - Un terminal peut émettre des trames vers un autre terminal du même LAN
 - Comment ?
 - en utilisant l'@MAC de diffusion
 - Un terminal -Oscar- peut capturer le trafic destiné à un autre -Alice- du même LAN
 - Comment ?
 - En obtenant l'@MAC d'Alice par ses requêtes ARP et en l'usurpant
 - En forgeant des réponses ARP frauduleuses sur l'@IP d'Alice et @MAC d'Oscar

VLANs

- **VLANs** (Virtual Local Area Networks)
- Segmenter un LAN en plusieurs **réseaux logiques indépendants**

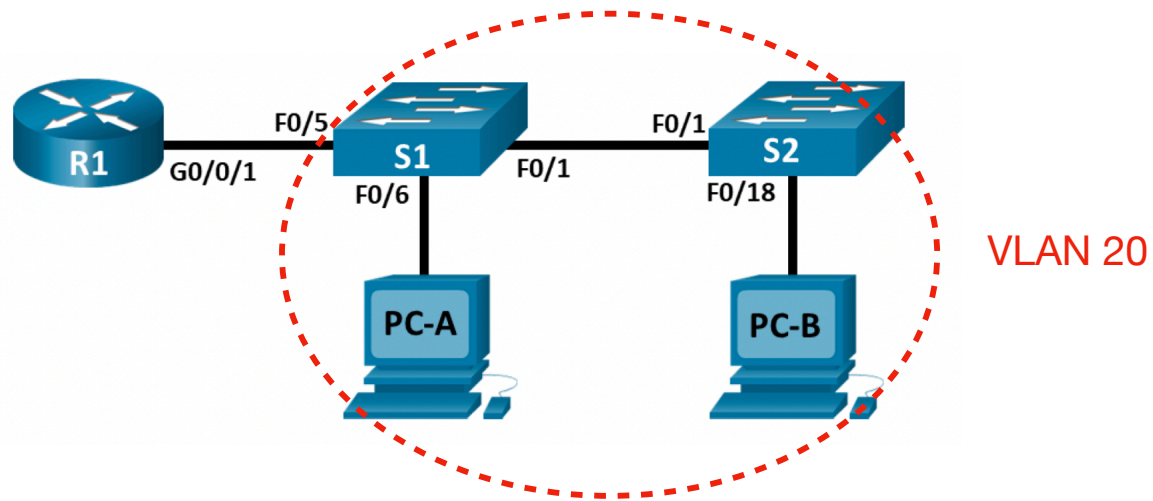


- **Segmentation du domaine de diffusion**
 - Une trame (même en diffusion) provenant d'un noeud du VLAN2 ne sera ré-émise que sur les ports du VLAN 2
 - Chaque VLAN définit un domaine de diffusion

En pratique

- VLANs sont **configurés sur les commutateurs**
 - définis sur les commutateurs
 - assignés sur les ports des commutateurs
- Commutateurs possèdent
 - **table de commutation** (appelée aussi table d'adresses MAC)
 - **table des VLANs**
- Ports des commutateurs peuvent être configurés en mode
 - **accès** : 1 seul VLAN autorisé sur le lien
 - **trunk** : plusieurs VLANs possibles sur le lien
- **Balise VLAN** (appelée aussi Tag VLAN)
 - contient le VLAN ID
 - ajoutée dans l'en-tête Ethernet d'une trame transmise sur un lien trunk
 - pour savoir à quel VLAN la trame appartient
- Nécessite d'avoir un **routage inter-VLANs** dès qu'on veut faire communiquer deux équipements qui n'appartiennent pas au même VLANs
 - avec un routeur
 - avec des commutateurs de niveau 3

Exercice



- Trame envoyée du PC-A au PC-B
 - Balise VLAN dans la trame transmise par le PC-A ?
 - Que fait S1 quand il reçoit le trame sur le port F0/6 ?
 - Balise VLAN dans la trame transmise par S1 vers S2 ?