

CHAPITRE 2

LES LANs VIRTUELS (VLANs)

Auditoire : D-LCS GLSI-IM

Plan

- Segmentation d'un VLAN
 - Problématiques et définitions
 - Avantages
 - Types de VLANs
 - Etiquetage des trames Ethernet
- Implémentation de VLANs
- Routage inter-VLANs

Problématique

- Constatation : quelques lacunes dans l'exploitation des ressources.



Ce qui nuit à l'efficacité et au rendement des employés

Stagiaire

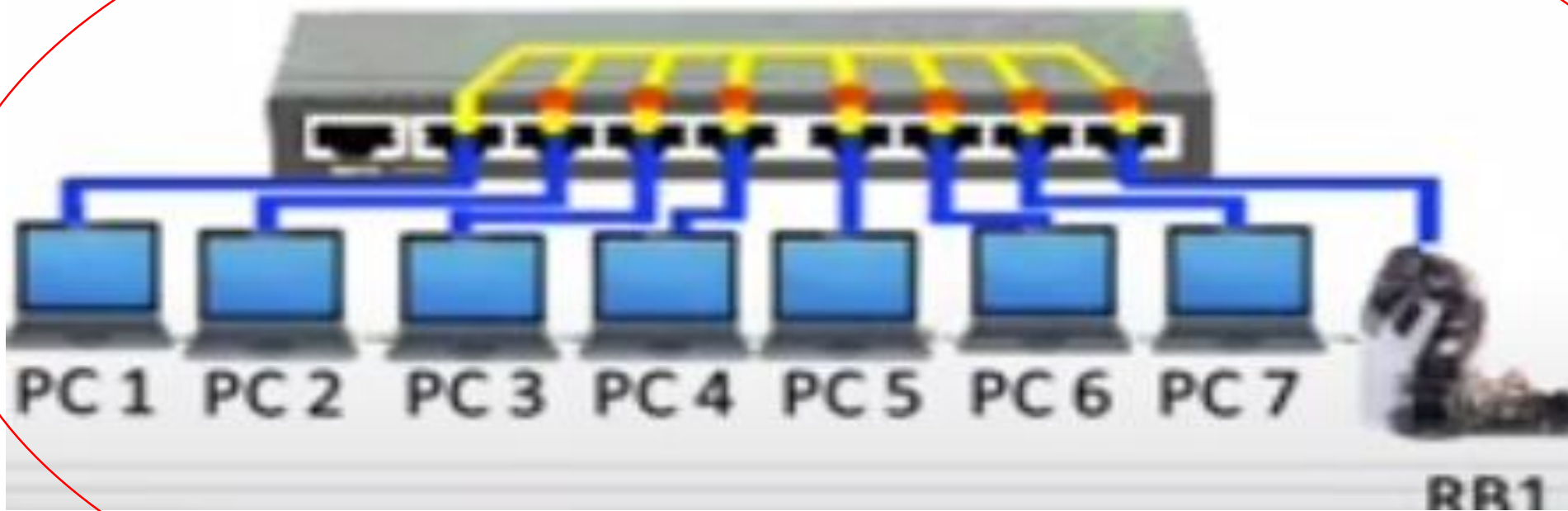
Dans l'entreprise: les machines et les serveurs sont connectés à des switches de couche 2 font partie du même segment réseau.



Direction d'entreprise

Problématique

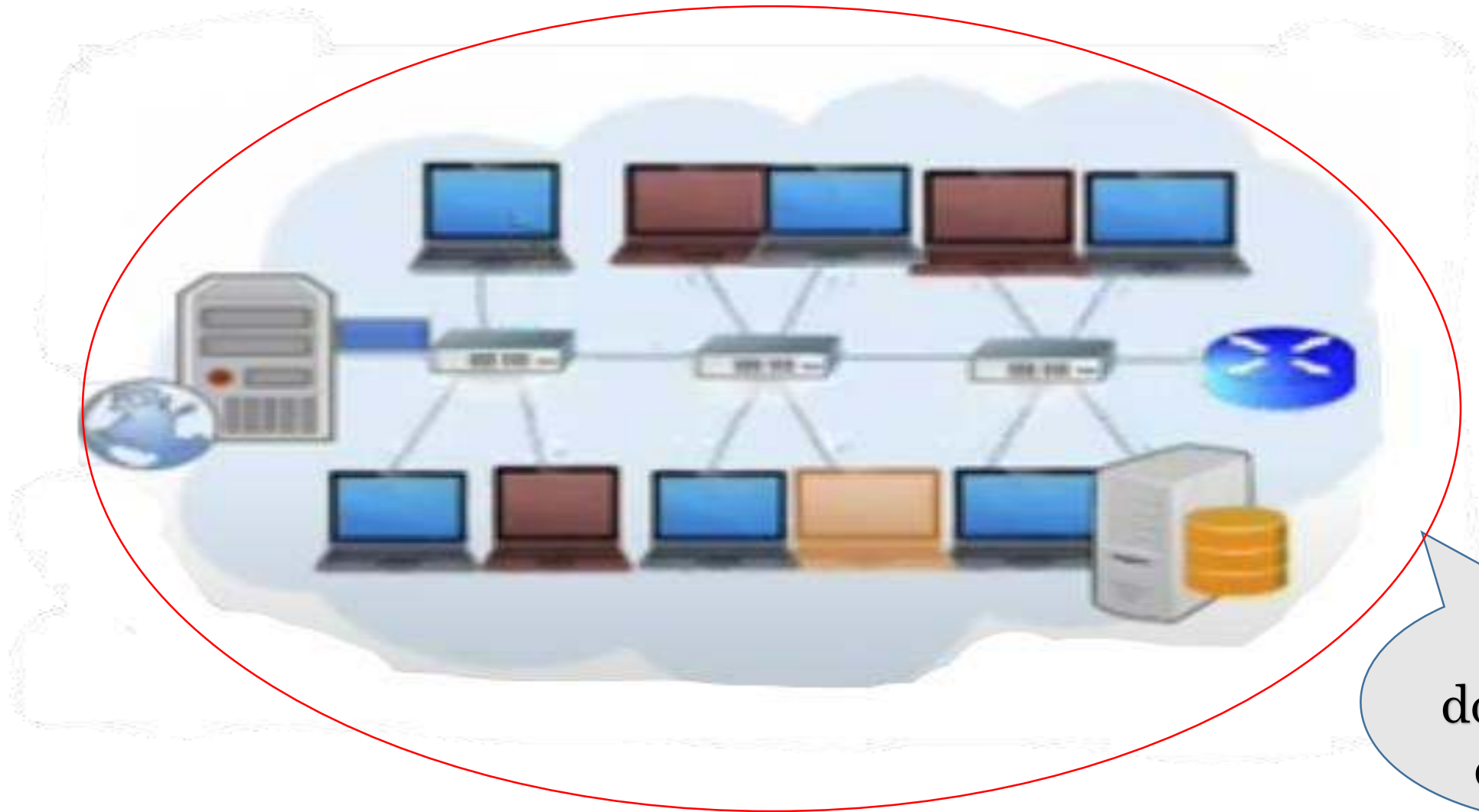
Switch



Un seul
domaine de
diffusion

PC1 envoie à tout le monde (**Broadcast**)

Problématique



Un seul
domaine de
diffusion

Problématique

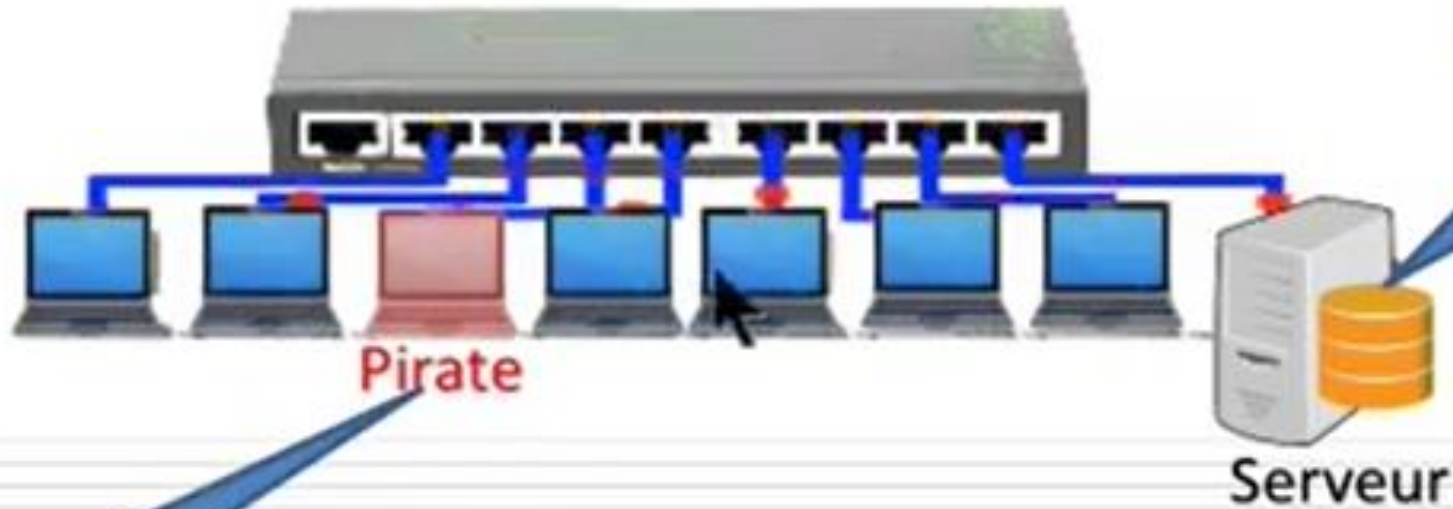
1_Des diffusions consomment la bande passante de façon inutile (surtout avec plusieurs PCs dans un LAN).



2_Chaque périphérique connecté à un commutateur peut transférer et recevoir des trames

Problématique

Switch



On me dérange trop
avec toutes ces
diffusions qui ne
m'intéressent pas



Je reçois
tout



Toute l'entreprise est reliée à un seul LAN, toutes les diffusions touchent toutes les machines et les équipements

Solution ???

Remplacer les
switches par des
routeurs

Les VLANS

Mais !!!!
Trop cher et pas pratique

C'est quoi !!??



Objectif du travail



Pour répondre à cette problématique, j'ai présenté une solution qui est développée autour des VLANS



➤ **Vlan?**

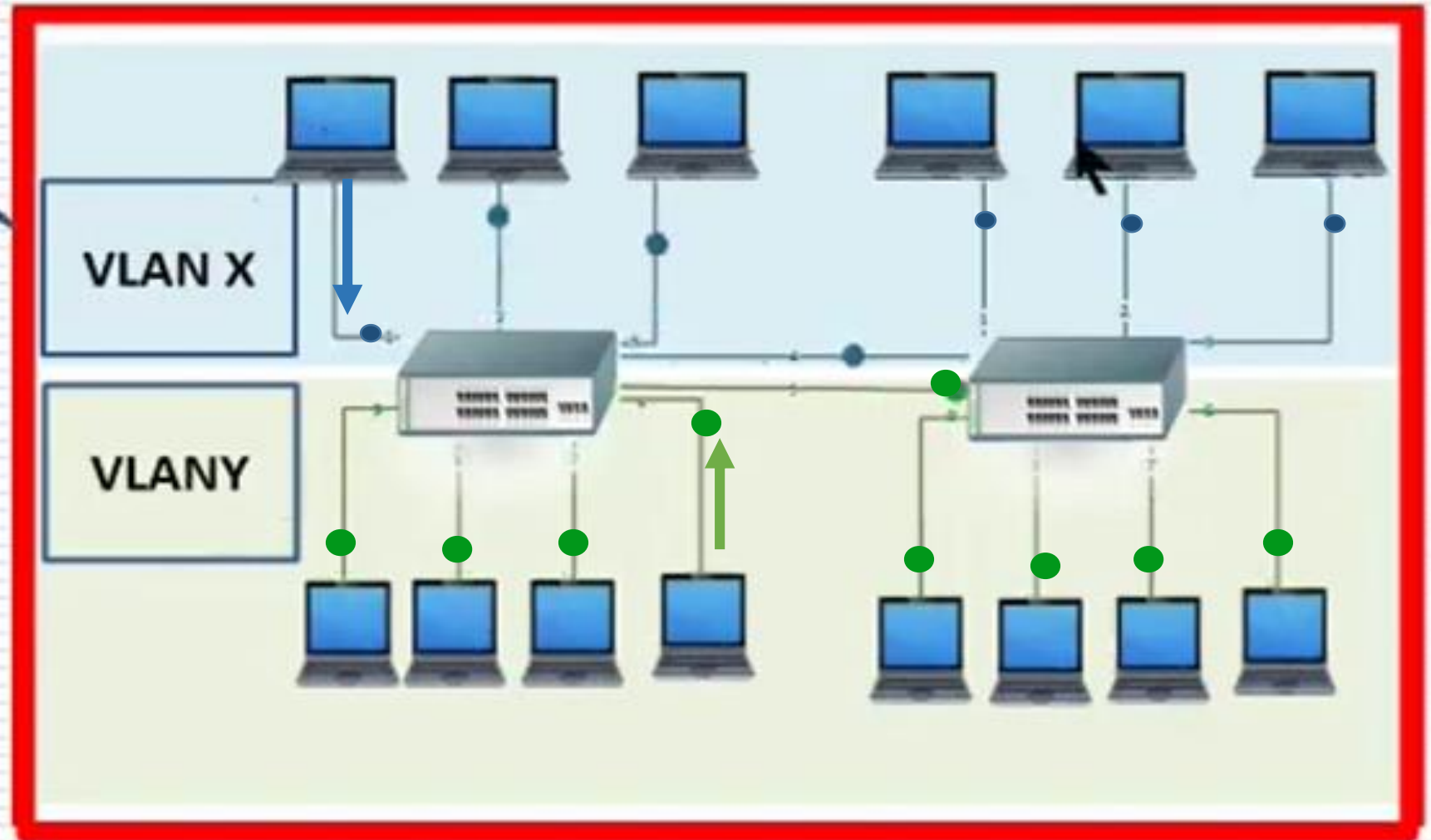
➤ **Pourquoi les réseaux locaux virtuels ?**

Réseaux locaux virtuels ?

LAN

Un seul LAN
peut être divisé
entre deux ou
plusieurs VLANs

Diffusions entre
les machines de
même VLAN

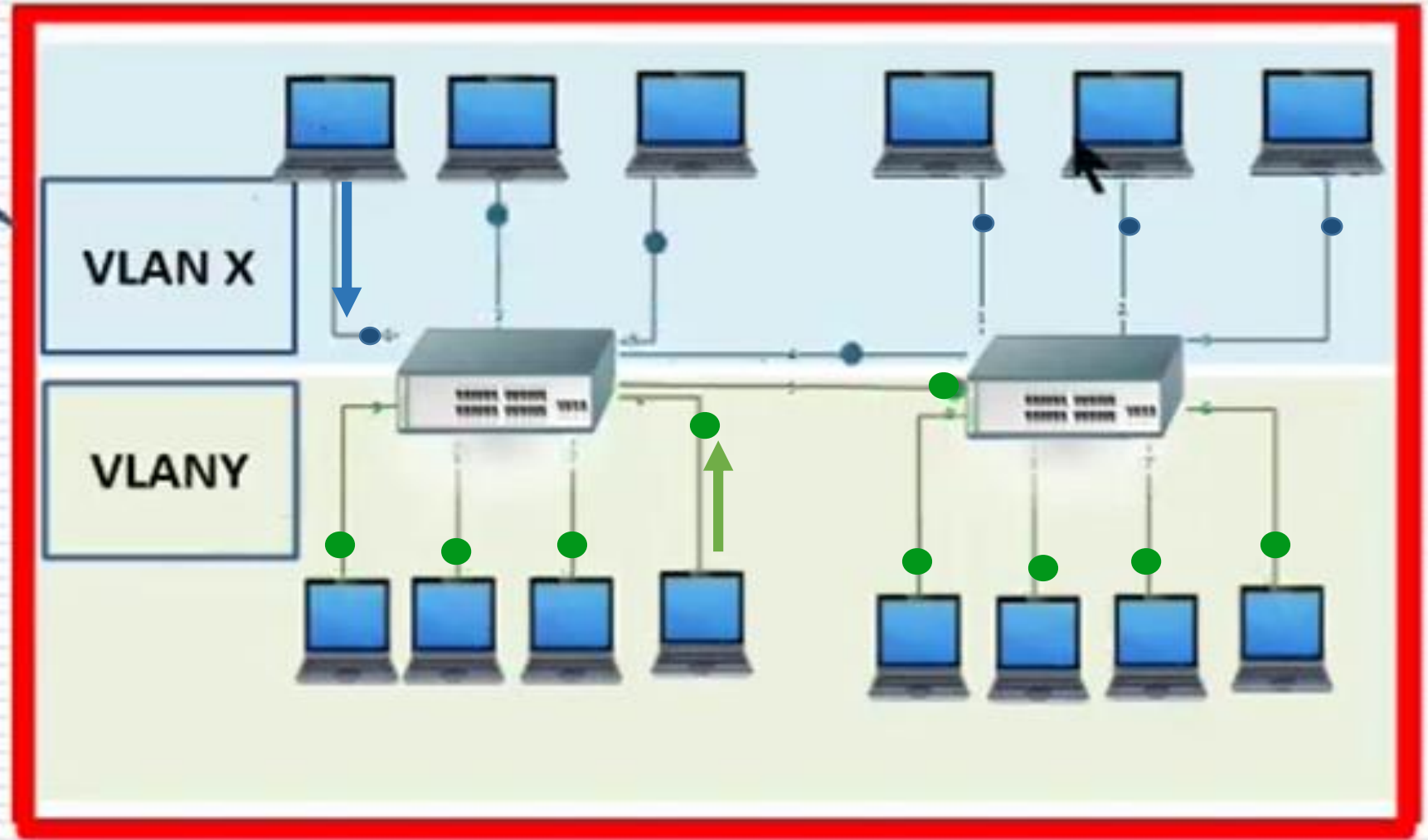


Réseaux locaux virtuels ?

LAN

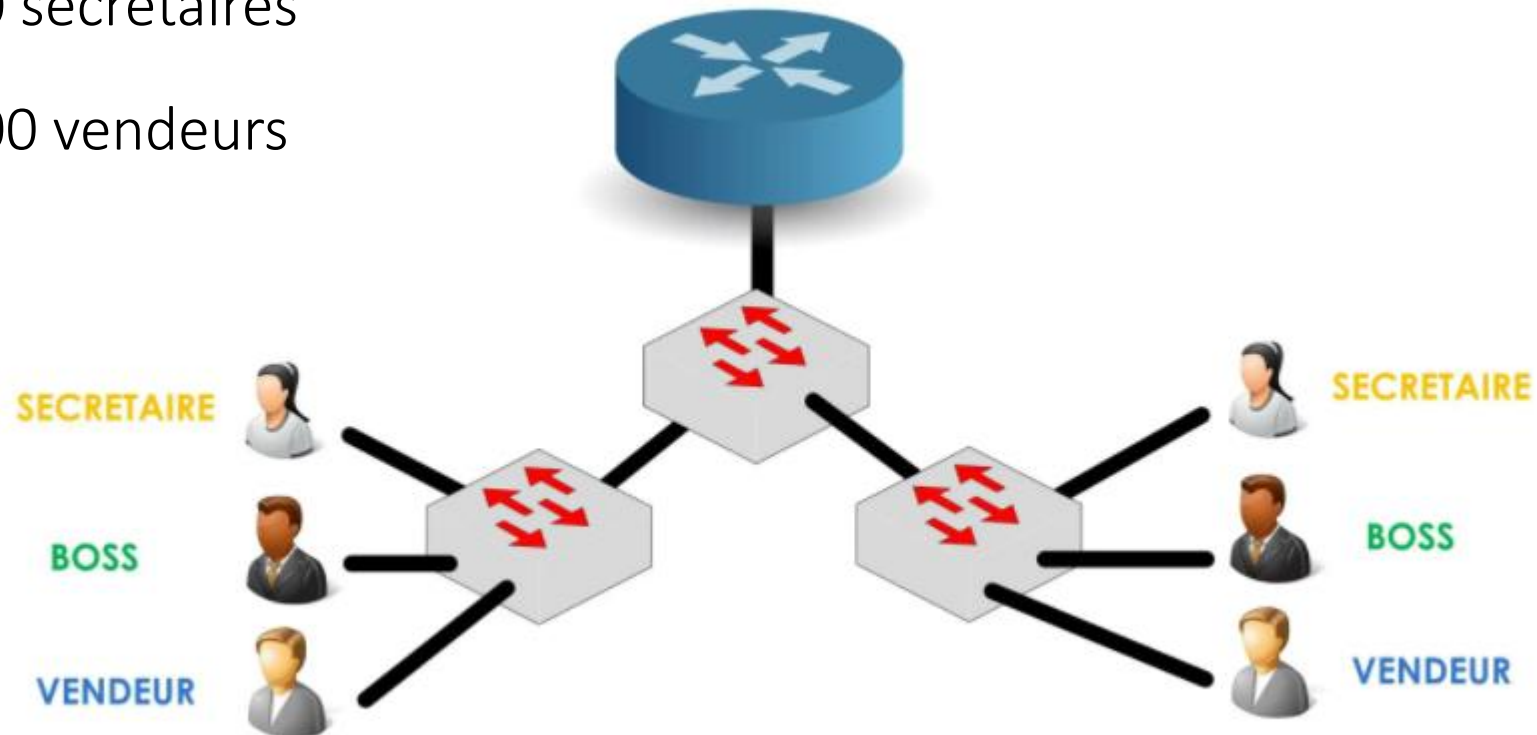
Un VLAN peut
exister sur
plusieurs
commutateurs

Un commutateur
peut contenir
plusieurs VLANs



LAN classique

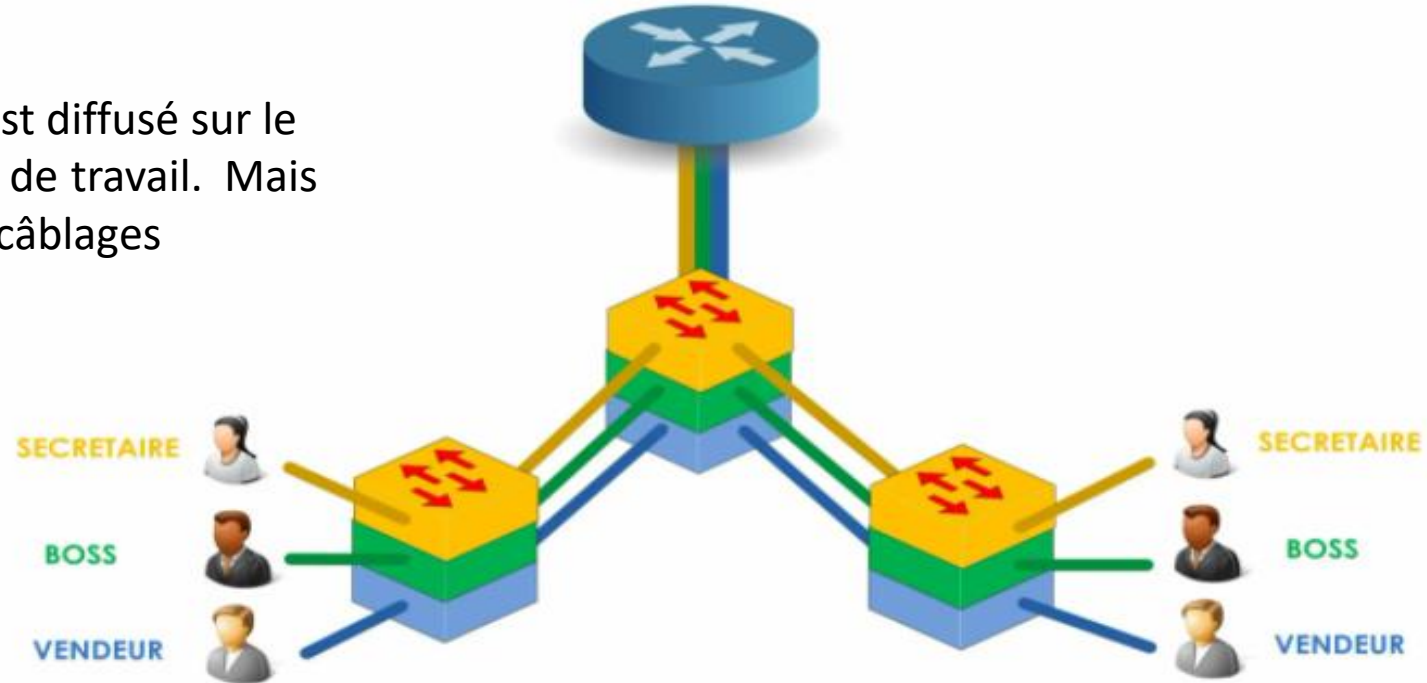
- 10 Boss
- 50 secrétaires
- 200 vendeurs



Un réseau d'entreprise standard

Solution pour regrouper les machines par fonction

Pour diminuer le nombre de broadcast diffusé sur le réseau on crée un réseau par groupe de travail. Mais cette solution requiert beaucoup de câblages



La solution : créer un réseau par groupe d'utilisateur

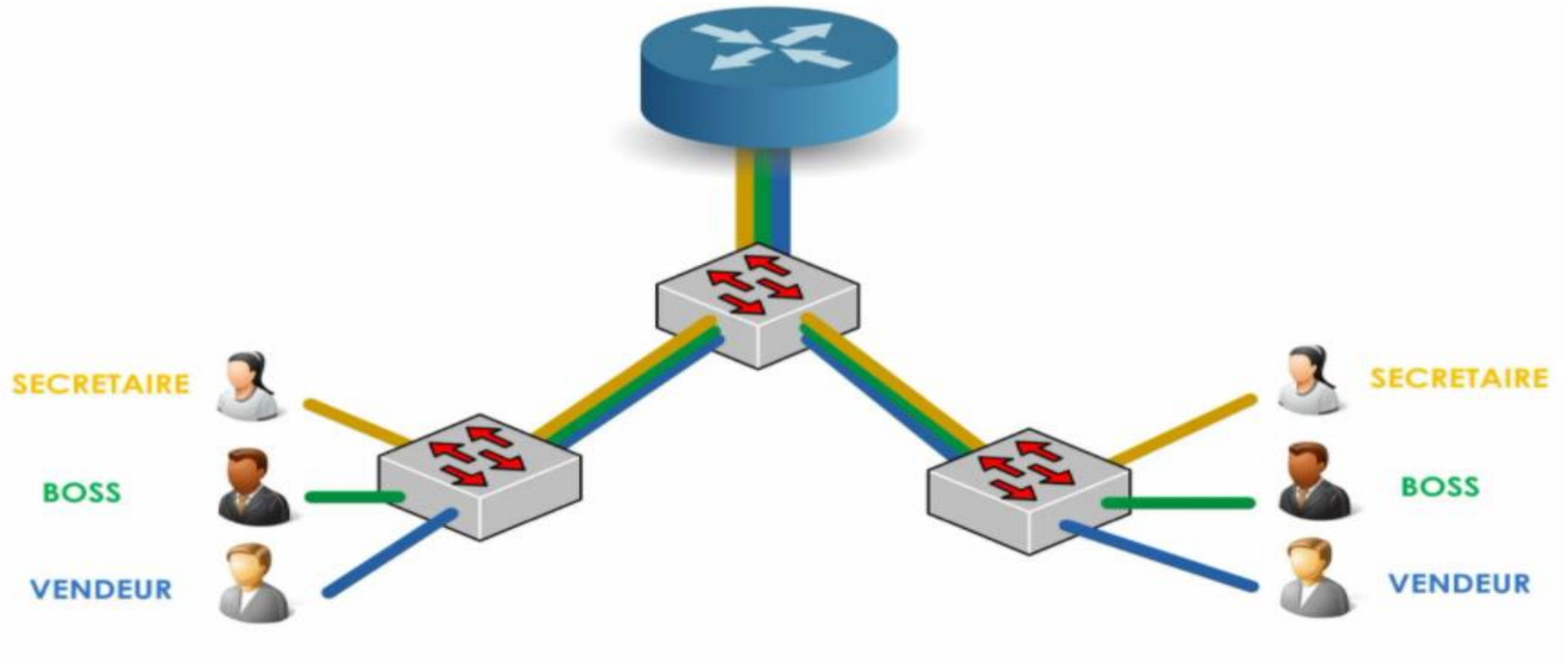
Résultat :

- Le réseau **Boss** (10 users) = Diminution du nombre de broadcasts reçu de **96,2%**
- Le réseau **Secrétaire** (50 users) = Diminution du nombre de broadcasts reçu de **80,8%**
- Le réseau **Vendeurs** (200 users) = Diminution du nombre de broadcasts reçu de **23,1%**

Ça coûte chère cette méthode

Solution : VLAN

- Architecture avec peu de matériel → VLAN



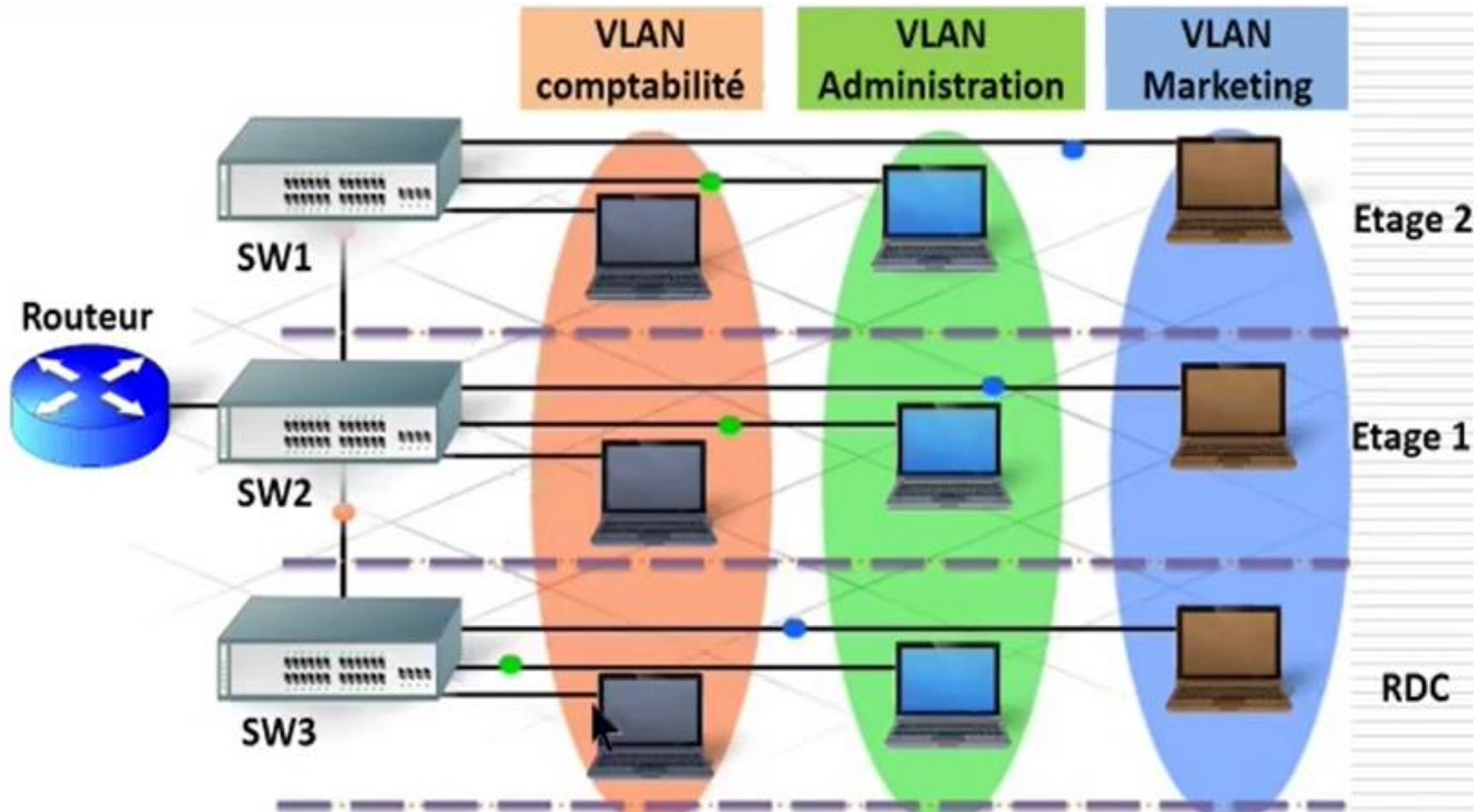
Les Virtual LAN

Les réseaux locaux virtuels

- Un VLAN est un regroupement logique pas physique :
 - Par fonction
 - Par équipe de projet
 - Par application
- Une diffusion est transmise uniquement aux machines du même VLAN, ce qui améliore :
 - La sécurité
 - Les performance du réseau

Chaque réseau local virtuel fonctionne donc comme
un réseau local **distinct**

VLANs : exemple

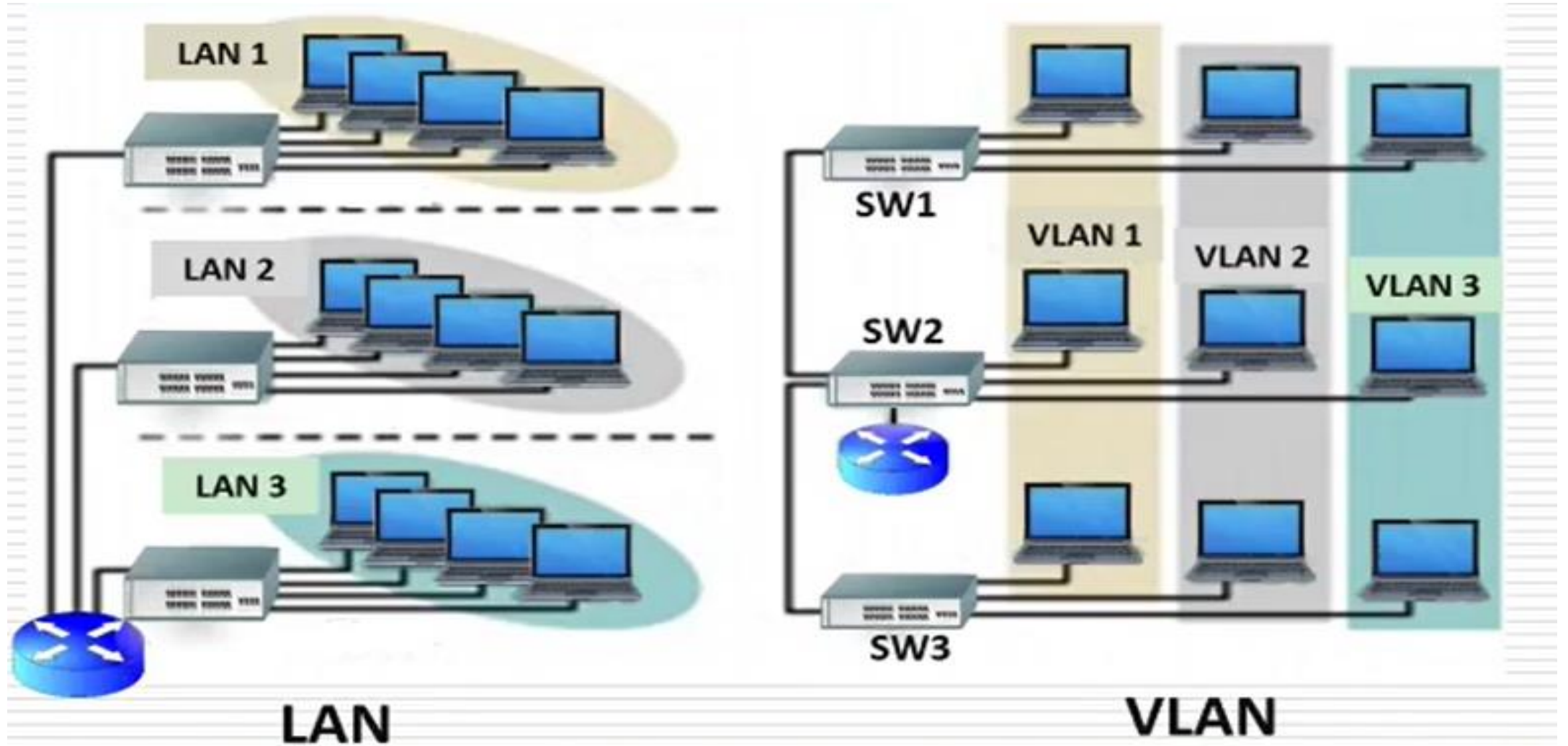


LAN

VS

VLAN

LAN vs VLAN



LAN vs VLAN

Une approche «traditionnelle» :

- ☐ Différents LAN utilisant des ponts, switch ou répéteurs
- ☐ Un routeur interconnectant ces différents LANs

Une approche «VLAN» :

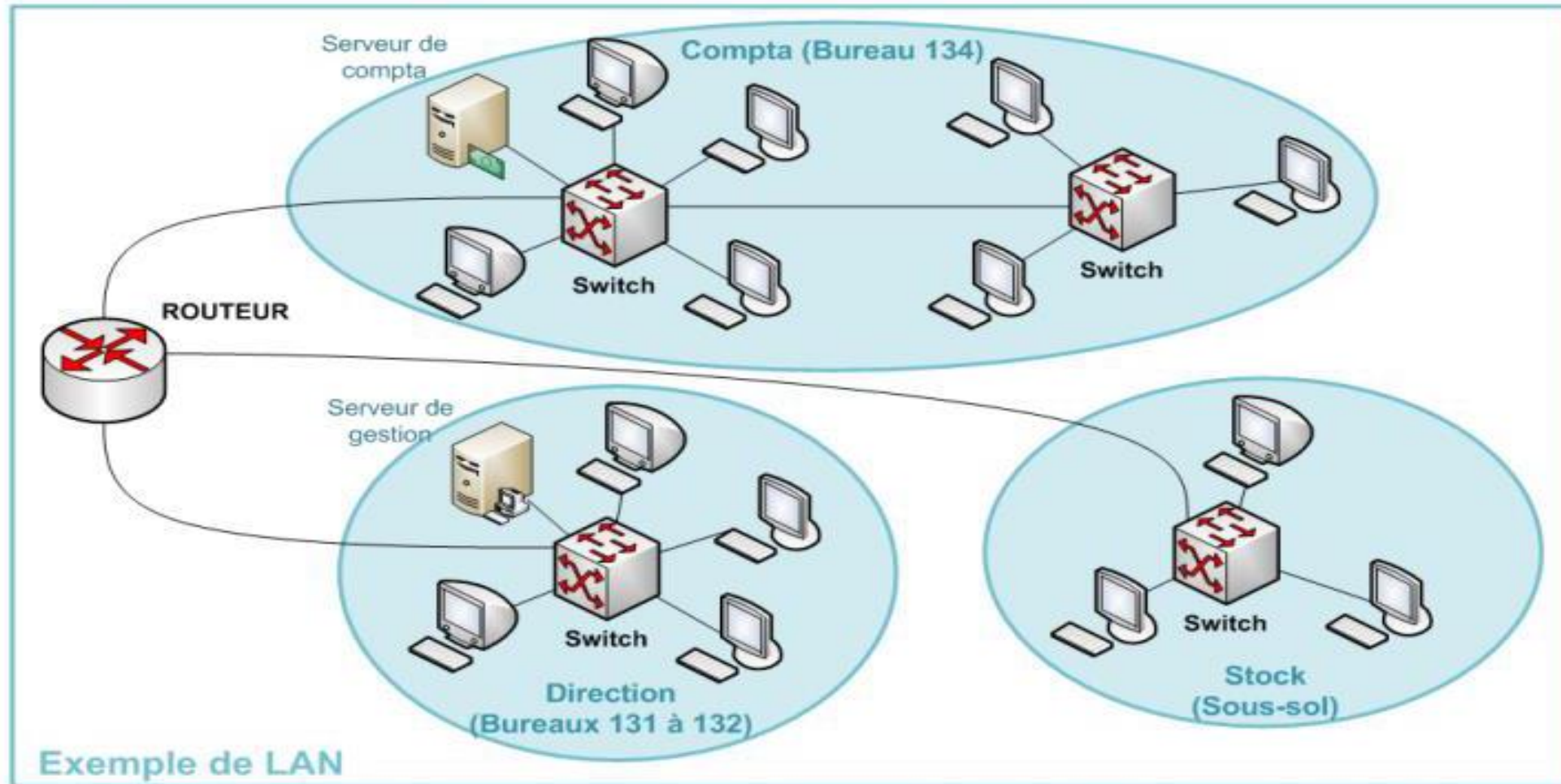
- ☐ Un ou plusieurs switch en mode VLAN
- ☐ Un routeur interconnectant ces différents VLANs

Fonctionnement du LAN

- ❑ Les LAN sont très souvent commutés
 - ❑ Les commutateurs relient des machines entre elles
 - ❑ Ils évoluent dans un seul domaine de broadcast
 - ❑ Sauf en cas de présence de routeurs
- ❑ Par définition, **les routeurs bloquent** le trafic de diffusion à une interface. Un routeur “**filtre**” le trafic de diffusion en ne le transférant pas.
- ❑ Les routeurs possèdent en général un nombre **restreint d'interfaces LAN**. **Le rôle principal d'un routeur** est de déplacer les données entre les réseaux, pas de fournir l'accès réseau aux périphériques finaux.

Fonctionnement du LAN

- Exemple : LAN segmenté avec routeur



Le routeur permet de diminuer la taille du domaine du broadcast mais pour un coût plus élevé

Virtualisation d'un LAN

❑ Définitions

- ❑ Un VLAN (Virtual LAN) en français (un réseau virtuel local)
- ❑ Un VLAN est une **segmentation** (**partition logique**) qui a lieu à l'intérieur d'un appareil de couche2 (un commutateur) pour réduire la taille de domaine de diffusion
- ❑ Les VLANs sont généralement intégrés à la **conception** réseau, ce qui permet de s'adapter aux **objectifs de l'entreprise**
- ❑ Les VLANs sont principalement utilisés dans les réseaux locaux commutés, les implémentations modernes leur permettent d'accéder aux réseaux métropolitains et étendus.

Virtualisation d'un LAN

❑ Définitions

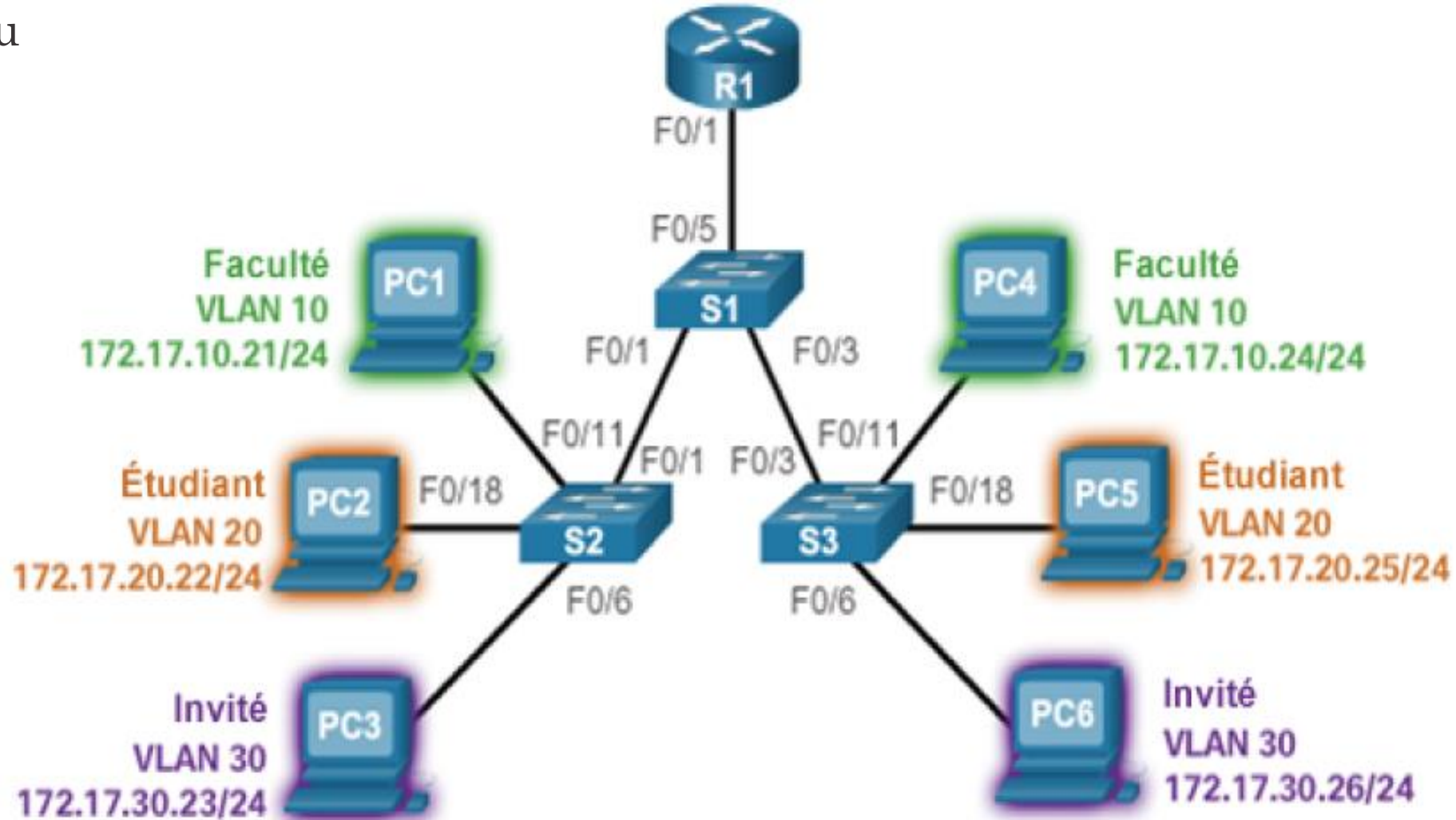
- ❑ Les VLAN permettent la mise en œuvre des stratégies d'accès et de sécurité en fonction de groupes d'utilisateurs précis
- ❑ Plusieurs partitions peuvent être créées pour permettre à plusieurs VLAN de **coexister**.
- ❑ Chaque VLAN constitue un domaine de diffusion distinct, généralement avec **son propre réseau IP**.
- ❑ la conception VLAN doit tenir compte de la mise en œuvre d'un système **d'adressage hiérarchique**
- ❑ Les VLAN sont **isolés** les uns des autres et les paquets ne peuvent circuler entre eux **qu'en passant par un routeur**.

Virtualisation d'un LAN

Chaque VLAN d'un réseau commuté correspond à un réseau IP ;

La conception VLAN maintien système d'adressage hiérarchique.

L'adressage **réseau hiérarchique** signifie que les numéros de **réseau IP** sont appliqués aux VLAN dans un ordre tenant compte de l'ensemble du réseau.



Virtualisation d'un LAN

Avantages des VLANs

- ❑ **Indépendance** de la couche physique
- ❑ **Séparation des flux** diminue les risque de violation de confidentialité, ce qui contribue à améliorer la **sécurité**.
- ❑ **Flexibilité** : allocation dynamique des utilisateurs dans un réseau indépendamment de l'emplacement
 - ❑ L'ajout ou déplacement facile et simple des postes de travail
- ❑ **Facilité de gestion** : QoS, classification, routage, filtrage
- ❑ **Performances** : diminution de la taille des domaines de Broadcast
 - ❑ Optimisation de la bande passante
- ❑ **Coût** abordable

Segmentation des VLANs

Méthodes d'affectation aux VLANs

Trois méthodes pour attribuer un équipement à un VLAN :

- Par port du switch auquel la machine est connecté
 - **VLAN niveau 1 (attribution statique)**
 - Les ports d'un switch peuvent être associés à des VLANs différents
- Par l'adresse MAC de la machine
 - **VLAN niveau 2 (attribution dynamique)**
 - Le switch lit l'adresse MAC de la machine et l'associe à son VLAN d'appartenance
- Par l'adresse IP de la machine **(attribution dynamique)**
 - **VLAN de niveau 3**
 - Le switch lit l'adresse IP de la machine et l'associe à son VLAN d'appartenance

Segmentation des VLANs

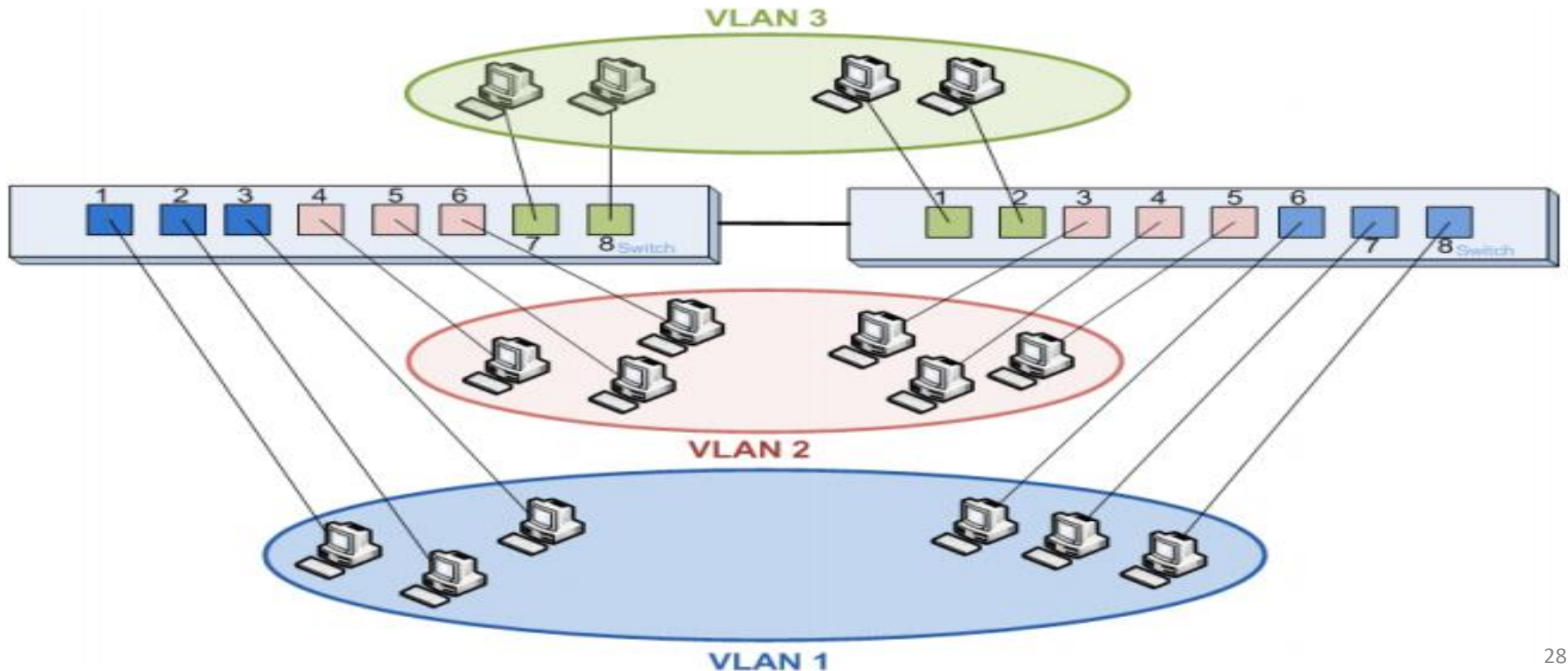
VLAN de niveau 1

- Les ports du commutateur prennent un identifiant VLAN.
- Cet identifiant logique définit l'étendue du domaine de diffusion .
- Le trafic de diffusion ne sera transféré que sur les ports ayant le même identifiant.
- Autrement dit, par exemple, le trafic de diffusion venant d'un port appartenant au VLAN 66 ne se sera transféré que sur les ports ayant pour attribution le VLAN 66.
- La séparation fonctionnelle entre deux ports ayant des identifiants VLAN différents correspond à une séparation physique.
- La technologie VLAN permet de diviser logiquement les ports du commutateur.

Segmentation des VLANs

VLAN de niveau 1

- Un exemple à base de 2 switches

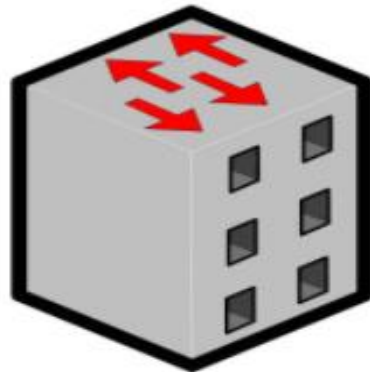


Segmentation des VLANs

VLAN de niveau 1

TABLE CAM

MAC	PORT
MAC01	Fa 0/1
MAC02	Fa 0/2
MAC03	Fa 0/3
MAC04	Fa 0/4
MAC05	Fa 0/5
MAC06	Fa 0/6



Avant

TABLE CAM VLAN 10

VLAN	MAC	PORT
10	MAC01	Fa 0/1
10	MAC02	Fa 0/2

TABLE CAM VLAN 20

VLAN	MAC	PORT
20	MAC03	Fa 0/3
20	MAC04	Fa 0/4

TABLE CAM VLAN 30

VLAN	MAC	PORT
30	MAC05	Fa 0/5
30	MAC06	Fa 0/6

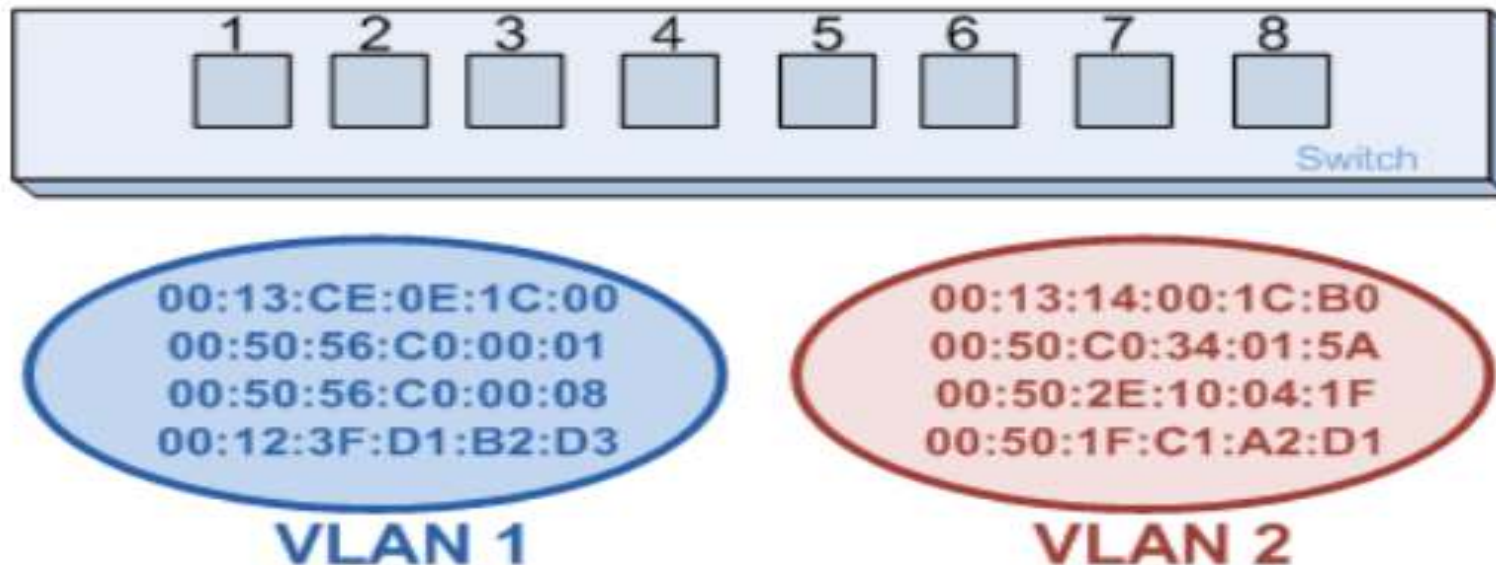


Après

Segmentation des VLANs

VLAN de niveau2

- L'adresse MAC est associée à un VLAN quelque soit le port utilisé
 - ◆ Nécessité de maintenir à jour la base de données des adresses MAC
 - ◆ L'appartenance à un VLAN ne dépend plus de l'emplacement de la machine



Segmentation des VLANs

VLAN de niveau 1

- Basé sur le protocole ou l'adresse IP
- L'appartenance à un VLAN est défini par l'adresse IP de la machine
 - Les VLANs sont définis par sous réseau
 - Cela exclue la possibilité d'utiliser DHCP
 - N'est plus utilisé aujourd'hui
- L'appartenance à un VLAN est défini par le protocole utilisé par la machine
 - Il devient possible de séparer en VLANs les machines utilisant TCP/IP
 - **Pas vraiment utilisé aujourd'hui**

Types de VLAN dans les réseaux modernes

Il existe différents types de VLAN utilisés dans les réseaux modernes.

Certains types de VLAN sont définis par les **classes de trafic**. D'autres types de VLAN sont définis par **leur fonction spécifique**.

- **VLAN de données** : est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.
- **VLAN par défaut** Tous les ports de commutateur font partie du VLAN 1 par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut.
- **VLAN natif** : un réseau local virtuel natif est affecté un port trunk 802.1Q
Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN

Types de VLAN dans les réseaux modernes

VLAN par défaut

VLAN 1

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

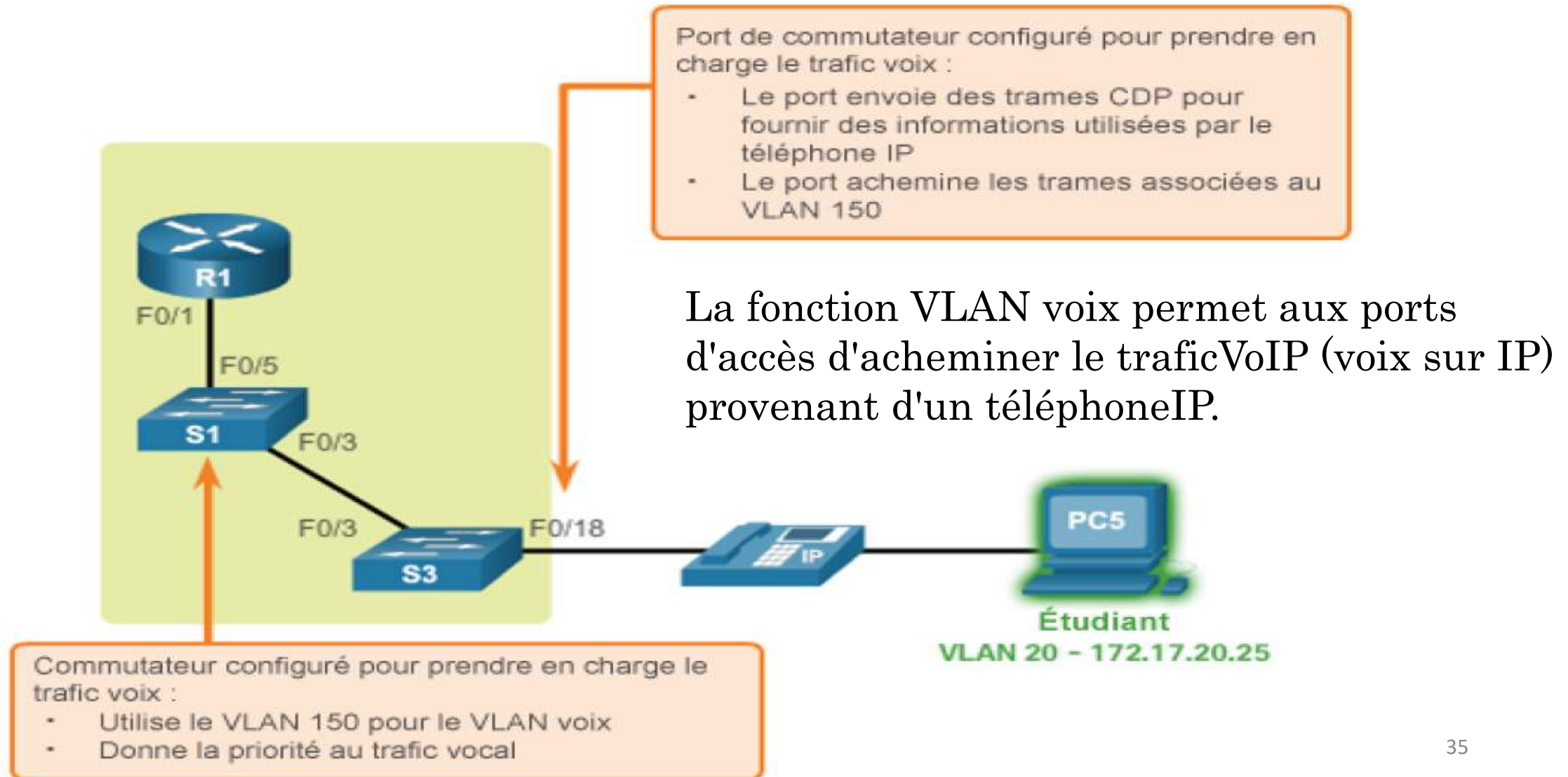
- Tous les ports affectés au VLAN 1 pour acheminer les données par défaut.
- Le VLAN natif est le VLAN 1 par défaut.
- Le VLAN de gestion est le VLAN 1 par défaut.
- Le VLAN 1 ne peut pas être renommé ni supprimé.

Types de VLAN dans les réseaux modernes

- **VLAN de gestion** : Un VLAN de gestion est un VLAN de données configuré spécifiquement pour le trafic de gestion réseau, y compris SSH, Telnet, HTTPS, HTTP et SNMP. Par défaut, le VLAN 1 est configuré comme VLAN de gestion sur un commutateur de couche 2
- **VLAN Voix** : Un VLAN distinct est nécessaire pour prendre en charge la voix sur IP (VOIP).
 - Priorité de transmission par rapport aux autres types de trafic réseau ;
 - Bande passante consolidée pour garantir la qualité de la voix ;
 - Possibilité de routage autour des zones encombrées du réseau ;
 - Délai inférieur à 150 ms sur tout le réseau.

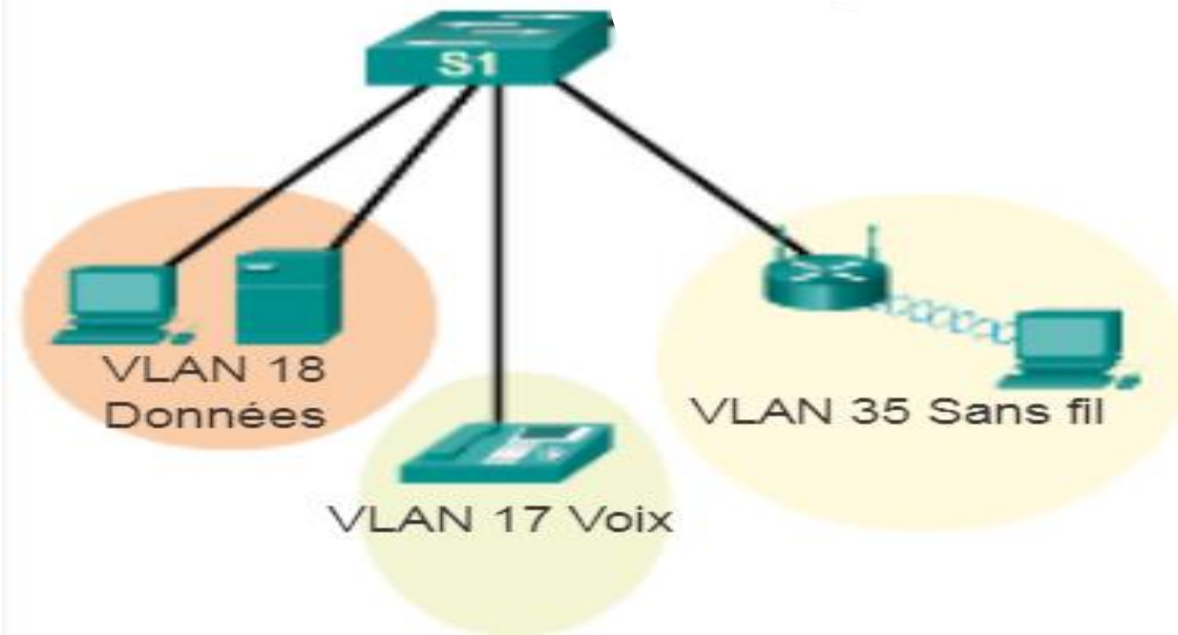
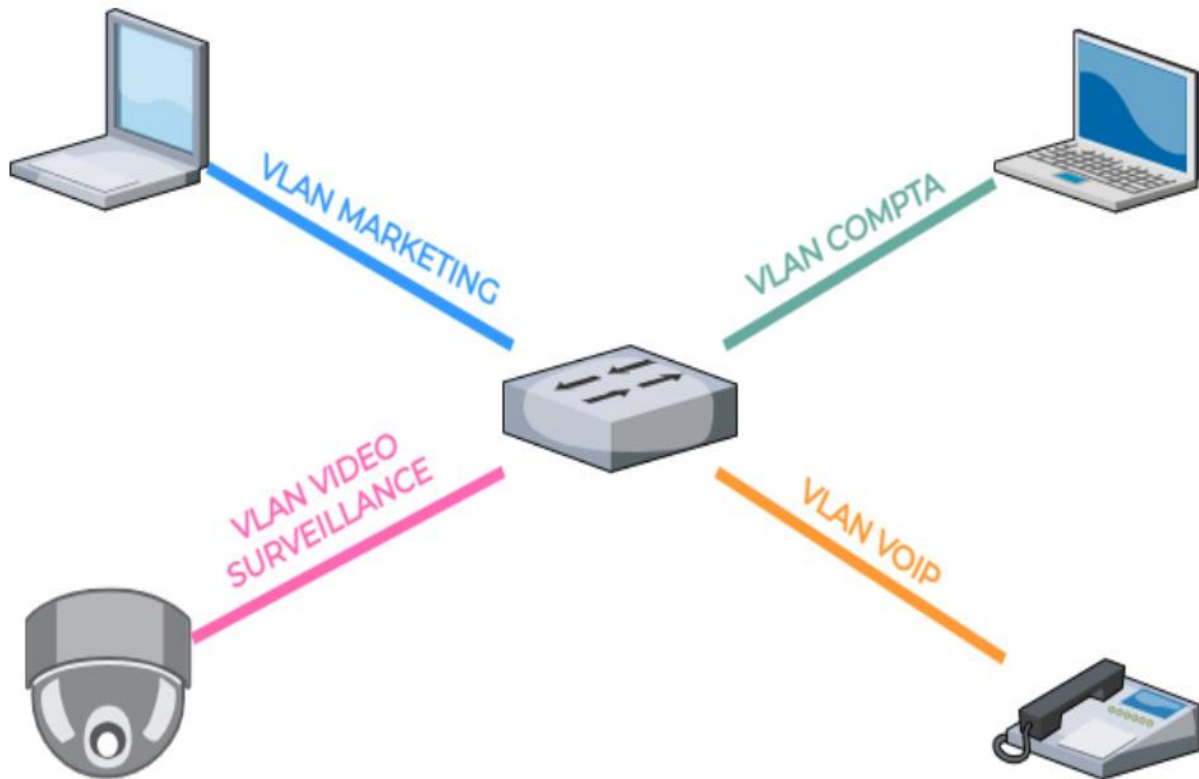
Types de VLAN dans les réseaux modernes

VLAN voix



Segmentation des VLANs

Plusieurs VLANs par un commutateur

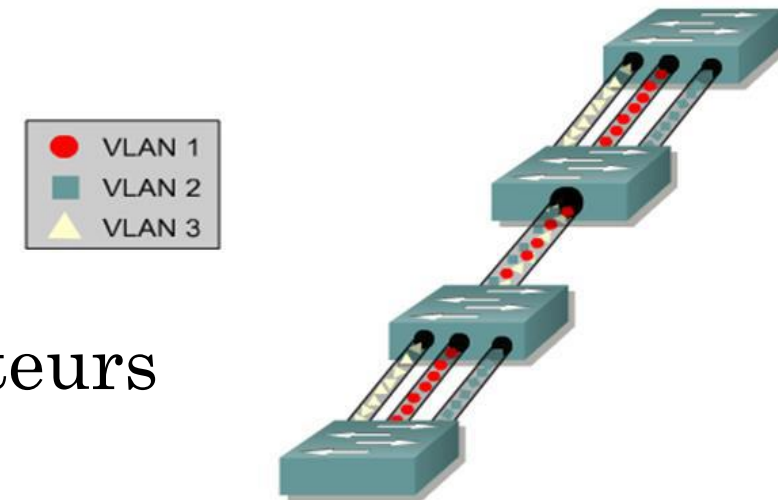


Segmentation des VLANs

VLAN dans un environnement à commutateurs multiples

Trunks de VLAN

- Un trunk est une liaison point à point entre deux périphériques réseau qui transporte plusieurs VLAN. Un trunk de VLAN permet d'étendre les VLAN à l'ensemble d'un réseau.
- Tout le trafic VLAN se propage entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur



Segmentation des VLANs

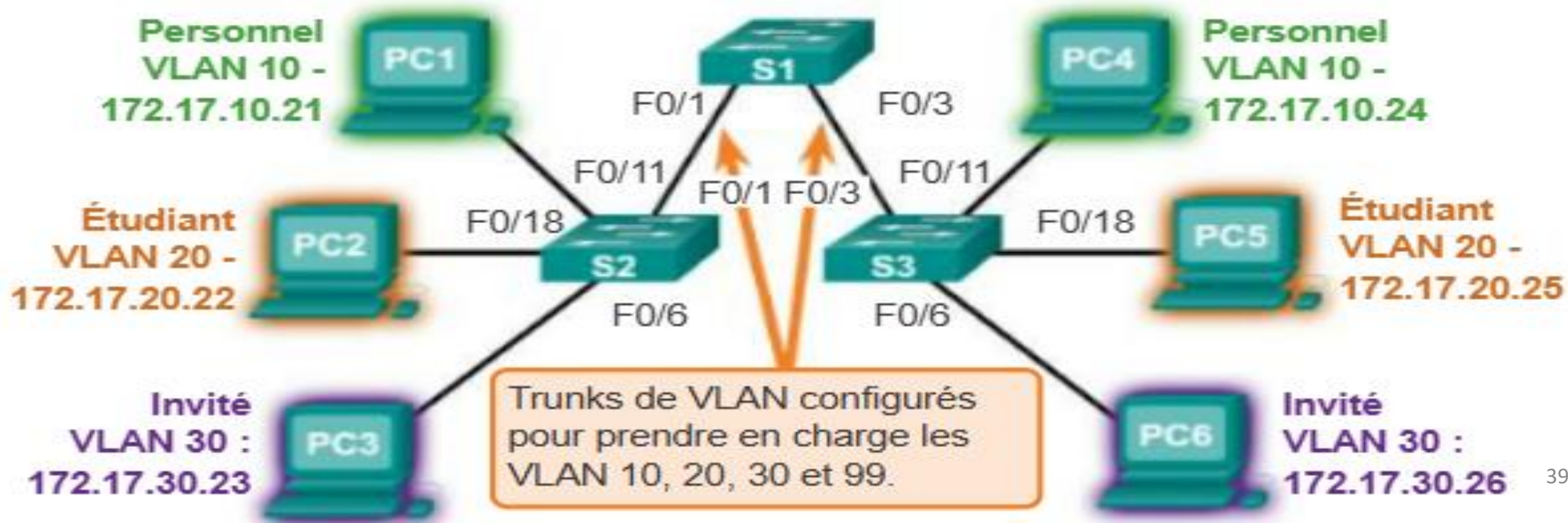
VLAN dans un environnement à commutateurs multiples

- Un trunk de VLAN n'est pas associé à un VLAN particulier.
- Un trunk (agrégation) résout le problème de liaisons multiples et préserve les ports
- Lorsque les trames Ethernet sont placées sur une agrégation, elles ont besoin **d'informations supplémentaires** sur les VLAN auxquels elles appartiennent
- **IEEE 802.1Q**, un protocole de trunk de VLAN très répandu.

Trunks de VLAN

VLAN 10 Personnel - 172.17.10.0/24
VLAN 20 Étudiants - 172.17.20.0/24
VLAN 30 Invité - 172.17.30.0/24
VLAN 99 Gestion et natif - 172.17.99.0/24

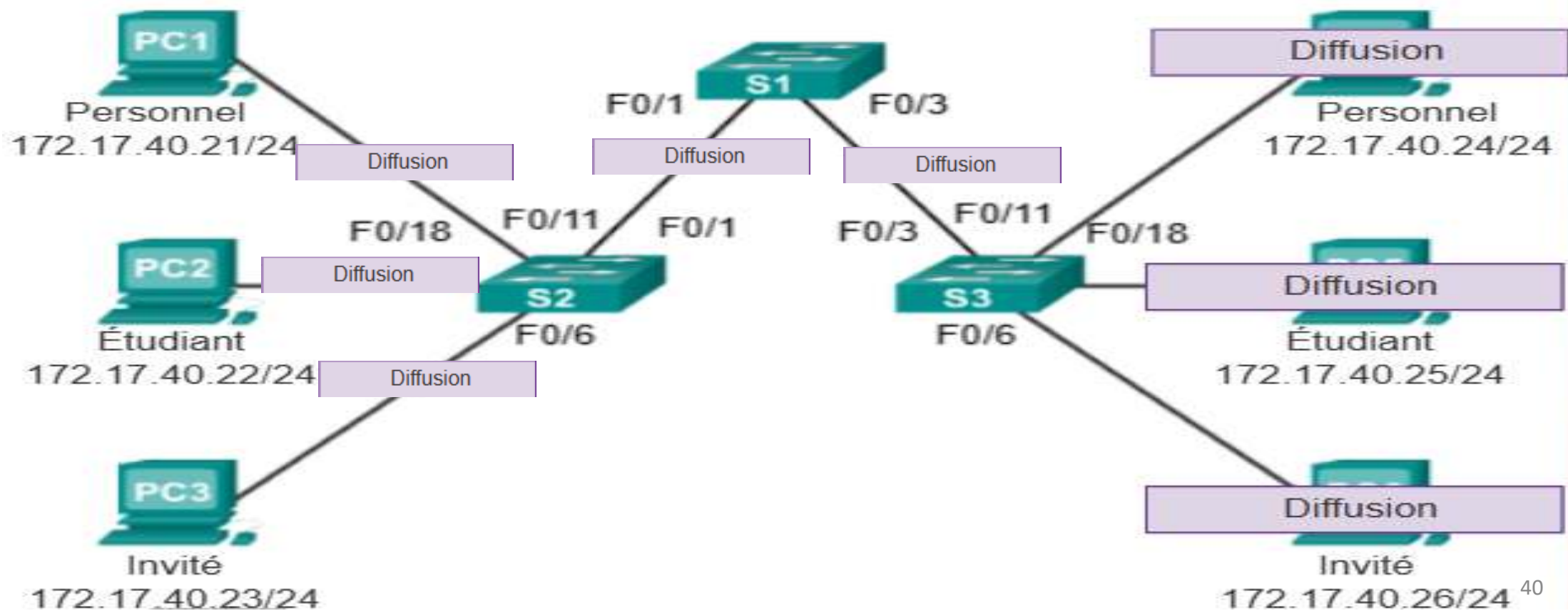
F0/1-5 sont des interfaces de trunk 802.1Q avec le VLAN 99 comme VLAN natif.
F0/11-17 se trouvent dans le VLAN 10
F0/18-24 se trouvent dans le VLAN 20.
F0/6-10 se trouvent dans le VLAN 30.



Contrôler les domaines de diffusion à l'aide des VLAN

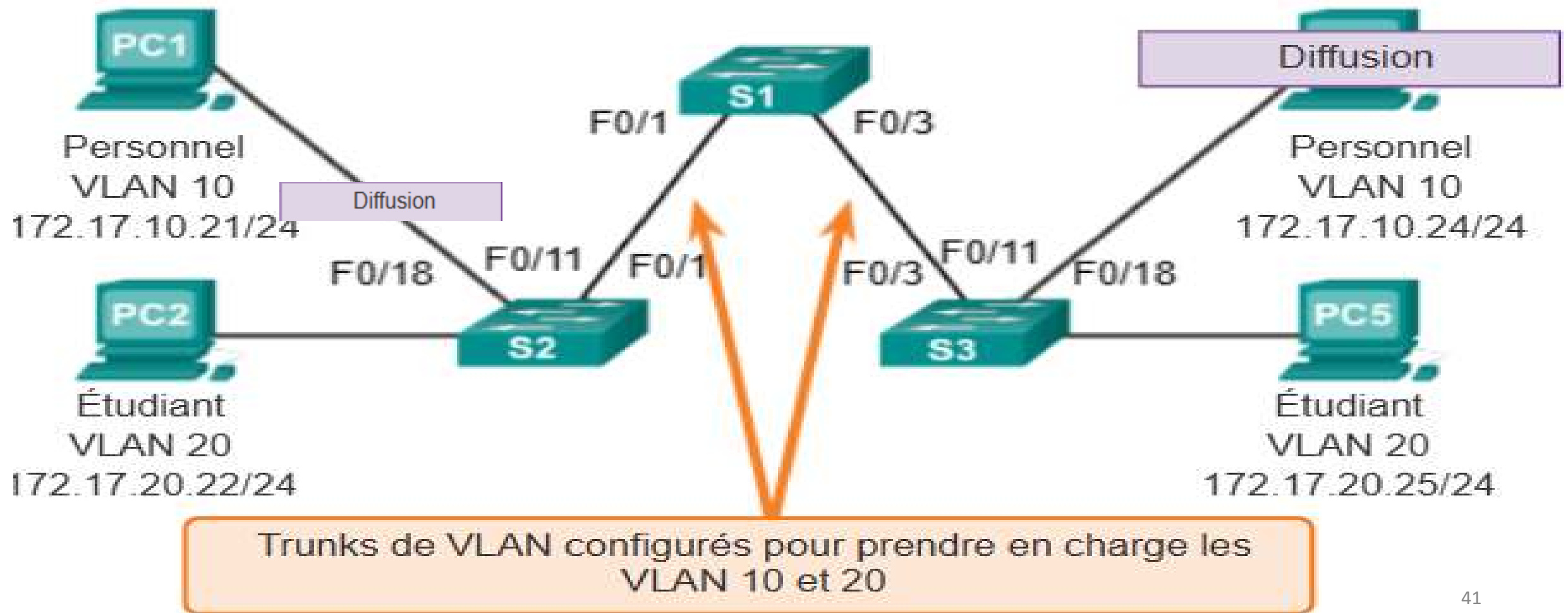
Sans segmentation de VLANs

PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion par tous les ports disponibles.



Avec segmentation VLAN

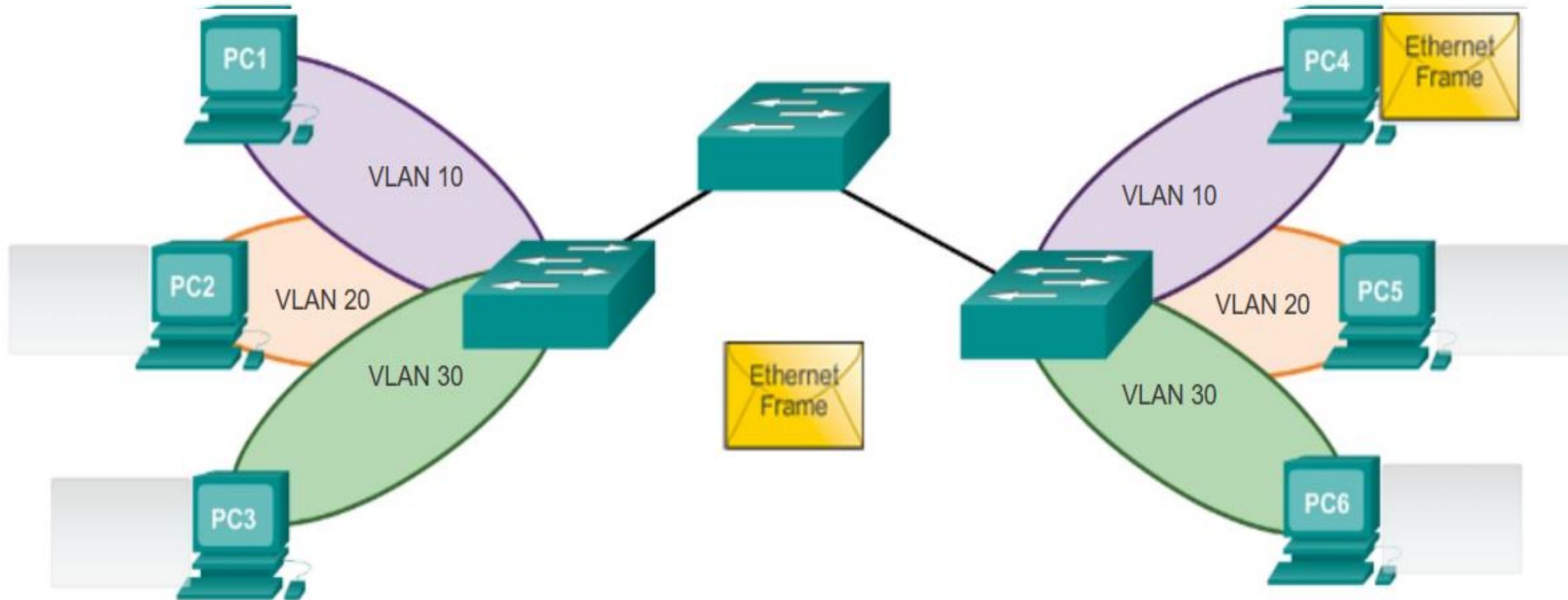
PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion uniquement par les ports configurés pour le VLAN 10.



Exercice - Scénario 1 : Trunks de VLAN en action

Déplacez les trames Ethernet (enveloppes de couleur jaune) vers leurs PC de destination pour le scénario. Toutes les enveloppes ne seront pas utilisées dans chaque scénario.

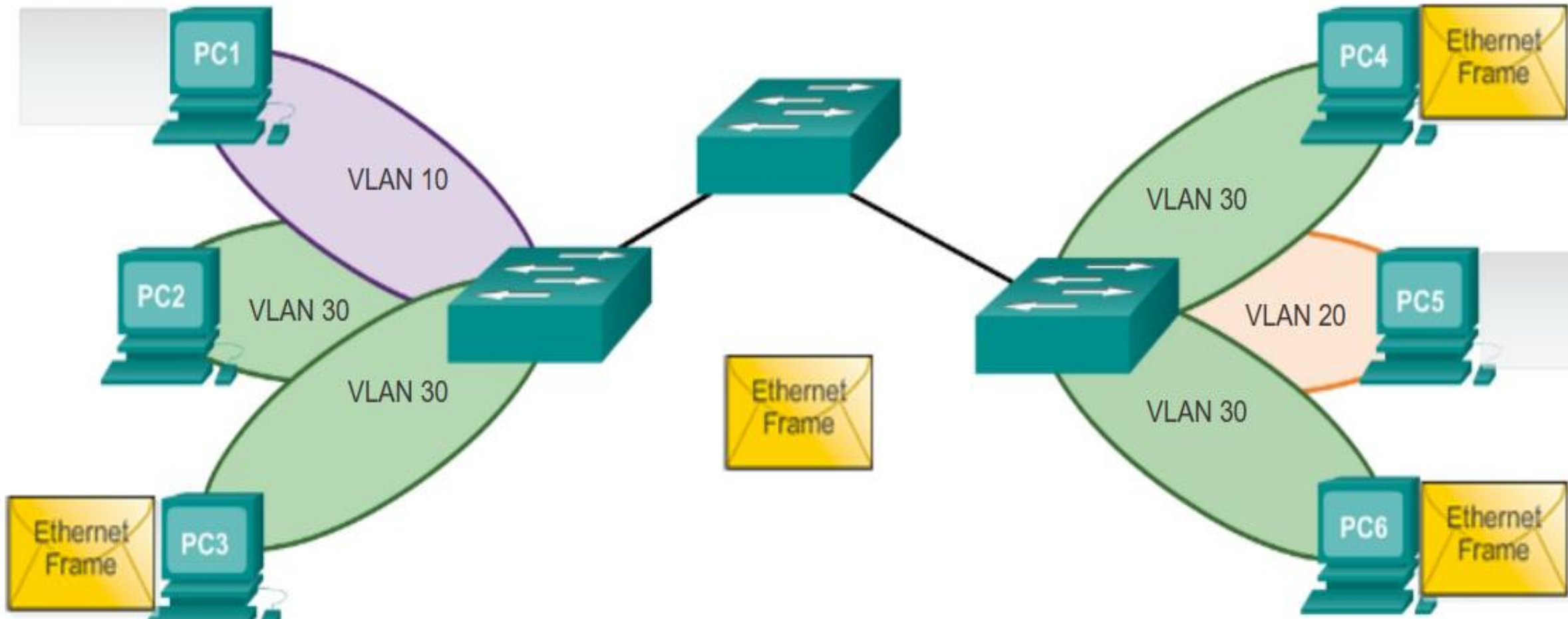
Scénario 1 : PC 1 envoie une diffusion. Quels PC vont recevoir une copie de la trame de diffusion ?



Exercice - Scénario 2 : Trunks de VLAN en action

Déplacez les trames Ethernet (enveloppes de couleur jaune) vers leurs PC de destination pour le scénario. Toutes les enveloppes ne seront pas utilisées dans chaque scénario.

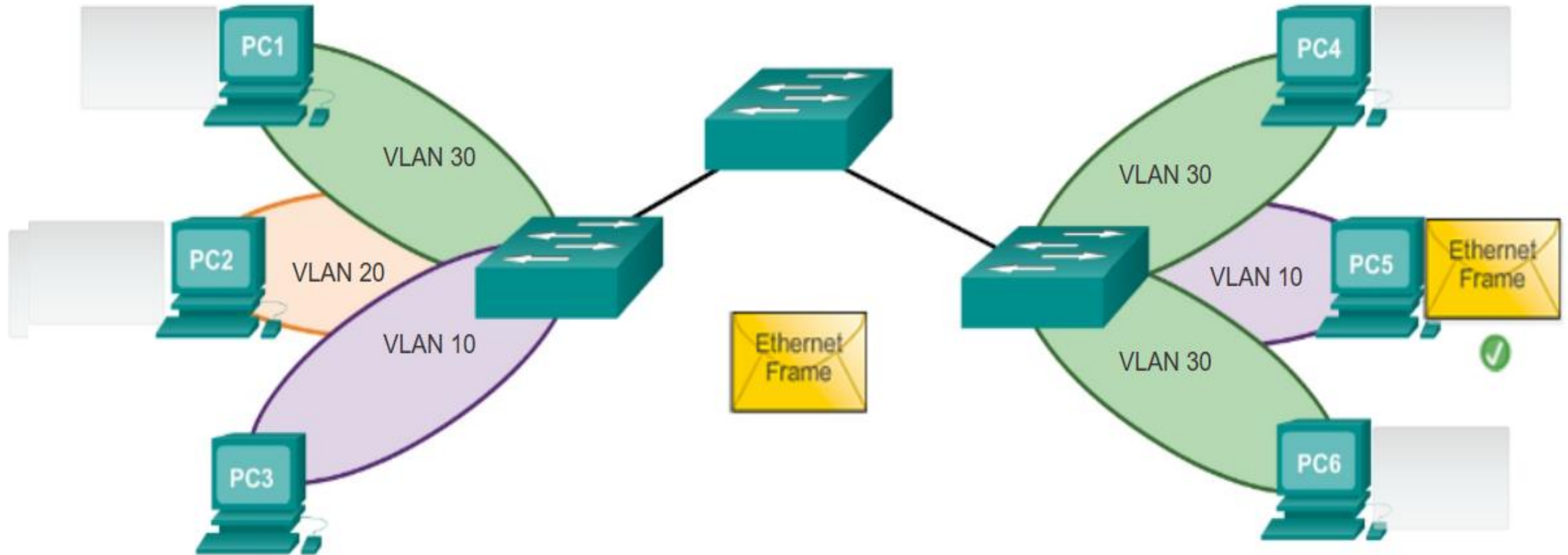
Scénario 2 : PC 2 envoie une diffusion. Quels PC vont recevoir une copie de la trame de diffusion ?



Exercice - Scénario 3 : Trunks de VLAN en action

Déplacez les trames Ethernet (enveloppes de couleur jaune) vers leurs PC de destination pour le scénario. Toutes les enveloppes ne seront pas utilisées dans chaque scénario.

Scénario 3 : PC 3 envoie une diffusion. Quels PC vont recevoir une copie de la trame de diffusion ?



Segmentation des VLANs

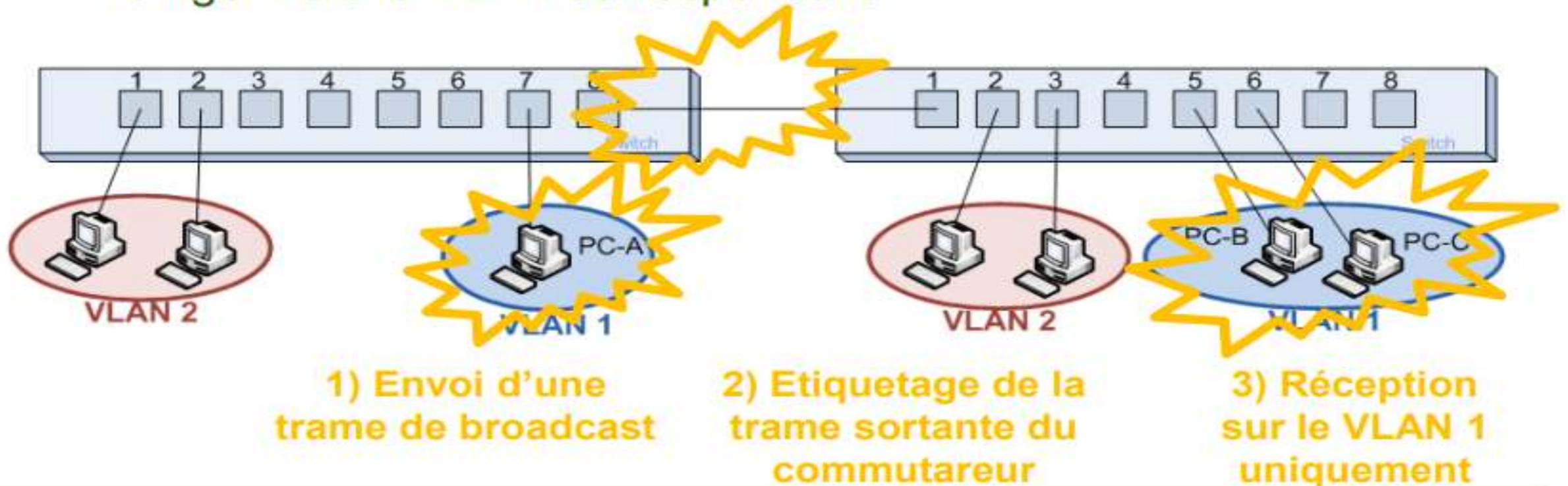
VLAN dans un environnement à commutateurs multiples

Lorsque plusieurs switchs doivent être reliés afin de créer les différents VLANs, il faut échanger entre ces switchs des trames appartenant à différents VLANs, il faut savoir à quel VLAN appartient une trame.

- On doit «**noter**» à quel VLAN chaque trame appartient.
- On utilise la norme IEEE 802.1Q:
 - Elle utilise le «**frame tagging**», c-à-d de l'étiquetage de trame
 - Les étiquettes permettent de savoir à quel domaine de diffusion appartient la trame ;

L'étiquetage des trames Ethernet pour l'identification des VLAN

- « Frame tagging »
- L'étiquetage consiste à marquer toutes les trames sortantes du commutateur avec le n° du VLAN d'appartenance
 - ◆ Le commutateur suivant peut alors repérer les trames et les diriger vers le VLAN correspondant



L'étiquetage des trames Ethernet pour l'identification des VLAN

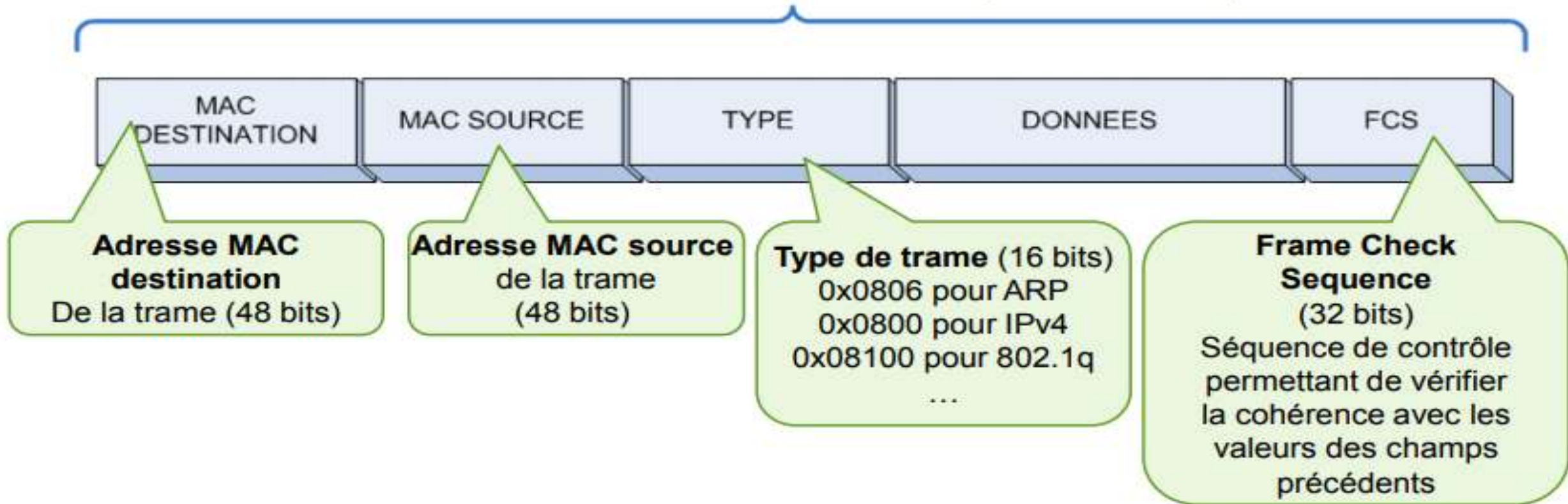
- ❑ L'étiquetage des trames consiste à ajouter un en-tête d'identification du VLAN à la trame, pour transmettre correctement plusieurs trames VLAN via un **trunk**.
- ❑ Le protocole **802,1Q** définit la structure de l'en-tête d'étiquetage ajouté à la trame.
- ❑ Les commutateurs ajoutent des étiquettes VLAN aux trames avant de les placer dans les **trunks**. Ils les enlèvent avant de transmettre les trames via les autres **ports d'accès** (non trunk).
- ❑ Une fois qu'elles sont correctement étiquetées, les trames peuvent traverser tous les commutateurs via les trunks. Elles resteront dans le VLAN approprié pour atteindre leur destination.

L'étiquetage des trames Ethernet pour l'identification des VLAN

La trame Ethernet (Rappel)

- Voici la composition d'une trame Ethernet classique

TRAME ETHERNET CLASSIQUE (Sans VLANs)

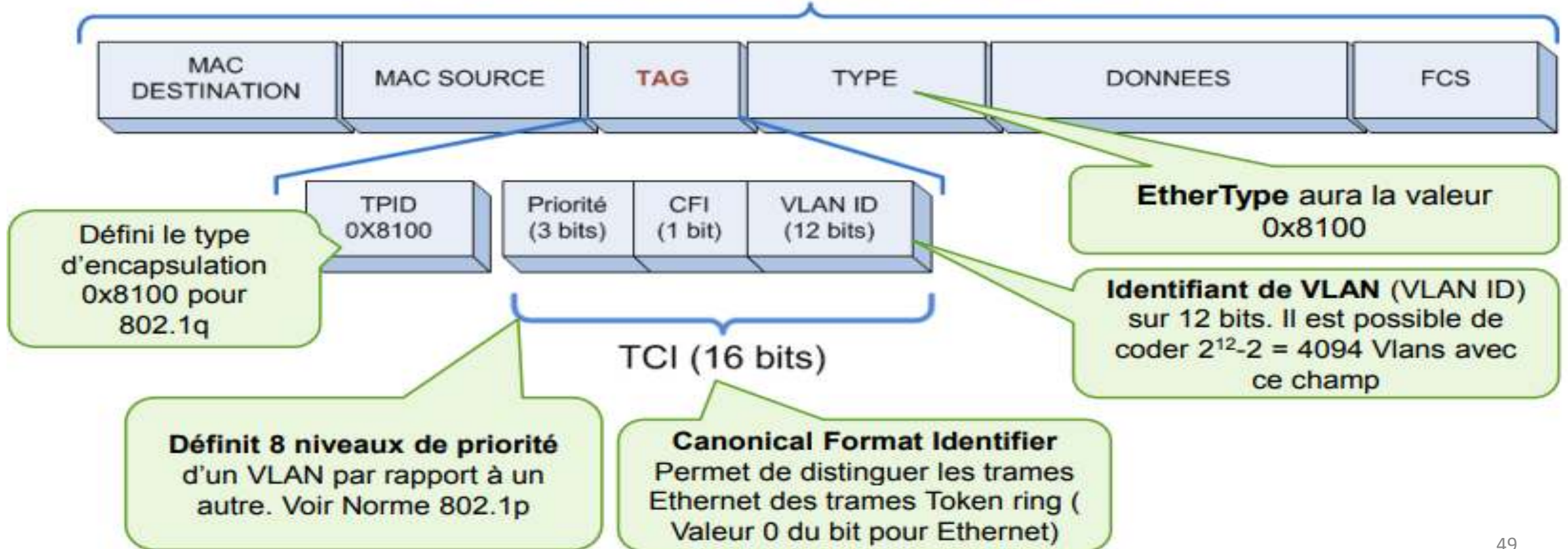


L'étiquetage des trames Ethernet pour l'identification des VLAN

La trame Ethernet 802.1Q

- L'étiquetage se fait grâce à la norme 802.1q (dot 1q)
- Les trames ont un champ supplémentaire

TRAME ETHERNET 802.1q (Avec étiquetage)



MAC Destination 6 bytes	MAC Source 6 bytes	Tag 4 bytes	Type 2 bytes	Données 46-1500 bytes	FCS 4 bytes
----------------------------	-----------------------	------------------------------	-----------------	--------------------------	----------------

Tag protocol ID 16 bits	Priority 3 bits	CFI 1bits	VLAN ID 12 bits
----------------------------	--------------------	--------------	--------------------

0: EHTERNET

De 0 à 4095

Remplace type et identifie la trame comme étant une trame de VLAN (valeur **0x8100**)

9100

9200

NORME: 802.1 P

1: la priorité faible

7: la plus forte

0: pas de priorité

Priorité des trames d'un VLAN relativement aux autres VLAN

0: la trame n'appartient à aucun VLAN

1: VLAN de gestion

4095: réservée

1002 à 1005: réservée

VLAN dans un environnement à commutateur multiples

- Le port est configuré en mode **access** ou **trunk**.

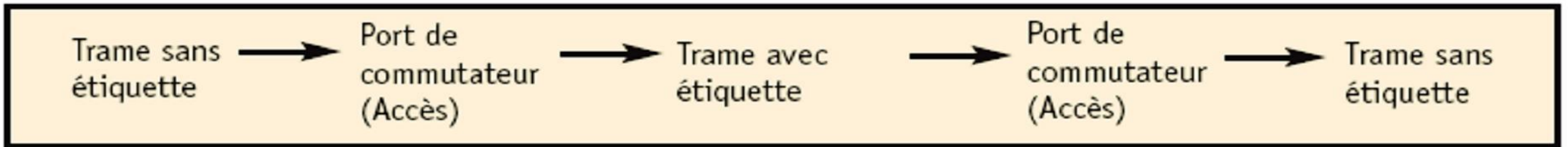
access utilisé pour la connexion terminale d'un périphérique (pc, imprimante,) appartenant à **un seul vlan**.

trunk utilisé dans le cas ou **plusieurs vlans** doivent circuler sur un même lien.

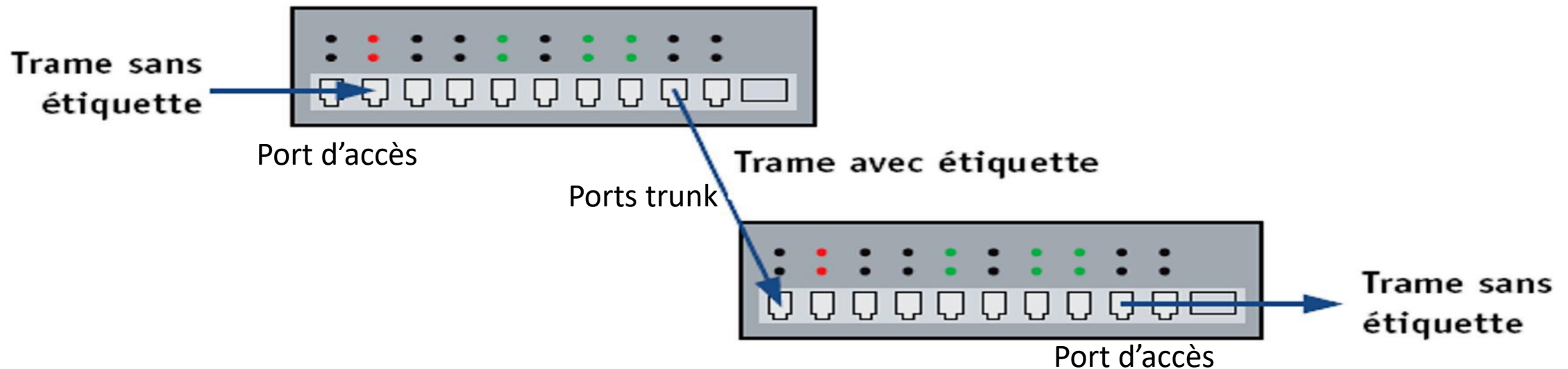


L'étiquetage des trames Ethernet pour l'identification des VLAN

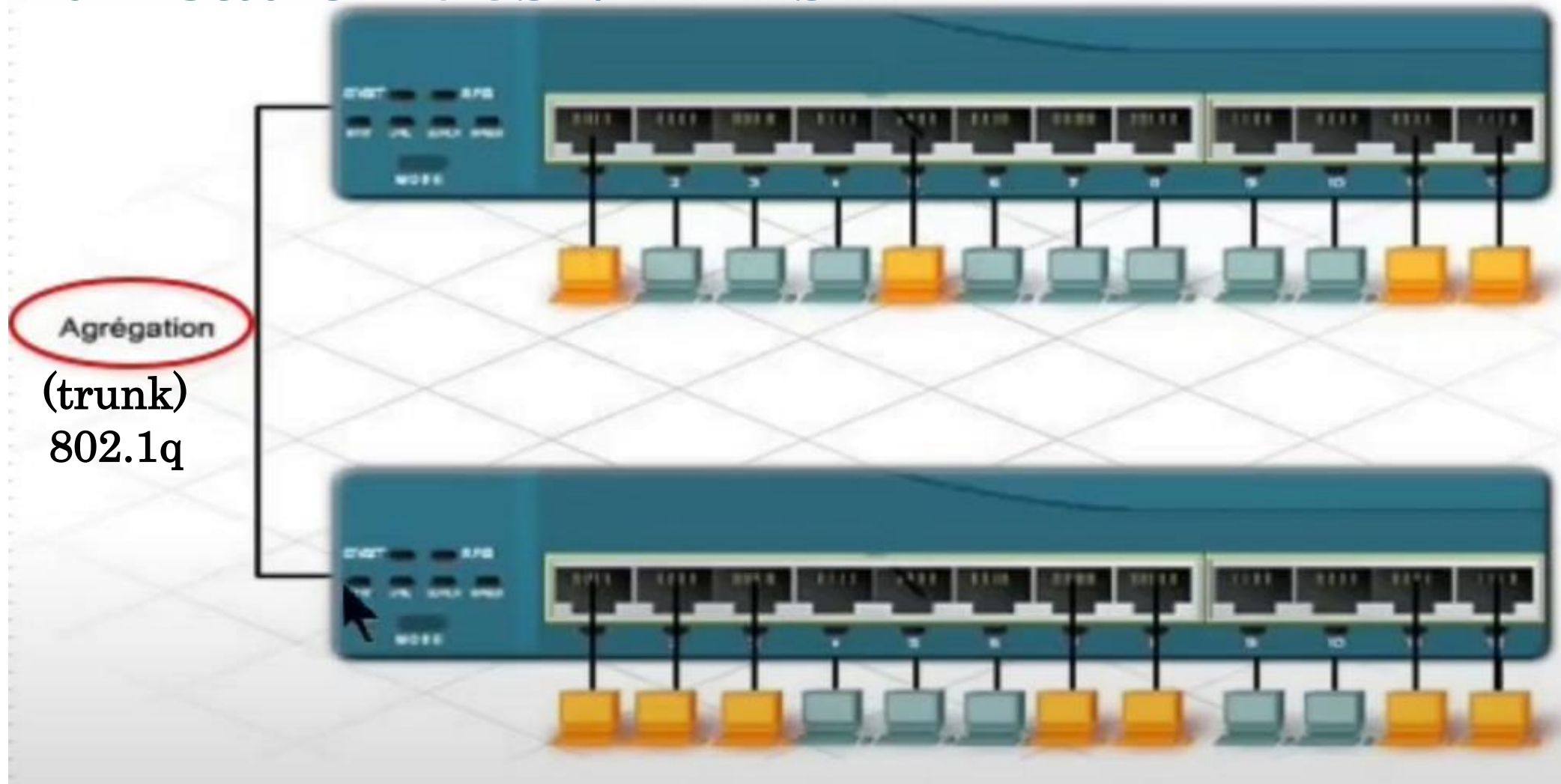
Port d'accès



Port d'agrégation (trunk)

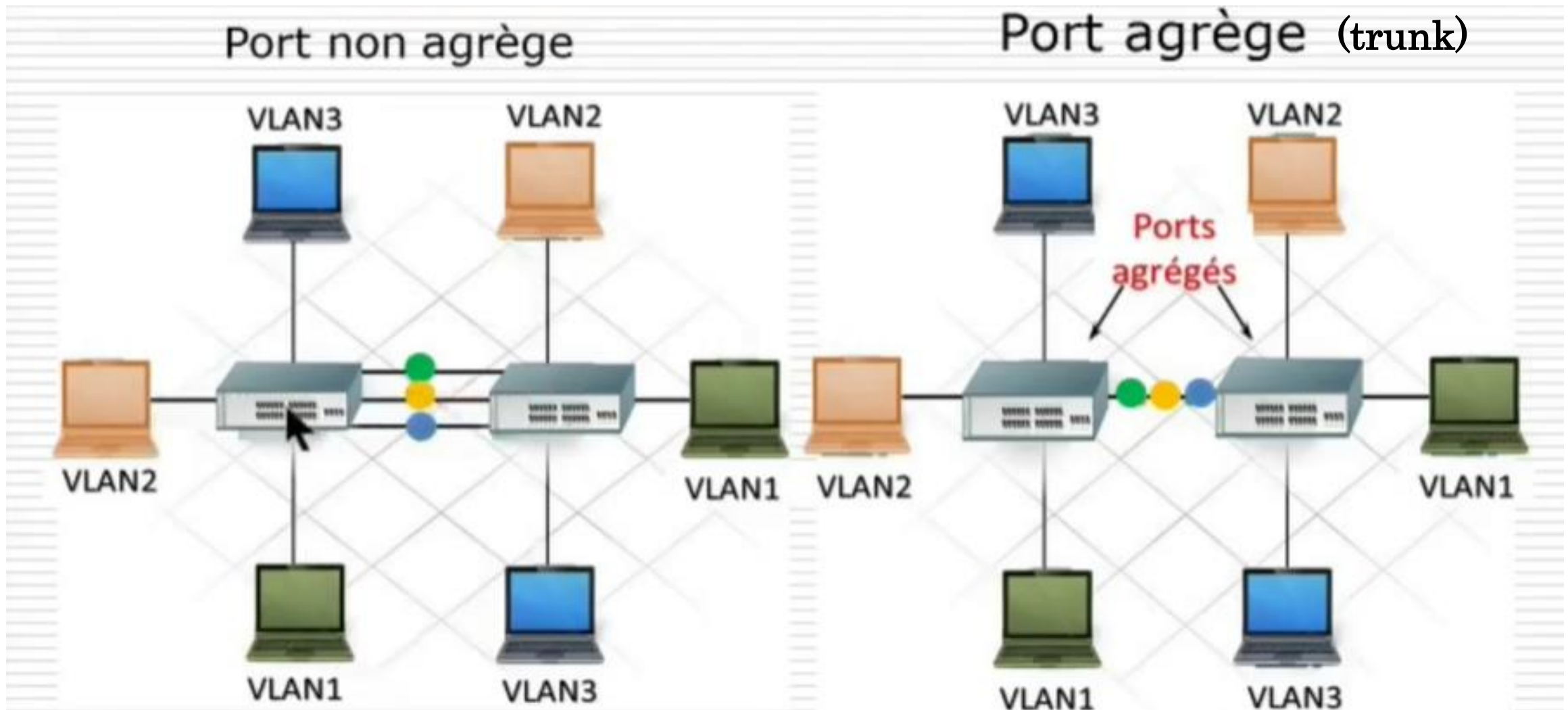


L'étiquetage des trames Ethernet pour l'identification des VLANs



Les agrégations transportent le trafic provenant de **plusieurs VLANs** via une **liaison unique**

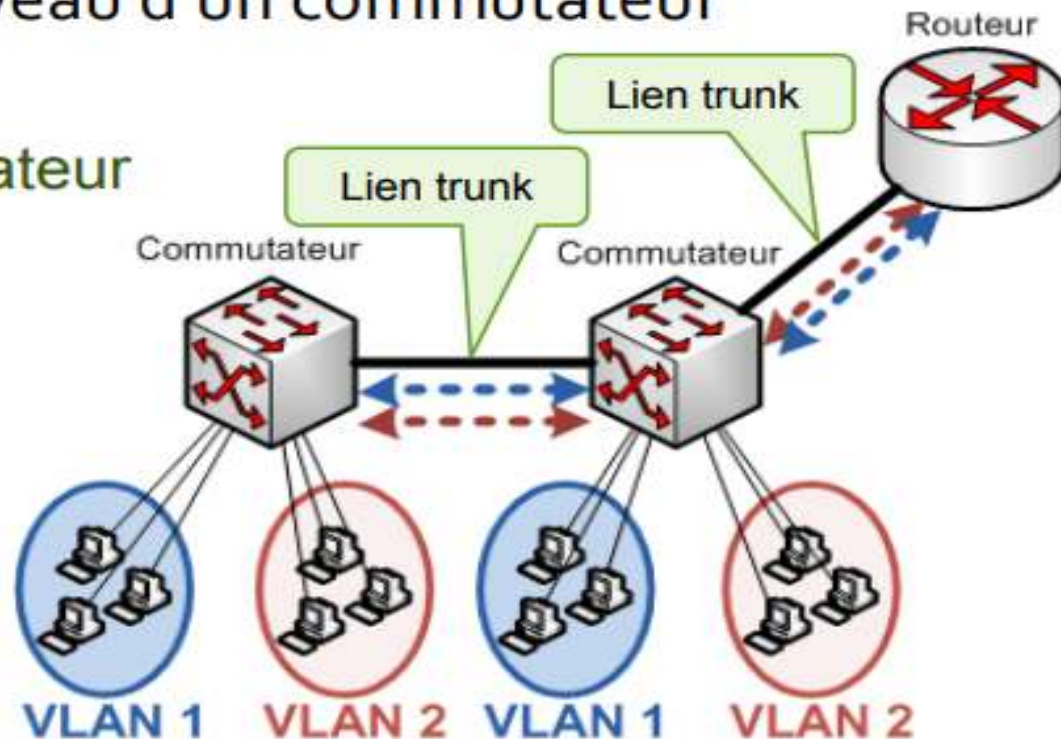
Ports agrégés versus ports non agrégés (accès)



L'étiquetage des trames Ethernet pour l'identification des VLAN

Lien Trunk

- Le lien Trunk véhicule le trafic venant de plusieurs VLANS
 - ◆ Les trames sont donc étiquetées lorsqu'elle sont envoyées par un lien Trunk
- Un lien trunk est défini au niveau d'un commutateur
 - ◆ Soit vers un routeur
 - ◆ Soit vers un autre commutateur



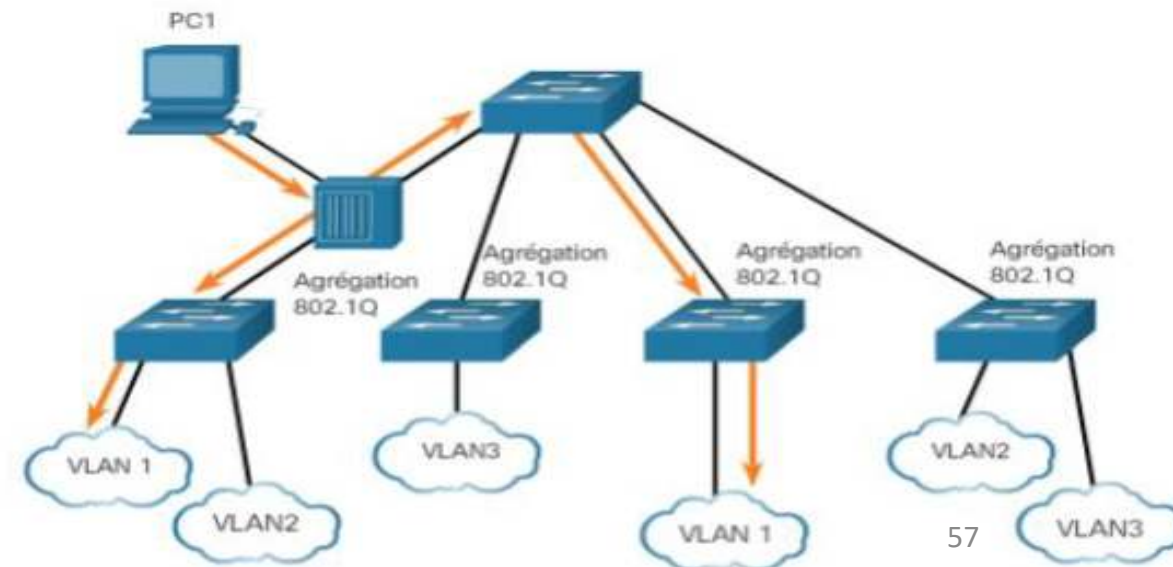
Les types de VLAN

- VLAN données : trafic généré par l'utilisateur
- VLAN par défaut (vlan 1): tous les ports du commutateur font partie initialement de ce VLAN, `show vlan brief`, il ne peut pas être supprimé
- VLAN natif : utilisé pour le trafic non étiqueté (associé aux ports d'agrégation)
- VLAN de gestion : utilisé pour accéder aux fonctionnalités de gestion
- VLAN voix: vlan dédié pour la voix pour assurer la QoS

VLAN dans un environnement à commutateurs multiples

VLAN natifs et étiquetage 802.1Q

- Le trafic de contrôle envoyé sur le VLAN natif ne doit pas être étiqueté.
- Les trames reçues sans étiquette restent sans étiquetage et sont placées dans le VLAN natif lors de la transmission.
- S'il n'y a pas de ports associés au VLAN natif et en l'absence d'autres trunks, une trame non étiquetée est ignorée.
- Lorsque vous configurez un port sur un commutateur Cisco, configurez les appareils de sorte qu'ils n'envoient pas de trames étiquetées sur le VLAN natif.
- Dans les commutateurs Cisco, le VLAN natif est le VLAN 1 par défaut.



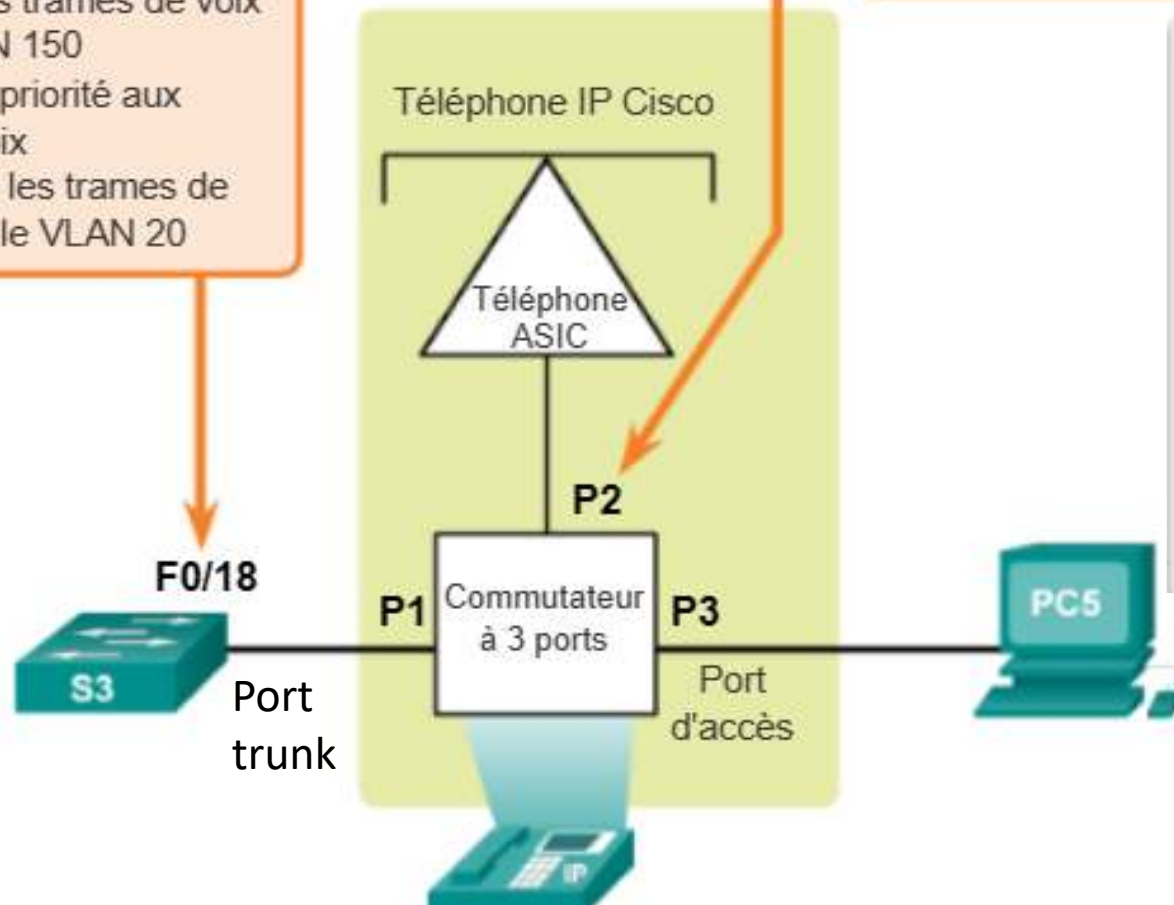
VLAN dans un environnement à commutateurs multiples

L'étiquetage du VLAN voix

Port de commutateur configuré pour prendre en charge le trafic voix :

- Demande au téléphone d'identifier les trames de voix avec le VLAN 150
- Donne la priorité aux trames de voix
- Transfère les trames de données sur le VLAN 20

Configuré pour affecter une étiquette VLAN 150 aux trames de trafic vocal



```
S1# sh interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)

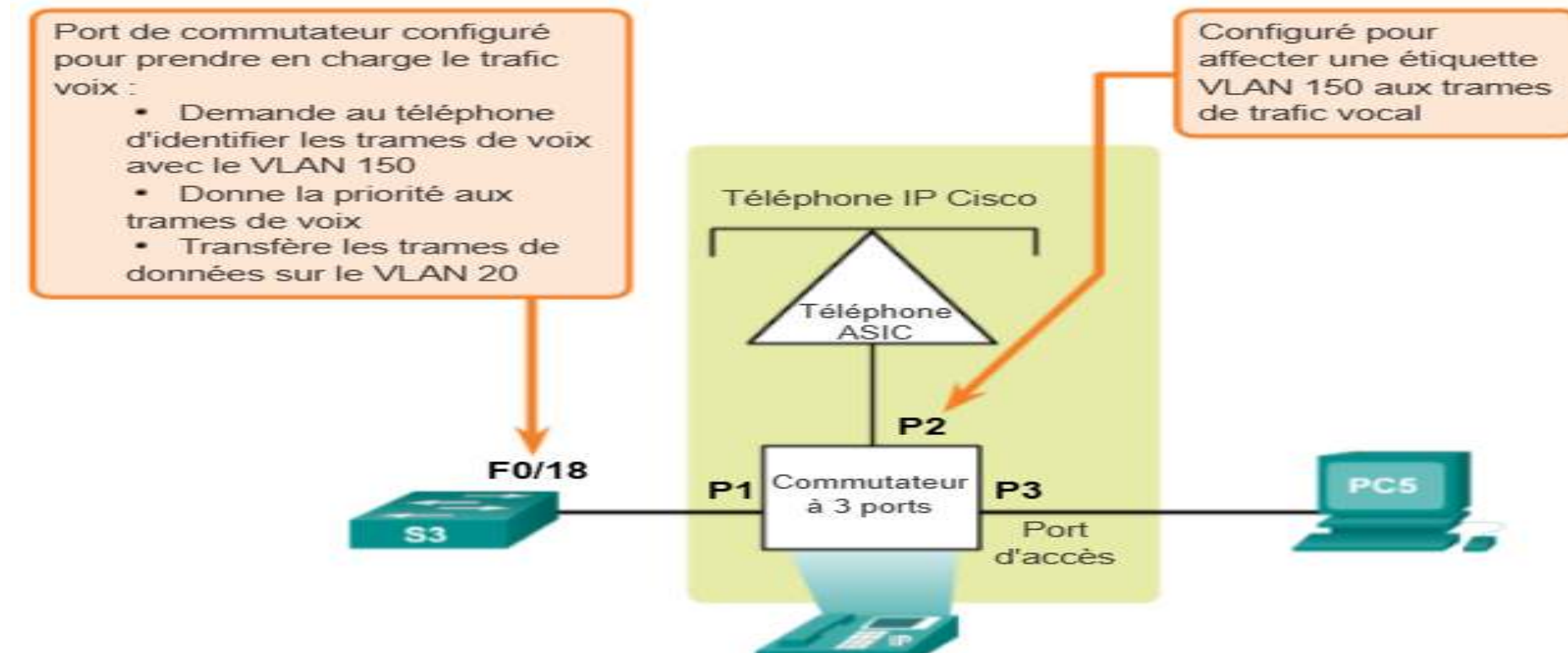
<résultat omis>
```

VLAN dans un environnement à commutateurs multiples

L'étiquetage du VLAN voix

Le téléphone IP Cisco contient un commutateur 10/100 à trois ports intégré. Les ports fournissent des connexions dédiées aux périphériques suivants :

- Le port 1 est connecté au commutateur ou à un autre périphérique de VoIP.
- Le port 2 est une interface 10/100 interne qui transporte le trafic du téléphone IP.
- Le port 3 (port d'accès) est connecté à un ordinateur ou autre périphérique.



Implémentation d'un VLAN

Les plages de VLAN sur les commutateurs Catalyst

- Les commutateurs Catalyst 2960 et 3560 prennent en charge plus de 4 000 VLAN.
- Ces VLAN se répartissent dans 2 catégories :
 - VLAN à plage normale
 - Ce sont les VLAN du numéro 1 au numéro 1 005.
 - Les configurations sont stockées dans le fichier vlan.dat (dans la mémoire Flash).
 - Les ID 1 002 à 1 005 sont réservés aux VLAN Token Ring et FDDI (Fiber Distributed Data Interface), qui sont créés automatiquement et que vous ne pouvez pas supprimer.
 - Réseaux locaux virtuels à plage étendue
 - Ce sont les VLAN du numéro 1 006 au numéro 4 096.
 - Les configurations sont stockées dans la configuration en cours (dans la mémoire NVRAM).
 - Le protocole VTP (VLAN Trunking Protocol) ne prend pas en compte les VLAN appartenant à la plage étendue.

Implémentation d'un VLAN

Les plages de VLAN sur les commutateurs Catalyst

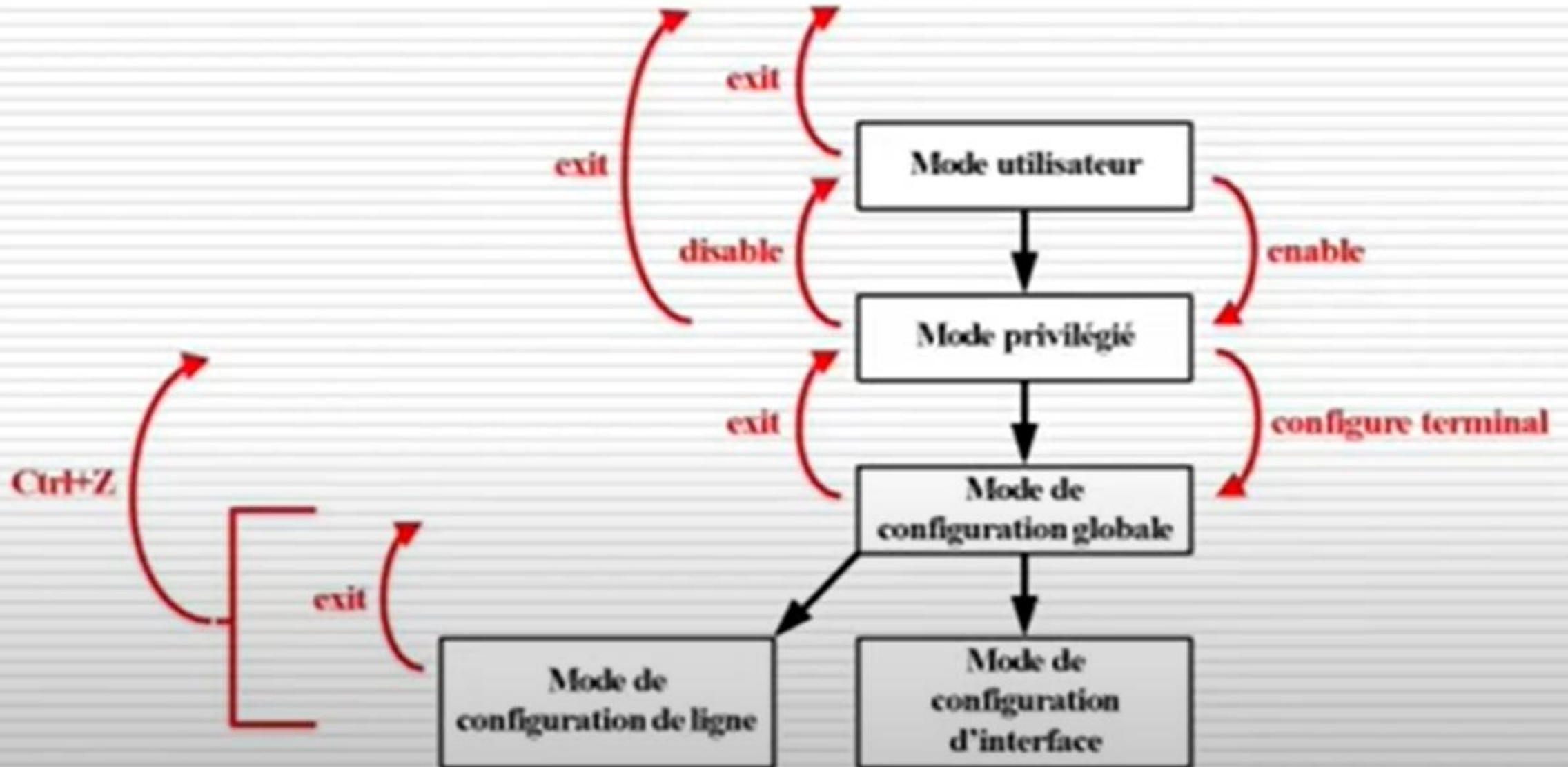
- Réseaux locaux virtuels à plage normale

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#
```

Configuration d'un commutateur



Configuration d'un commutateur

2960-RG> **enable** ou **en**

2960-RG# **configure terminal** ou **conf t**

2960-RG(config)# **interface fa0/1** ou **int fa0/1**

2960-RG(config-if)# **exit** ou **ex**

2960-RG(config)# **vlan 2**

2960-RG(config-vlan)# **ex**

2960-RG(config)# **ex** **2960-RG#** **Disable** ou **ex** **2960-RG>**

Création de VLAN sur switch Cisco

Commandes IOS de commutateur CISCO Création de VLAN

Mode de configuration global	switch1# configure terminal
VLAN avec ID ou un VLAN-range	switch1(config)# vlan { vlan-id vlan-range }
Indiquer un nom unique pour identifier le VLAN	switch1(config-vlan)# name vlan-name
Supprimer un VLAN	switch1(config-vlan)# no vlan vlan-id
Passer en mode exécution	switch1(config-vlan)# end

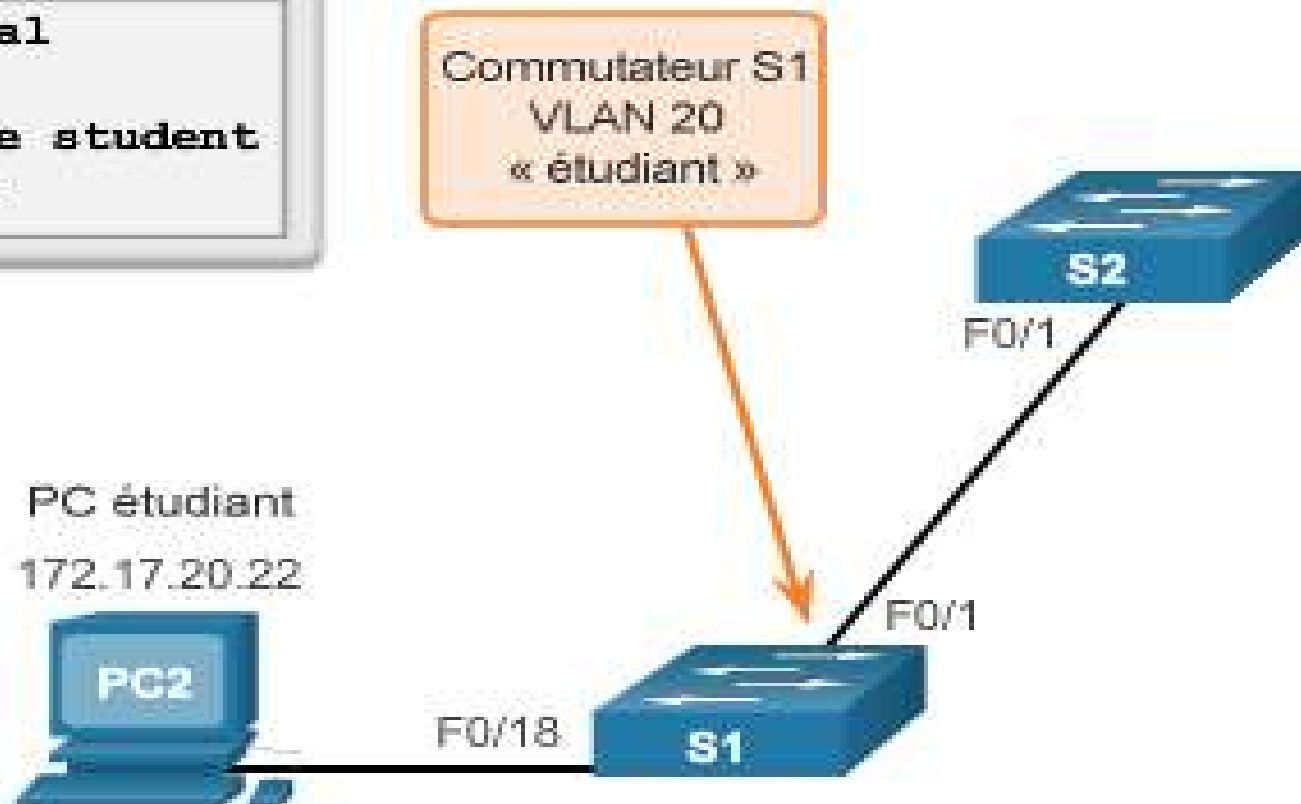
Exemple de datacenter qui prévoit d'avoir 1000 vlans

```
switch1(config)# vlan 1-1001
```

Création de VLAN sur switch Cisco

Exemple de configuration

```
S1# configure terminal  
S1(config)# vlan 20  
S1(config-vlan)# name student  
S1(config-vlan)# end
```



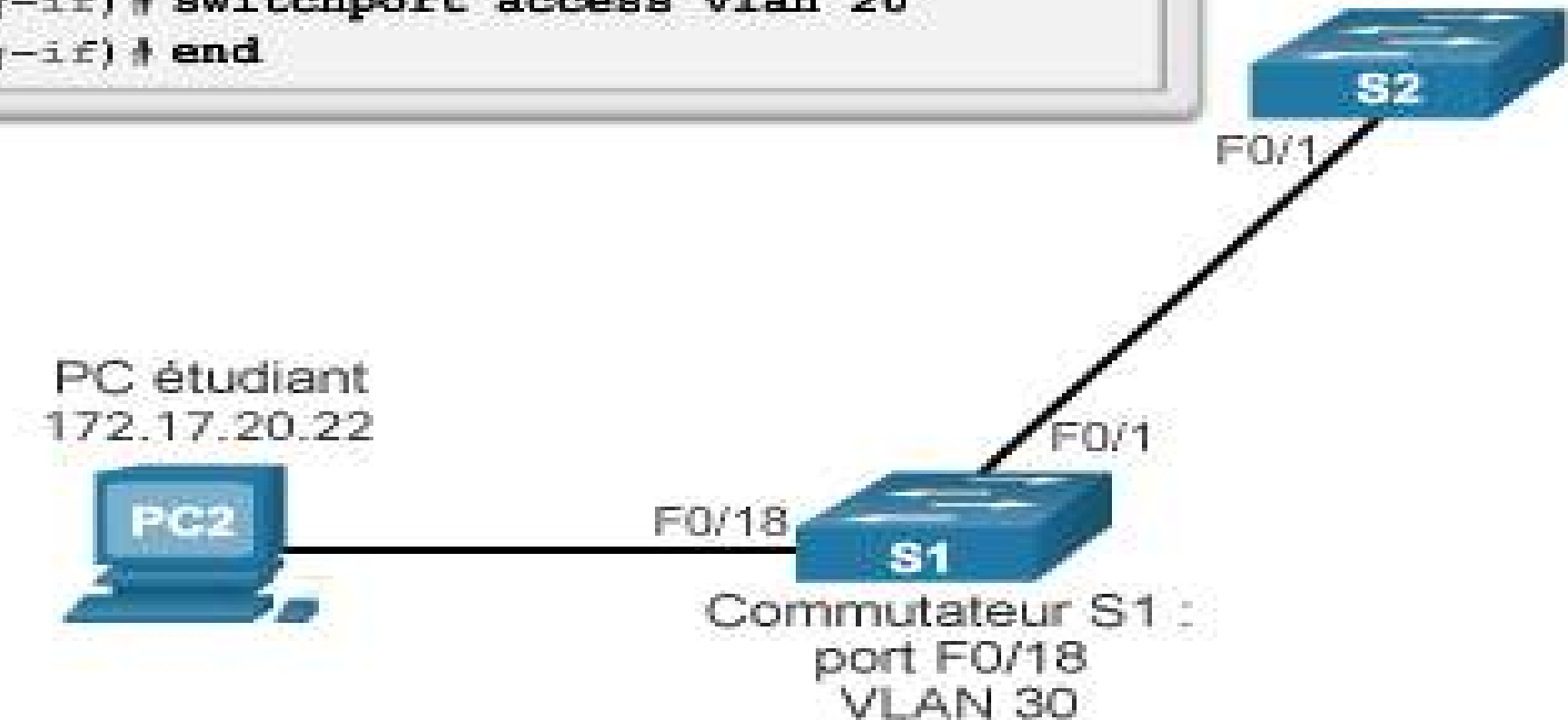
Affectation de ports à des VLAN

Commandes IOS de commutateur CISCO Attribution des ports aux VLAN

Mode de configuration globale	switch1# configure terminal
Mode de configuration d'interface SVI	switch1(config)# interface interface-id
Définir le port en mode d'accès	switch1(config-if)# switchport mode access
Affecter le port au réseau virtuel	switch1(config-if)# switchport access vlan valn-id
Passer en mode exécution	switch1(config-if)# end

Affectation de ports à des VLAN

```
s1# configure terminal  
s1(config)# interface F0/18  
s1(config-if)# switchport mode access  
s1(config-if)# switchport access vlan 20  
s1(config-if)# end
```



Vérification des informations du VLAN

Commande `show vlan`

Syntaxe de commande de l'interface en ligne de commande Cisco IOS

`show vlan [brief | id vlan-id | name vlan-name | summary ] .`

Afficher une ligne pour chaque VLAN comportant le nom du VLAN, son état et ses ports.

`brief`

Afficher des informations sur un VLAN unique identifié par un numéro d'ID de VLAN.

La valeur `id de vlan` peut être comprise entre 1 et 4094.

`id id de vlan`

Afficher des informations sur un VLAN unique identifié par un nom de VLAN. Le nom de VLAN est une chaîne ASCII de 1 à 32 caractères de long.

`name nom_vlan`

Afficher un résumé sur les VLAN.

`summary`

Vérification des informations du VLAN

Commande `show interfaces`

Syntaxe de commande de l'interface en ligne de commande Cisco IOS

<code>show interfaces [<i>interface-id</i> <i>vlan</i> <i>vlan-id</i>] switchport</code>	
Les interfaces autorisées comprennent les ports physiques (y compris le type, le module et le numéro de port) et les canaux de port. La plage des canaux de port est comprise entre 1 et 6.	<i>id</i> <i>d'interface</i>
Identification du VLAN. La plage est comprise entre 1 et 4094.	vlan <i>id de</i> <i>vlan</i>
Afficher l'état administratif et opérationnel d'un port de commutation, y compris les paramètres de blocage et de protection du port.	switchport

Création de VLAN sur switch Cisco

Trunks de VLAN

- Pour configurer un port de commutateur sur l'extrémité d'une liaison trunk, utilisez la commande **switchport mode trunk**. Avec cette commande, l'interface passe en mode trunking permanent.

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	<code>S1#configure terminal</code>
Passer en mode de configuration d'interface pour SVI.	<code>S1(config)# interface interface_id</code>
Forcer la liaison à devenir une liaison trunk.	<code>S1(config-if)# switchport mode trunk</code>
Indiquer un VLAN natif pour les trunks 802.1Q non étiquetés.	<code>S1(config-if)# switchport trunk native vlan vlan_id</code>
Indiquer la liste des VLAN autorisés sur la liaison trunk.	<code>S1(config-if)# switchport trunk allowed vlan vlan-list</code>
Repasser en mode d'exécution privilégié.	<code>S1(config-if)# end</code>

Création de VLAN sur switch Cisco

Trunks de VLAN

Exemple de topologie

```
VLAN 10 - Faculty/Staff - 172.17.10.0/24  
VLAN 20 - Students - 172.17.20.0/24  
VLAN 30 - Guest - 172.17.30.0/24  
VLAN 99 - Native - 172.17.99.0/24
```

Faculté
VLAN 10
172.17.10.21



Étudiant
VLAN 20
172.17.20.22



Invité
VLAN 30
172.17.30.23



F0/1

Trunk

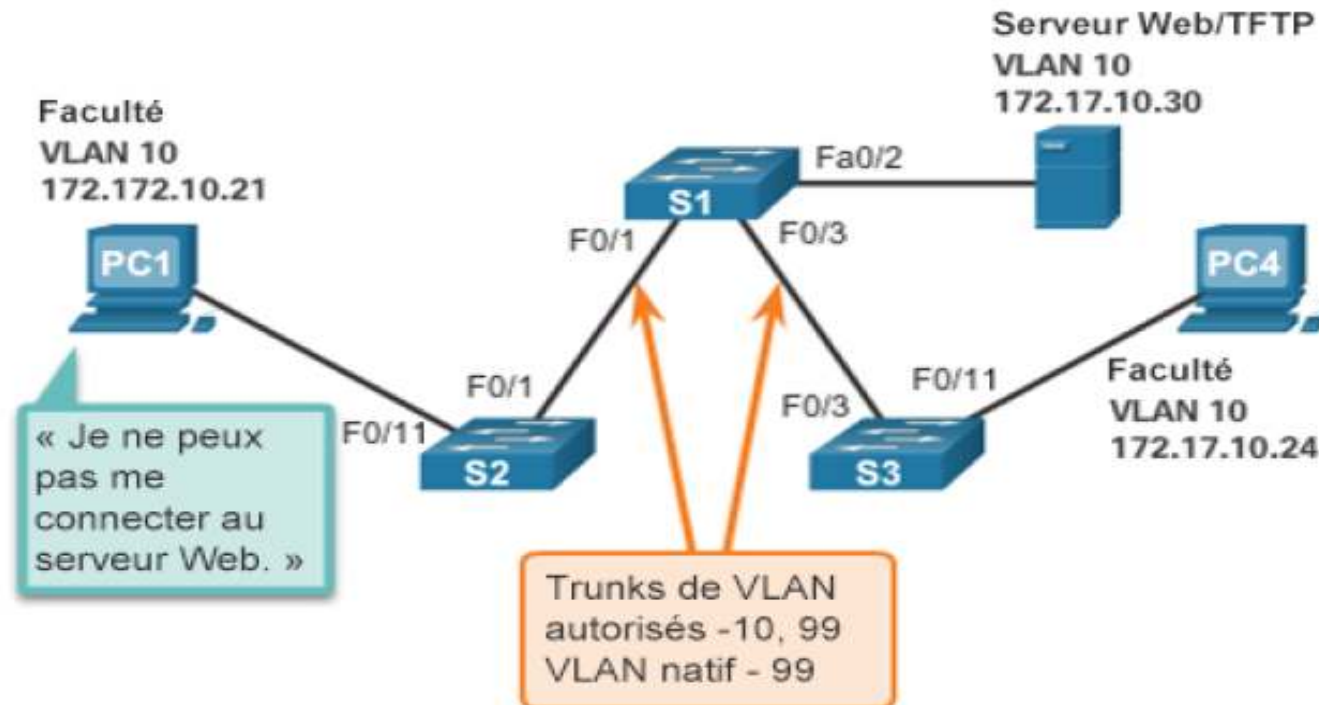
F0/1

S2

```
S1(config)# interface FastEthernet0/1  
S1(config-if)# switchport mode trunk  
S1(config-if)# switchport trunk native vlan 99  
S1(config-if)# switchport trunk allowed vlan 10,20,30,99  
S1(config-if)# end
```

Les problèmes d'adressage IP avec les VLAN

- Il est très fréquent d'associer un VLAN à un réseau IP.
- Comme les différents réseaux IP communiquent uniquement via un routeur, tous les appareils d'un VLAN doivent appartenir au même réseau IP pour communiquer.
- La figure montre que le PC1 ne peut pas communiquer avec le serveur parce que son adresse IP est incorrecte.



Liste de VLAN incorrecte

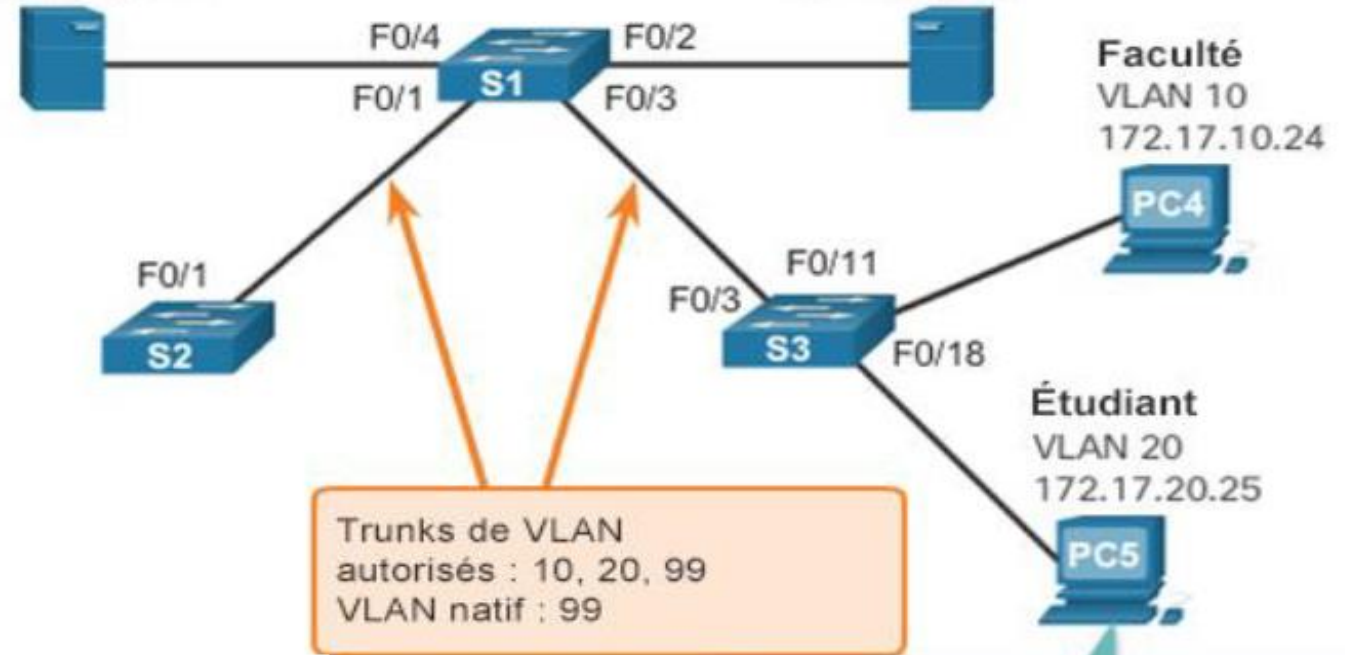
Topologie du scénario

Serveur de messagerie
des étudiants
VLAN 20
172.17.20.10

Serveur Web/TFTP
VLAN 10
172.17.10.30

Faculté
VLAN 10
172.17.10.24

Étudiant
VLAN 20
172.17.20.25



« Je ne peux pas me connecter au serveur de messagerie des étudiants. »

Résultats du commutateur S1

```
S1# show interfaces trunk
Port      Mode      Encapsulation  Status  Native vlan
Fa0/1     on        802.1q         trunking  99
Fa0/3     on        802.1q         trunking  99
Port      Vlans allowed on trunk
Fa0/1     10,99
Fa0/3     10,99
---
```

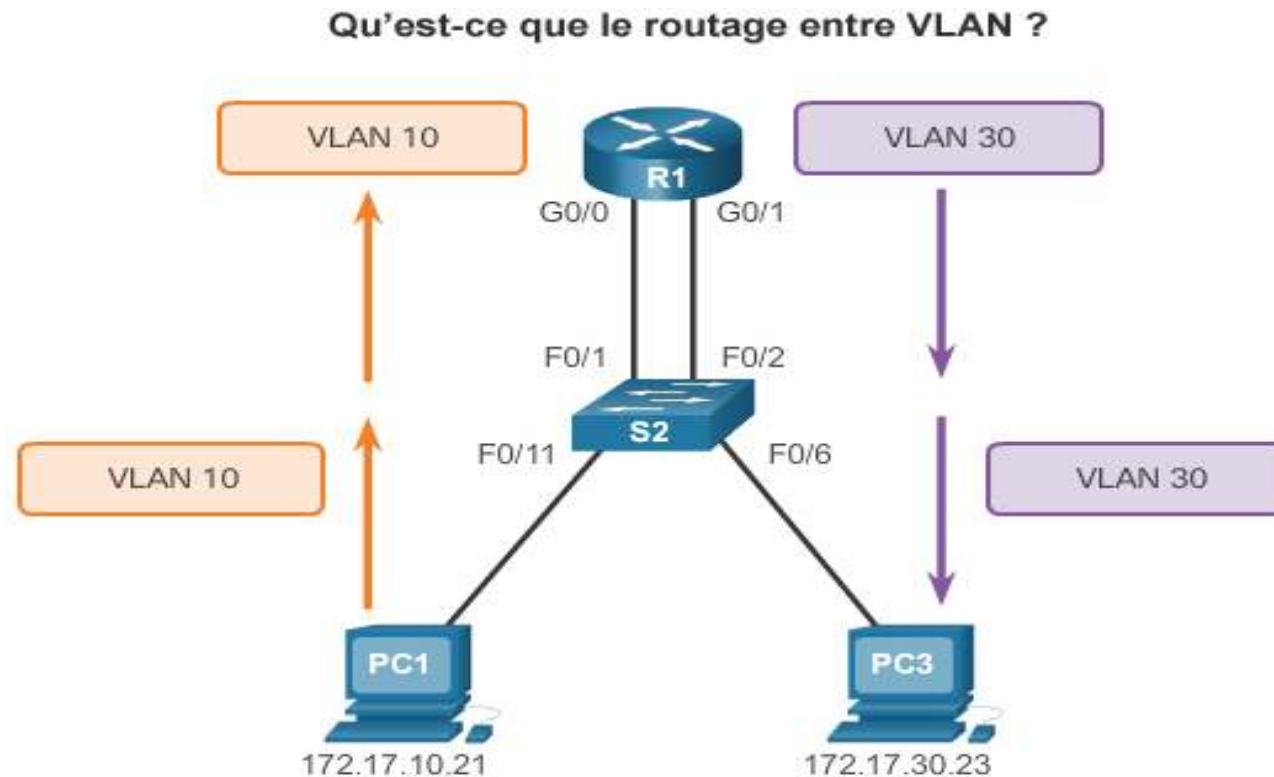
S1#

Liste de VLAN incorrecte (suite)

- Les VLAN doivent être autorisés dans le trunk avant que leurs trames ne puissent être transmises sur la liaison.
- Utilisez la commande **switchport trunk allowed vlan** pour indiquer quels VLAN sont admis dans un trunk.
- Utilisez la commande **show interfaces trunk** pour vérifier que les VLAN appropriés sont autorisés dans un trunk.

Routage inter-VLAN avec des routeurs

- ❑ Les commutateurs de couche 2 ne peuvent pas acheminer le trafic entre les VLAN sans l'aide d'un routeur.
- ❑ Le routage inter-VLAN consiste à acheminer du trafic réseau d'un VLAN à un autre grâce à un routeur.

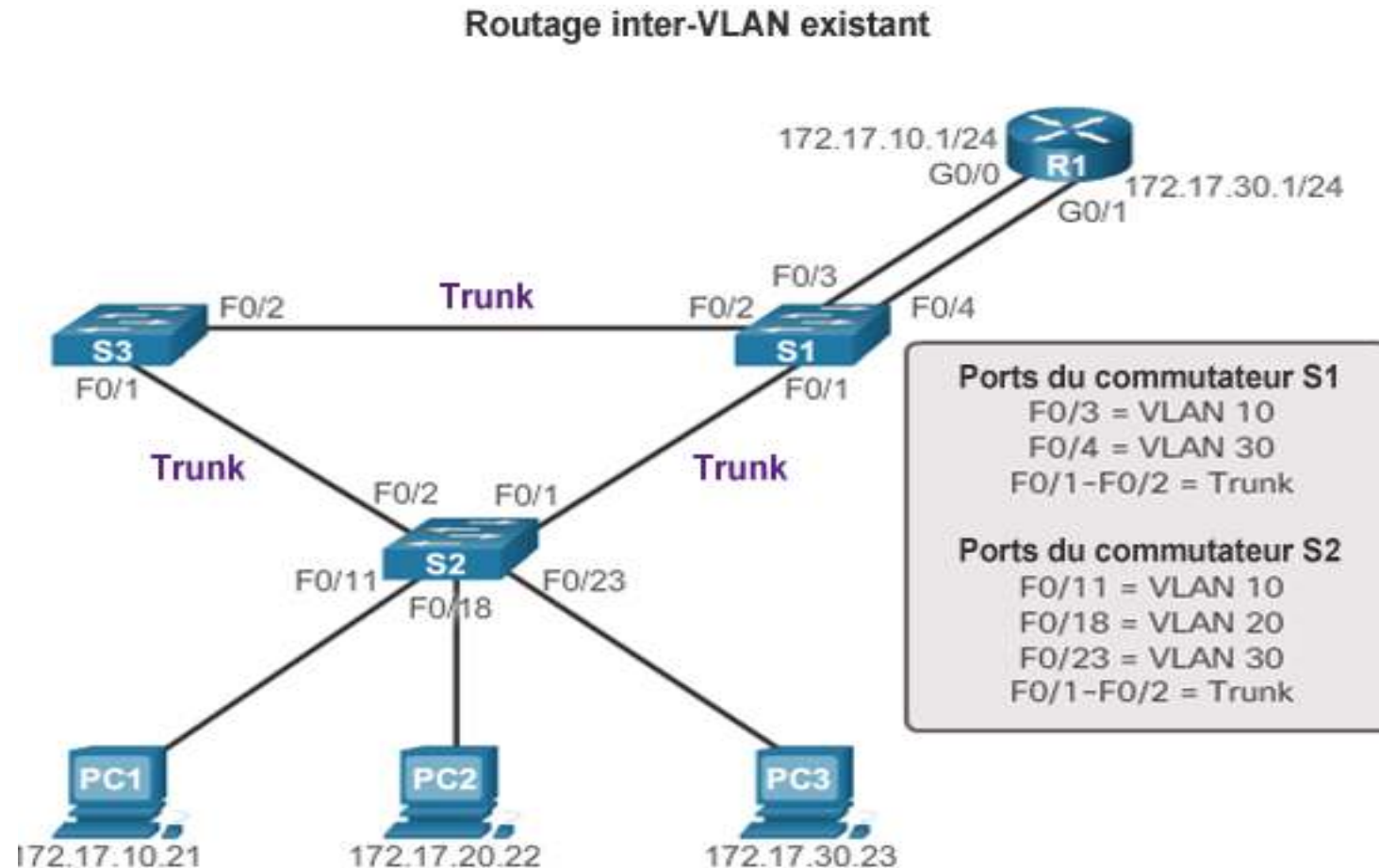


Le routage inter-VLAN existant

- ❑ Des routeurs réels étaient utilisés pour acheminer du trafic entre les VLAN.
- ❑ Chaque VLAN était connecté à une interface physique différente du routeur.
- ❑ Les paquets arrivaient sur le routeur par l'une des interfaces, étaient acheminés, puis ressortaient par une autre.
- ❑ Comme les interfaces du routeur étaient connectées aux VLAN et que leurs adresses IP correspondaient à un VLAN spécifique, le routage entre les VLAN pouvait être assuré.
- ❑ Les grands réseaux comptant un grand nombre de VLAN avaient besoin de nombreuses interfaces de routeur

Le routage inter-VLAN existant

Dans cet exemple, le routeur a été configuré avec deux interfaces physiques distinctes pour interagir avec les différents VLAN et effectuer le routage.



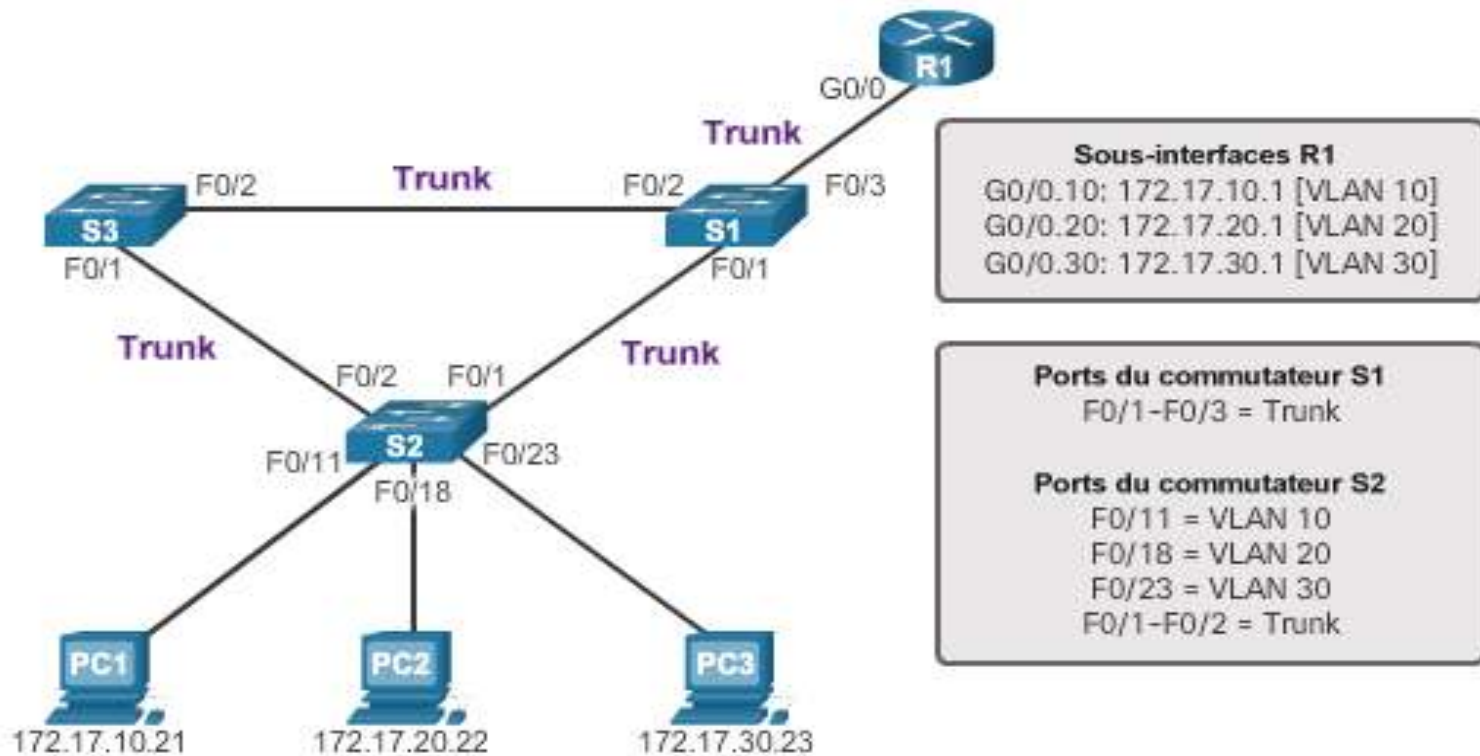
Le routage inter-VLAN

«Router-on-a-Stick»

- ☐ L'approche «Router-on-a-Stick» utilise une seule interface physique du routeur.
- ☐ Une des interfaces physiques du routeur est configurée en tant que port trunk 802.1Q afin de comprendre les balises VLAN.
- ☐ Des sous-interfaces logiques sont créées (une seule par VLAN).
- ☐ Chaque sous-interface est configurée avec une adresse IP du VLAN qu'elle représente.
- ☐ Les membres (hôtes) du VLAN sont configurés pour utiliser l'adresse de la sous-interface comme passerelle par défaut.

Le routage inter-VLAN «Router-on-a-Stick»

Routage inter-VLAN « Router-on-a-Stick »



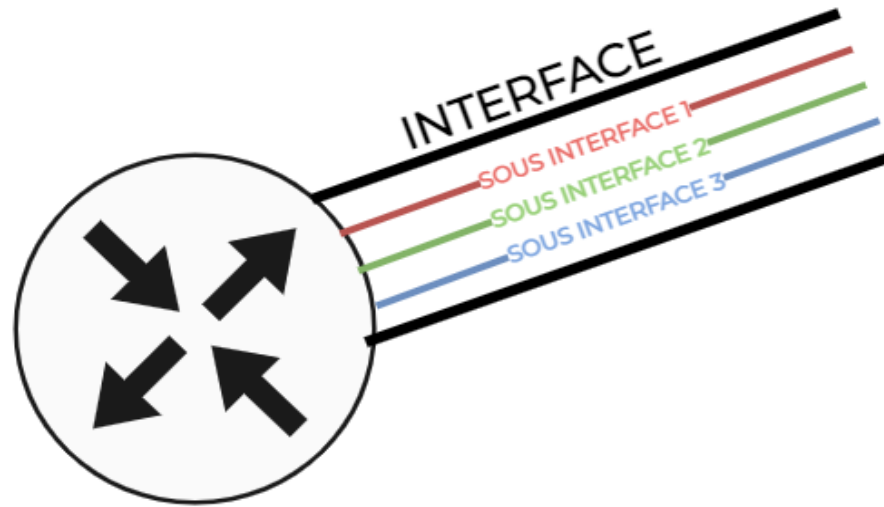
L'interface du routeur est configurée pour fonctionner comme une liaison trunk et est connectée à un port de commutateur configuré en mode trunk.

Configuration du routage «Router-on-a-Stick»

- Pour remplacer l'ancien routage inter-VLAN, vous pouvez recourir au trunking VLAN et aux sous-interfaces.
- Le trunking VLAN permet à une seule interface physique de routeur d'acheminer le trafic de plusieurs VLAN.
- L'interface physique du routeur doit être connectée à une liaison d'agrégation sur le commutateur adjacent.
- Sur le routeur, des sous-interfaces sont créées pour chaque VLAN unique.
- Chaque sous-interface reçoit une adresse IP spécifique selon son sous-réseau ou son VLAN et est également configurée pour étiqueter les trames pour ce VLAN.

Configuration du routage «Router-on-a-Stick»

- Créez des sous-interfaces et reliez vos VLANs à Internet



Créer des sous-interfaces dépendantes de l'interface GigabitEthernet **0/0/1** :

- GigabitEthernet **0/0/1.1** correspond au VLAN 1
- GigabitEthernet **0/0/1.2** correspond au VLAN 2
- GigabitEthernet **0/0/1.3** correspond au VLAN 3
-

```
Router(config)#interface fastEthernet0/0.1
Router(config-subif)#encapsulation dot1Q 1 native
Router(config-subif)#ip address 192.168.1.254 255.255.255.0
Router(config-subif)#exit
```

```
Router(config)#interface fastEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.2.254 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

```
Router(config)#interface fastEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.3.254 255.255.255.0
Router(config-subif)#no shutdown
```

```
Router(config-subif)#interface fastEthernet0/0.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip address 192.168.99.254 255.255.255.0
Router(config-subif)#no shutdown
```

```
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
```

Configuration du routage «Router-on-a-Stick»

- Pour relier vos VLANs aux routeurs, vous devez créer des **sous-interfaces** et leur attribuer un VLAN et une adresse IP. Cette interface deviendra le **gateway** du VLAN :
 - Router(config)#int fastEthernet 0/0.X
 - Router(config-subif)#encapsulation dot1Q X
 - Router(config-subif)#ip address adresse-ip masque
 - Router(config-subif)#exit
- Une fois vos VLANs reliés au routeur, le routeur crée les routes permettant la communication entre eux.

Synthèse

- Expliquer la fonction des VLAN dans un réseau commuté.
- Expliquer comment un commutateur transmet des trames en fonction de la configuration du VLAN dans un environnement à commutateurs multiples.
- Configurer un port de commutateur à attribuer à un VLAN en fonction des conditions requises.
- Configurer un port trunk sur un commutateur LAN.
- Dépanner des configurations de VLAN et de trunk dans un réseau commuté.
- Décrire les deux options permettant de configurer le routage inter-VLAN.
- Configurer le routage entre réseaux locaux virtuels avec la méthode «Router-on-a-stick».