VLANs (802.1Q)

Nicolas Ollinger, Université d’Orléans

M2 SIR Sécurité des réseaux — **S4** 2017/2018

Partitioner ses LAN

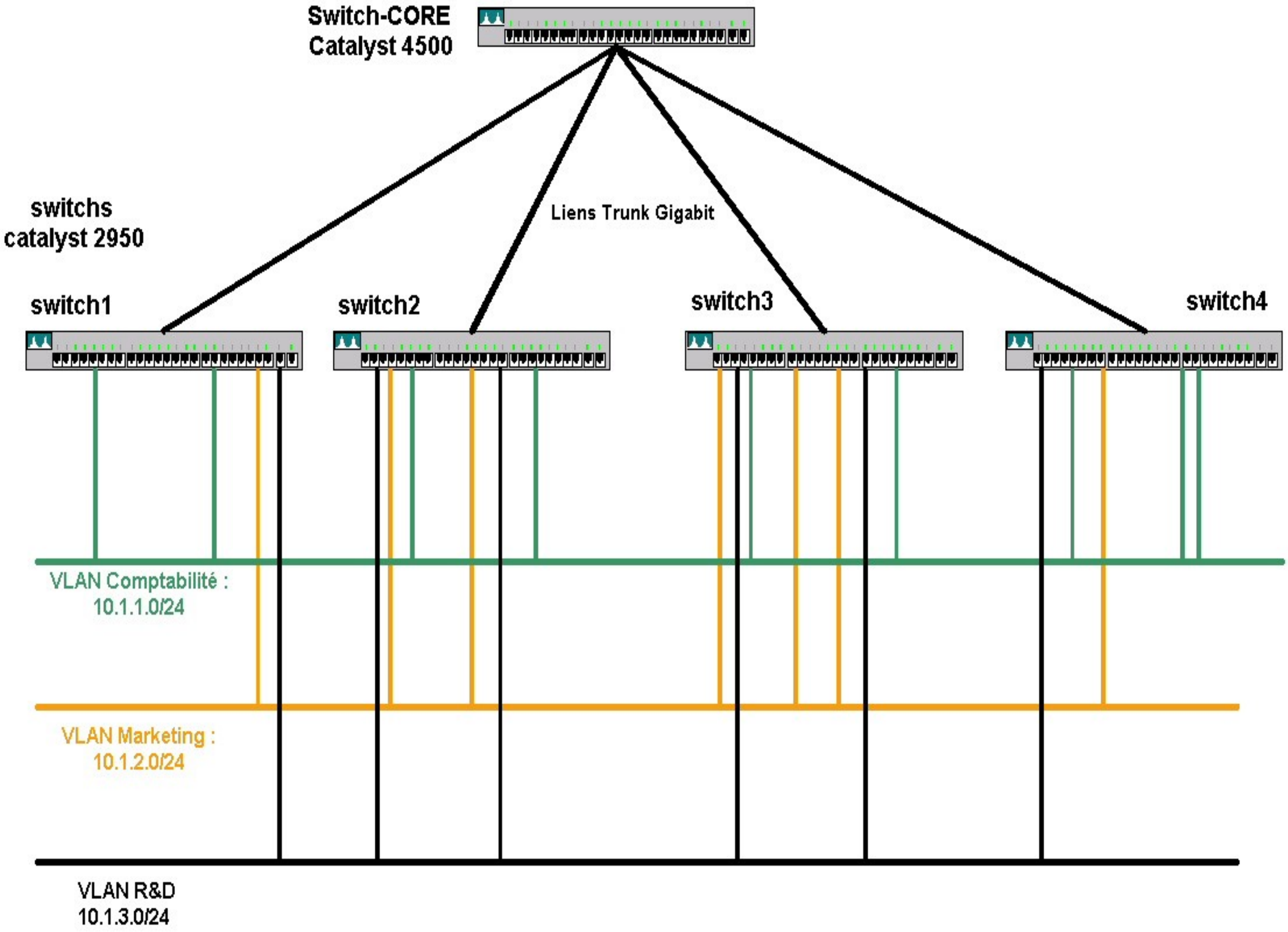
- Lorsque le **nombre de machines** devient **important** (quelques centaines), pour augmenter les performances.

- Pour **isoler** des classes d'utilisateurs différents : clients différents, séparation des différents services de l'entreprise.

Comment partitioner ?

- **Physiquement** : déployer un réseau local (arborescence de **switches**) par LAN.
  +++ : architecture dédié, cloisonnement physique
  ––– : coûteux en matériel et en câblage

- **Virtuellement** : partitioner les ports d'une arborescence de switches en autant de VLANs (norme IEEE 802.1Q).
  +++ : architecture mutualisée, coût négligeable
  ––– : tributaire de la qualité de l'implémentation


Switch-CORE
Catalyst 4500
switchs
catalyst 2950
Liens Trunk Gigabit
switch1
switch2
switch3
switch4
VLAN Comptabilité :
10.1.1.0/24
VLAN Marketing :
10.1.2.0/24
VLAN R&D
10.1.3.0/24

Entêtes 802.1Q (trunk)

Flag	MAC dst	MAC src	Ethertype	Data	CRC
8	6	6	2	46-1500	4

VLAN tagging

Flag	MAC dst	MAC src	**Tag**	Ethertype	Data	CRC
8	6	6	**4**	2	46-1500	4

16 bits	3 bits	1 bit	12 bits
TPID `0x8100`	PCP	DEI	**VID**

VID = Identifiant de VLAN ≠ `0x000` ou `0xfff`

VLAN sous IOS (Cisco)

```
switch> enable
switch# vlan database
switch(vlan)# vlan 10 name enseignement
switch(vlan)# exit
```

```
switch# configure terminal
switch(config)# interface f0/2
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10

switch(config-if)# interface f0/5
switch(config-if)# switchport mode trunk encapsulate dot1q

switch# show vlan brief
```

VTP

- Les noms de chaque VLAN sont à définir sur chaque switch : c'est fastidieux et source d'erreur potentielle.

- **VTP** est un protocole propriétaire Cisco qui permet de distribuer les informations concernant les VLANs le long des liens **trunk**.

- À tester en salle E11 si vous avez la curiosité et le temps de le faire.

STP

Spanning-Tree Protocol

- Protocole **dynamique** permettant d'**élire** un arbre couvrant les switches d'un LAN pour éviter les cycles et offrir de la redondance.
- Fonctionne par VLAN chez Cisco et VDE.
- Reconfiguration en moins d'une minute.
- Actif a priori sur tous les ports du switch !

Attaque par inondation

Principe : Saturer le switch en le bombardant de trames avec des adresses MAC différentes.

Objectif : Faire basculer le switch en mode hub.

Effectivité : Les switches modernes permettent de limiter le nombre d’adresse par port ou de désactiver automatiquement les ports saturants.

Trunk spoofing

Principe : Envoyer des trames avec tag.

Objectif : Passer le port en mode trunk.

Effectivité : Ne fonctionne que si l'activation dynamique de liens trunk est activée (DTP).

Attaque par STP

Principe : Déni de service sur STP ou encore participation à l'élection pour se faire élire racine.

Objectif : Déni de service ou écoute du trafic.

Effectivité : Ne fonctionne que si les ports des machines participent au protocole STP : désactiver STP sur ces ports résout le problème !