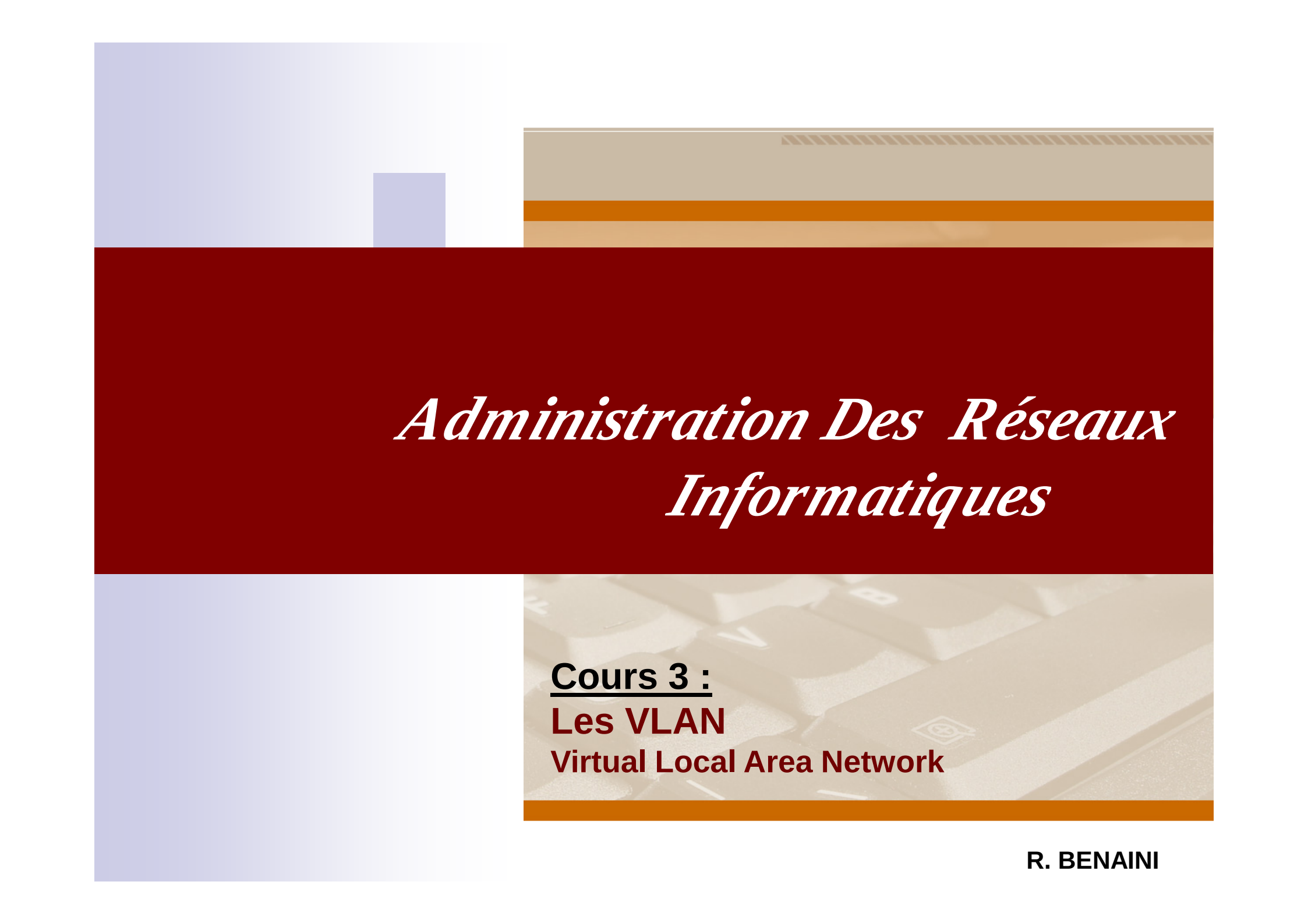




Administration Des Réseaux Informatiques

Cours 3 :

Les VLAN

Virtual Local Area Network



Plan

- ❑ Définition VLAN
- ❑ Types de VLAN
- ❑ Interconnexion inter-VLAN
- ❑ Exemple d'application



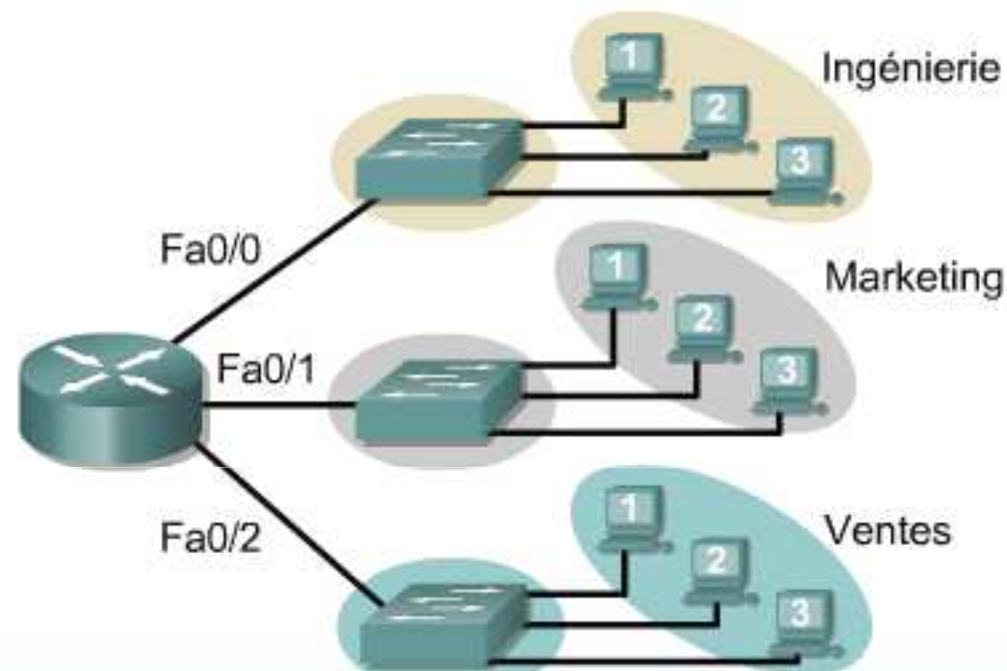
Définition VLAN

- ❑ Un **VLAN** est un réseau local virtuel
- ❑ L'emplacement géographique des éléments du VLAN peut être quelconque, ce qui implique d'émuler un réseau local, même si l'ensemble des clients est réparti géographiquement sur plusieurs commutateurs
- ❑ Un VLAN est doté de mécanismes assurant la diffusion sélective des informations (Le standard 802.1q)

Notions de base:

- VLAN par défaut toujours présent (VLAN1)
- Technologie en standard sur les switchs actuels
- Configuration au niveau de l'équipement

Organisation Réseau sans VLANs



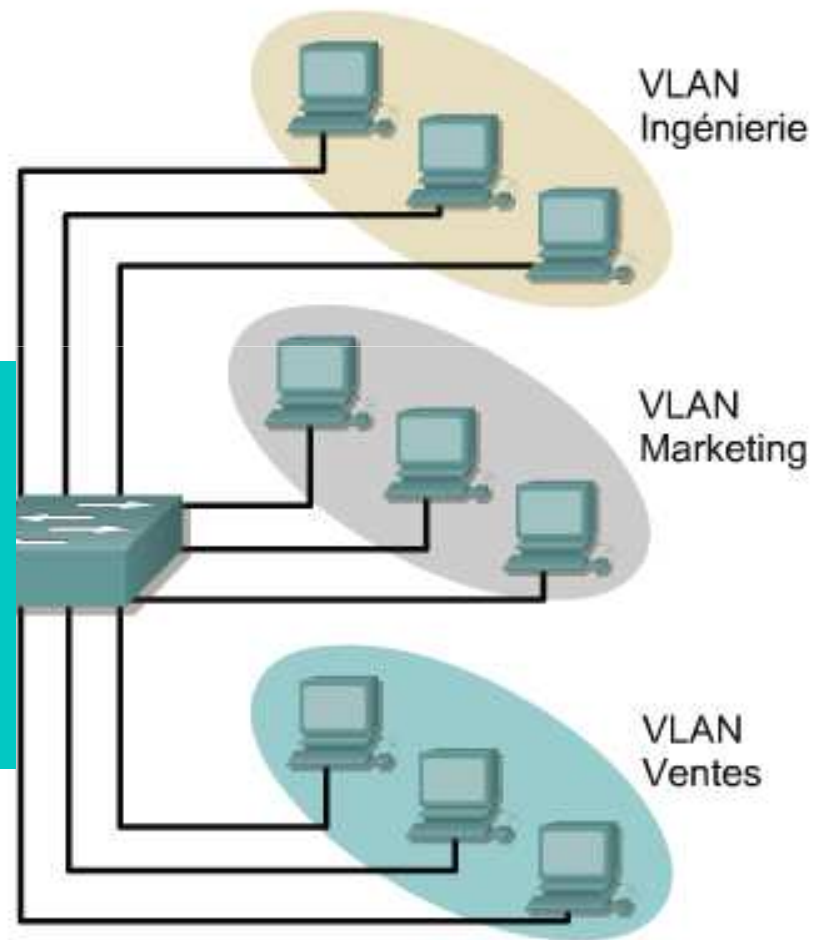
Trois commutateurs et un routeur peuvent être utilisés sans VLAN :

- Un commutateur pour le service Ingénierie
- Un commutateur pour le service Ventes
- Un commutateur pour le service Marketing
- Chaque commutateur considère tous les ports comme appartenant à un domaine de broadcast.
- Le routeur est utilisé pour acheminer les paquets sur les trois domaines de broadcast.

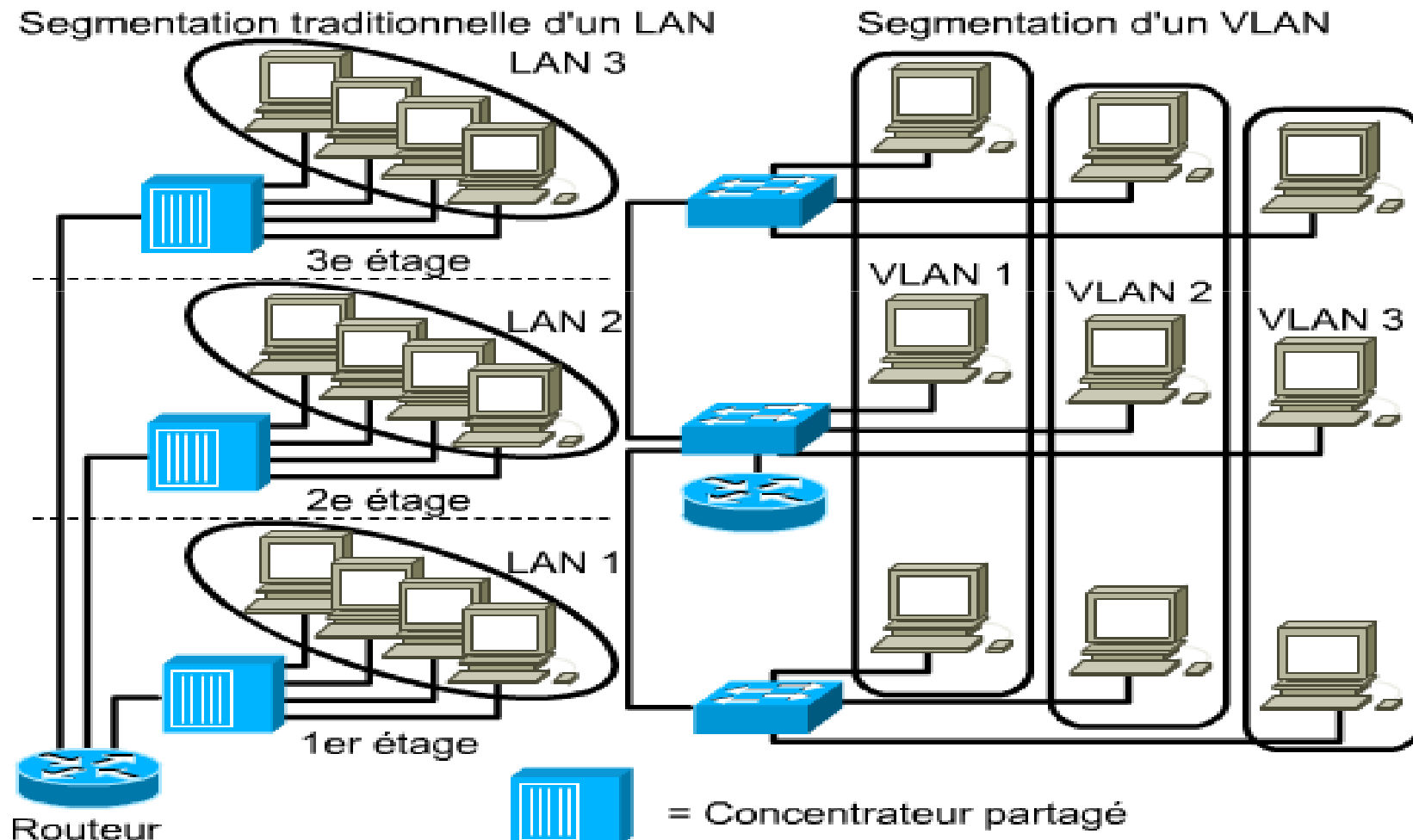
Organisation Réseau avec VLANs sur un seul commutateur

Les VLANs segmentent les réseaux commutés de manière logique :

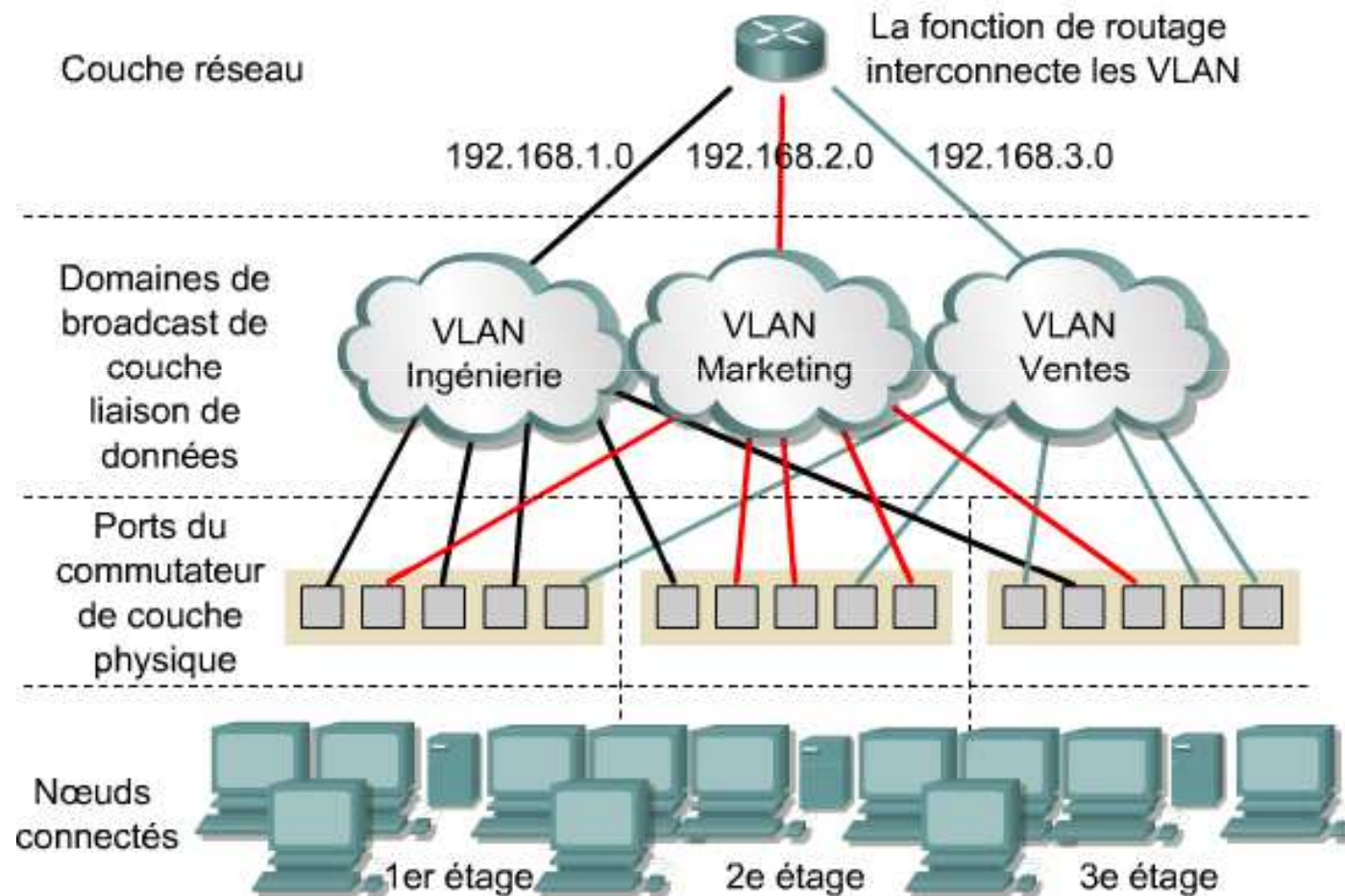
- Sur la base des fonctions,
- Des équipes de projet
- Des applications de l'entreprise,
- Etc.



Organisation Réseau avec VLANs sur plusieurs commutateurs



Exemple des VLANs sur plusieurs commutateurs





Differences entre LAN commuté et VLANs

- ❑ Les VLANs permettent de contrôler les broadcast
- ❑ Le dialogue inter-VLAN est assurée par les routeurs
- ❑ Les VLANs augmentent la sécurité
- ❑ Les VLANs regroupent les utilisateurs de manière logique (workgroup)



Types de VLANs

Définitions par ...

- ❑ Numéro de port physique sur commutateur (niveau 1)
- ❑ Adresse MAC utilisée (niveau 2)
- ❑ Adresse IP (adresse de niveau 3)
- ❑ Par type de Protocole Réseau (niveau 3)

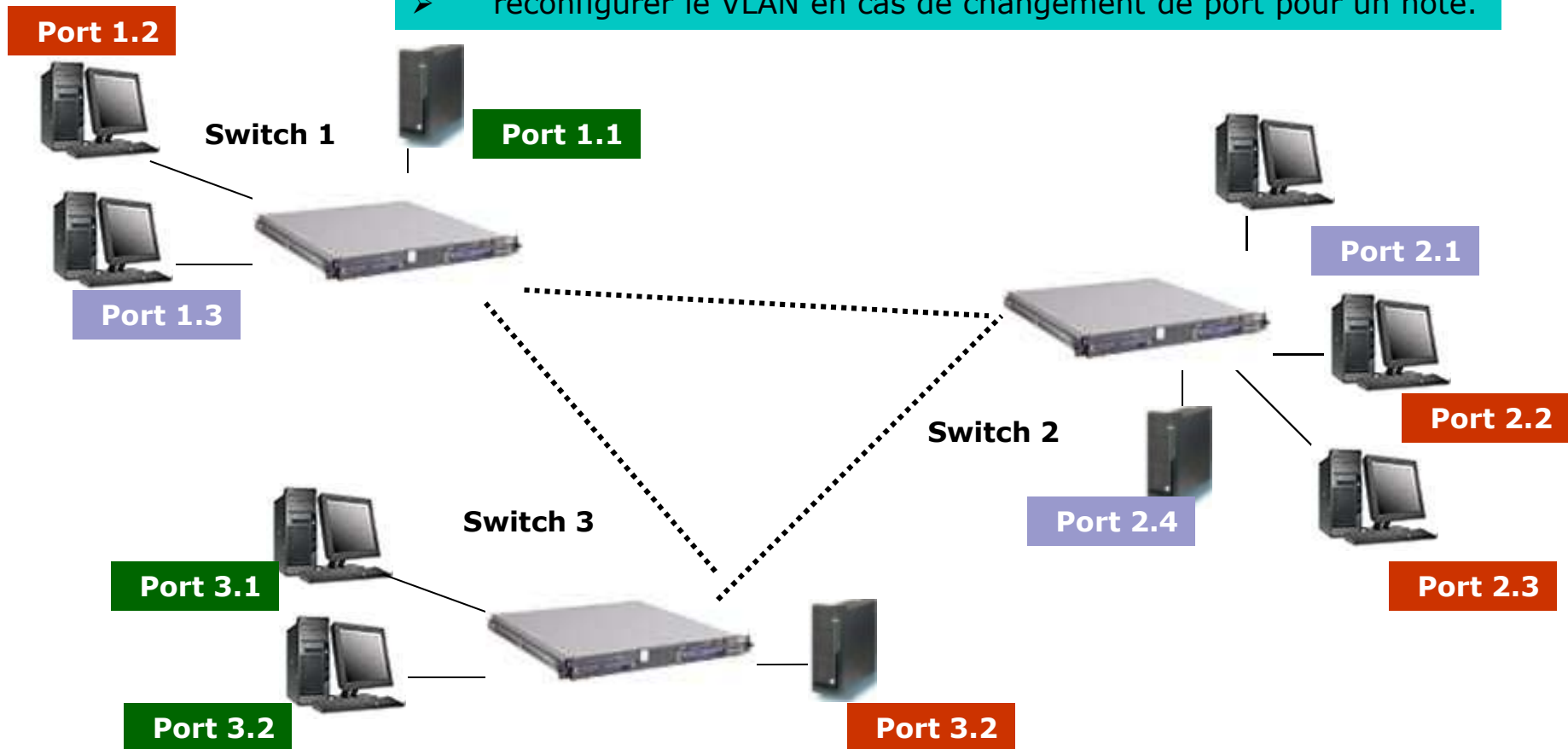
VLAN : Par numéro de port

Avantage :

- performant en temps de traitement.

Inconvénient :

- reconfigurer le VLAN en cas de changement de port pour un hôte.



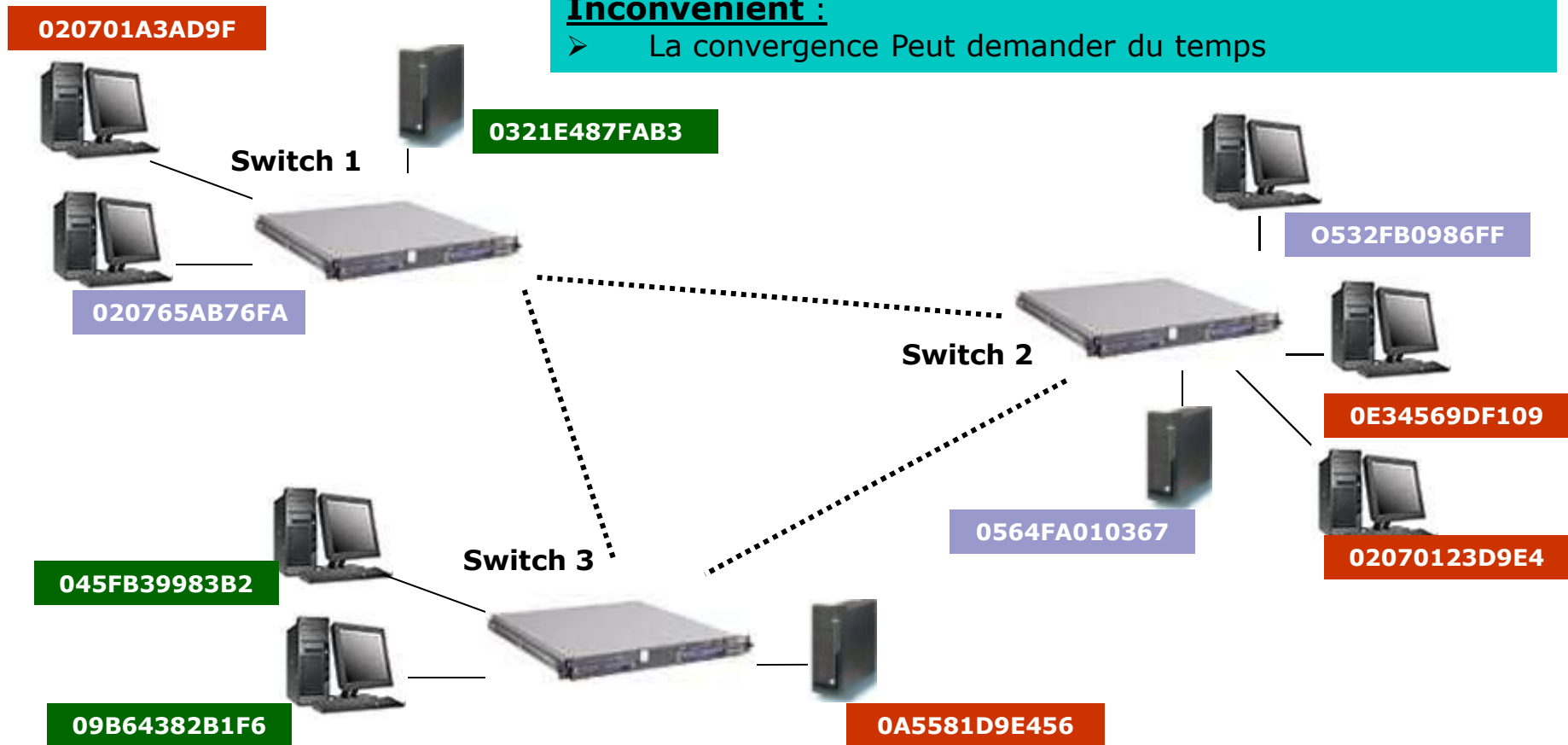
VLAN : Par adresse MAC

Avantages :

- indépendance de la localisation de la station
- le déplacement d'un utilisateur entraîne une redéfinition dynamique de la topologie du VLAN.

Inconvénient :

- La convergence Peut demander du temps



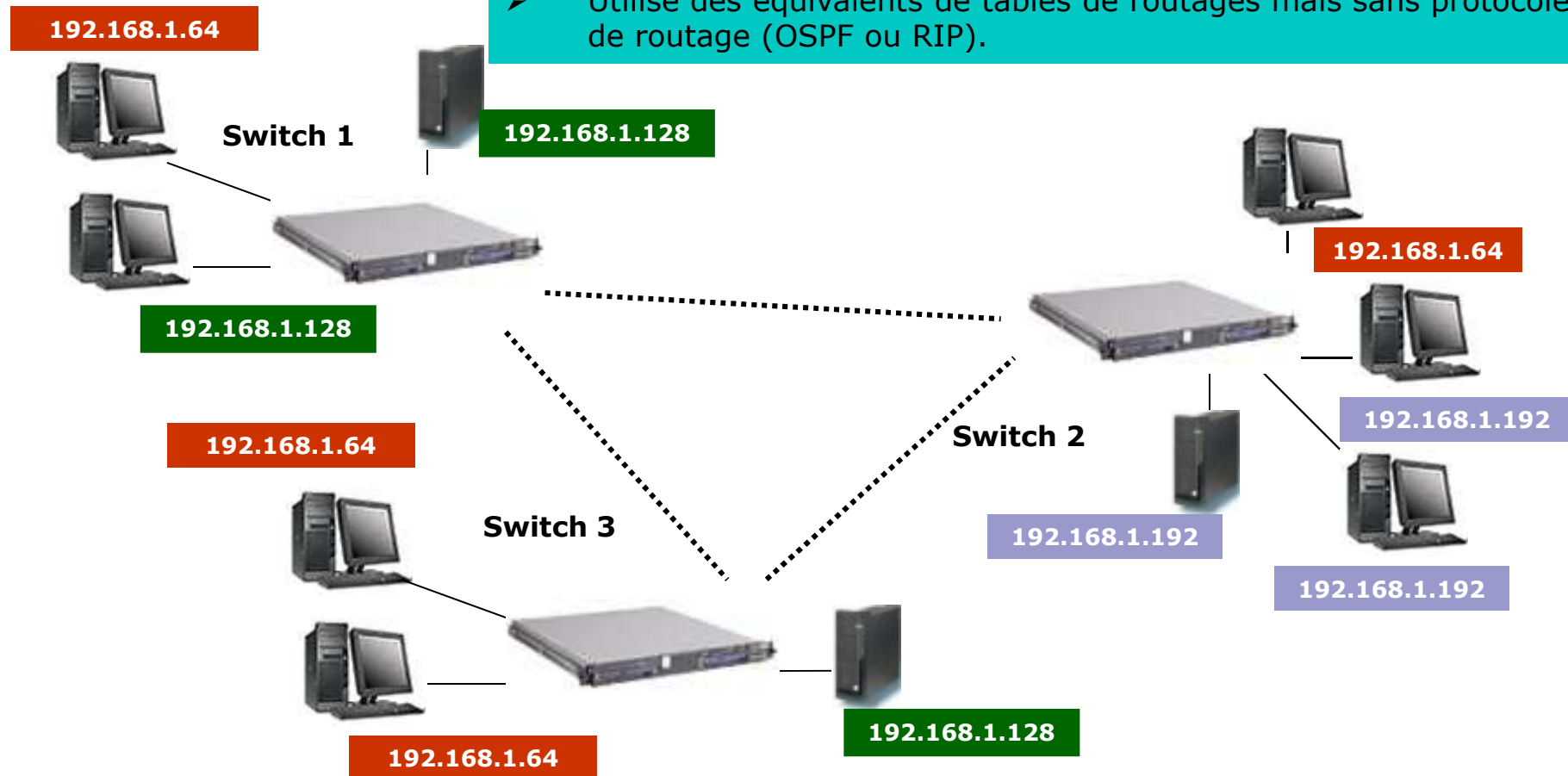
VLAN : Par sous-réseaux IP

Avantages :

- Permet la même souplesse que la solution à base de MAC

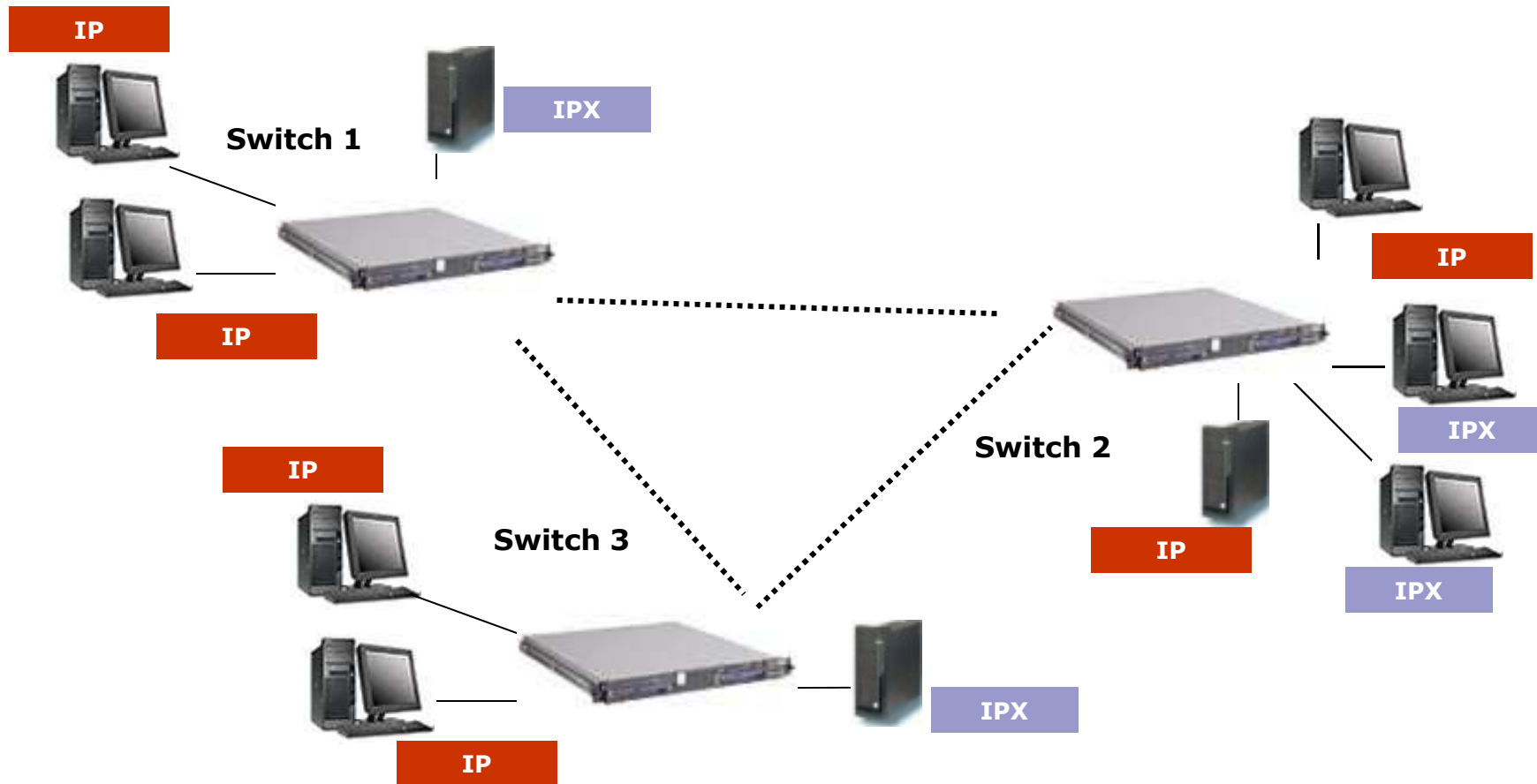
Inconvénient :

- Utilise des équivalents de tables de routages mais sans protocole de routage (OSPF ou RIP).



Vlan : par protocole

Du fait de l'hégémonie du protocole IP, cette solution tend à disparaître.



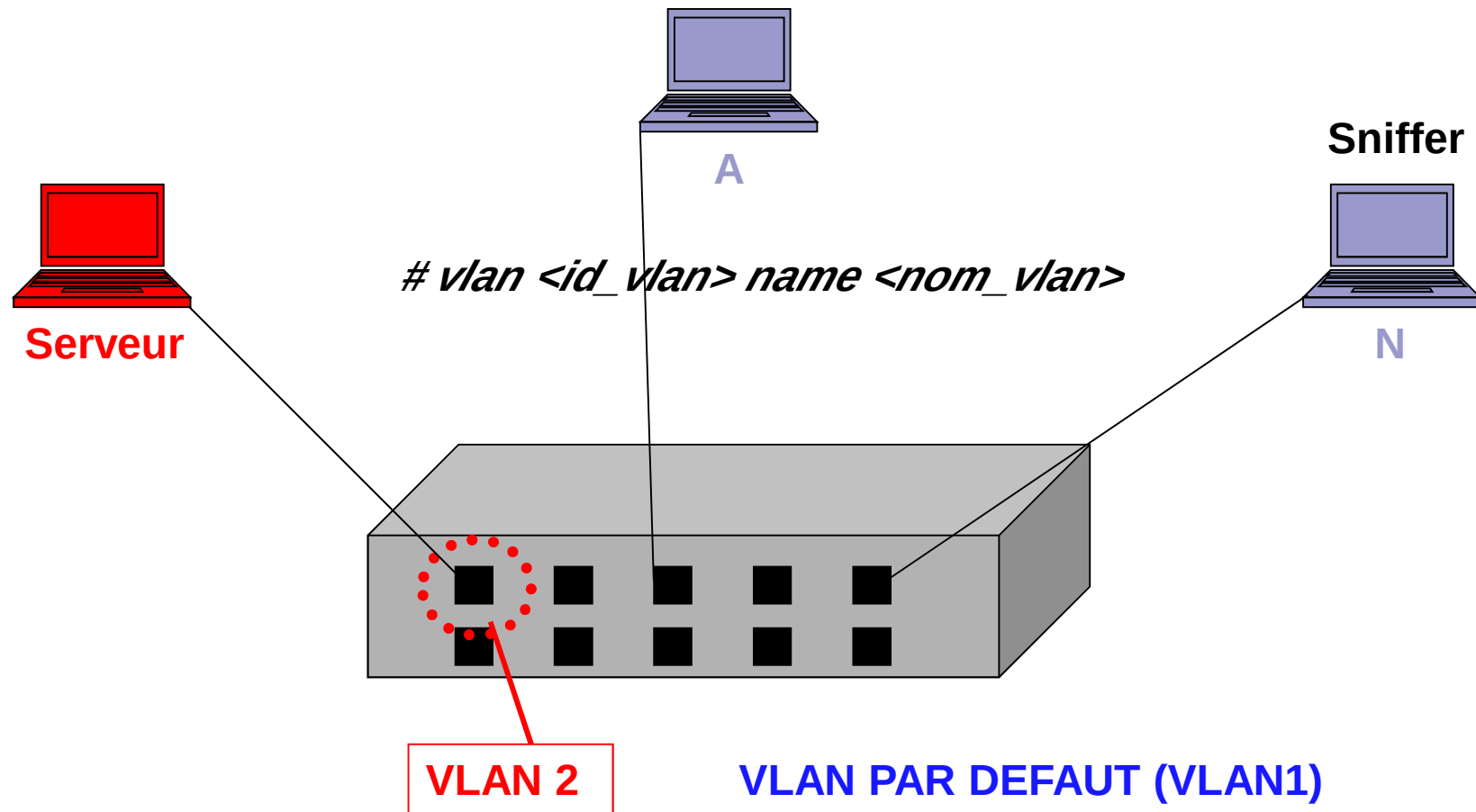


@MAC serveur ↔ @IP

The diagram illustrates a network setup for ARP flooding. A central switch, labeled "VLAN PAR DEFALT (VLAN1)", has four ports. Each port is connected to a device: "Serveur" (left), "A" (top), "N" (right), and an unlabeled bottom port. All four connections are labeled "ARP" in red. A dotted blue line encircles the switch's front panel. Above the switch, green text reads "@MAC serveur ↔ @IP" and "@MAC Serveur ?". A "Sniffer" laptop is connected to port "N".

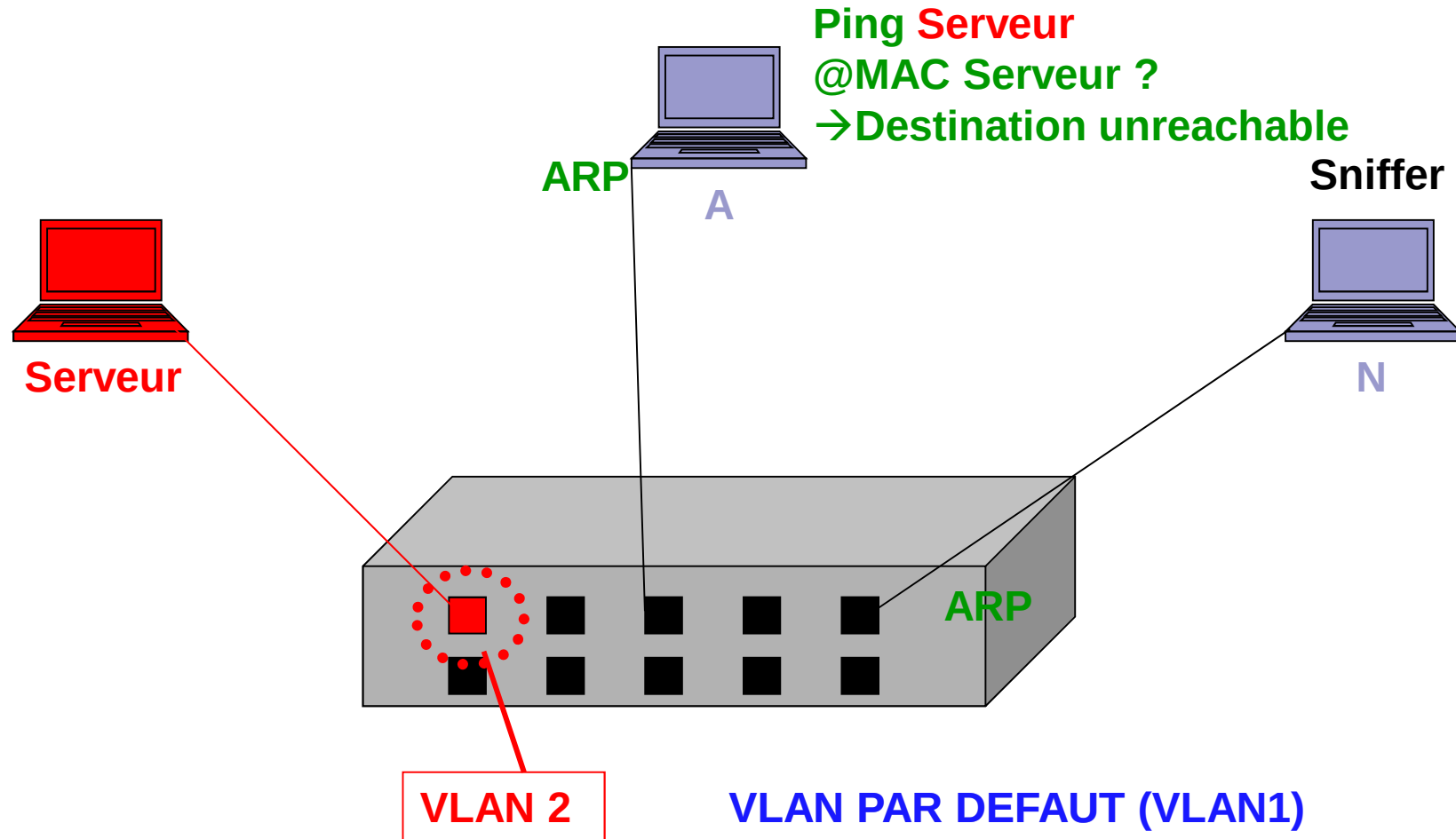
VLAN - Démonstration

Situation 1 : Serveur dans VLAN « 1 » , A & N dans VLAN DEFAULT



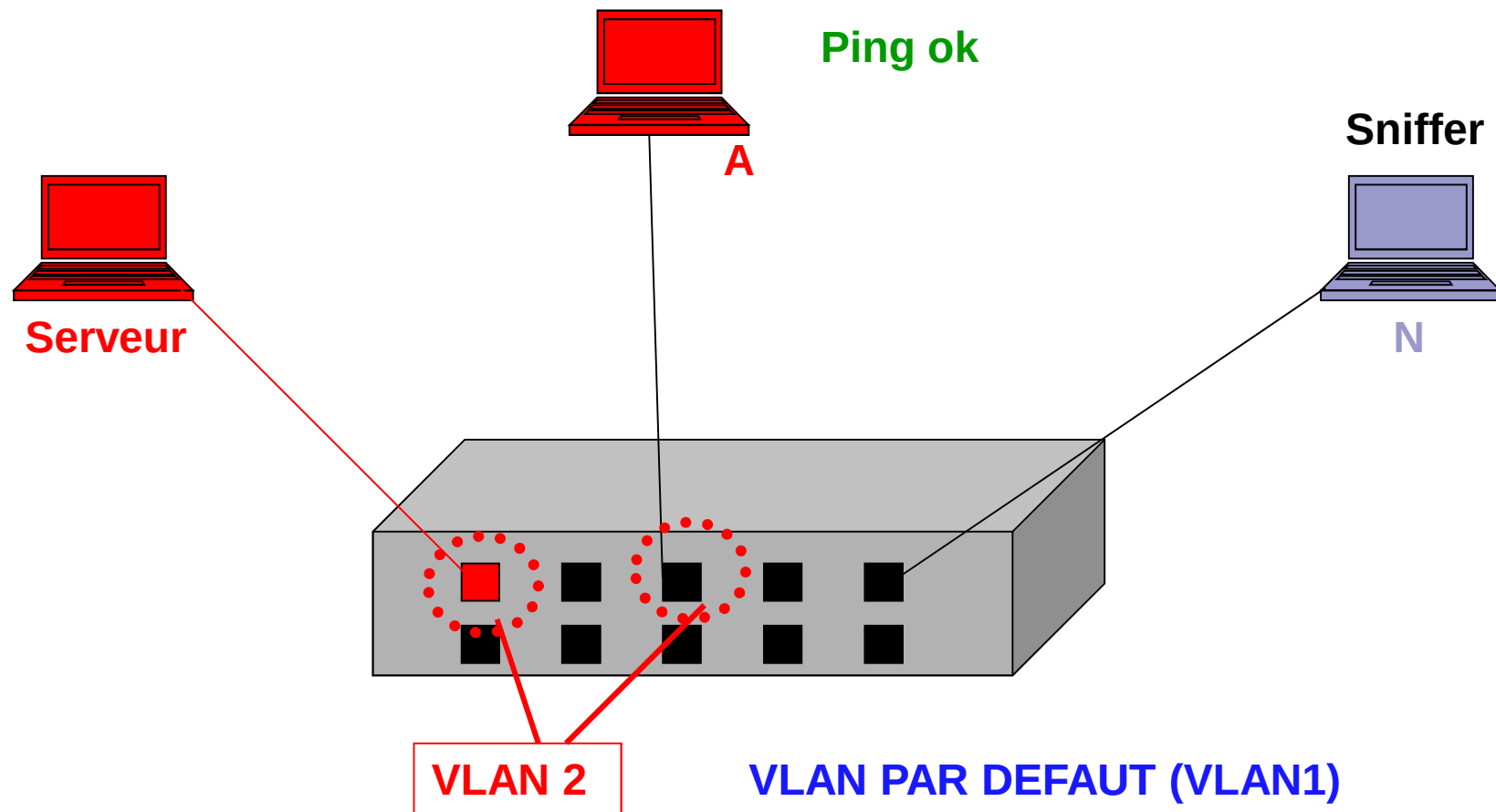
VLAN - Démonstration

Situation 2 : Serveur dans VLAN « 1 » , A & N dans VLAN DEFAULT



VLAN - Démonstration

Situation 3 : Serveur & A dans VLAN « 1 » , N dans VLAN DEFAULT



Communication inter-VLAN

➤ comment propager l'appartenance à un VLAN d'un commutateur vers un autre ?

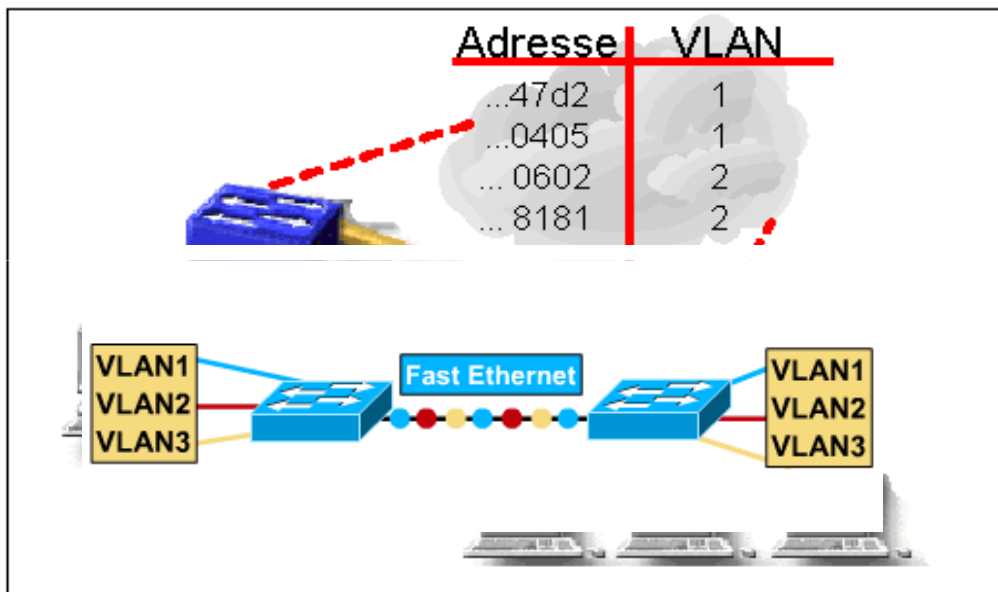
Problématique : lorsqu'une trame circule d'un commutateur à un autre, comment identifier son appartenance à un vlan ?



2 techniques:

- Filtrage de trames (vieille technologie)
- 'Frame tagging' (nouvelle méthode)

Filtrage de trames (ancienne méthode)



- Utilise une table de filtrage basée sur:
 - l'adresse physique (MAC) de la couche 2
 - l'adresse logique (IP) de la couche 3
 - le type d'application

- Une table de filtrage par commutateur
- Échange des tables de filtrage entre les commutateurs
- Le commutateur prend l'action appropriée

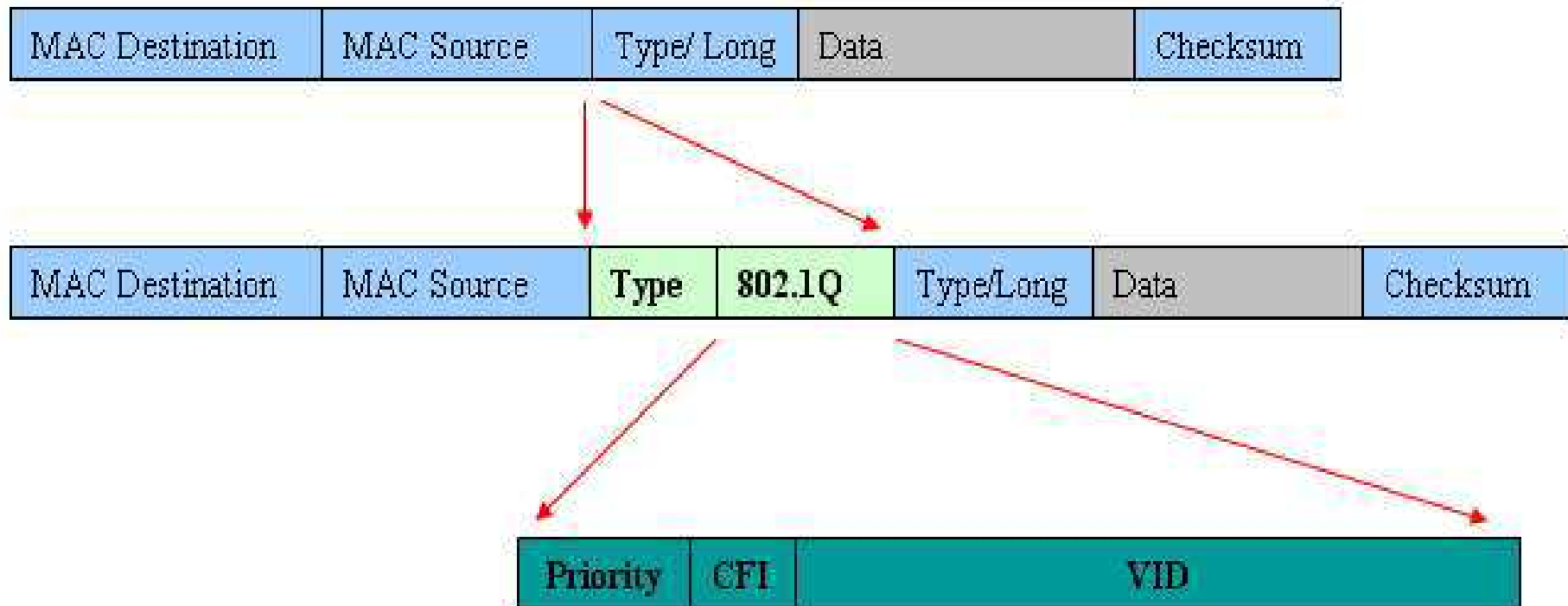


Identification de trames (Frame tagging : 802.1 Q) (nouvelle méthode)

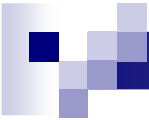
- Place un identificateur unique dans l'en-tête de trame
- L'identificateur est retiré par le commutateur lorsqu'il arrive au segment final (horizontal)
- Utilise moins de ressources que le filtrage

Étiquette VLAN 802.1Q

- Extension du format Ethernet, ajout de 4 octets



- Type : « 0x8100 » pour le protocole 802.1Q
- 802.1Q :
 - Priority (3 bits)
 - CFI (1 bit) : utilisé seulement dans le cas de token ring
 - VID (12 bits) : VLAN ID



Qualité de service : 802.1p

- Utilise trois premiers bits du champ de 4 octets (type) pour la définition potentielle de 8 niveaux de priorités.
- Non géré par les stations d'extrémité et pas gérés par tous les commutateurs du marché.
- Dans les faits, peu exploité ...

La préférence va au champ ToS d'IPV4 et V6 (QoS Diffserv)

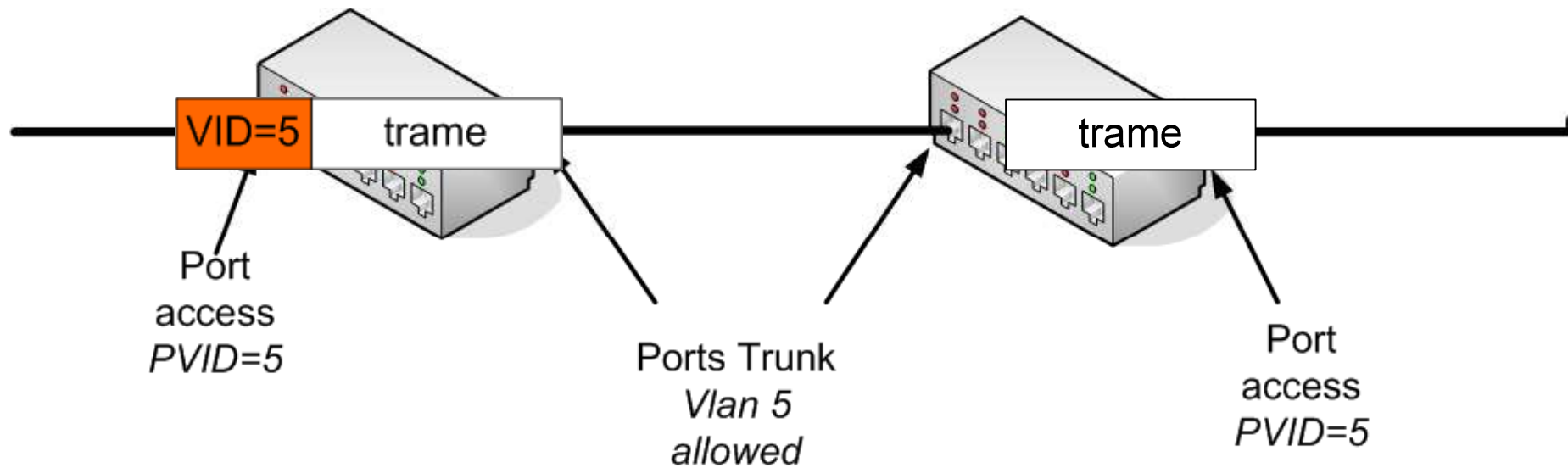


802.1Q – Démonstration

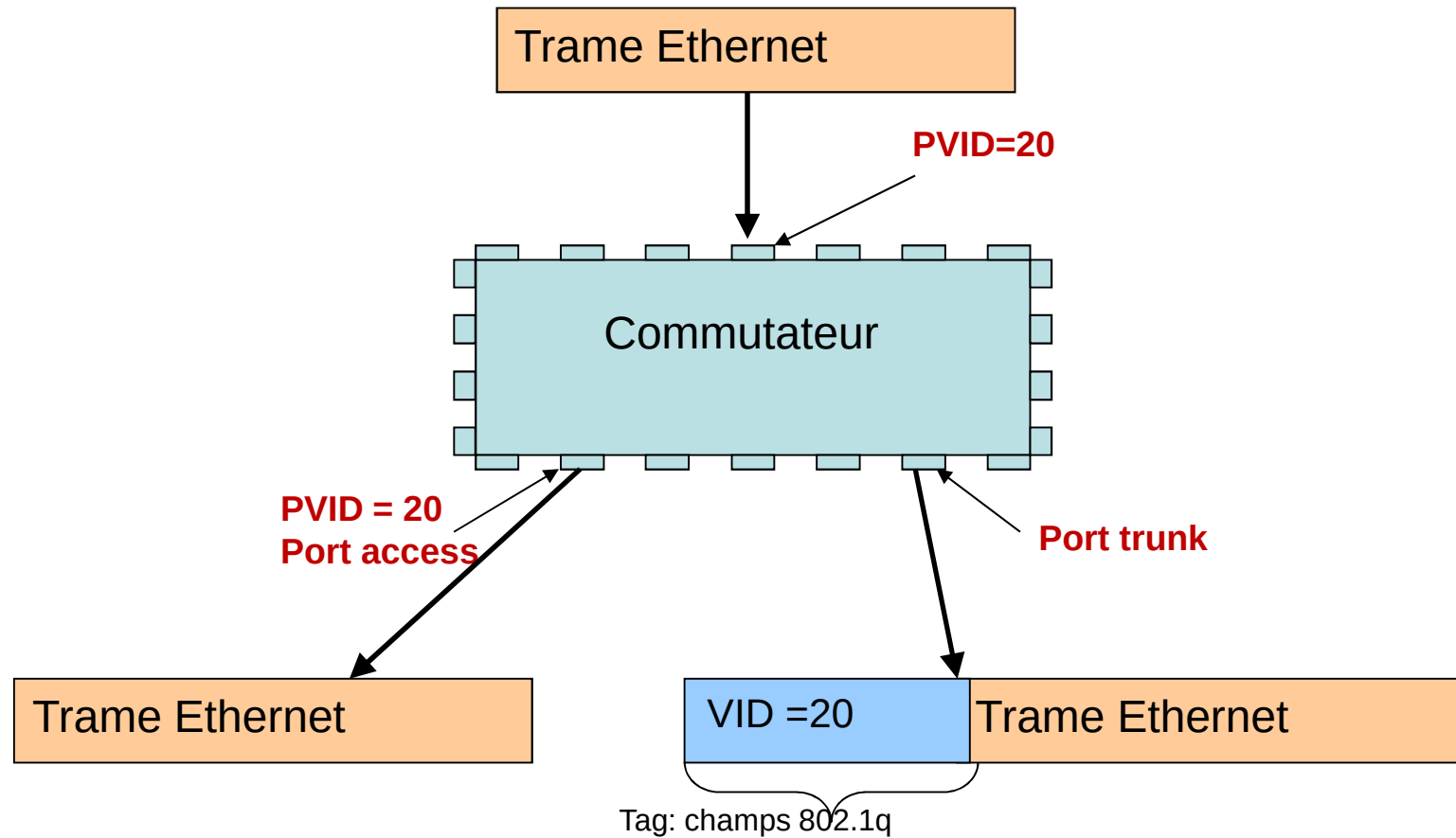
un extrait de capture, réalisée avec Wireshark, qui illustre les champs de la balise IEEE 802.1Q.

```
Frame 103 (1518 bytes on wire, 1518 bytes captured)
Ethernet II, Src: 00:14:f2:75:ed:72, Dst: 00:10:5a:de:9d:d7
  Destination: 3com_de:9d:d7 (00:10:5a:de:9d:d7)
  Source: Cisco_75:ed:72 (00:14:f2:75:ed:72)
  Type: 802.1Q Virtual LAN (0x8100) ①
802.1Q Virtual LAN
  000. .... = Priority: 0 ②
  ...0 .... = CFI: 0 ③
  .... 0000 0110 0100 = ID: 100 ④
  Type: IP (0x0800)
Internet Protocol, Src: 172.17.0.2 (172.17.0.2), Dst: 172.16.80.19 (172.16.80.19)
Transmission Control Protocol, Src Port: www (80), Dst Port: 1548 (1548)
```

802.1Q – Démonstration

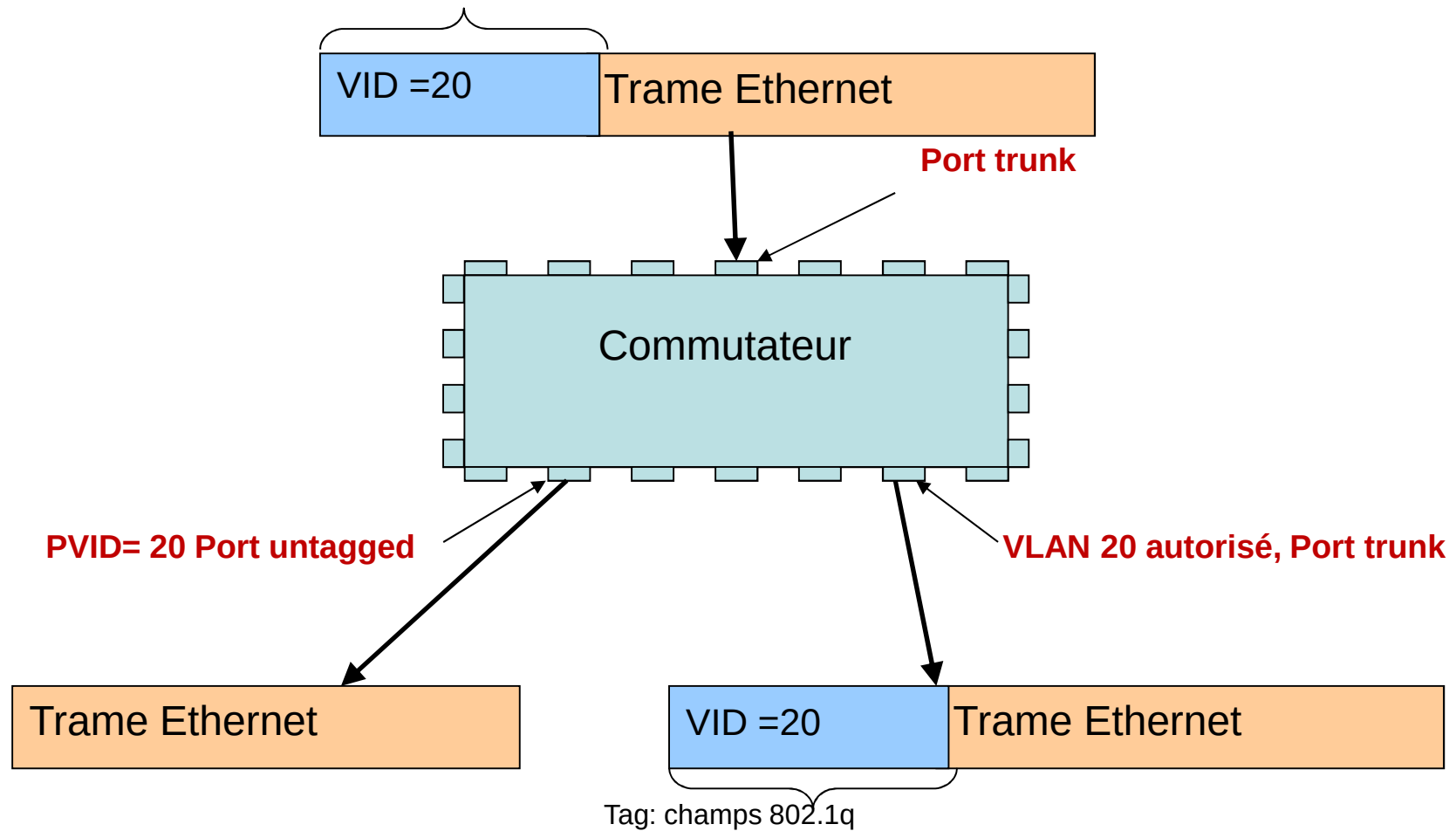


802.1Q – Exemple



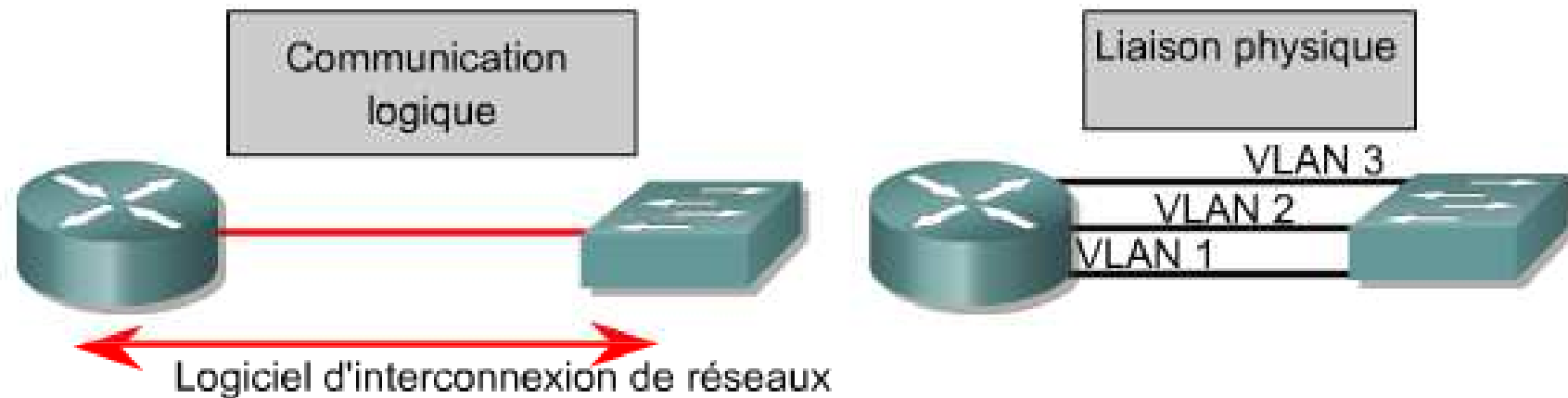
802.1Q – Exemple

Tag: champs 802.1q



Communication inter-VLAN via un routeur

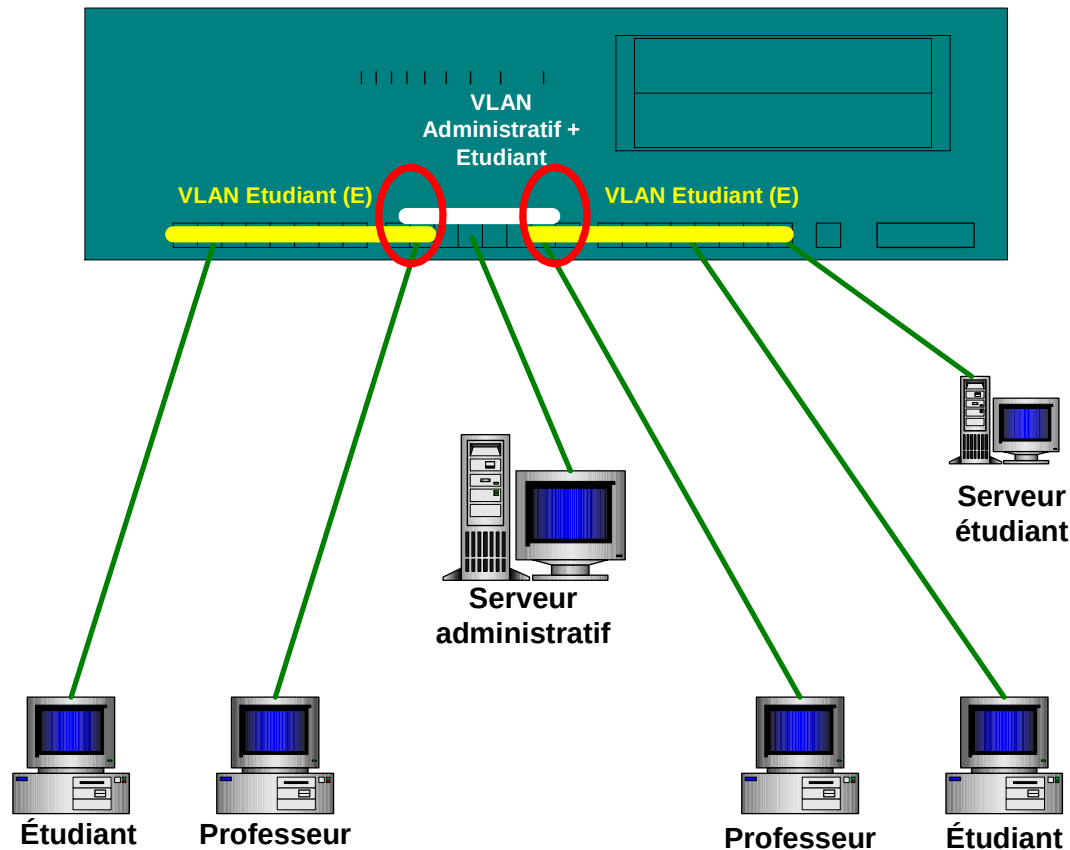
Deux approches de topologie physique



L'utilisation de routeurs de couche 3 pour lier les VLAN procure les avantages suivants :

- Cela apporte plus de sécurité et améliore la gestion.
- Les liaisons logiques conservent les ports physiques.
- Les routeurs contrôlent l'accès aux VLAN.
- 255 VLAN ou plus peuvent être pris en charge par chaque routeur.

Overlapping VLANs



- Un port peut appartenir à plus d'un VLAN à la fois
- Nombre limité de configurations
- Problème de sécurité physique



Configuration de VLAN: Membership Mode

- 1. Static access** : A static-access port can belong to one VLAN and is manually assigned. By default, all ports are static-access ports assigned to VLAN 1.
- 2. Multi-VLAN** : A multi-VLAN port can belong to up to 250 VLANs (some models only support 64 VLANs) and is manually assigned. You cannot configure a multi-VLAN port when a trunk is configured on the switch.
- 3. Trunk** : Ex: ISL or 802.1q. A trunk is a member of all VLANs in the VLAN database by default, but membership can be limited by configuring the allowed-VLAN list.

```
config-if# switchport mode xxxxx (access, multi ou trunk)
```



Configuration de VLAN

	Command	Purpose
Step 1	Router# vlan database	Enter VLAN configuration mode.
Step 2	Router(vlan)# vlan <i>vlan_id</i>	Add an Ethernet VLAN.
Step 3	Router(vlan)# exit	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	Router# show vlan name <i>vlan_name</i>	Verify the VLAN configuration.



Exemple de Création d'un VLAN

- Pour ajouter un VLAN à un commutateur, entrez les commandes:

```
Switch#vlan database  
Switch(vlan)# vlan 3  
VLAN 3 added: Name: VLAN0003
```

- Pour enlever un VLAN entièrement d'un commutateur, entrez les commandes:

```
Switch#vlan database  
Switch(vlan)#no vlan 3
```



Affectation des ports à un VLAN

Enter configuration commands, one per line. End with CNTL/Z.

```
SydneySwitch#configure terminal
```

```
SydneySwitch(config)#interface fastethernet 0/9
```

```
SydneySwitch(config-if)#switchport access vlan 300
```

```
SydneySwitch(config-if)#exit
```

```
SydneySwitch(config)#exit
```


Verification de la Configuration VLAN

Cisco

SydneySwitch#show vlan

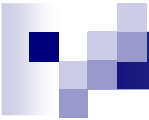
VLAN	Name	Status	Ports							

VLAN	Name	Status	Ports							

1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4							
2	VLAN2	active	Fa0/5, Fa0/6, Fa0/7							
3	VLAN3	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12							
1002	fddi-default	active								
1003	token-ring-default	active								
1004	fddinet-default	active								
1005	trnet-default	active								

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2

1	enet	100001	1500	-	-	-	-	-	1002	1003
2	enet	100002	1500	-	-	-	-	-	0	0



Question ?

- 1. Peut-on associer une trame à plusieurs Vlan ?**
- 2. Cela implique-t-il qu'un port de commutateur ne doit être associée qu'à un seul Vlan ?**
- 3. La carte réseau d'un poste peut-elle être associée à plusieurs Vlan ?**



Réponse

Peut-on associer une trame à plusieurs Vlan ?

Non. En effet une trame associée à un VLAN quelle que soit la méthode d'association ne peut être adressée qu'à une carte réseau associée à ce VLAN. l'entête 802.1Q n'admet qu'un seul identifiant VLAN (VID) pour une trame

Cela implique-t-il qu'un port de commutateur ne doit être associée qu'à un seul Vlan ?

s'il n'est associé qu'à un seul Vlan comment répartir un Vlan sur plusieurs commutateurs, car les ports d'interconnexion doivent pouvoir faire transiter des trames en provenance de différents Vlan ? Mais si une trame non étiquetée arrive sur ce port il doit pouvoir l'associer sans ambiguïté avec un VID. Dans la pratique les ports seront affectés à un seul Vlan et les ports d'interconnexion entre commutateurs à plusieurs Vlan.

La carte réseau d'un poste peut-elle être associée à plusieurs Vlan ?

Si oui comment savoir à quel Vlan appartient une trame émise par une telle carte réseau ? Si non comment partager l'accès à des ressources communes entre différentes Vlan ? Une réponse serait des Vlan de niveau 3



Résumé

- Le concept de réseau local virtuel (VLAN) est une fonctionnalité importante de la commutation Ethernet. Un VLAN est un groupement logique d'unités ou d'utilisateurs. Ces unités ou ces utilisateurs peuvent être regroupés par fonction, service, application, etc., et ce, quel que soit le segment physique LAN où ils se trouvent.
- Les VLAN augmentent les performances globales du réseau en regroupant les utilisateurs et les ressources qui communiquent le plus fréquemment les uns avec les autres.
- Les VLAN peuvent améliorer l'évolutivité, la sécurité et la gestion des réseaux. Les routeurs dans les topologies VLAN offrent des services de filtrage des broadcasts, de sécurité et de gestion du flux du trafic.
- Les VLAN peuvent être créés sous forme de réseaux de bout en bout qui englobent l'ensemble de la matrice de commutation ou exister à l'intérieur de frontières géographiques. Les VLAN de bout en bout permettent de regrouper les équipements en fonction de l'utilisation des ressources.
- Les VLAN statiques correspondent aux ports d'un commutateur qui sont affectés manuellement à un VLAN via une application de gestion de VLAN ou directement à l'intérieur d'un commutateur.
- Les VLAN offrent une grande souplesse de conception et de mise en œuvre aux ingénieurs réseau.