

# Chapitre 2: Les VLAN

# Chapitre 2: Les VLAN

## Plan

1. Principe d'un VLAN
2. Trunking
3. VTP
4. Routage inter-VLAN

# Chapitre 2: Les VLAN

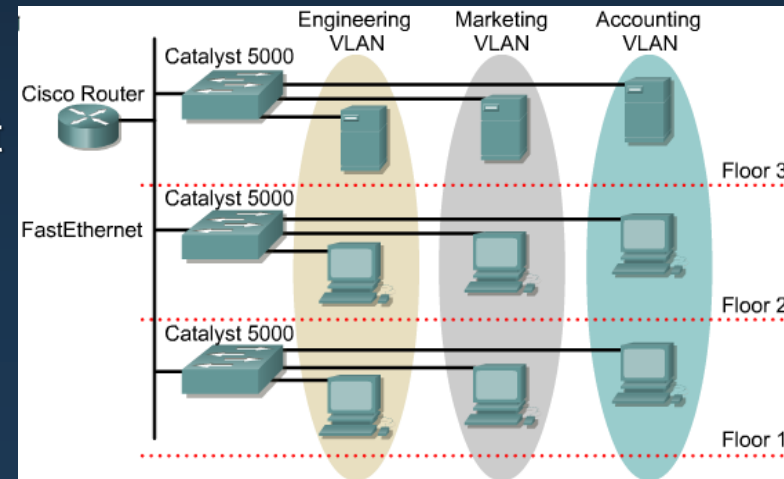
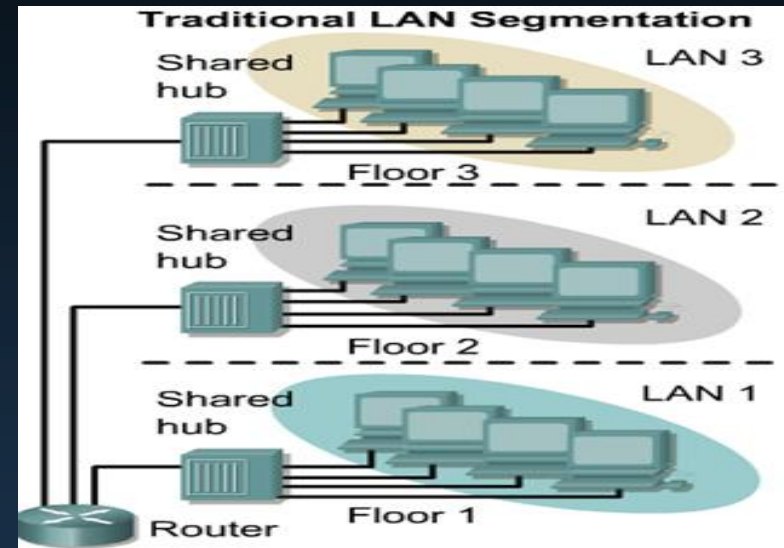
## 1. Principe du VLAN

### ❑ Commutation classique:

- Topologie physique liée à la topologie logique
- Pour communiquer entre les LAN, chaque segment doit avoir un port séparé
- Postes de travail groupés par leur proximité du commutateur : chaque groupe se trouve au même endroit

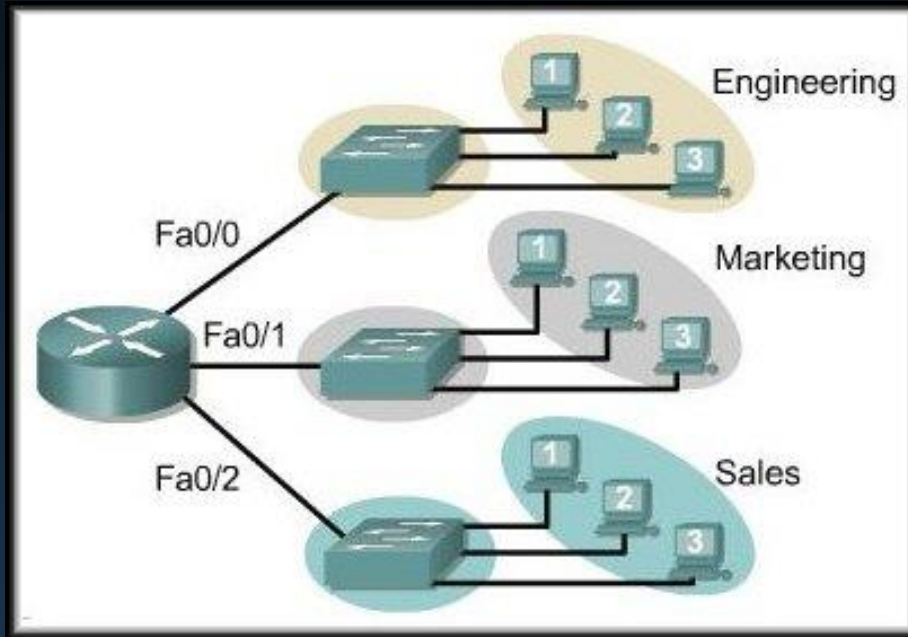
### ❑ Commutation avec VLAN :

- Ils segmentent de façon logique les réseaux sur les fonctions, équipes de travail ou des applications indépendamment de l'emplacement physique ou des connections réseaux.
- Un VLAN permet à un administrateur réseau de créer des groupes de périphériques en réseau logique qui se comportent comme s'ils se trouvaient sur un réseau indépendant

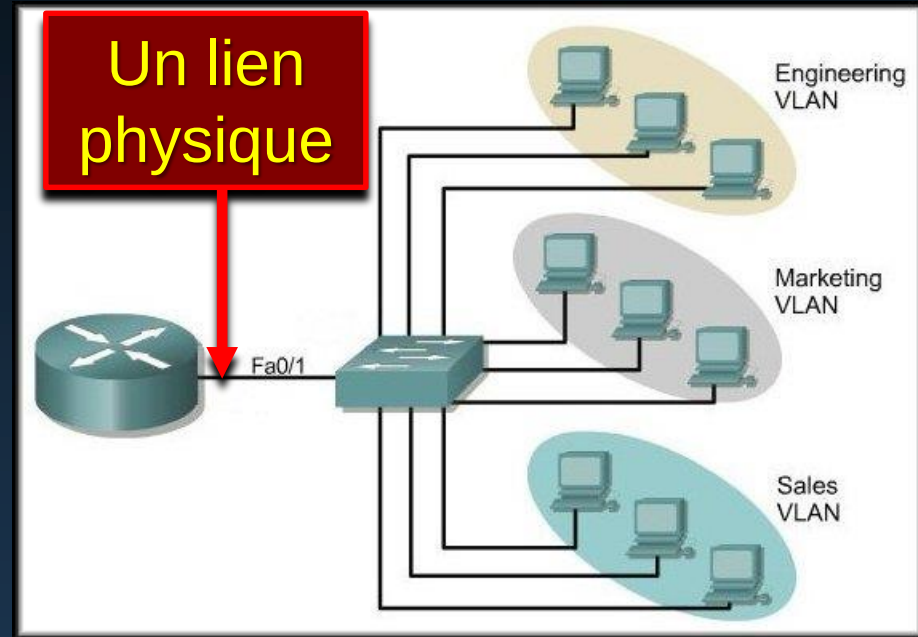


# Chapitre 2: Les VLAN

## 1. Principe du VLAN



- 3 domaines de diffusion séparés créés à l'aide d'un routeur avec 3 ports et 3 commutateurs.
- Le routeur filtre les broadcasts pour chaque LAN.



- La conception crée quand même les 3 domaines de diffusion séparés, mais ne nécessite que 1 commutateur.
- Le routeur fournit un filtrage des broadcasts à travers un lien unique.



# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### □ Notions de base sur les VLAN

- Les VLAN peuvent être créés sous forme de réseaux de bout en bout ou exister à l'intérieur de frontières géographiques.
- Un réseau VLAN de bout en bout a les caractéristiques suivantes:
  - Les utilisateurs sont regroupés en VLAN qui dépendent de leur groupe de travail ou de leur fonction, mais pas de leur localisation physique.
  - Tous les utilisateurs d'un VLAN doivent avoir les mêmes modèles de flux de trafic
  - Lorsqu'un utilisateur se déplace sur le campus, son appartenance à un VLAN ne doit pas changer.
  - Chaque VLAN est caractérisé par un ensemble commun de besoins de sécurité pour tous les membres.
- Une adresse réseau de couche 3 unique doit être affectée à chaque VLAN. Cela permet aux routeurs de commuter les paquets entre les VLAN (communication inter-VLAN)
- Les VLAN peuvent assurer la sécurité des réseaux en définissant les nœuds réseaux qui peuvent communiquer entre eux.
- Le nombre de VLAN dans un commutateur varie en fonction des facteurs suivants:
  - Modèles de trafic
  - Types d'application
  - Besoins d'administration réseau
  - Standardisation de groupes

# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### ❑ Plages d'ID de VLAN

#### ■ Plage normale : 1 – 1005

- Utilisés dans les réseaux de petites, moyennes et grandes entreprises.
- Les ID de 1002 à 1005 sont réservés aux VLAN Token Ring et aux FDDI (fibre optique). Ils sont automatiquement créés et ne peuvent pas être supprimés.
- Les configurations sont stockées dans un fichier vlan.dat stocké dans la mémoire flash du commutateur..
- Le protocole VTP (VLAN Trunking Protocol), permet de gérer des configurations de VLAN entre des commutateurs.

#### ■ Plage étendue : 1006 - 4096

- Permettent d'étendre les infrastructure à un plus grand nombre de clients.
- Prennent en charge moins de fonctionnalités VLAN que les VLAN à plage normale.
- Sont enregistrés dans le fichier de configuration en cour.
- **Le protocole VTP ne prend pas en compte les VLAN à plage étendue.**

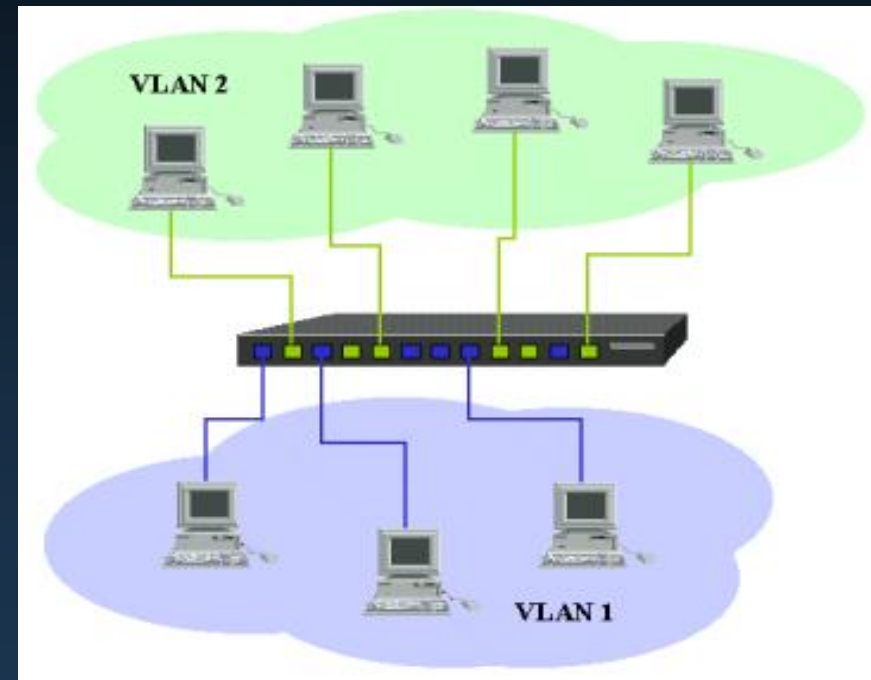
# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### □ Niveaux de VLAN

#### ➤ Les Vlan par port (Vlan de niveau 1)

- Associer chaque port du commutateur à un VLAN particulier.
- 90% des VLAN sont des VLAN par port
- Manquent de souplesse: tout déplacement d'une station nécessite une reconfiguration des ports.
- Toutes les stations reliées sur un port par l'intermédiaire d'un concentrateur, appartiennent au même VLAN.



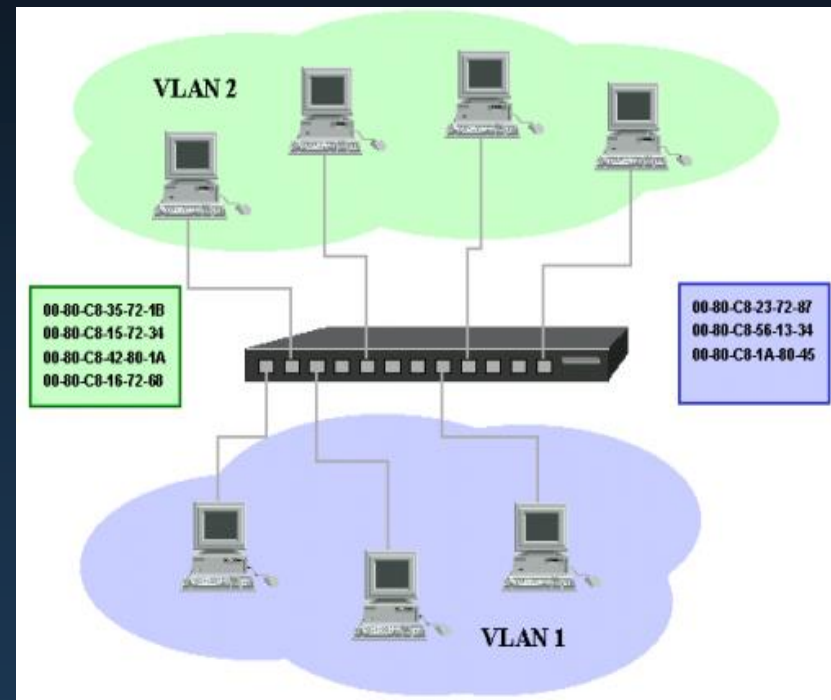
# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### □ Niveaux de VLAN

#### ➤ Les Vlan par @MAC (Vlan de niveau 2)

- On affecte chaque adresse MAC à un VLAN.
- à partir de l'association Mac/VLAN, affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.
- indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).
- Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.



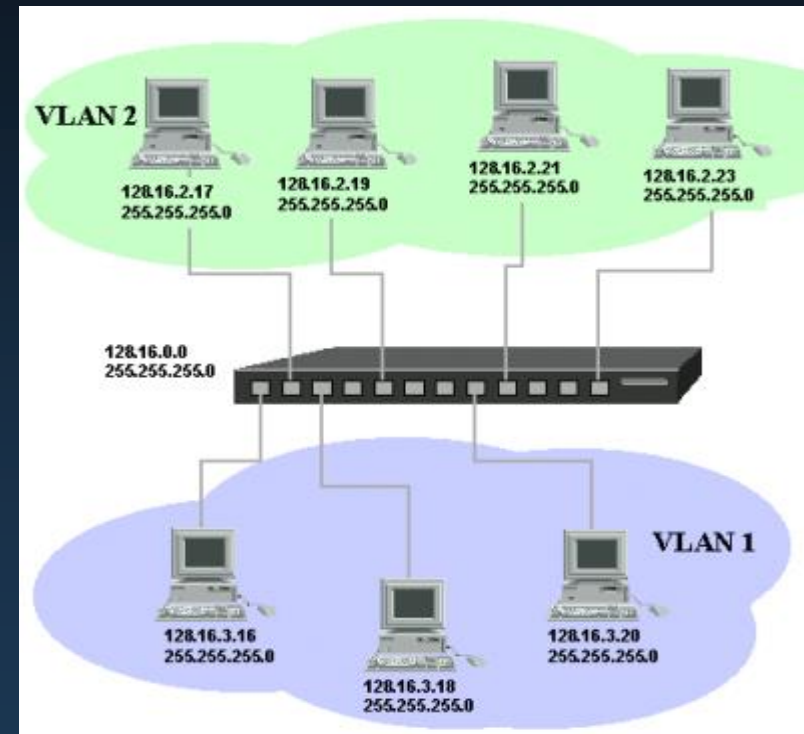
# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### □ Niveaux de VLAN

#### ➤ Les Vlan de niveau 3

- Le VLAN par sous-réseau (*Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Solution souple car la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station.
- Le VLAN par protocole (*Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.



# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### Types de VLAN

#### 1. Vlan de données

Configuré pour ne transporter que le trafic généré par l'utilisateur.

#### 2. VLAN par défaut

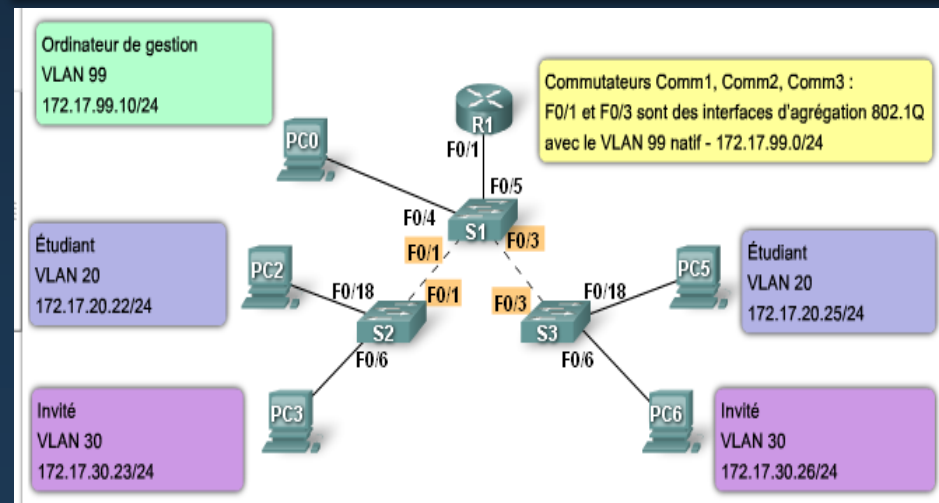
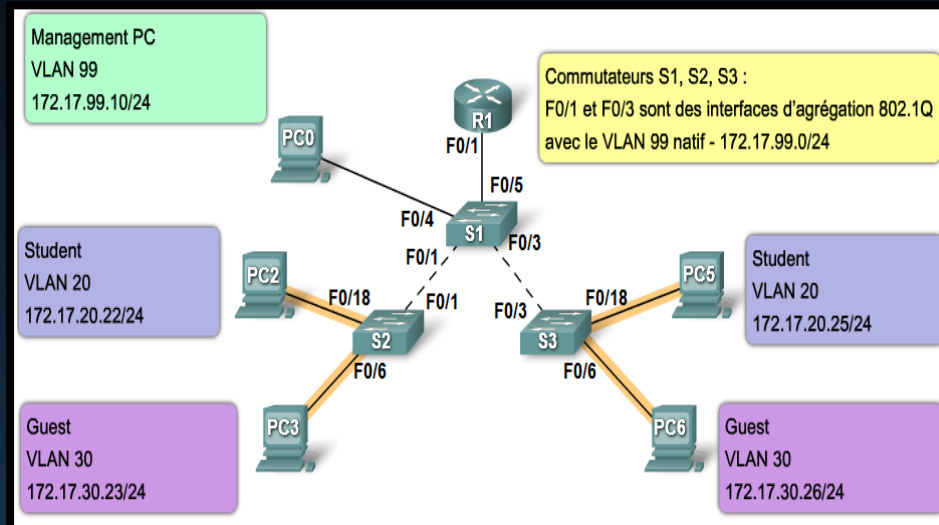
Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur.

N'importe quel périphérique connecté à n'importe quel port du commutateur communique avec d'autres périphériques sur d'autres ports du commutateur.

Le VLAN par défaut des commutateurs

Cisco est le **VLAN 1**

On ne peut ni le renommer, ni le supprimer.



# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### Types de VLAN

### 3. VLAN natif

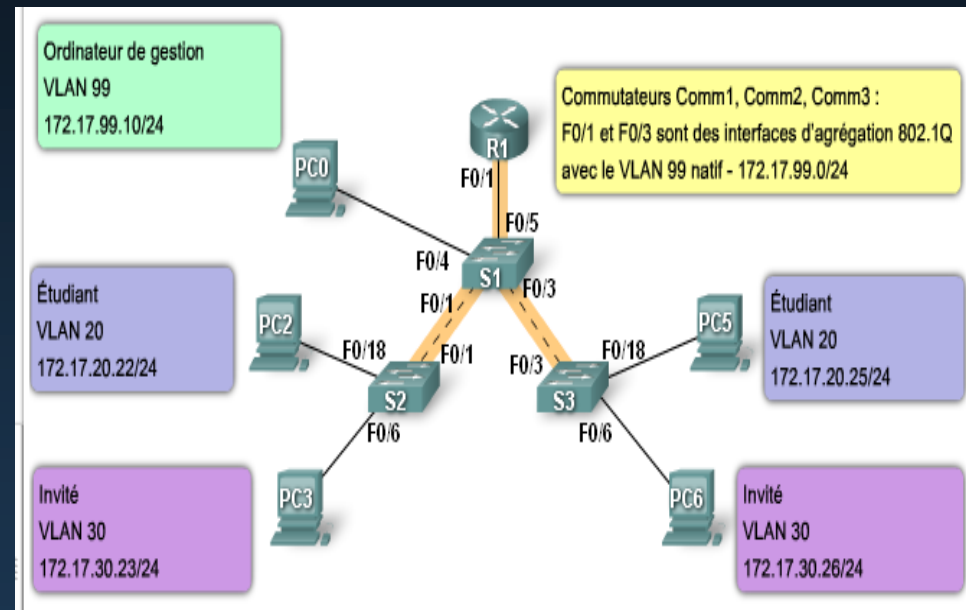
Un VLAN natif est affecté à un **port d'agrégation 802.1Q** : prend en charge le trafic provenant de **nombreux VLAN** (**trafic étiqueté ou « tagged traffic »**), ainsi que le trafic qui ne provient pas d'un VLAN (**trafic non étiqueté ou « untagged traffic »**).

Le port d'agrégation 802.1Q place le trafic non étiqueté sur le VLAN natif.

Dans la figure, le VLAN natif est le **VLAN 99**.

Le trafic non étiqueté est généré par un ordinateur connecté à un port du commutateur sur lequel est configuré le VLAN natif.

Les VLAN natifs sont définis dans la spécification IEEE 802.1Q. Il est recommandé d'utiliser un autre VLAN que le VLAN 1 comme VLAN natif.





# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### Types de VLAN

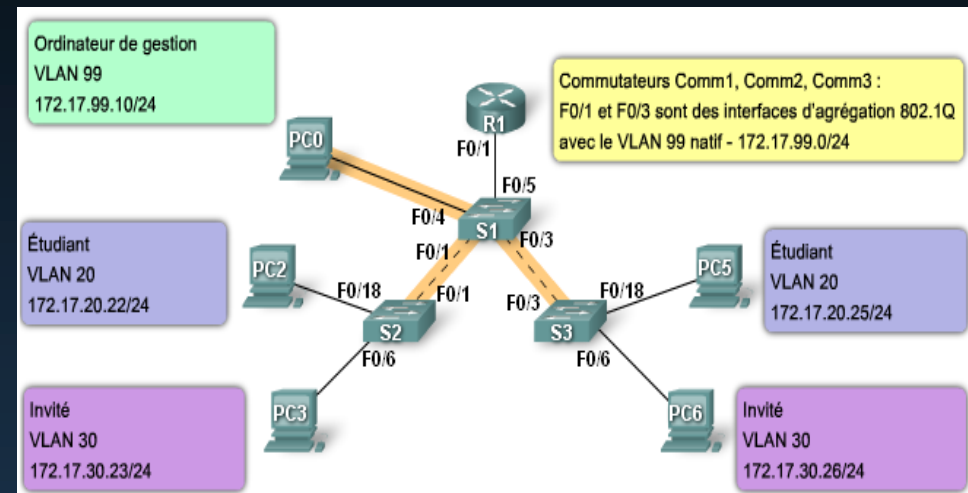
## 4. VLAN de gestion

Permet d'accéder aux fonctionnalités de gestion d'un commutateur.

On attribue au VLAN de gestion une @IP et un masque de sous-réseau.

## 5. VLAN Voix

- Le trafic de voix sur IP requiert les éléments suivants :
  - bande passante consolidée pour garantir la qualité de la voix ;
  - priorité de transmission par rapport aux autres types de trafic réseau ;
  - possibilité de routage autour des zones encombrées du réseau ;
  - délai inférieur à 150 millisecondes (ms) sur le réseau.
- Pour remplir ces conditions, le réseau entier doit être conçu pour prendre en charge la voix sur IP





# Chapitre 2: Les VLAN

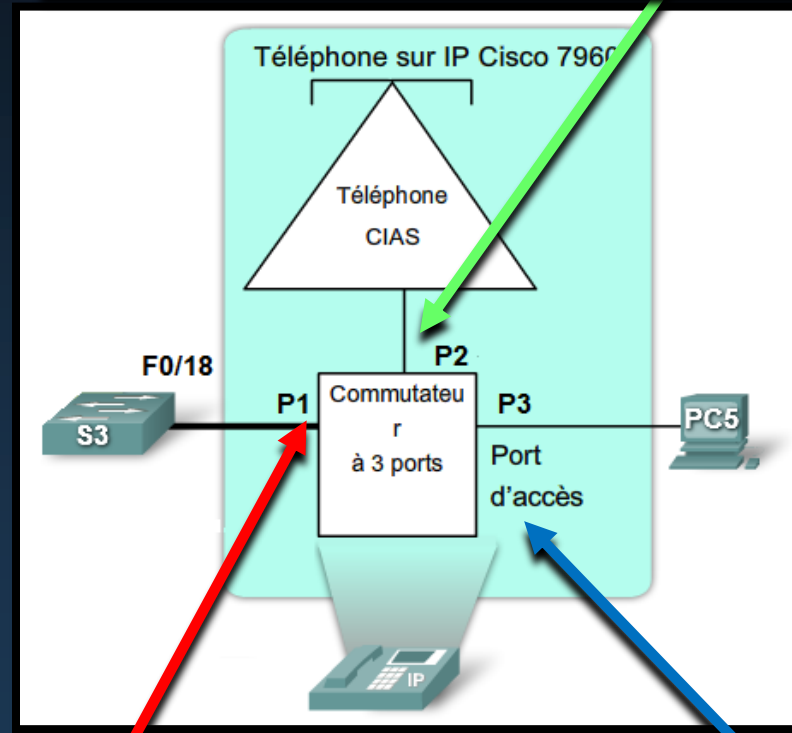
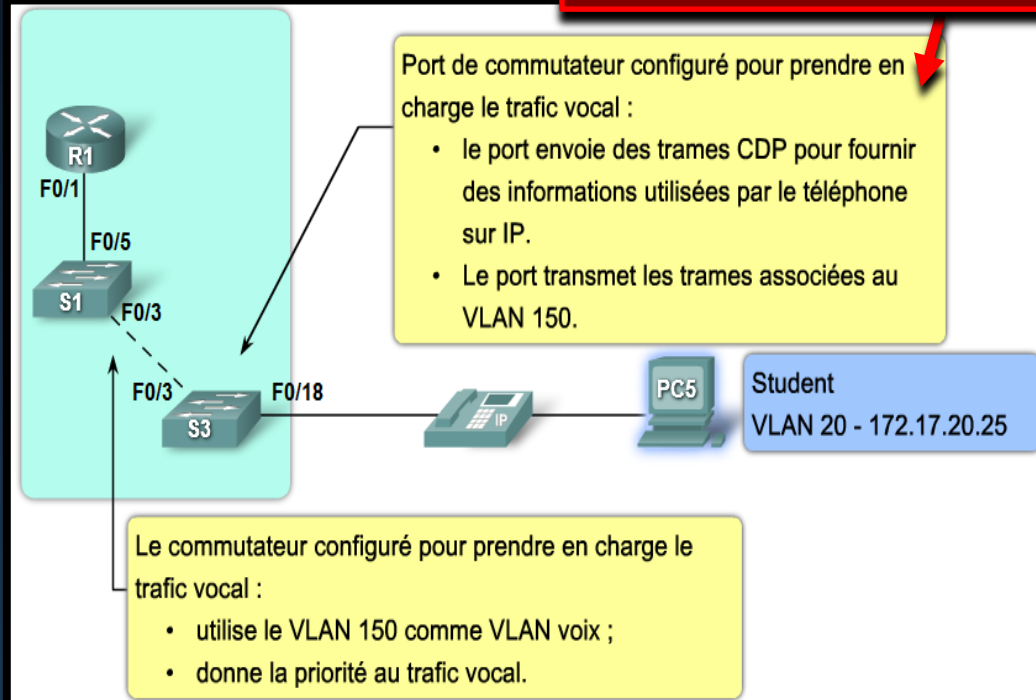
## 1. Principe du VLAN

### Types de VLAN

### 5. VLAN Voix

VLAN 150 configuré pour prendre en charge le trafic voix.

Le Port 2 est une interface interne 10/100 qui supporte le trafic téléphonique.



Un téléphone IP Cisco est un commutateur

Le Port 1 est connecté à un commutateur ou un appareil VOIP.

Le Port 3 est connecté à un PC ou un autre appareil.

# Chapitre 2: Les VLAN

## 1. Principe du VLAN

### ❑ Configuration de VLAN statique

- Affectation manuelle des ports d'un commutateur à un VLAN via une application de gestion de VLAN ou directement en travaillant sur le commutateur
  - Les lignes directrices suivantes doivent être suivies lors de la configuration de VLAN sur des commutateurs Cisco 29xx:
    - Le nombre maximum de VLAN dépend du commutateur.
    - Le VLAN 1 est l'un des VLAN par défaut.
    - Le VLAN 1 est le VLAN Ethernet par défaut.
    - Des annonces CDP (Cisco Discovery Protocol) et VTP (VLAN Trunking Protocol) sont envoyées sur le VLAN 1. (VTP sera abordé plus tard)
    - L'adresse IP de 29xx est associée par défaut au domaine de broadcast du VLAN 1.
    - Le commutateur doit être en mode serveur VTP pour créer, ajouter ou supprimer des VLAN.
- ```
Switch#vlan numéro_vlan  
Switch(vlan)#name nom du vlan
```
- En quittant cette commande, le VLAN est appliqué au commutateur. L'étape suivante consiste à affecter le VLAN à une ou à plusieurs interfaces:

```
Switch(config)#interface fastethernet 0/9  
Switch(config-if)#switchport access vlannuméro_vlan
```

# Chapitre 2: Les VLAN

## 1. Principe du VLAN

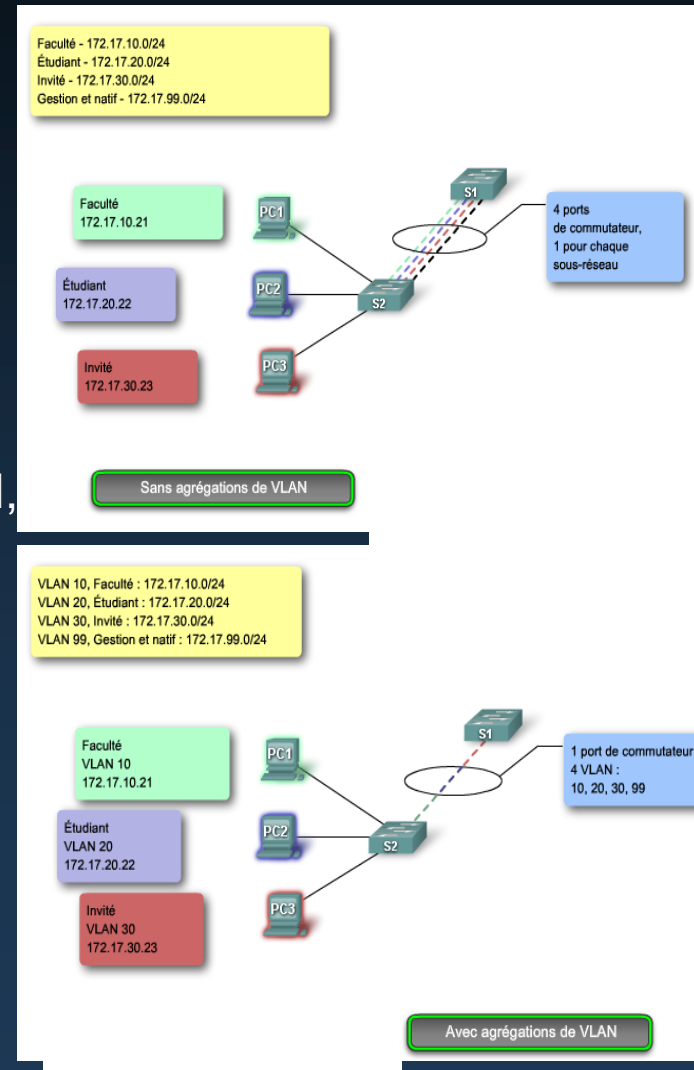
### □ Avantages d'un VLAN

- **Sécurité** : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité,
- **Réduction des coûts** : des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existante.
- **Meilleures performances** : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Atténuation des tempêtes de diffusion** : le fait de diviser un réseau en plusieurs réseaux VLAN réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion.
- **Efficacité accrue du personnel informatique** : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN.
- **Gestion simplifiée de projets ou d'applications** : La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application
  - Déplacer facilement des stations de travail sur le LAN
  - Ajouter facilement des stations de travail au LAN
  - Modifier facilement la configuration LAN

# Chapitre 2: Les VLAN

## 2. Trunking (agrégation)

- Permet à un commutateur de transmettre à un autre commutateur via un seul port, le trafic de plusieurs VLAN
- Différents trafics isolés (de différents VLAN) doivent emprunter un seul câble: plusieurs trafics logiques sur une liaison physique : un trunk.
- Afin d'identifier l'appartenance des trames aux VLAN, on utilise un système d'étiquetage (ou encapsulation) sur ce lien. Il en existe deux protocoles :
  - **ISL** (Inter Switch Link) : protocole propriétaire Cisco.
  - **802.1q** qui est un standard de l'IEEE.



# Chapitre 2: Les VLAN

## 2. Trunking (agrégation)

### ❑ Protocole ISL

- il ne peut être appliqué qu'à des commutateurs Cisco.
- la trame originelle est encapsulée entre un en-tête de 26 octets et un en-tail de 4 octets
- DA : Adresse multicast de destination
- Type : Indique le type de trame (Ethernet, Token Ring, etc.).
- Util : Indique la priorité de traitement de la trame.
- SA : Adresse MAC source.
- LEN : Longueur de la trame encapsulée moins les 18 bits des champs DA, Type, Util., SA, LEN et FCS.
- AAAA03 : Champ SNAP d'une valeur fixe 0xAAAA03.
- HSA : Contient la portion constructrice de l'adresse MAC source.
- VLAN : Identifiant de VLAN.
- BPDU : Utilisé par le Spanning Tree pour déterminer les informations topologiques.
- INDEX : Employé à des fins diagnostiques uniquement.
- RES : Utilisé quand une trame Token Ring ou FDDI est encapsulée dans une trame ISL.

**Trame ISL**

| En-tête ISL | Trame Ethernet encapsulée | FCS      |
|-------------|---------------------------|----------|
| 26 octets   |                           | 4 octets |

**Composition de l'en-tête ISL**

| DA      | Type   | Util.  | SA      | LEN     | AAAA03  | HSA     | VLAN    | BPDU  | INDEX   | RES     |
|---------|--------|--------|---------|---------|---------|---------|---------|-------|---------|---------|
| 40 bits | 4 bits | 4 bits | 48 bits | 16 bits | 24 bits | 24 bits | 16 bits | 1 bit | 16 bits | 16 bits |

# Chapitre 2: Les VLAN

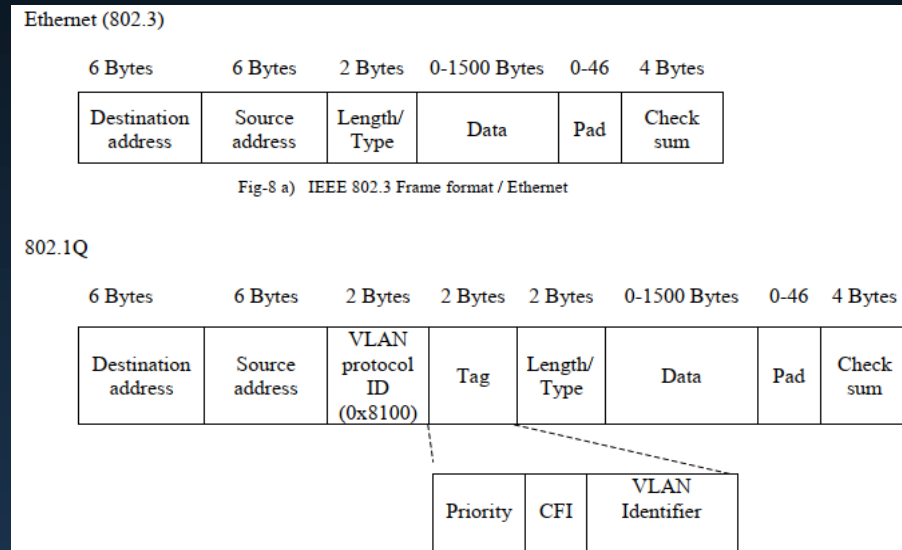
## 2. Trunking (agrégation)

### ❑ Protocole 802.1q

- lorsque les trames Ethernet sont placées sur une agrégation, elles ont besoin d'informations supplémentaires sur les VLAN auxquels elles appartiennent.
- Il faut alors utiliser l'en-tête d'encapsulation 802.1Q.

### ❑ Commandes associées

- switchport mode trunk
  - o Depuis le mode de configuration spécifique du port, active le trunking.
- switchport trunk [allowed | encapsulation | native | pruning]
  - o Quand l'interface est en mode trunking permet respectivement, de spécifier le type de caractéristiques VLAN, le type d'encapsulation (ISL, 802.1q), les caractéristiques natives et les caractéristiques de pruning des VLANs.
- show port capabilities [numéro/sous-numéro]
  - o Affiche les fonctionnalités supportées par l'interface.
- show trunk :
  - o Permet de vérifier la configuration du trunking.





# Chapitre 2: Les VLAN

## 2. Trunking (agrégation)

### □ DTP (Dynamic trunking protocol)

- Le mode d'agrégation définit la manière dont le port local négocie à l'aide de DTP pour configurer une liaison agrégée (trunk) avec son port homologue (distant).

#### 1- Mode Actif (par défaut)

- Le port de commutation envoie régulièrement des trames DTP (annonces), au port distant.
- La commande utilisée est la suivante : **switchport mode trunk**.
- Le port de commutateur local annonce au port distant qu'il passe dynamiquement à l'état d'agrégation. Ensuite, quelles que soient les informations DTP envoyées par le port distant en réponse à l'annonce, le port local passe à l'état d'agrégation.
- Il est dans un état d'agrégation inconditionnel (toujours actif).

#### 2- Mode dynamique automatique

- Le port de commutation envoie régulièrement des trames DTP au port distant.
- La commande utilisée est la suivante : **switchport mode dynamic auto**.
- Le port de commutateur local annonce au port de commutateur distant qu'il est en mesure d'effectuer l'agrégation, mais ne demande pas à passer à l'état d'agrégation.
- Après une négociation DTP, le port local ne passe à l'état d'agrégation que si le mode d'agrégation du port distant a été défini comme actif ou souhaitable.



# Chapitre 2: Les VLAN

## 2. Trunking (agrégation)

### □ DTP (Dynamic trunking protocol)

#### 3- Mode dynamique souhaitable

- Des trames DTP sont envoyées régulièrement au port distant.
- La commande utilisée est la suivante : `switchport mode dynamic desirable`.
- Le port de commutateur local annonce au port de commutateur distant qu'il est en mesure d'effectuer l'agrégation et lui demande de passer à l'état d'agrégation.
- Si le port local détecte que le port distant a été configuré en mode actif, souhaitable ou automatique, il passe à l'état d'agrégation. Si le port de commutateur distant est en mode de non-négociation, le port local reste un port de non-agrégation.

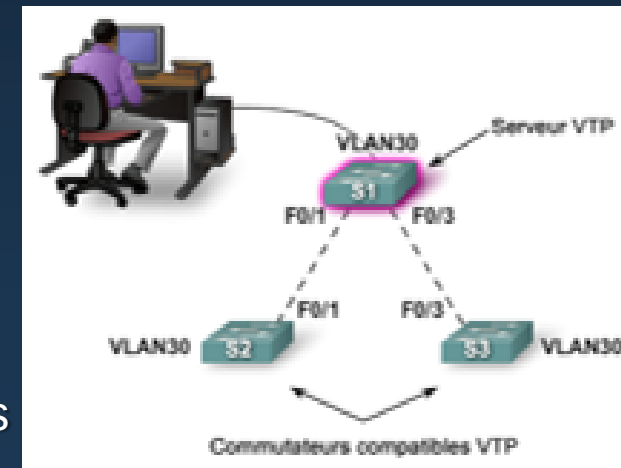
#### Désactiver le DTP

- Désactiver le protocole DTP pour l'agrégation afin que le port local n'envoie pas de trames DTP au port distant.
- Utilisez la commande `switchport nonegotiate`.
- Le port local est alors considéré comme étant dans un état d'agrégation inconditionnel

# Chapitre 2: Les VLAN

## 3. VTP (Virtual Trunking Protocol)

- Protocole propriétaire CISCO
- Permet aux commutateurs et aux routeurs d'échanger des informations de configuration des VLAN
- Diffuse ses mises à jour (maj) dans le domaine VTP toutes les 5mn ou quand une modification à eu lieu
- Les mises à jour comportent :
  - Un numéro de révision qui s'incrémente à chaque nouvelle diffusion: Commutateur sont à jour
  - Le nom et numéro de VLAN
- On distingue trois modes de fonctionnement :
  1. VTP serveur
  2. VTP client
  3. VTP transparent
- Commutateur configuré en VTP serveur: crée, modifie, supprime les VLAN et envoie à serveurs ou clients
- Commutateur configuré en VTP client : reçoit les maj de configuration, ne modifie pas les VLAN
- Commutateur configuré en VTP transparent: ne tient pas compte des maj. Configure que leurs propres VLAN Transmettent aux autres commutateurs les maj reçues



# Chapitre 2: Les VLAN

## 3. VTP (Virtual Trunking Protocol)

- Les commutateurs en mode VTP serveur et client font la maj de leur base de données VLAN quand ils reçoivent maj VTP domaine où le numéro de révision est supérieur à celui déjà présent dans leur base
- Le VTP minimise les problèmes provoqués par des configurations incorrectes ou incohérentes.
- Le VTP pruning empêche la propagation des trafics de broadcast aux commutateurs qui ne sont pas concernés.

### ❑ Commandes associées

- `ntp domain nom de domaine { password mot de passe | pruning | v2-mode | {server | client | transparent}}`
  - o Mode de configuration de VLAN
  - o Spécifie les paramètres VTP.
- `show ntp status`
  - o Mode privilégié
  - o Affiche la configuration VTP et le statut du processus.

| Fonction                                                   | Mode Serveur | Mode Client | Mode Transparent |
|------------------------------------------------------------|--------------|-------------|------------------|
| Envoi de messages VTP                                      | OUI          | NON         | NON              |
| Réception des messages VTP ;<br>Synchronisation VLAN       | OUI          | OUI         | NON              |
| Transmission des messages VTP reçus                        | OUI          | OUI         | OUI              |
| Sauvegarde de configuration VLAN<br>(en NVRAM ou Flash)    | OUI          | NON         | OUI              |
| Edition des VLANs<br>(création, modification, suppression) | OUI          | NON         | OUI              |

# Chapitre 2: Les VLAN

## 4. Routage inter-VLAN

- Le routage inter-VLAN est le processus de router l'information entre VLANs.
- Le routage inter-VLAN nécessite un routeur ou un commutateur de niveau 3.
- Le routage inter-VLAN traditionnel :  
Le routeur doit posséder plusieurs interfaces et chaque interface est connectée à un VLAN différent.
- Le routage router on a stick :  
Utilise des sous-interfaces pour se connecter à un commutateur de niveau 2.  
Chaque sous-interface doit être configuré avec :
  - une adresse IP
  - un numéro de VLAN
- Configuration du routage inter-VLAN
  - Configurer les ports du commutateur reliés au routeur au bon VLAN.
  - Configurer chaque sous-interface du routeur à une adresse du réseau du VLAN et au numéro du VLAN correspondant.
- Toujours vérifier la configuration sur le routeur ET sur le commutateur,

# Chapitre 2: Les VLAN

## 4. Routage inter-VLAN

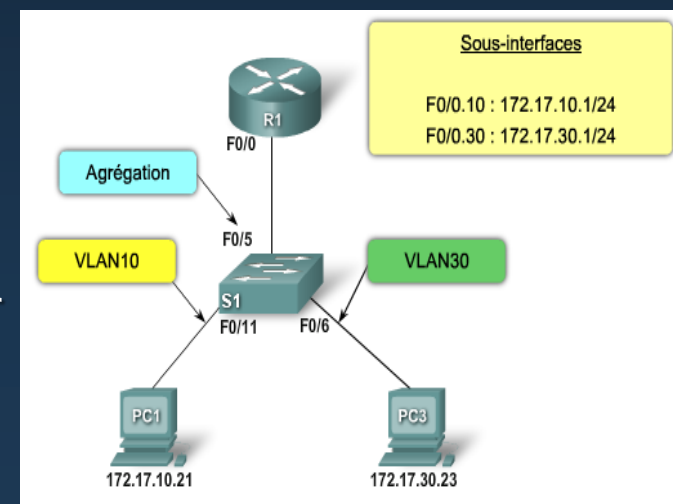
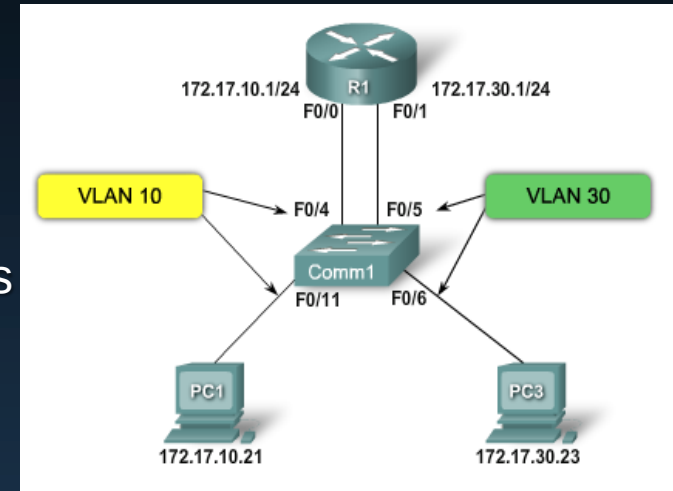
### 1- Routage traditionnel entre VLAN

Connecter différentes interfaces de routeur physique à différents ports de commutateur physiques. Chaque interface de routeur peut alors accepter le trafic du VLAN associé à l'interface de commutateur à laquelle elle est connectée, et le trafic peut être acheminé vers les autres VLAN connectés aux autres interfaces.

### 2- Routage router on a stick

une seule interface physique achemine le trafic entre plusieurs VLAN d'un réseau. Comme vous pouvez le voir dans la figure, le routeur est connecté au commutateur Comm1 à l'aide d'une seule connexion réseau physique.

L'interface de routeur est configurée pour fonctionner comme **liaison agrégée** et est connectée à un port de commutateur configuré en mode d'agrégation. Le routeur effectue le routage entre VLAN en acceptant le trafic étiqueté VLAN sur l'interface agrégée provenant du commutateur adjacent et en effectuant le routage en interne entre les VLAN à l'aide de **sous-interfaces**.



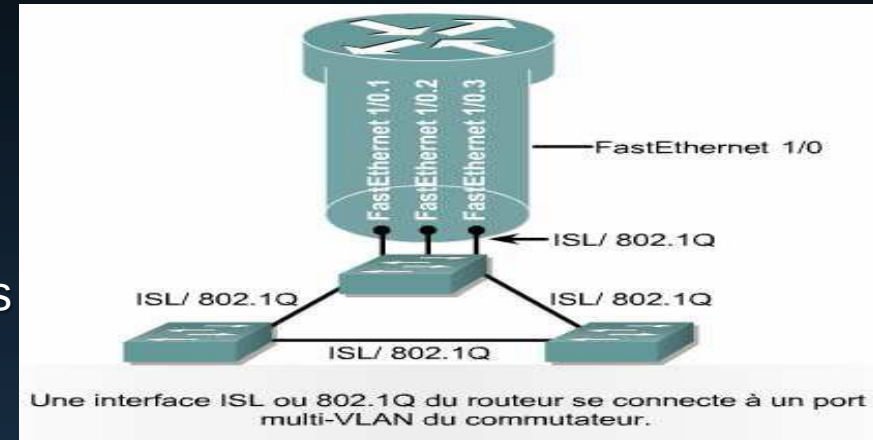
# Chapitre 2: Les VLAN

## 4. Routage inter-VLAN

La norme IEEE 802.1Q est utilisée pour réunir des VLAN en une agrégation sur des liaisons Fast Ethernet.

Le routeur peut prendre en charge de nombreuses interfaces logiques sur des liaisons physiques individuelles.

Par exemple, l'interface Fast Ethernet 1/0 pourrait supporter trois interfaces virtuelles s'appelant FastEthernet 1/0.1, 1/0.2 et 1/0.3. Chaque sous-interface prend en charge un VLAN et dispose d'une adresse IP affectée. Pour que plusieurs unités d'un même VLAN communiquent, les adresses IP de toutes les sous-interfaces maillées doivent être *sur le même réseau ou sous-réseau*.



| Interface physique                               | Sous-interface                                        |
|--------------------------------------------------|-------------------------------------------------------|
| Une interface physique par VLAN                  | Une interface physique pour de nombreux VLAN          |
| Aucun conflit de bande passante                  | Conflit de bande passante                             |
| Connectée au port de commutateur en mode d'accès | Connectée au port de commutateur en mode d'agrégation |
| Plus coûteuse                                    | Moins coûteuse                                        |
| Configuration de connexion plus complexe         | Configuration de connexion moins complexe             |



# Chapitre 2: Les VLAN

## 4. Routage inter-VLAN

### □ Interface ou sous-interface

#### Limite de quantité de port

Les sous-interfaces permettent au routeur d'accommoder plus de VLANs que le nombre d'interfaces physiques disponible.

#### Performance

Avec des interfaces, toute la bande passante est allouée au VLAN.

Avec les sous-interfaces, le trafic de chacun des VLANs doit compétitionner pour la bande passante : goulot d'étranglement.

#### Access Ports et Trunk Ports

Interface, les ports du commutateur sont configurés en port d'accès "access ports".

Sous-interface, le port du commutateur est configuré en agrégation "trunk".

#### Coût

Un routeur possédant plusieurs interfaces est plus dispendieux.

Chaque interface est connectée à un port différent sur le commutateur, donc le commutateur utilise plus de ports.

#### Complexité

Sous-interface, moins complexe physiquement, mais plus complexe au niveau de la programmation.



# Chapitre 2: Les VLAN

## Dépannage des VLAN

