Chapitre 2:

Les VLAN (Virtual LAN)

Plan du chapitre

1. Principe du VLAN
2. Trunking
3. VTP
4. DTP
5. Routage inter-VLAN

Chapitre 2: Les VLAN

1. Principe du VLAN

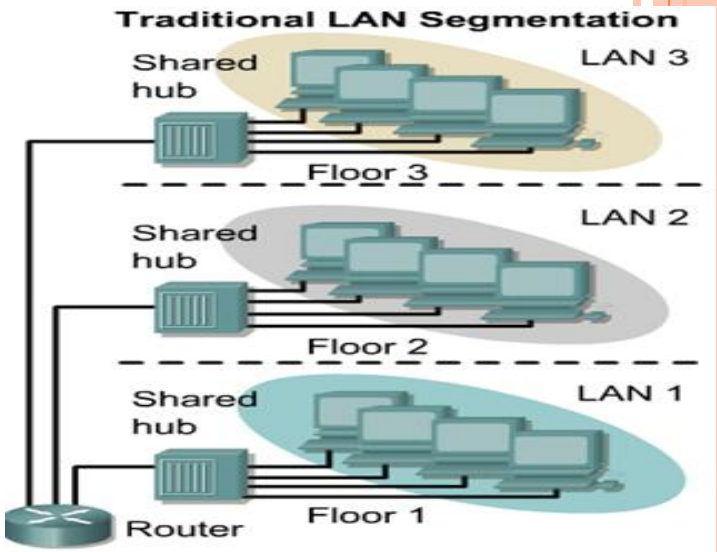
❑ Commutation classique:

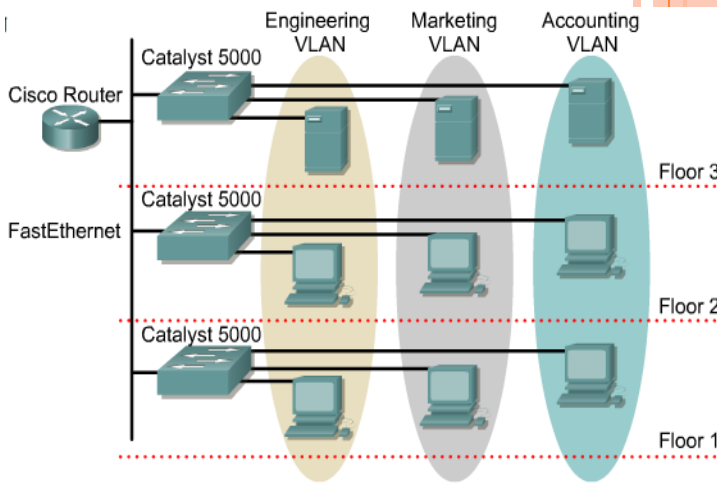
- Pour communiquer entre les LAN, chaque segment doit avoir un port séparé

❑ Commutation avec VLAN :

- Ils segmentent de façon logique les réseaux sur les fonctions, équipes de travail ou des applications.
- 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

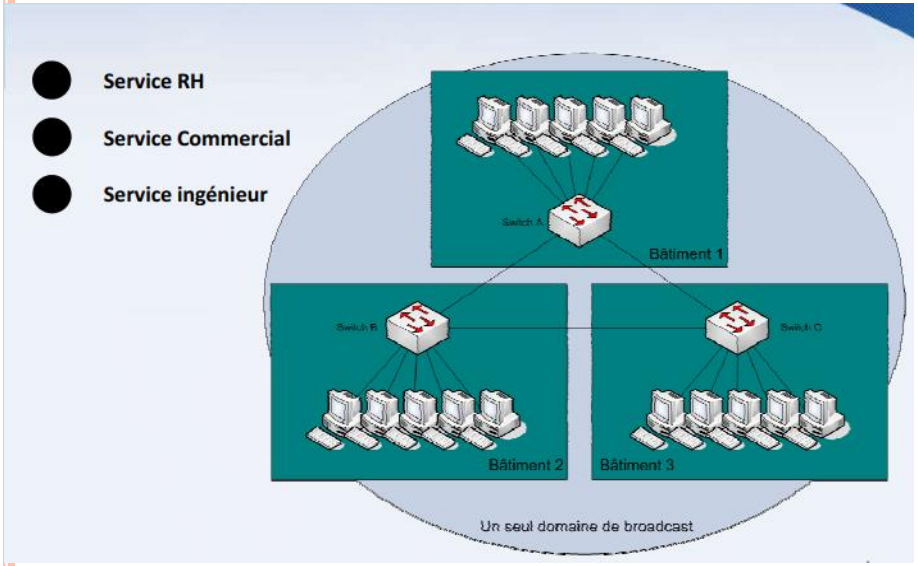
Avec des VLAN, les machines d'un même sous réseau ne sont plus regroupées de manière physique (connectées au même switch), mais de manière logique.

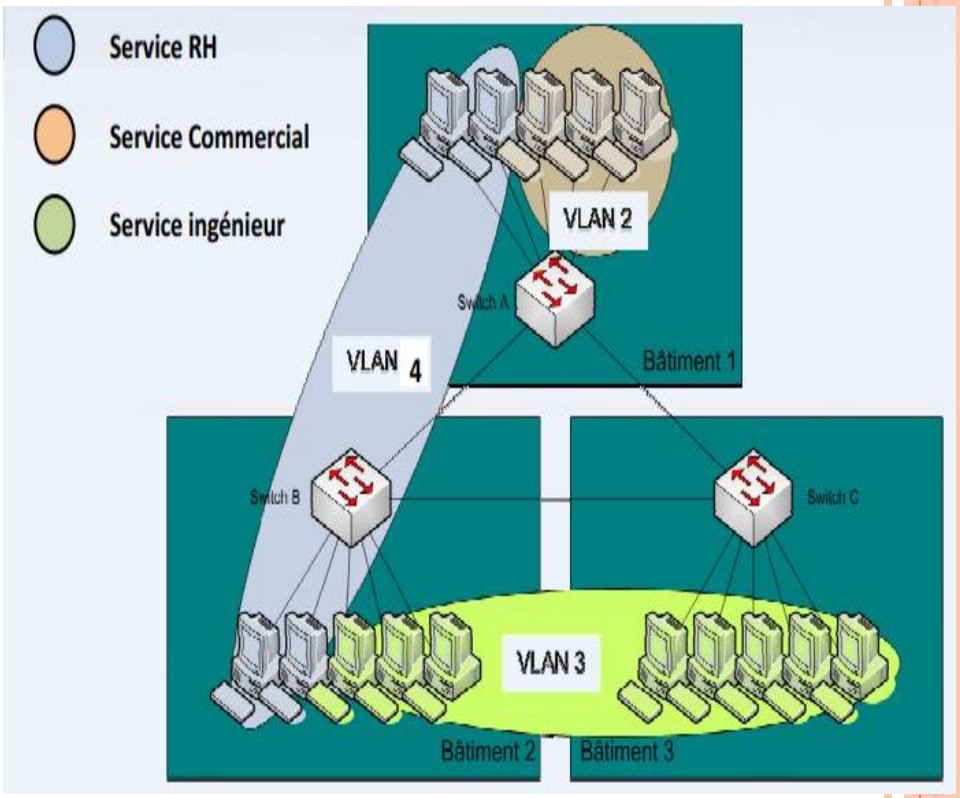


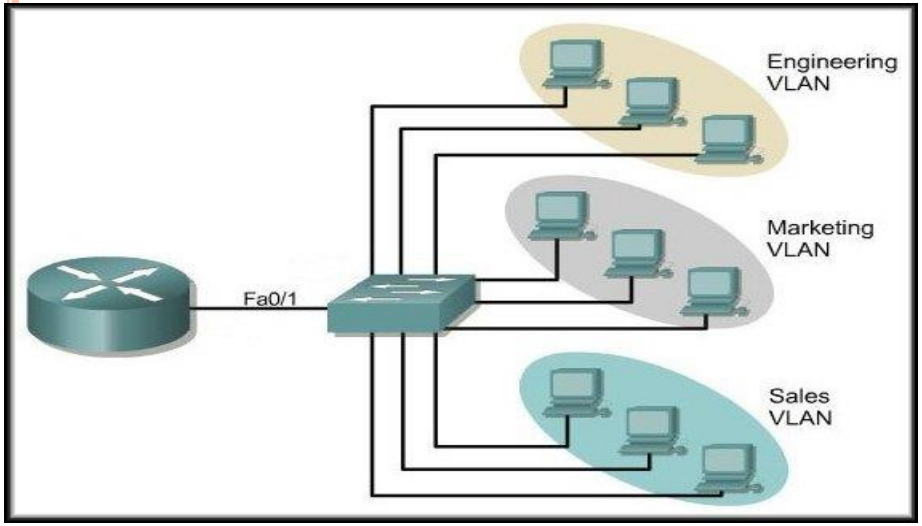


Chapitre 2: Les VLAN

1. Principe du VLAN







Diminuer le domaine de Broadcast

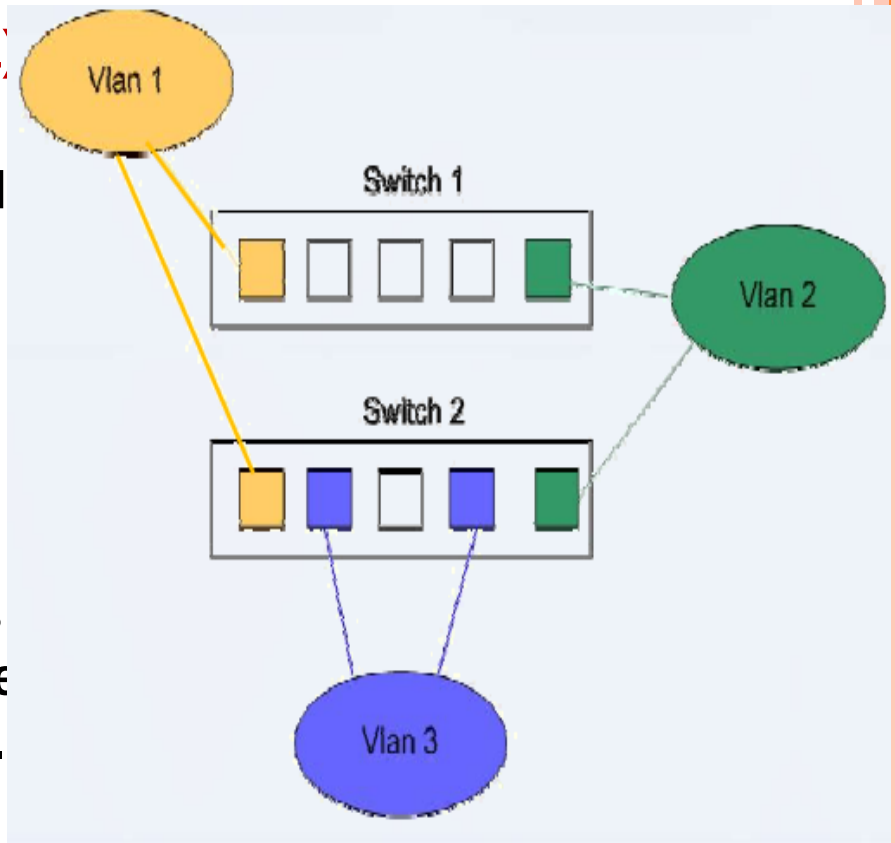
1 domaine de Broadcast par VLAN

Chapitre 2: Les VLAN

1. Principe du VLAN

❑ Niveaux de VLAN

➢ **Les Vlan par port (Vlan de niveau 1) :**



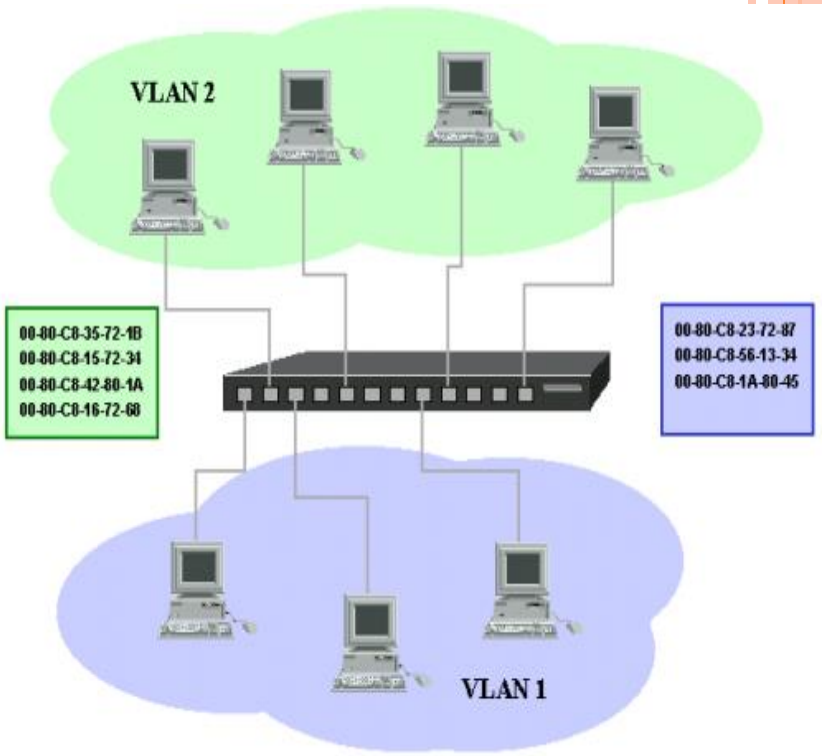
- **C'est le port qui détermine le VLAN auquel appartient les stations associées**
- **90% des VLAN sont des VLAN par port**
- **La configuration est statique**
- **C'est le plus sécurisé. Les stations qui lui sont raccordées à un port ne peut appartenir qu'à un seul VLAN.**
- **Manquent de souplesse: tout déplacement d'une station nécessite une reconfiguration des ports.**

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). La commutation, s'effectuant au niveau MAC, autorise un faible temps de latence**
- **Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.**

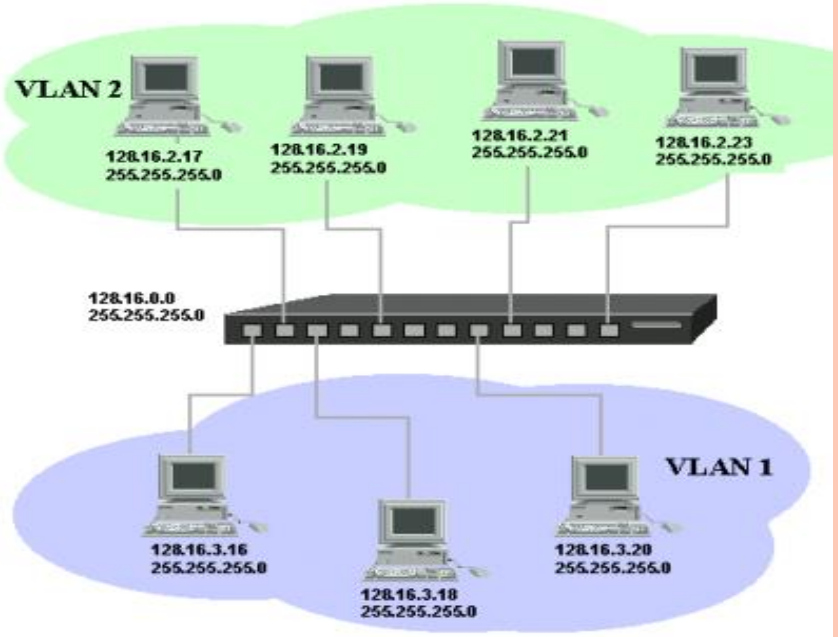
Chapitre 2: Les VLAN

1. Principe du VLAN

❑ Niveaux de VLAN

➢ **Les Vlan de niveau 3**

- **Le VLAN par sous-réseau (*Network Address-Based VLAN*) : Permet de regrouper les machines suivant le sous réseau auquel elles appartiennent „.**
  Solution souple car la configuration des commutateurs se modifient 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.**
- **Un pirate peut assez facilement déterminer l'adresse IP ou le protocole utilisé par un utilisateur pour l'usurper son identité.**
- **Nécessite un Switch de niveau 3 (relativement chère)**

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.**
- **Le VLAN par défaut des commutateurs Cisco est le VLAN 1 : Ethernet**
- **On ne peut ni le renommer, ni le supprimer.**

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 »),

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 (bande passante consolidée,priorité de transmission, possibilité de routage autour des zones encombrées du réseau ; délai inférieur à 150 millisecondes (ms))

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.**
  - **Le protocole VTP ne prend pas en compte les VLAN à plage étendue.**

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

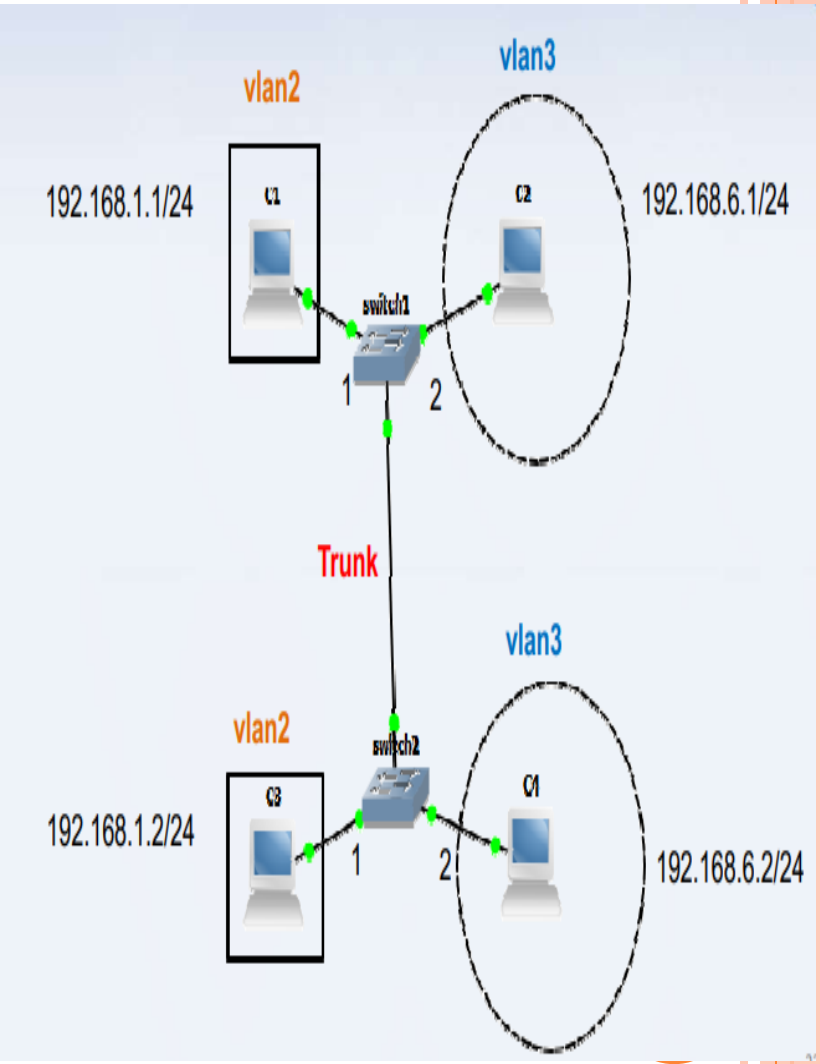
Chapitre 2: Les VLAN

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.**
- **Un Trunk n'appartient pas à un réseau local virtuel spécifique; c'est plutôt un conduit pour plusieurs VLAN.**
- **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 :

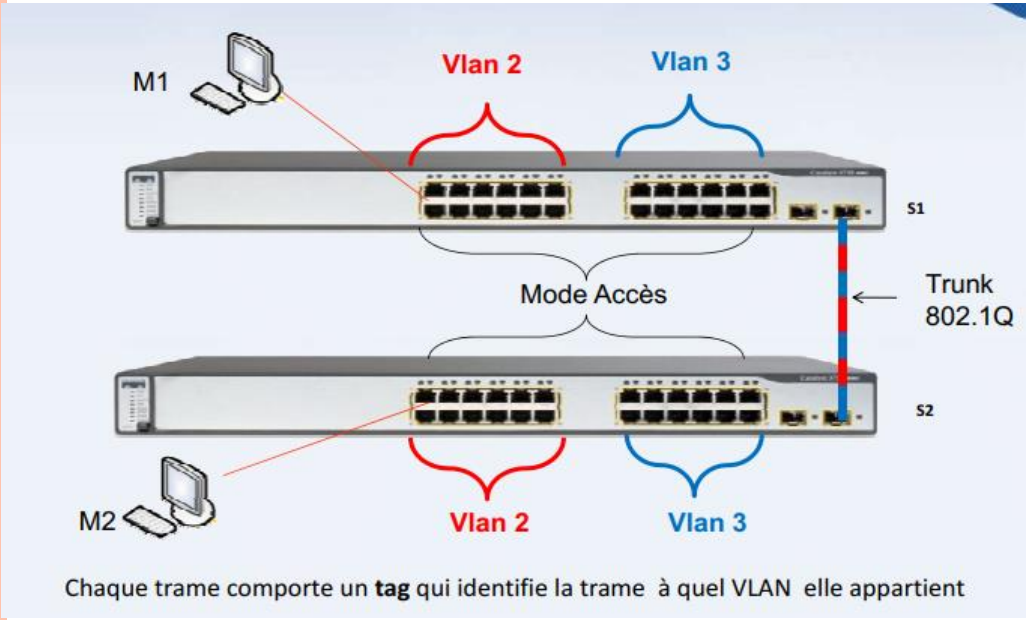
- **ISL (Inter Switch Link) : protocole propriétaire Cisco.**
- **802.1q qui est un standard de l'IEEE.**



Chapitre 2: Les VLAN

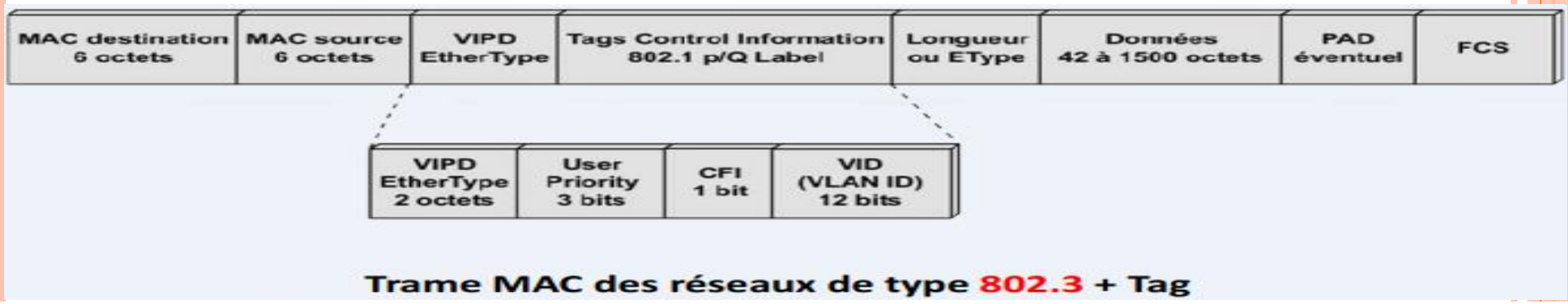
2. Trunking (agrégation)

❑ Protocole 802.1q



Chaque trame comporte un **tag** qui identifie la trame à quel VLAN elle appartient

- La norme 802.1Q introduisent quatre octets supplémentaires dans la trame MAC. Ils permettent d'identifier les VLAN (*VLAN tagging*) et de gérer les niveaux de priorité (*QoS*).

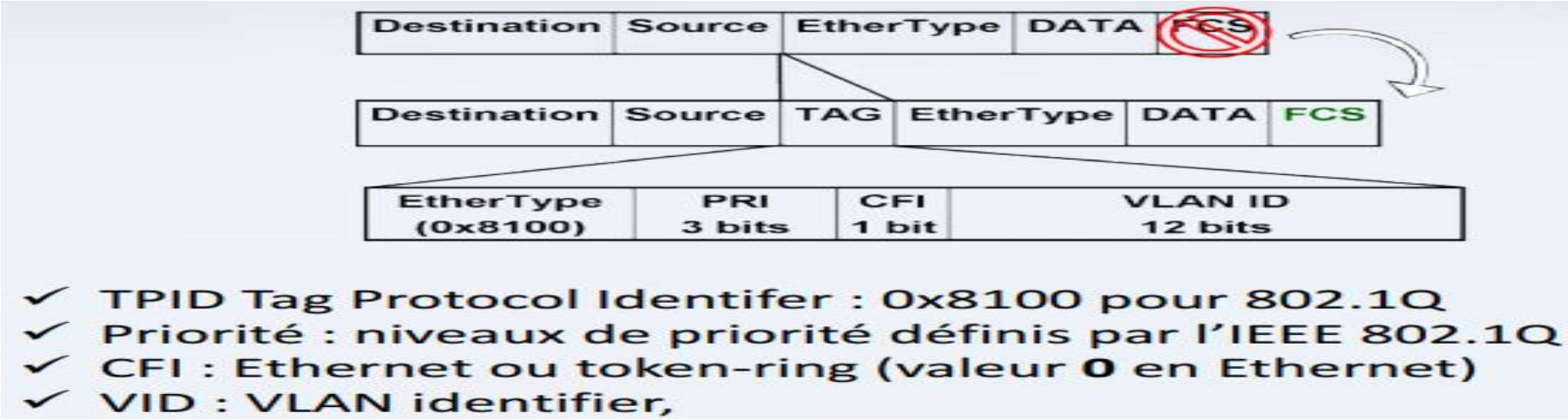


Trame MAC des réseaux de type 802.3 + Tag

Chapitre 2: Les VLAN

2. Trunking (agrégation)

❑ Protocole 802.1q



- ✓ TPID Tag Protocol Identifer : 0x8100 pour 802.1Q
- ✓ Priorité : niveaux de priorité définis par l'IEEE 802.1Q
- ✓ CFI : Ethernet ou token-ring (valeur **0** en Ethernet)
- ✓ VID : VLAN identifier,

❑ Commandes associées

 # switchport mode trunk

o Depuis le mode de configuration spécifique du port, active le trunking.

 # show trunk :

o Permet de vérifier la configuration du trunking.

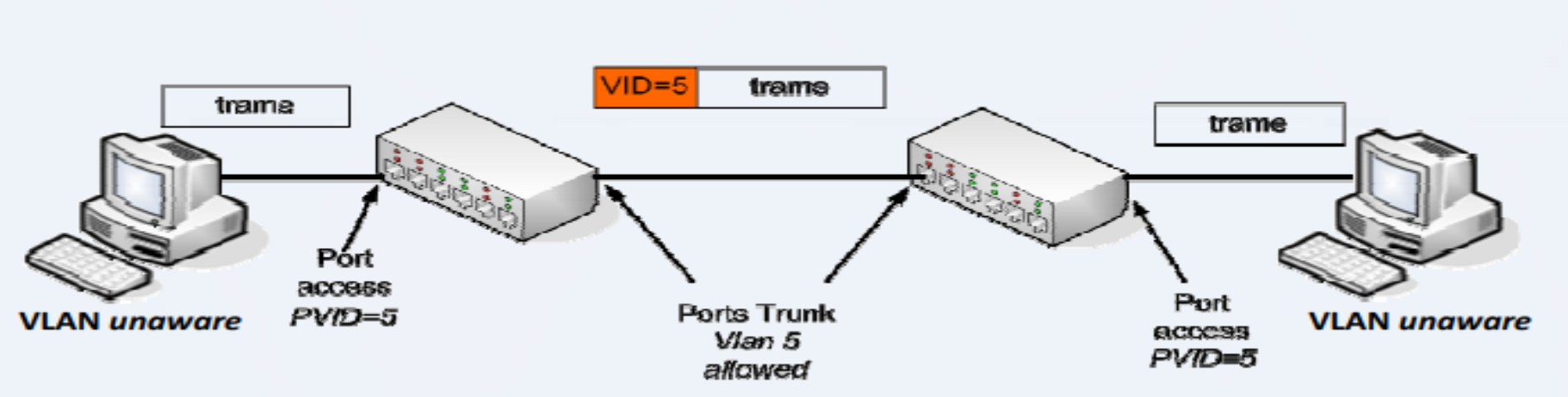
Chapitre 2: Les VLAN

2. Trunking (agrégation)

❑ Types de ports

Les deux types de ports possibles au sein d'un environnement VLAN sont les ports d'accès et les ports de liaison.

- **Ports d'accès** (untagged) :
  Par lesquels une trame entre et ressort d'un réseau VLAN.
  Lorsqu'un port d'accès reçoit une trame, celle-ci ne comporte pas d'étiquette VLAN……
- **Ports de liaison** Port trunk ou tagged (étiqueté):
  La différence entre les ports d'accès et de liaison est que les ports de liaison ne retirent pas l'étiquette VLAN de la trame lorsqu'ils l'envoient.



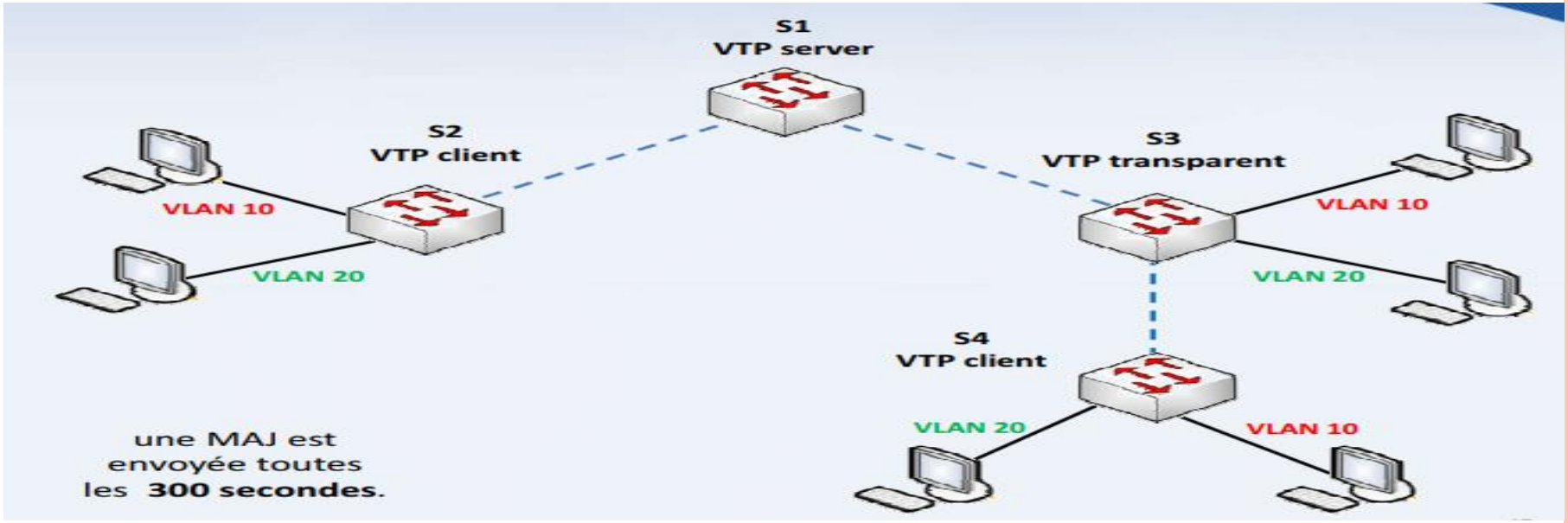
Chapitre 2: Les VLAN

3. VTP(VLAN Trunking Protocol)

- Il sert à la propagation de **création/suppression/modification** de VLAN sur tous les Switchs d'un réseau à partir d'un seul Switch (serveur).
- C'est un protocole propriétaire Cisco. De part sa simplicité et sa puissance, l'IEEE a sorti un protocole similaire afin de permettre cette fonctionnalité entre Switchs de constructeurs différents: GVRP (GARP *VLAN Registration Protocol*). La norme est IEEE 802.1ak…..
- Le Switch possède 3 modes VTP: client, transparent ou server
  - VTP Server: Switch qui crée les annonces VTP
  - VTP Client: Switch qui reçoit, se synchronise et propage les annonces VTP
  - VTP Transparent: Switch qui ne traite pas les annonces VTP, Ils permet à l'administrateur de faire toute modification sur les VLANs en **local uniquement**
- Les Swtichs doivent avoir un même nom de domaine VTP, pour qu'ils s'échangent des MAJ. De plus, il est possible de configurer un mot de passe pour le domaine……
- Le VTP minimise les problèmes provoqués par des configurations incorrectes ou incohérentes

Chapitre 2: Les VLAN

3. VTP(VLAN Trunking Protocol)



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

Chapitre 2: Les VLAN

4. DTP (Dynamic trunking protocol)

La configuration des Trunk sur tous les liens inter-switchs de l'entreprise peut être très fatiguant . Cisco a créé un protocole qui va monter automatiquement un Trunk entre 2 switchs, c'est le protocole DTP.
Le principe est très simple, lorsqu'un port monte, des annonces DTP sont envoyées;

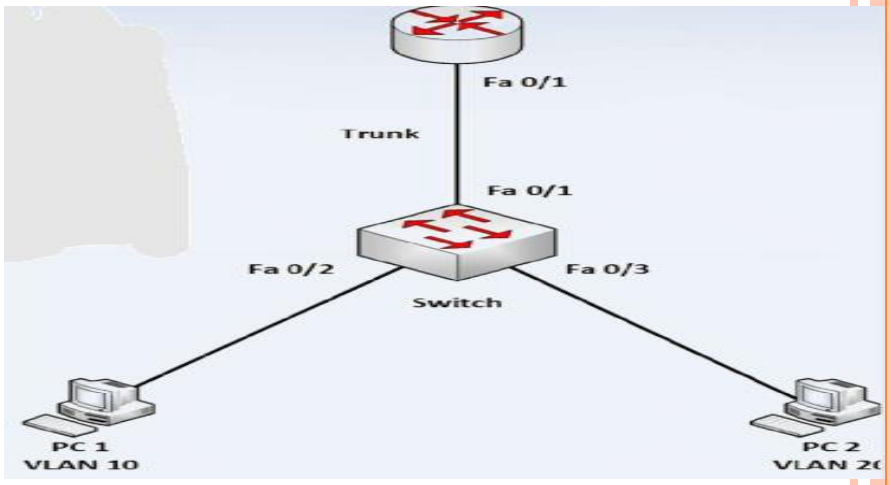
- **Si le port est connecté à un switch voisin, ce dernier va recevoir l'annonce**
- **Si le port est connecté à un pc, ce dernier ne répondra pas à l'annonce car il comprend pas le protocole. Sur le port du switch, le Trunk n'est pas activé et donc reste en mode Access**

Chapitre 2: Les VLAN

5. Routage inter-VLAN

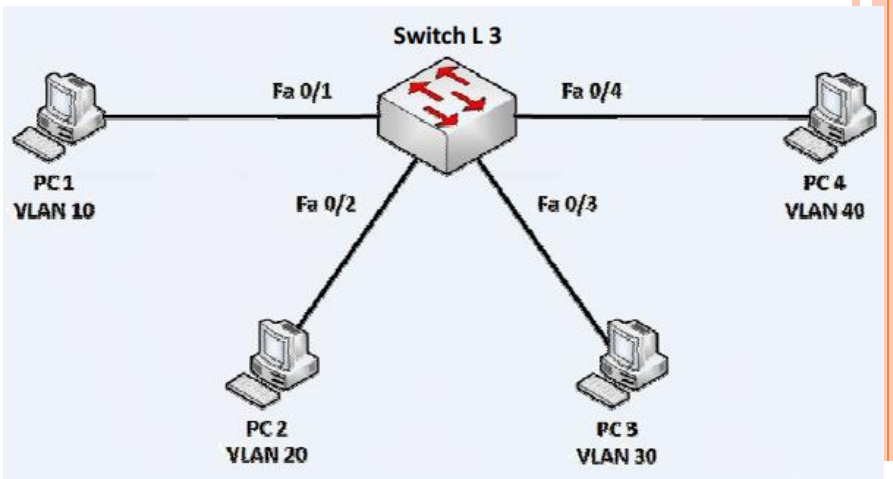
- Un VLAN = un sous réseau
- Plusieurs VLAN, donc plusieurs sous réseaux, sur un même switch
- Un même VLAN sur plusieurs switchs
- Un routeur constitue la limite

d'un VLAN comme celle d'un LAN.
En conséquence, pour
que des VLANs communiquent
ensemble, une fonction de
routage est nécessaire. On
parle de "routage inter-VLAN".



- Peut être remplie par des

Commutateurs de niveau 3,
(*Multilayer switches*). Ils sont
capables de transférer du trafic de
VLANs différents à partir d'un port
connu comme port d'agrégation VLAN.

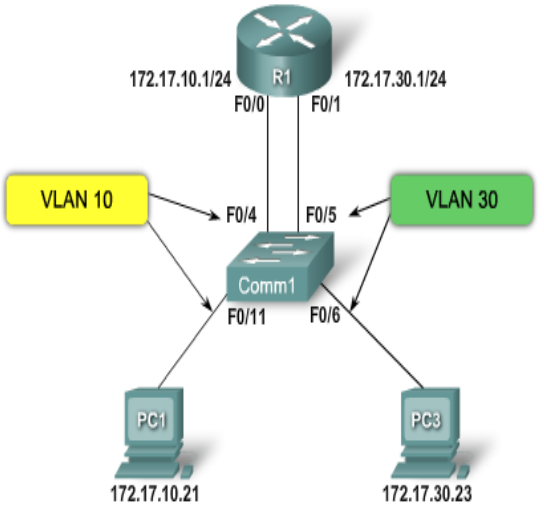


Chapitre 2: Les VLAN

5. Routage inter-VLAN

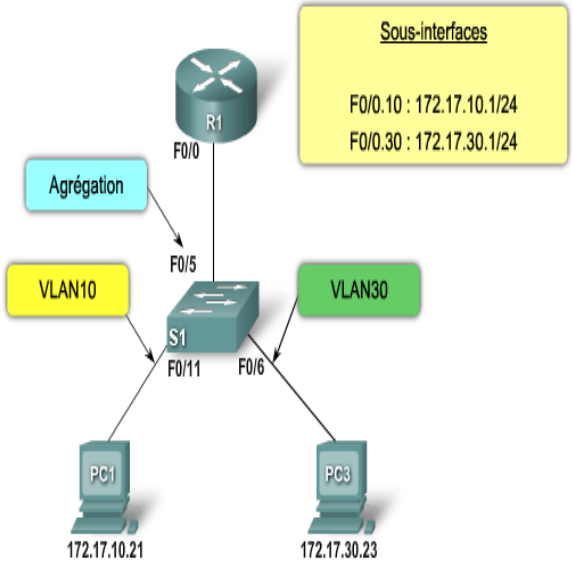
1- Routage traditionnel entre VLAN

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. 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

5. Routage inter-VLAN

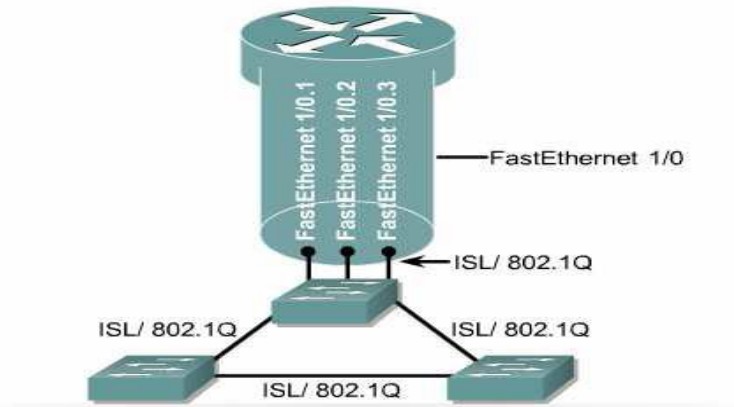
La norme IEEE 802.1Q est utilisée pour réunir des VLAN en une agrégation sur des liaisons Fast Ethernet.

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*.



Une interface ISL ou 802.1Q du routeur se connecte à un port multi-VLAN du commutateur.

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

5. 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