



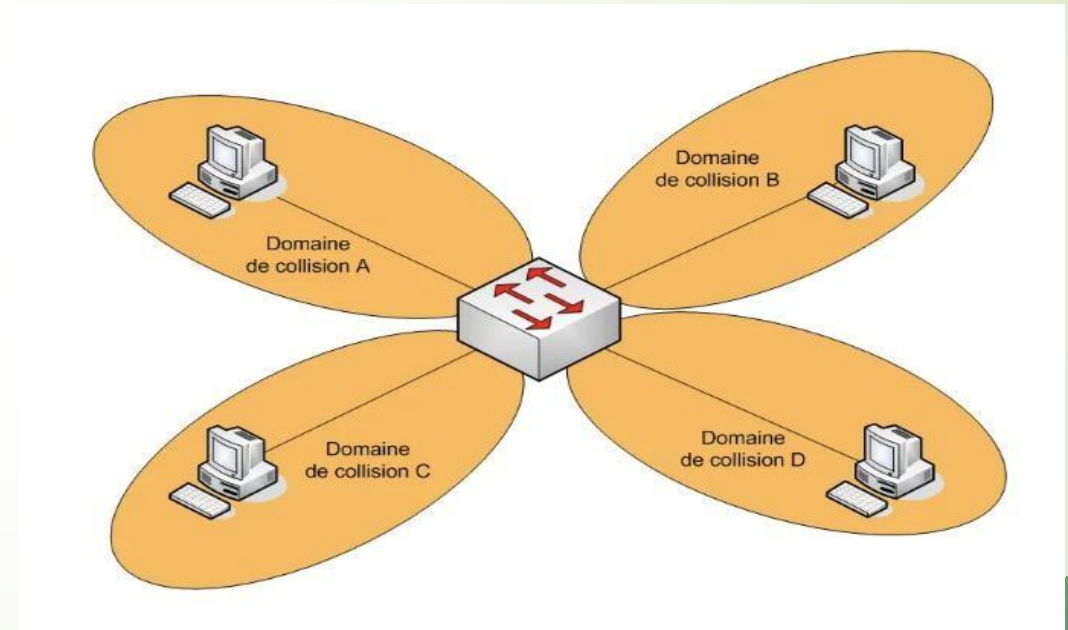
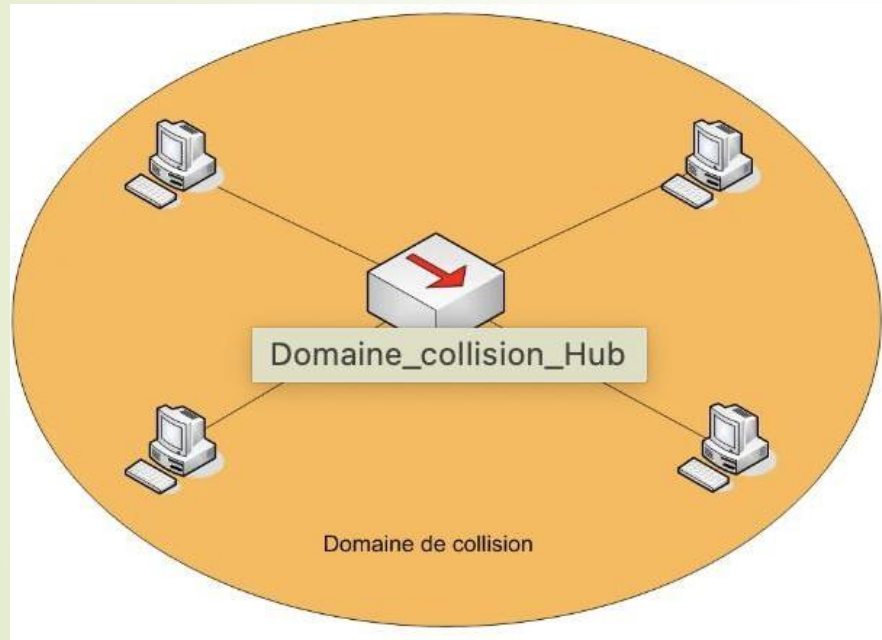
Institut Supérieur du Numérique

Réseaux locaux virtuels (VLAN)

Année universitaire 2024-2025

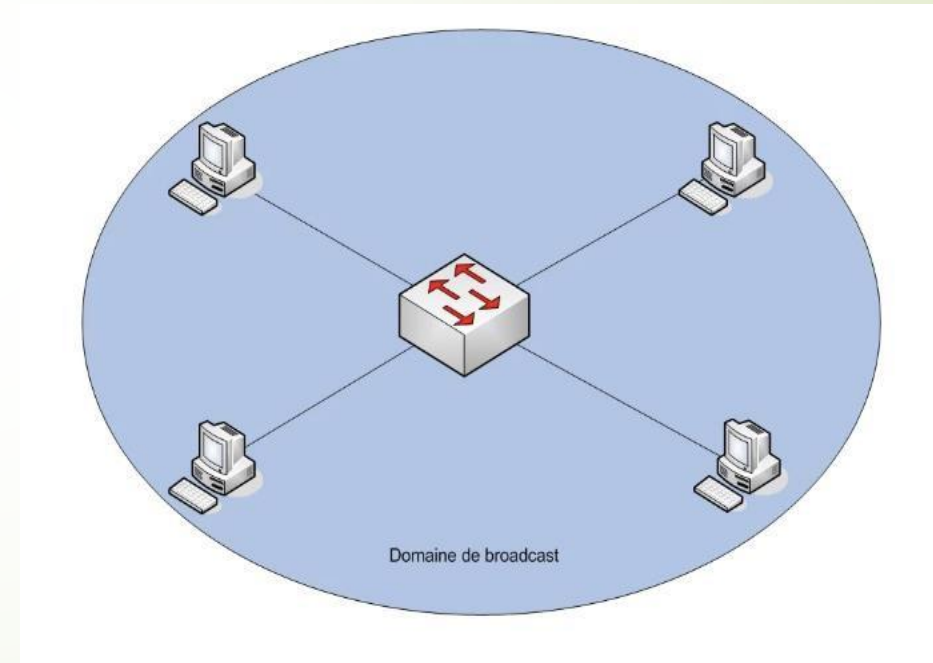
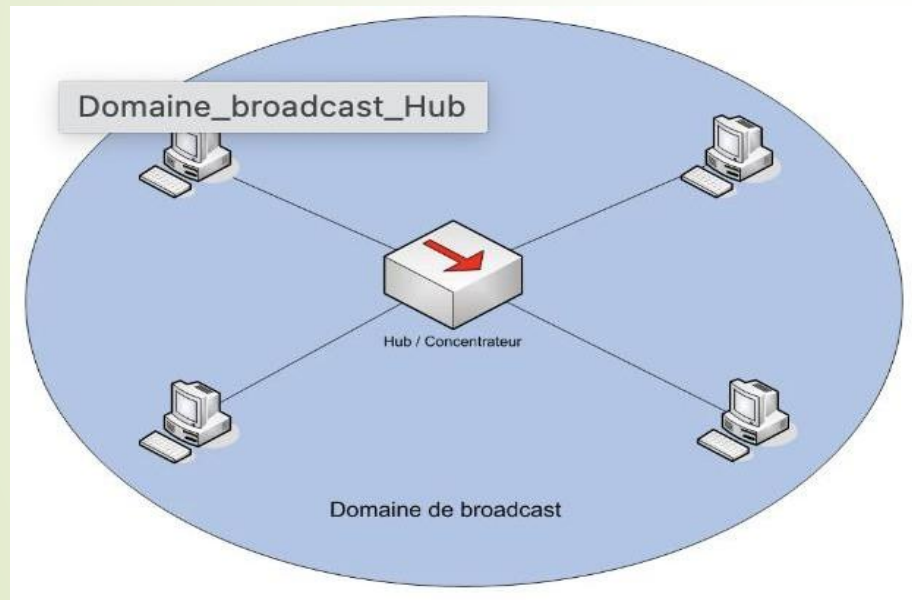
Domaine de Collision

- ❑ Une collision est quand deux paquets sont émis en même temps sur un segment de réseau.
- ❑ La congestion du réseau (ou augmentation du trafic) arrive quand le réseau est très fortement ralenti.



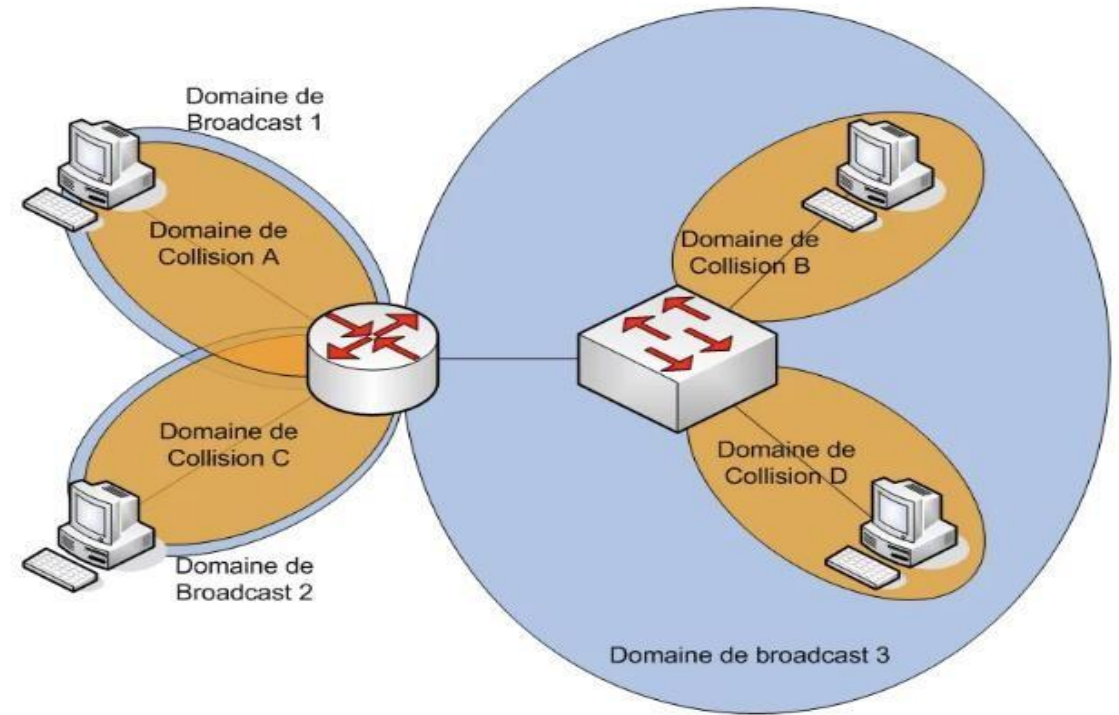
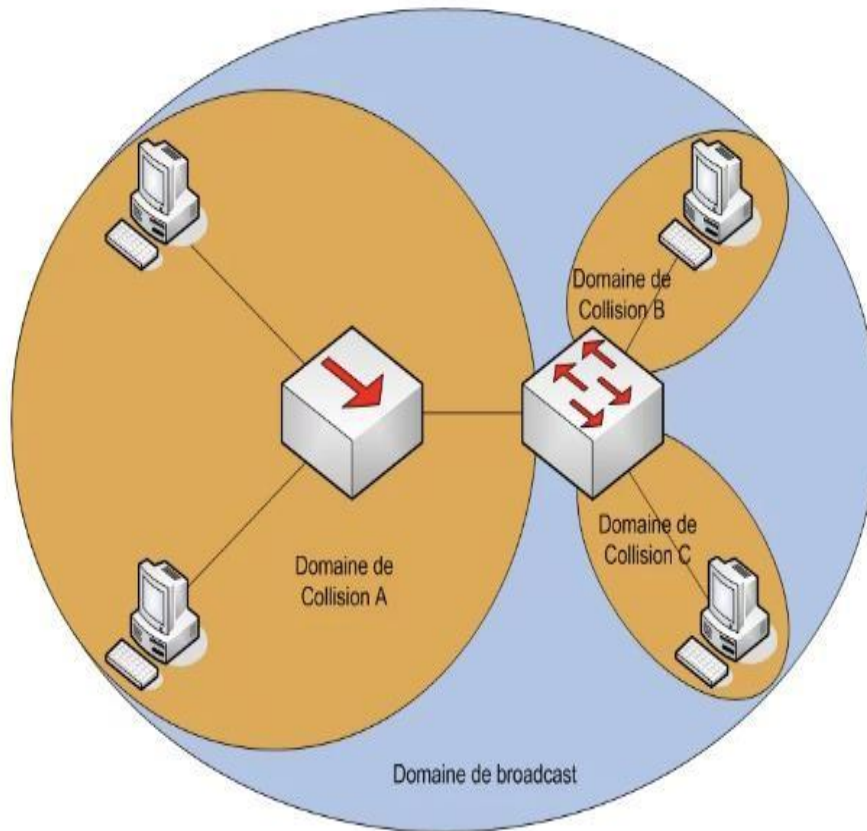
Domaine de Diffusion

- Diffusion : lorsqu'un appareil émetteur envoie un message en diffusion, tous les participants du domaine reçoivent cette transmission.



Domaine de Collision et Domaine de Diffusion

Avec la **présence d'un routeur**, la notion de domaine de broadcast **explose** et on a un domaine de broadcast par interface du routeur.



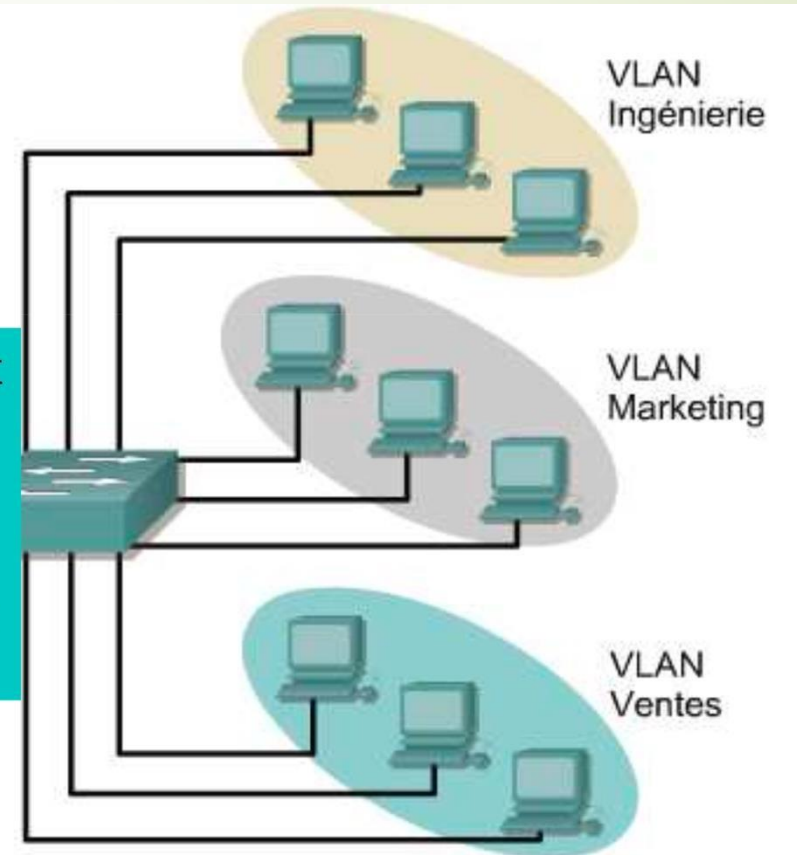
Les VLANs

- ❑ Les VLANs agissent au niveau 2 du modèle OSI ;
- ❑ Ils permettent la segmentation d'un support physique en segments logiques ;
- ❑ Les VLANs permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application, quel que soit l'emplacement physique de l'utilisateur ou du périphérique.
- ❑ Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique qui prend en charge le routage.
- ❑ Les VLANs améliorent les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits.

Organisation Réseau avec VLAN

Les VLANs segmentent les réseaux commutés de manière logique :

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



Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement

Les avantages des VLANs

Les principaux avantages des VLAN sont les suivants :

- ❑ **Sécurité** : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité. Comme l'illustre la figure, les ordinateurs du personnel enseignant se trouvent sur le VLAN 10 et sont complètement séparés du trafic des données des étudiants et des invités.
- ❑ **Réduction des coûts** : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons montantes existantes.
- ❑ **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.
- ❑ **Réduction des domaines de diffusion** :- la division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion. Comme l'illustre la figure, il y a six ordinateurs dans ce réseau, mais seulement trois domaines de diffusion : Personnel, Étudiant et Invité.

Les avantages des VLAN

- ❑ **Efficacité accrue du personnel informatique** : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié. Dans la figure, pour qu'ils puissent être facilement identifiables, le VLAN 10 a été nommé « Personnel », le VLAN 20, « Étudiant » et le VLAN 30, « Invité ».
- ❑ **Gestion simplifiée de projets et d'applications** : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée. Une plate-forme de développement d'e-learning pour le personnel enseignant est un exemple de ce type d'application.

Types des VLANs

- ❑ **VLAN de données** : Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN acheminant du trafic de voix ou de gestion ne peut pas faire partie d'un VLAN de données. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données. Un VLAN de données est parfois appelé un VLAN 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 par défaut (VLAN 1 sur commutateur CISCO) après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur.
- ❑ **VLAN natif** : Un réseau local virtuel natif est affecté à 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. Il est généralement recommandé de configurer le VLAN natif en tant que VLAN inutilisé, distinct du VLAN 1 et des autres VLAN.

Types des VLANs

- ❑ **VLAN de gestion** : Un VLAN de gestion est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion d'un commutateur. Le VLAN 1 est le VLAN de gestion par défaut. Pour créer le VLAN de gestion, l'interface virtuelle du commutateur (SVI) de ce VLAN se voit attribuer une adresse IP et un masque de sous-réseau, ce qui permet de gérer le commutateur via HTTP, Telnet, SSH ou SNMP. Sachant que la configuration initiale d'un commutateur Cisco utilise le VLAN 1 par défaut, il n'est pas judicieux de le choisir comme VLAN de gestion.

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	

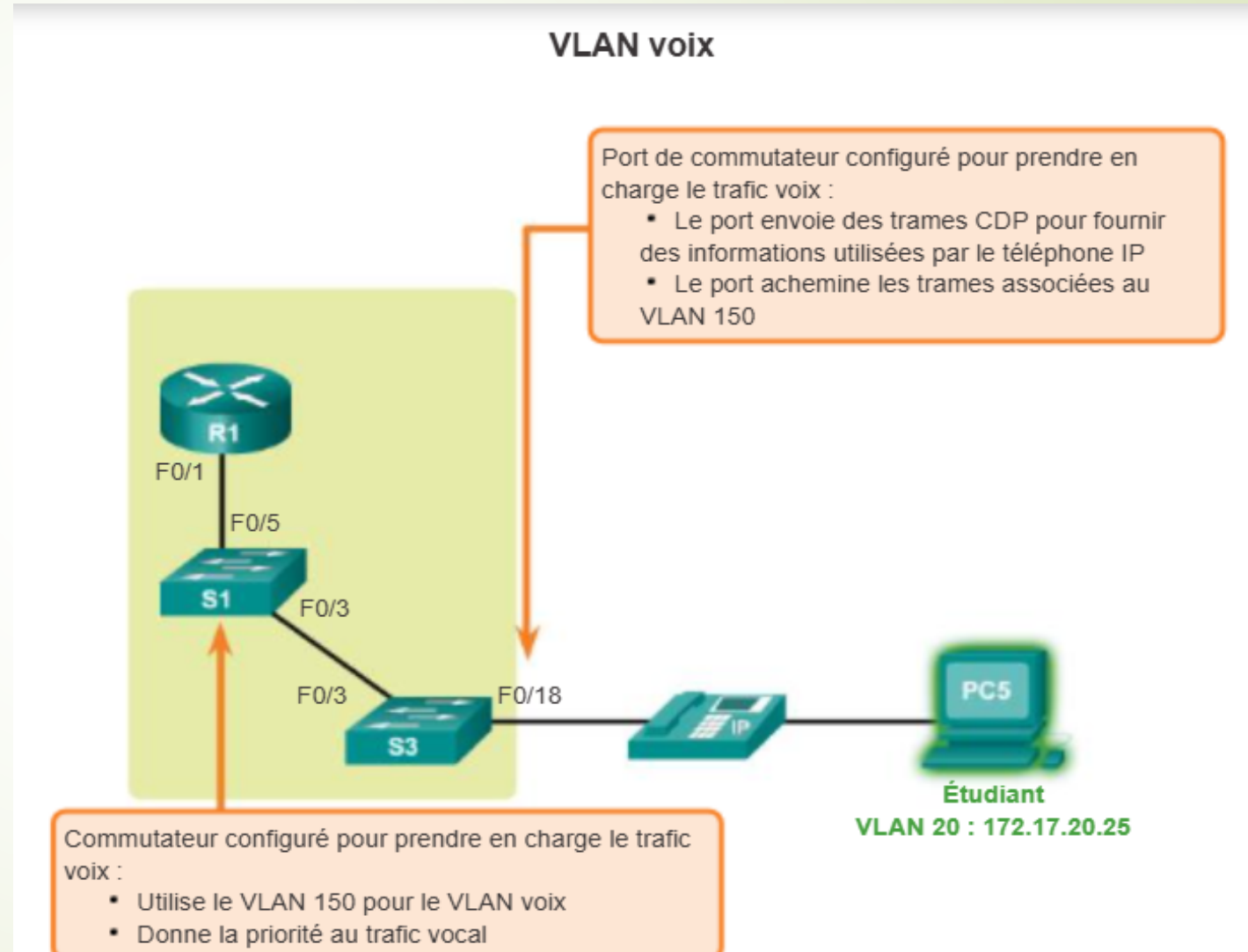
- Tous les ports affectés au VLAN 1 pour acheminer les données par défaut.
- Le VLAN natif est le VLAN 1 par défaut.
- Le VLAN de gestion est le VLAN 1 par défaut.
- Le VLAN 1 ne peut pas être renommé ni supprimé.

VLAN Voix

Un VLAN distinct est nécessaire pour prendre en charge la voix sur IP (VoIP). 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 ms sur tout le réseau.

Pour remplir ces conditions, le réseau entier doit être conçu pour prendre en charge la voix sur IP.



Les Vlan par port (Vlan de niveau 1)

- ❖ Les Vlan par port associent un port d'un switch à un numéro de Vlan.
- ❖ On dit alors que le port est tagué suivant le Vlan donné.
- ❖ Le taggage des ports peut se faire de manière statique ou de manière dynamique

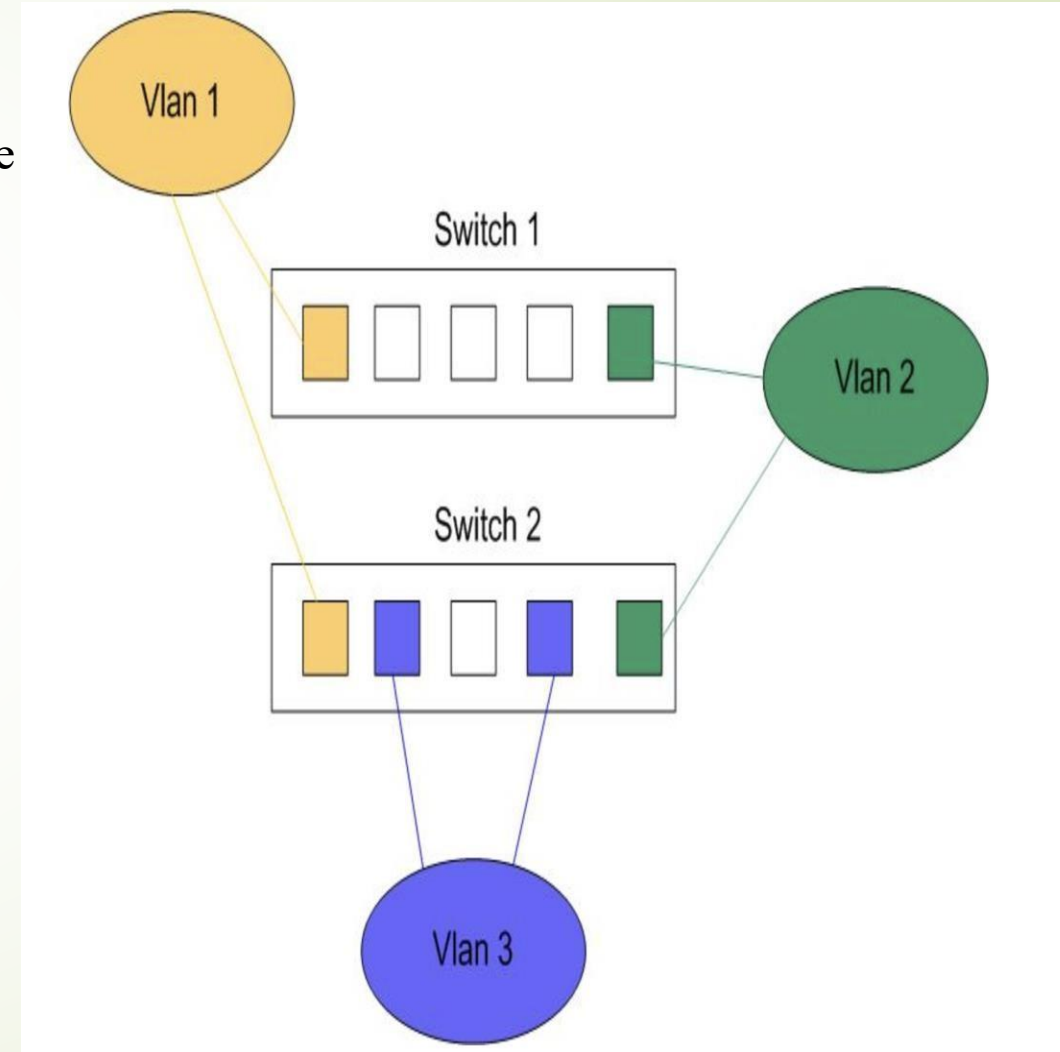
✓ Avantages :

permet une étanchéité maximale des Vlan. Une attaque extérieure ne pourra se faire qu'en branchant le PC pirate sur un port tagué. Le pirate a donc besoin d'avoir accès à la machine physique pour pénétrer le Vlan.

Le Vlan par port offre une facilité de configuration. L'administrateur peut sans difficulté choisir les ports à taguer sans avoir d'information de la part des machines auxquelles sont reliés les ports.

✓ Inconvénient :

- Nécessite une configuration lourde et contraignante sur chaque switch. A chaque déplacement de poste, il faut modifier les switchs correspondant pour maintenir une qualité de service.
- Le mécanisme de Vlan par port ne possède pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration. Chaque switch possède sa table de correspondance indépendamment du contenu des autres switchs.



Les Vlan par adresse MAC (Vlan de niveau 2)

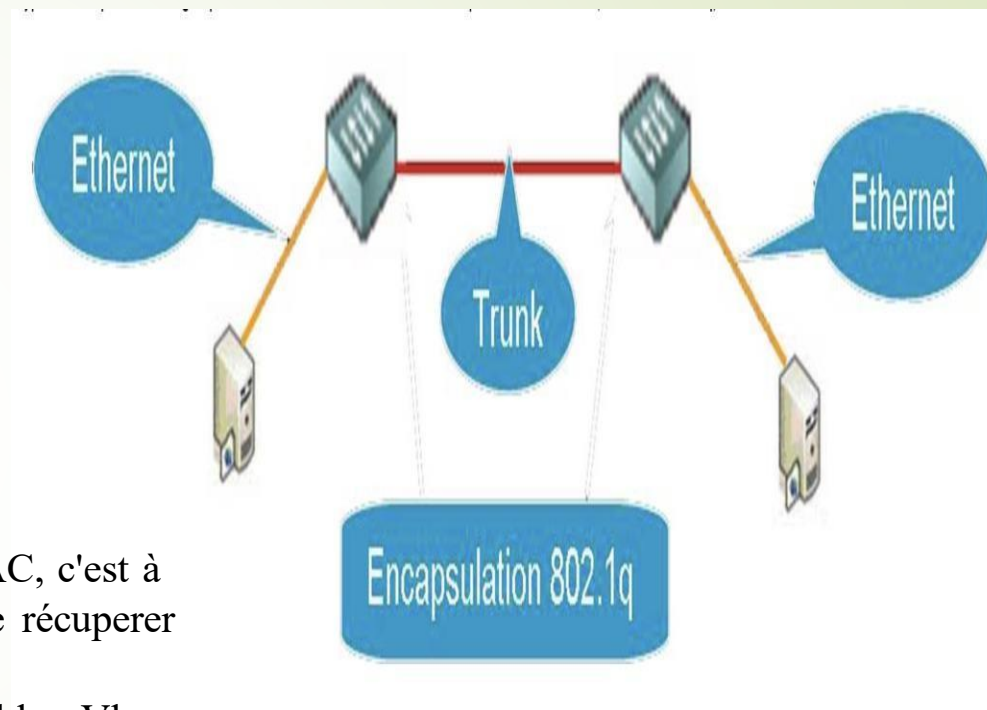
- ❑ Le Vlan de niveau 2 segmente le réseau en fonction de l'adresse MAC de l'utilisateur. On associe ainsi des adresses à des Vlan pour permettre à un utilisateur de se déplacer sans pour autant changer de profil. Ce type de Vlan est généralement utilisé pour regrouper les utilisateurs par service.
- ❑ Ce type de Vlan permet de regrouper au sein d'un même lien et de les transporter sur le réseau (voir norme 802.1q).

✓ Avantages

- Les Vlan de niveau 2 permettent une sécurité au niveau de l'adresse MAC, c'est à dire qu'un pirate souhaitant se connecter sur le Vlan devra au préalable récupérer une adresse MAC du Vlan pour pouvoir entrer.
- Les Vlan de niveau 2 offrent des possibilités de centralisation des tables Vlan adresses MAC. Chaque Switch interroge ensuite cette table pour connaître les informations nécessaires à une adresse MAC donnée.

✓ Inconvénients

Le Vlan de niveau 2 offre une sécurité moindre que le Vlan par port de par la possibilité de spoofer l'adresse MAC. De plus, il n'y a pas de contrôle de flux prévu ce qui nécessite un bon dimensionnement du réseau.



Les Vlan par adresse de Niveau 3 (VLAN de niveau 3)

- ❑ Les Vlan de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent. La mise en place de Vlan de niveau 3 est conditionné par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...).
- ❑ L'attribution des Vlan se fait de manière automatique en décapsulant le paquet jusqu'a l'adresse source. Cette adresse va déterminer à quel Vlan appartient la machine.
- ❑ Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

✓ Avantages

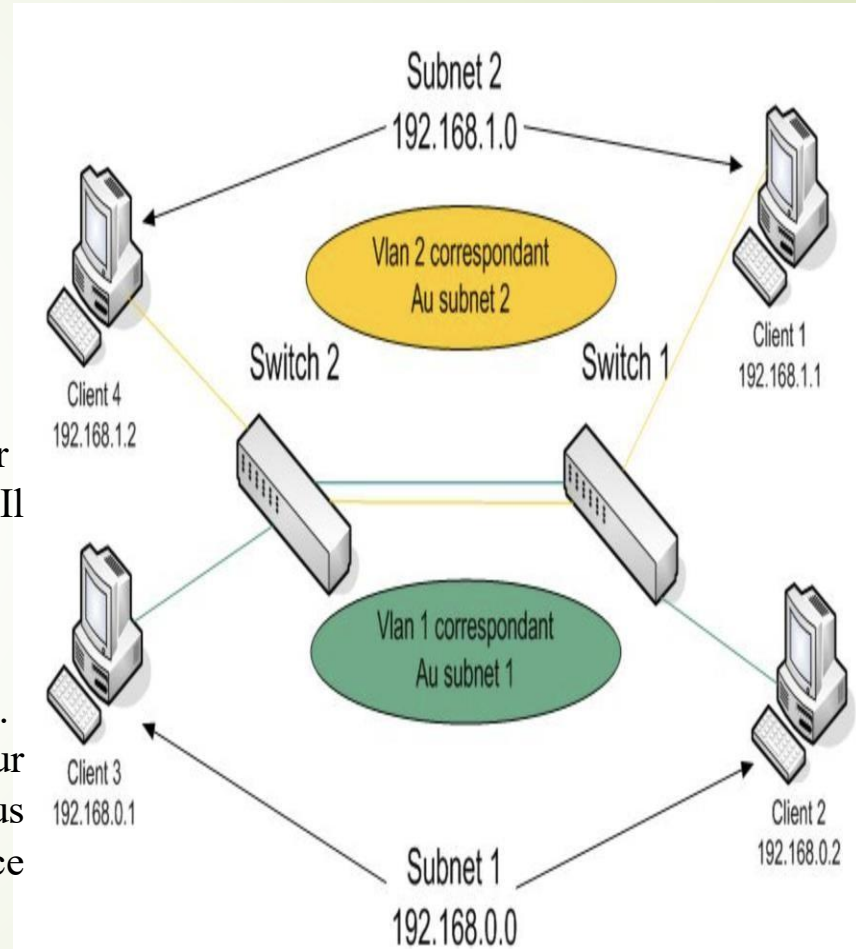
permet une affectation automatique à un Vlan suivant une adresse IP. Par conséquent, il suffit de configurer les clients pour joindre les groupes souhaités. Il est aussi possible de séparer les protocoles par Vlan.

✓ Inconvénients

Les Vlan de niveau 3 souffrent de lenteur par rapport aux Vlan de niveau 1 et 2. En effet, le switch est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel Vlan il appartient. Il faut donc des équipements plus coûteux (car ils doivent pouvoir décapsuler le niveau 3) pour une performance moindre.

La sécurité est beaucoup plus faible par rapport aux Vlan de niveau 1 et 2. En effet, l'analyse de l'adresse IP rend le spoofing IP possible. Or le spoofing IP est beaucoup plus simple à réaliser que le spoofing MAC.

Les Vlan de niveau 3 sont restreints par l'utilisation d'un protocole de routage pour avoir l'identifiant niveau 3 et ainsi se joindre au Vlan correspondant



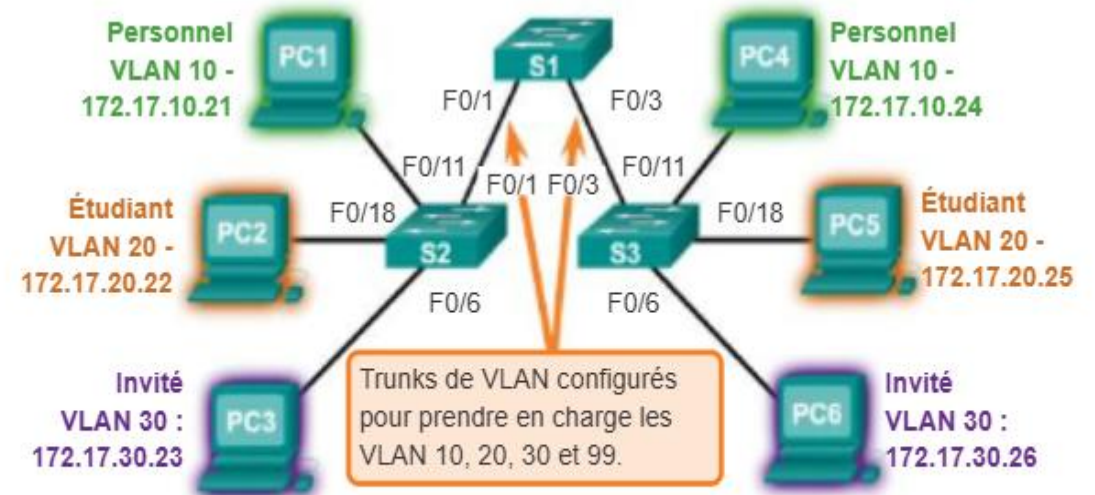
Trunk VLAN (802.1Q)

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.

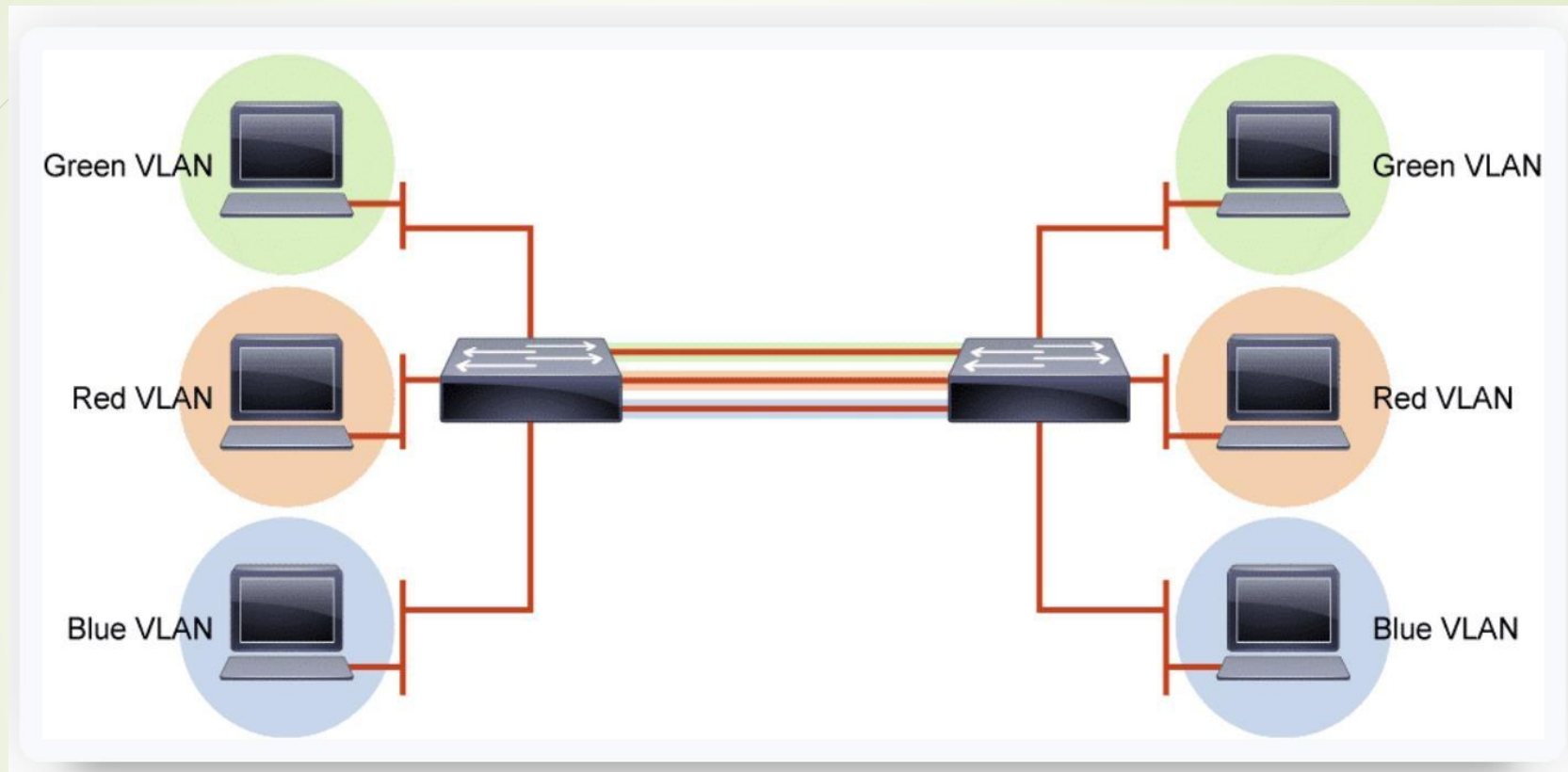
Trunks de VLAN

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.



Trunk VLAN (802.1Q)



- ✓ Pour éviter de gâcher des ressources sur le switch, on utilise un **lien Trunk**.
- ✓ Ainsi il sera possible de faire passer plusieurs VLAN sur un même lien.



Le trunk est le mécanisme qui permet d'insérer **l'identifiant du VLAN** sur une trame pour permettre le transport de trames de différents VLAN.

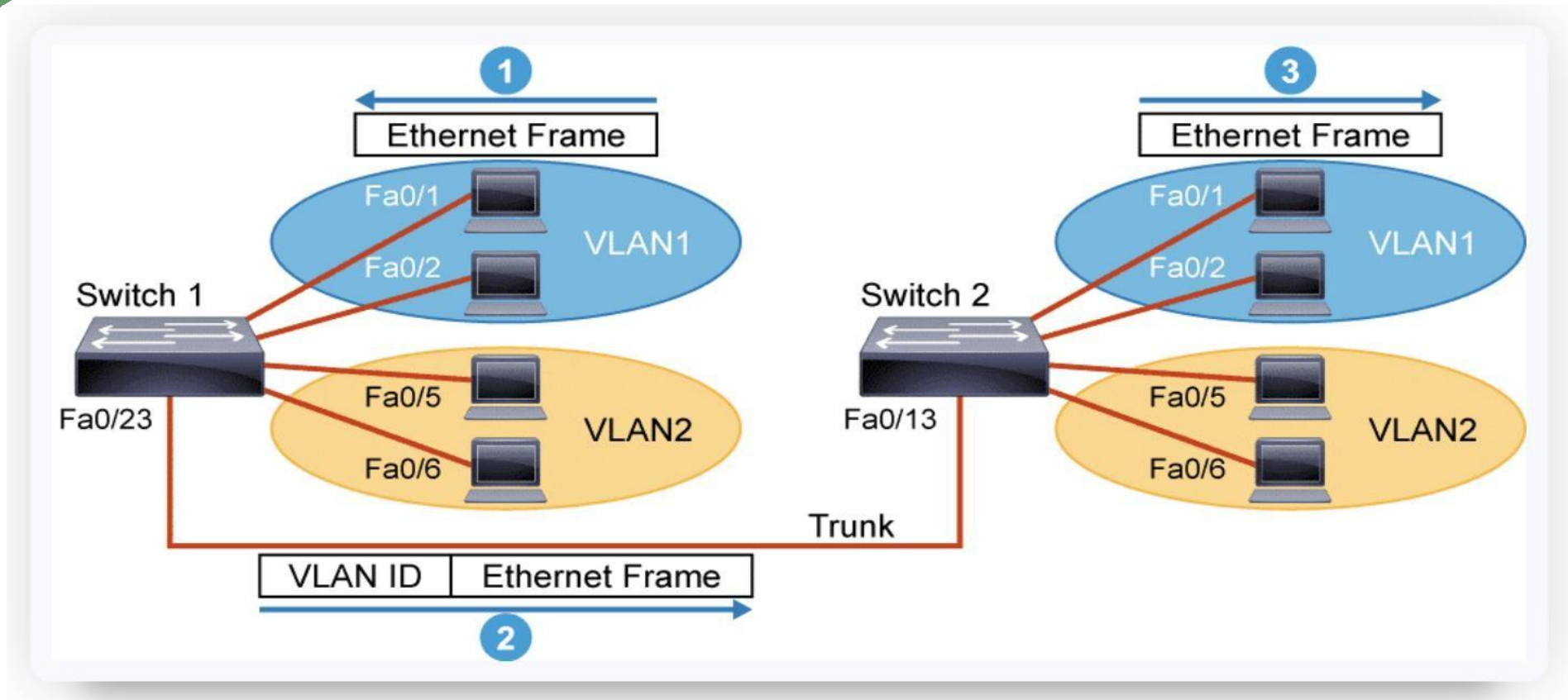
- ✓ Chaque trame qui passe sur ce lien est taguée par un numéro correspondant à son numéro de VLAN.
- ✓ Le switch transmettra les trames au vlan correspondant en fonction de ses tags.

Un Tag, c'est comme une étiquette qu'on colle au paquet afin de savoir à quel groupe il appartient. gfc

Trunk 802.1Q

Baliser le VLAN

Le trunk marque le VLAN sur l'entête du paquet, avant de l'envoyer sur l'autre switch.



Le VTP (Vlan Trunking Protocol)

- ❑ Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, Cisco a développé un protocole permettant une héritage de VLANs entre commutateur. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.
- ❑ Un commutateur doit alors être déclarés en serveur, on lui attribut également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créés sur le commutateur serveur.
- ❑ Pour créer une interface vlan, il faut entrer dans la base de données des VLANs avec la commande *vlan database*:
- ❑ Le VLAN Trunking Protocol (VTP) minimise donc l'administration dans le réseau commuté. Ceci réduit avantageusement le besoin de configurer les mêmes VLANs sur chaque commutateur individuellement.

Le VTP (Vlan Trunking Protocol)

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

- le mode serveur
- le mode client VTP
- le mode transparent

