CNAM DE PARIS

RSX 101

Commutation dans les LAN's

Introduction aux VLAN

2023-2024

CNAM PARIS

292, rue Saint Martin

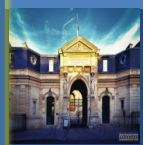
75003 Paris

Plan

- Introduction aux VLANSs
- Qu’est ce que un réseau LAN Virtuel ?
- Avantages des VLAN’s
- Appartenance à un VLAN (types de VLAN’s)
- Exemple : conception de réseau
- VLANs multi-switch
- Communication inter-VLANs

Résumé

Communication inter-VLANs « Exemples »



Sommaire

Introduction aux VLANs

Qu'est ce que un réseau LAN Virtuel ?

Avantages des VLAN's

VLANs multi-switch

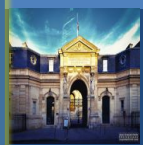
Exemple : conception de réseau

Appartenance à un VLAN (types de VLAN's)

Communication inter-VLANs

Résumé

Exemples



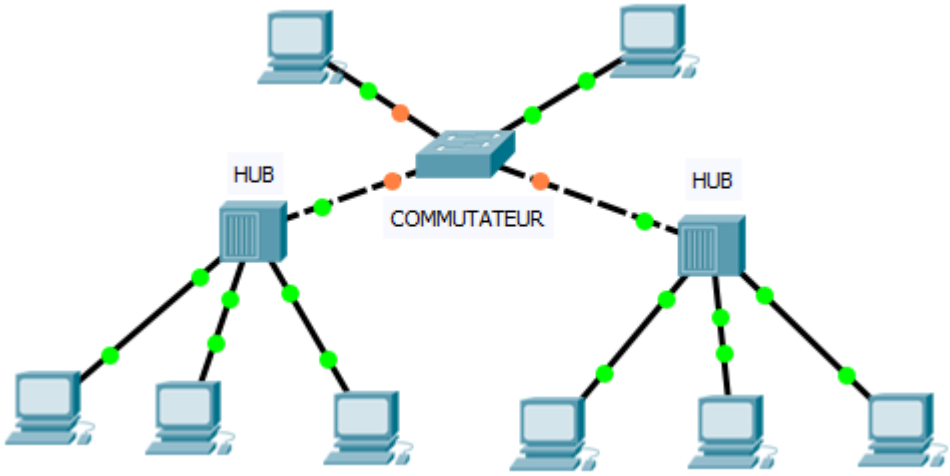
Définitions

Virtual
Local
Area
Network

Introduction aux VLANs (cont.)

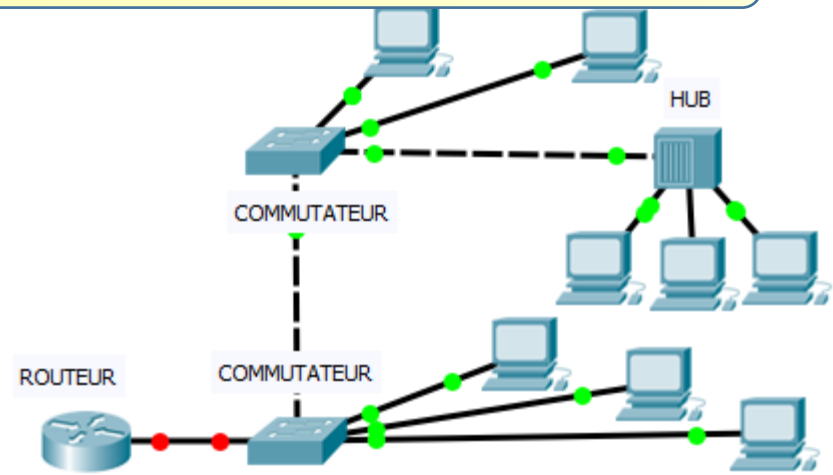
La commutation

- Meilleur accès au média
  - bande passante dédiée,
  - moins de conflits d'accès
  - collisions réduites
- Le trafic est dirigé vers la station spécifiée
- Les "broadcast" sont diffusés plus vite
- L'évolutivité reste un problème



Le réseau local commuté

- Domaines de collisions réduits
- Intelligence dans le port du commutateur
- Regroupement logique des utilisateurs
- Meilleur contrôle de la bande passante et des changements dans le réseau
- Centralisation de l'administration
- Routeur pour la communication inter-réseau



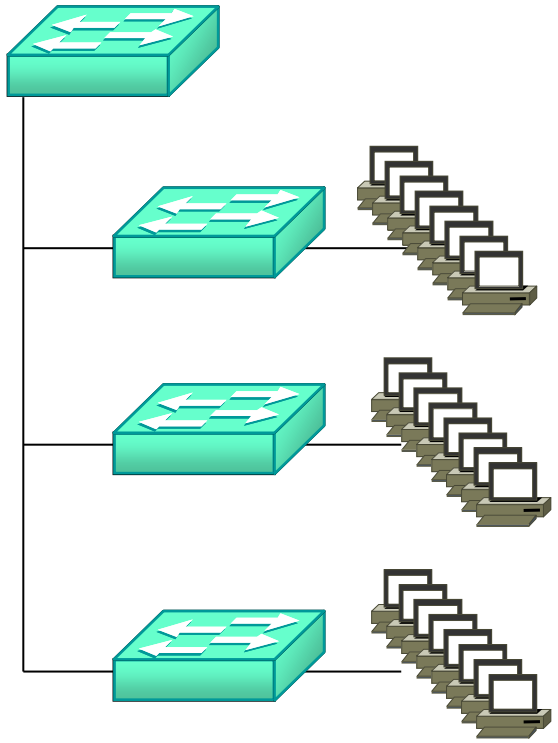
Introduction aux VLANs (cont.)

Rappel des avantages du switch

- Moins de collisions que le hub :
  - ➔ Bande passante utilisée de manière efficace.
- Grâce à la table des adresses Mac, chacun reçoit uniquement ses trames, à partir du moment où il a déjà parlé :
  - ➔ Bande passante utilisée de manière efficace.
- Forte densité des ports :
  - ➔ permet la micro-segmentation
  - ➔ permet le fonctionnement en full-duplex
  - ➔ permet plusieurs communications simultanées
  - ➔ Bande passante utilisée de manière efficace.
- Utilise des ASICs :
  - ➔ rapidité de commutation
  - ➔ grande capacité de commutation
- MAIS : par défaut, tout le monde reçoit les broadcast de tout le monde :
  - ➔ Bande passante utilisée de manière inefficace.

Introduction aux VLANs (cont.)

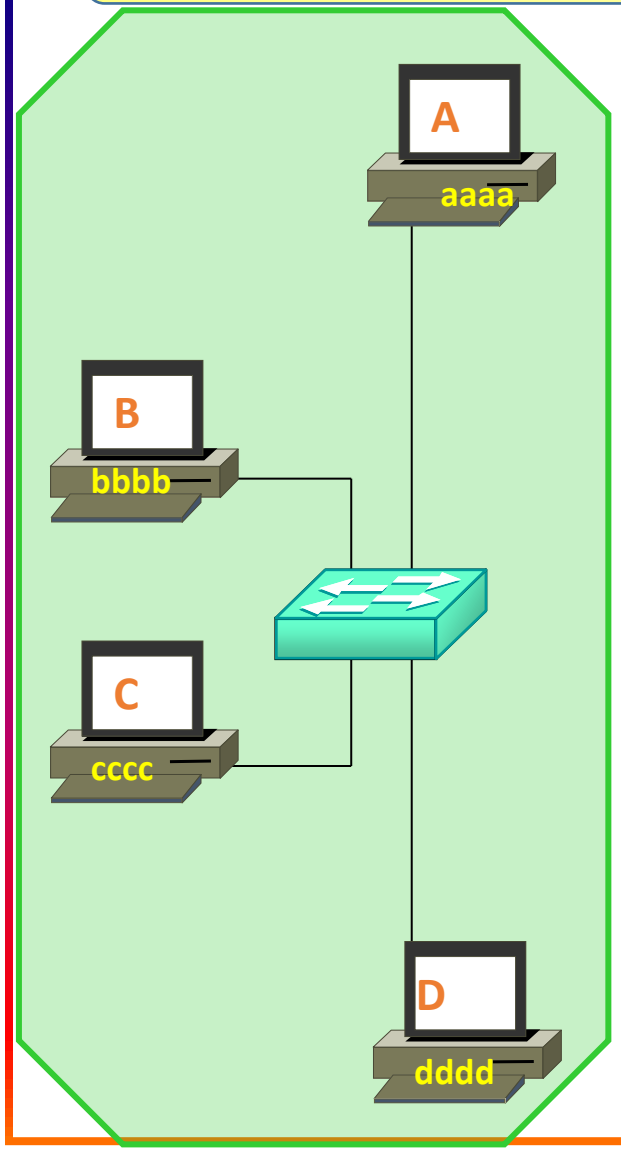
Problèmes rencontrés dans un réseau commuté à plat



- Chaque broadcast innonde le réseau
  - consomme la bande passante du réseau
  - consomme du CPU sur les hôtes
- Chaque multicast innonde le réseau.
  - consomme la bande passante du réseau
- Chaque 'unknown unicast' est envoyé sur tous les ports du switch
  - consomme la bande passante du réseau
  - présente des risques de sécurité

Introduction aux VLANs (cont.)

Domaine de broadcast



- Un équipement placé autour d'un SWITCH reçoit les broadcasts de tous les équipements placés autour de ce SWITCH :

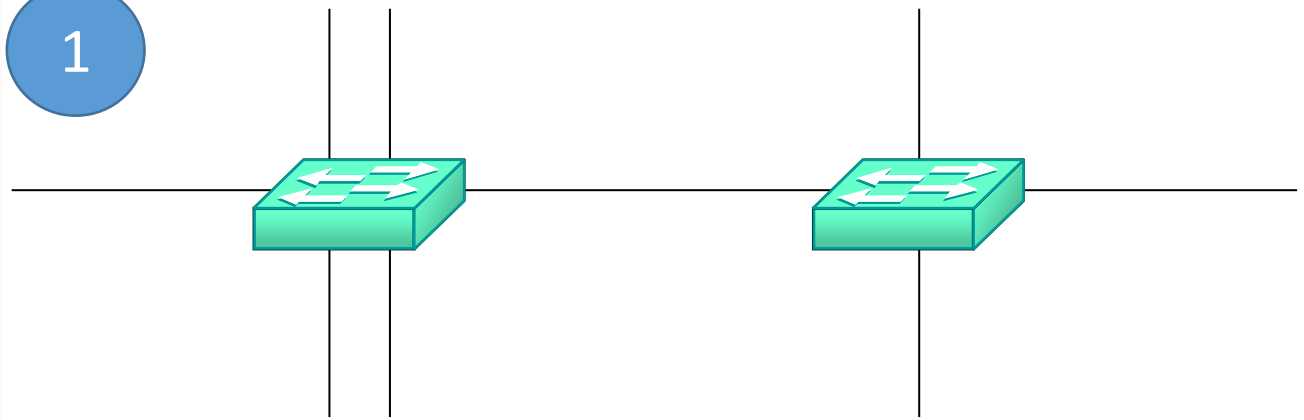
- Ils sont dans le même domaine de broadcast.

Introduction aux VLANs (cont.)

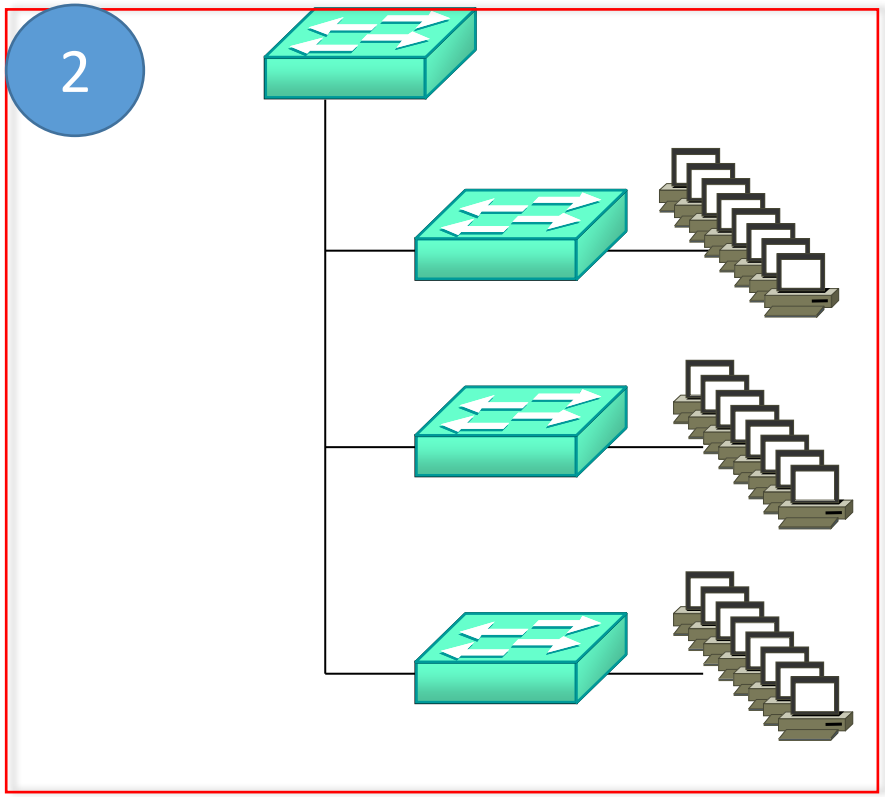
Domaine de broadcast

Combien y a-t-il de domaine de broadcast ?

1



2



Introduction aux VLANs (cont.)

Trois nécessités pour introduire le concept

1. *Limiter les domaines de broadcast*
2. *Garantir la sécurité*
3. *Permettre la mobilité des utilisateurs*

Une nouvelle manière d'exploiter la technique de commutation pour donner plus de flexibilité aux réseaux locaux

C'est un réseau logique

- Créer plusieurs VLANs sur le switch
- Chaque VLAN représente un domaine de Broadcast :
  - ➢ le switch ne permettra aucune communication entre 2 VLANs
- Chaque VLAN est identifié par un numéro entre 1 et 4096

Introduction aux VLANs (cont.)

mémo

- **Plages d'ID de VLAN**
  - Les réseaux locaux virtuels d'accès sont divisés selon une plage normale ou une plage étendue.

- **Réseaux locaux virtuels à plage normale**
  - Utilisés dans les réseaux de petites, moyennes et grandes entreprises.
  - Identifiés par un ID de VLAN compris entre **1 et 1005.**
  - Les ID de **1002 à 1005** sont réservés aux VLAN Token Ring et aux VLAN à interface de données distribuées sur fibre (FDDI).
  - L'ID 1 est le numéro attribué par défaut au réseau local commuté => vus ne pouvez pas l'utiliser pour l'affecter à un VLAN utilisateur
  - Les ID **1 et 1002 à 1005** sont automatiquement créés et ne peuvent pas être supprimés.

Qu'est ce que un réseau LAN Virtuel ?

Définition

- **LANs virtuel :**
  - Un LAN virtuel est un ensemble logique d'unités regroupées en domaine de broadcast quelque soit l'emplacement de leur segment physique.
  - Ils peuvent <u>être regroupés en fonction :</u>
    - ⇨ **du service** auquel ils appartiennent,
    - ⇨ des **applications utilisées**,
    - ⇨ des **protocoles**, etc.

Qu'est ce que un réseau LAN Virtuel ? (cont.)

Exemple :

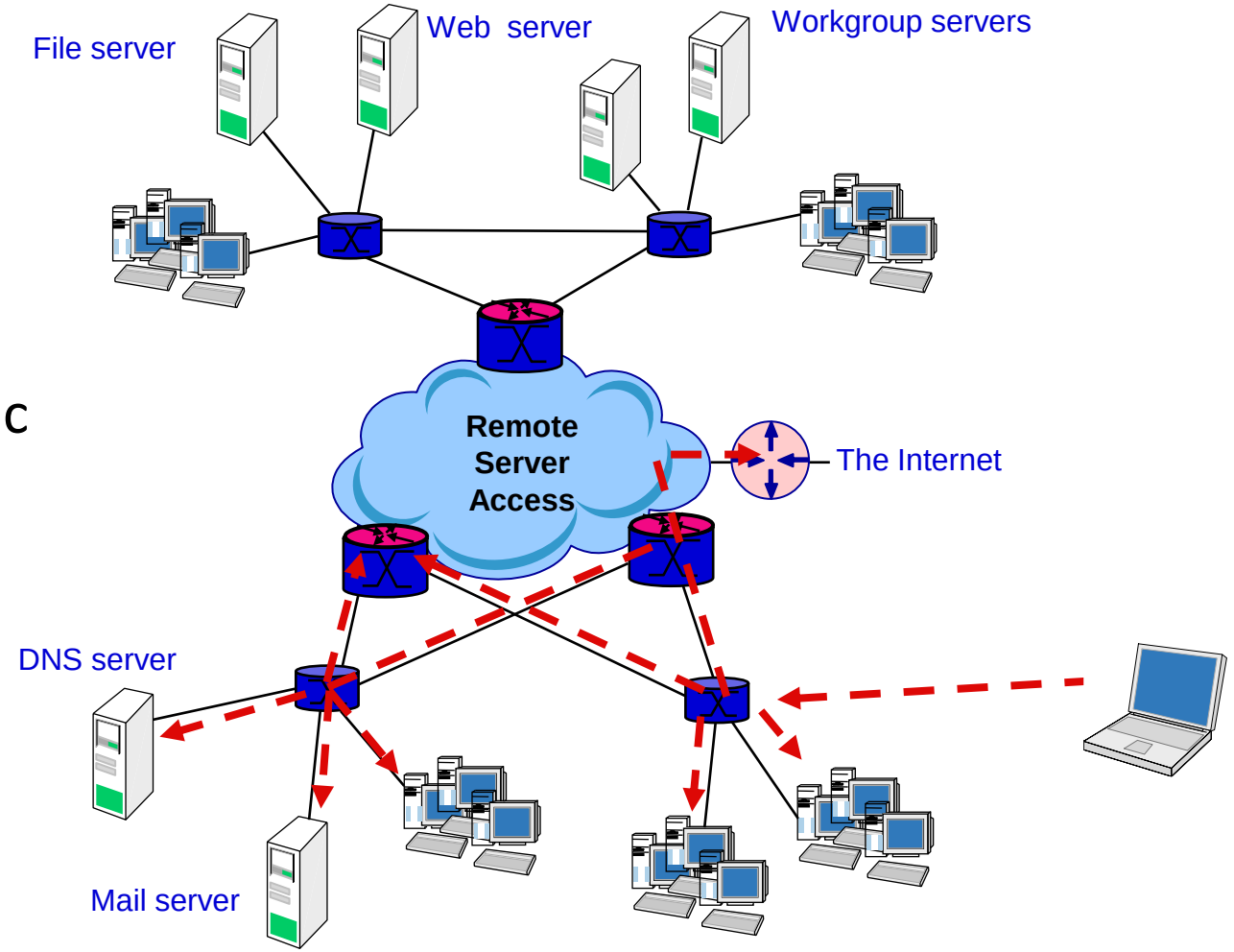
- **Les commutateurs ont beaucoup plus de connectivité que les ponts**
  - **Les commutateurs peuvent mettre en communication plusieurs centaines d'utilisateurs**
- **L'utilisation de la diffusion de trames (⇔ broadcast des trames) est très courante**
  - **Par exemple, un client DHCP utilise des requêtes de diffusion pour localiser un serveur DHCP**
  - **ARP utilise aussi la diffusion (ou broadcast) de trames**

- **Le trafic de diffusion peut avoir un impact important**
  - **Interrompt tous les systèmes dans le domaine de diffusion**
  - **Les clients répètent généralement leur demande après un délai d'attente (TimeOut) relativement court**
    - » ***Peut-être simplement dû à une réponse lente du serveur***
    - » ***Des diffusions répétées peuvent entraîner des tempêtes de diffusion***
  - **Peut entraîner des retards anormaux pour les autres trafics client/serveur**

Qu'est ce que un réseau LAN Virtuel ? (cont.)

Exemple :

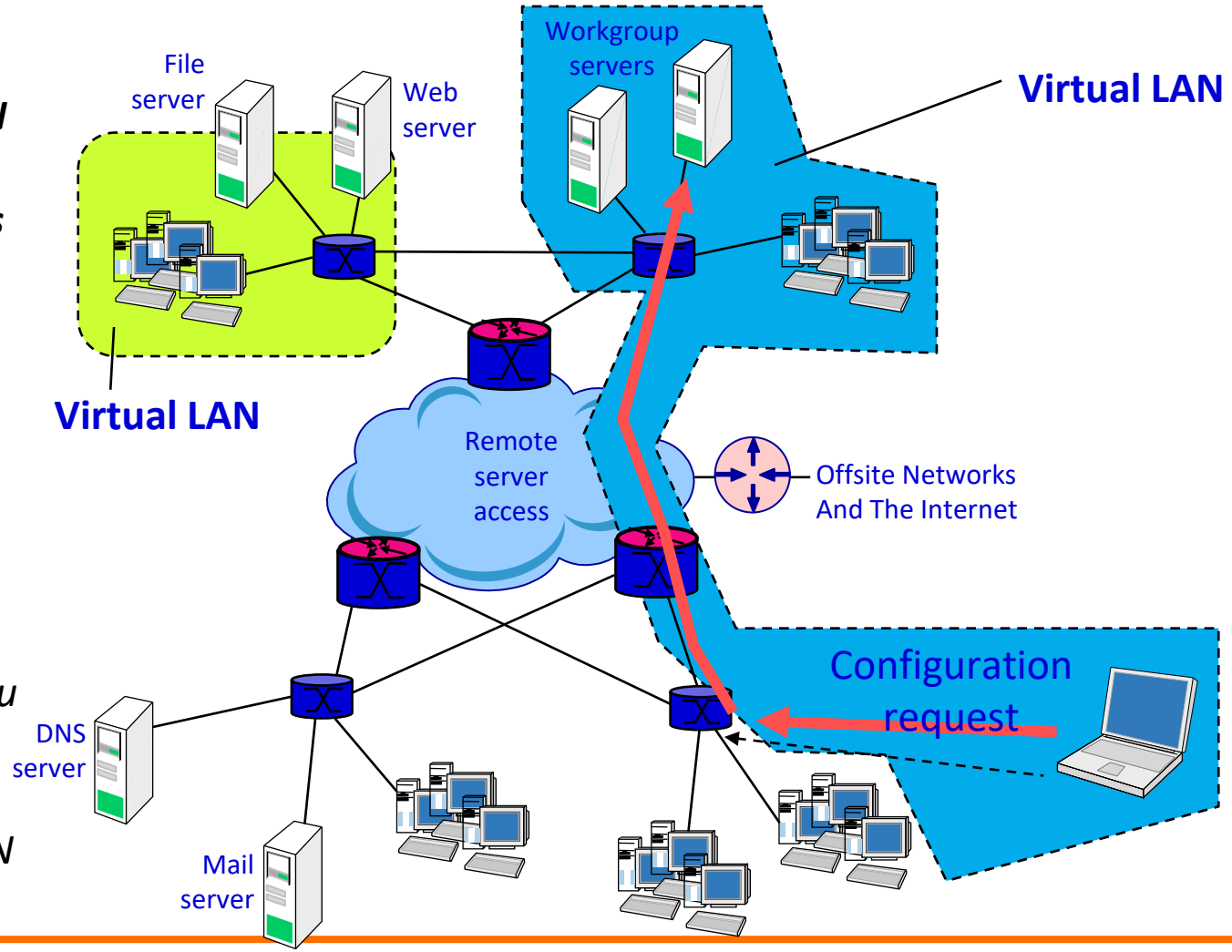
- Topologie de base
  - Broadcast DHCP
  - Broadcast ARP
  - Délais importants pour le trafic client / Serveur



Qu'est ce que un réseau LAN Virtuel ? (cont.)

Exemple : (ce qui est apporté par les VLAN's)

- **Les VLANs séparent la structure d'une organisation physique du réseau**
  - ***VLAN peut faire partie d'un seul LAN physique***
  - ***Ou bien de plusieurs LANs physiques***
- **Fournissent une segmentation logique**
- **l'administrateur définit des groupes d'utilisateurs et des ressource**
  - ***Le trafic Broadcast*** *est limité à l'intérieur des VLAN's*
  - *Pas de nécessité de* ***modifier ni le câblage, ni déplacement physique des équipements***
  - ***Amélioration de la sécurité*** *au niveau de la couche 2*
  - ***Limite le trafic LAN*** *aux seuls équipements faisant partie d'un VLAN*

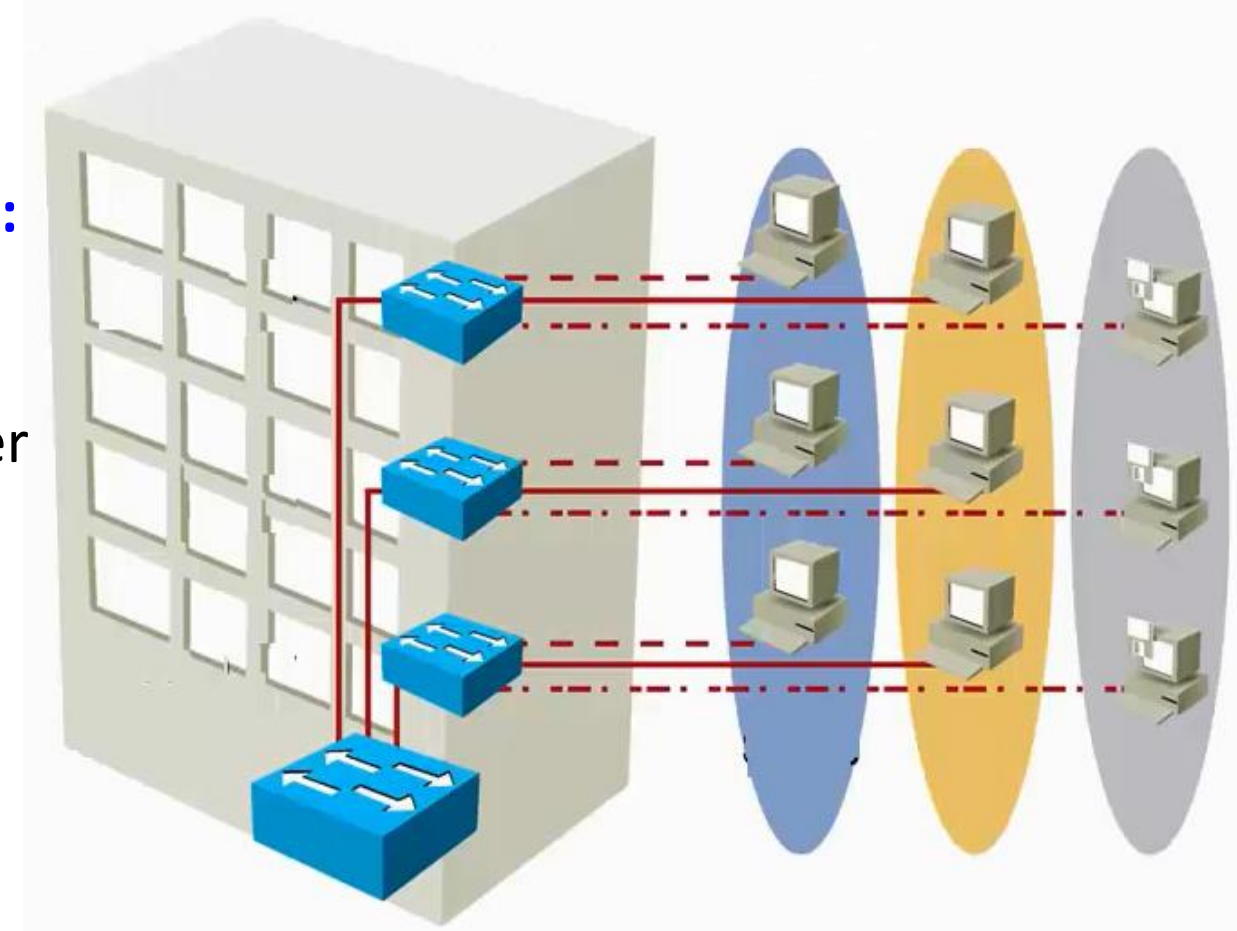


Avantages des VLAN's (sur un exemple simple)

Avantages :

1. *Segmentation*
2. *Flexibilité*
3. *sécurité*

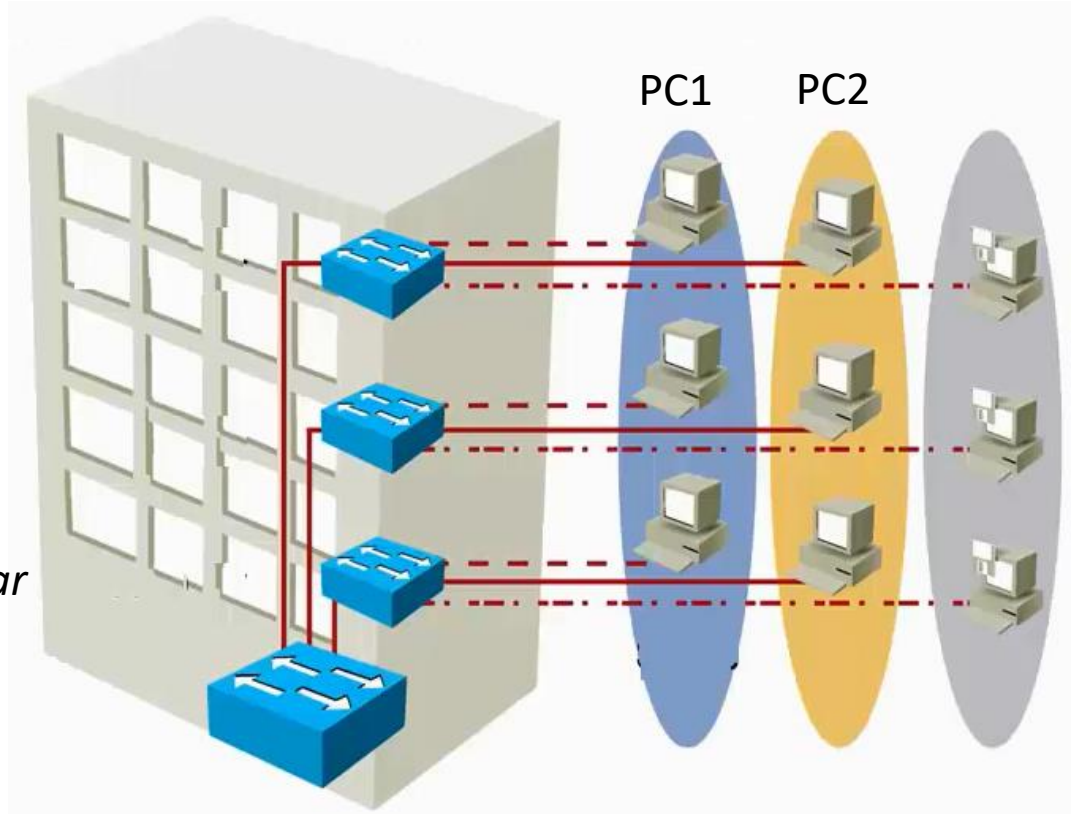
- **Exemple : un immeuble de trois étages :**
  - Un commutateur dans chaque étage
  - Un switch fédérateur pour connecter l'ensemble à l'internet par exemple



Avantages des VLAN's (cont.)

1. Segmentation

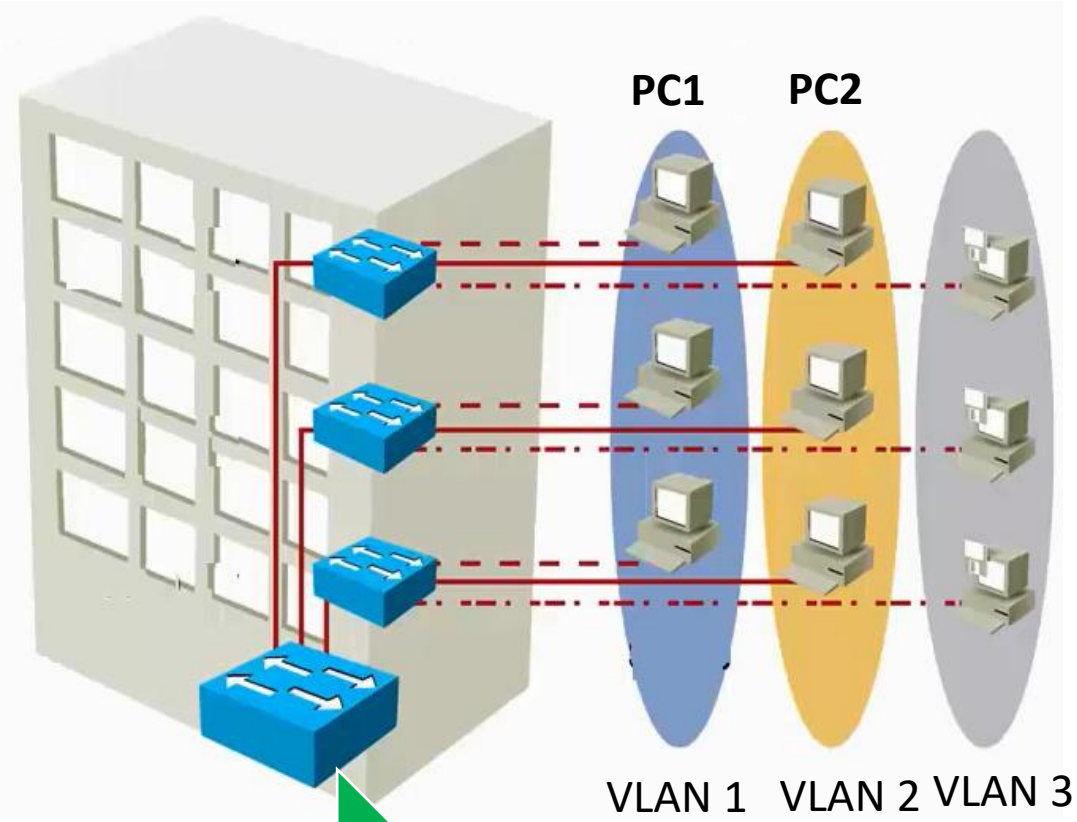
- **PC's configurées correctement**
- **PC1 et PC2 sont au 3ième étage**
- **Sans configuration particulière,**
- **Si PC1> ping PC2**
  - *Récupération de l'adresse MAC de PC2 ⇔ ARP*
  - *Envoie d'une **requête ARP en Broadcast** qui serait reçu par l'ensemble des PC's sur la topologie quelque soit l'endroit physique*
  - *Donc, une **consommation inutile de la bande passante***



Avantages des VLAN's (cont.)

1. Segmentation - suite

- **Maintenant, si on crée trois VLANs : VLAN1, VLAN2, et VLAN3**
- **Si maintenant PC1> envoie un Braodcast , il sera envoyé uniquement aux stations appartenant à la même VLAN**
- **Conséquence :**
  - On élimine pas le Broadcast
  - Mais on réduit la taille de domaine de Broadcast



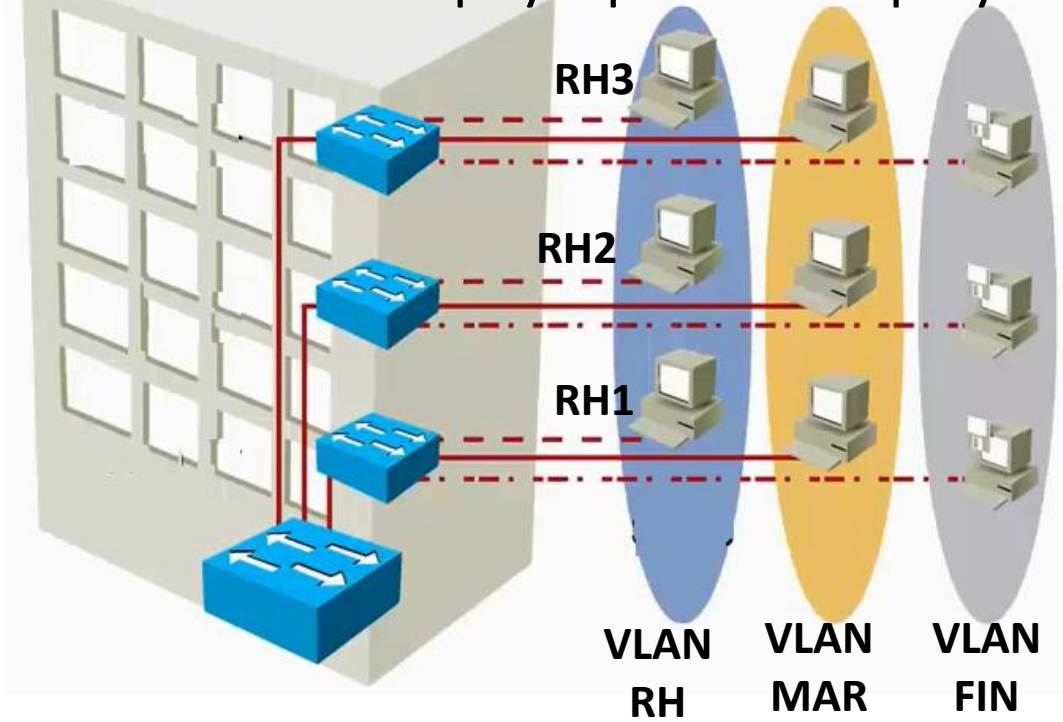
VLAN = Domaine de Broadcast (Diffusion) = Réseau logique (Sous réseau

Avantages des VLAN's (cont.)

2. Flexibilité

- **Exemple : entreprise avec plusieurs entités**
  - *Entité RH*
  - *Entité Marketing*
  - *Entité Finance*
  - ***Contrainte** : pour le service RH, il faut qu'il y ait une personne de la RH qui se trouve dans chaque étage*
- **Actions** :
  - Création de 3 VLANs : chaque VLAN est défini au niveau des trois switch (⇔ trois domaines de Broadcast)
  - Affecter un port de chaque switch à chaque VLAN
  - Les trois personnes appartiennent au même VLAN ⇔ au même domaine de Broadcast

Conclusion : Flexibilité par rapport à l'endroit physique des employés

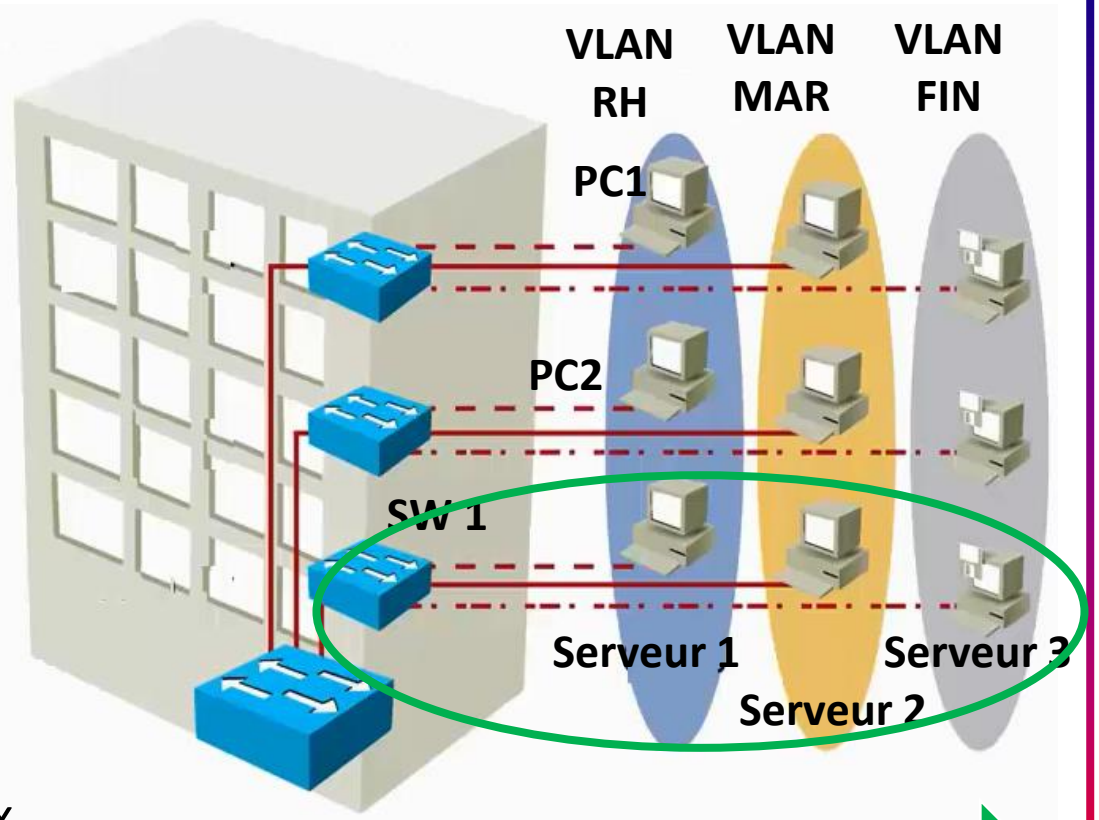


Conclusion : Flexibilité par rapport à l'endroit physique des employés

Avantages des VLAN's (cont.)

3. Sécurité

- **Exemple : au 1er étage, on a mis les serveurs**
  - Objectif : isoler les serveurs
- **Démarche** :
  - *Créer un VLAN au niveau de switch 1*
  - *Relier les trois serveurs aux trois ports : P1, P2 et P3 sur le switch SW1*
- **Conséquence** : les trois serveurs appartiennent maintenant au VLAN 4 (VLAN en vert)
  - *Si maintenant, on envoie un Broadcast depuis PC1, il sera reçu uniquement par PC2*
- **Remarques:**
  - Si on veut faire communiquer les VLANs entre eux, il faut faire intervenir le routage **inter-VLANs**
  - **Par défaut, pas de communication entre les VLANs**

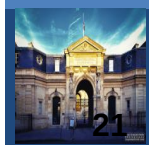


Conclusion : amélioration de la sécurité en isolant les trois serveurs

Résumé

Spécifiés des VLANs

- Les LAN virtuels fonctionnent au niveau **des couches 2 et 3 du modèle OSI**.
  - La communication inter-LAN virtuels est assurée par **le routage de couche 3.**
- Les LAN virtuels fournissent **une méthode de contrôle des Broadcasts.**
- Les LAN virtuels permettent d'effectuer une segmentation **selon certains critères:**
  - ***Des collègues travaillant dans le même service.***
  - ***Une équipe partageant le même applicatif.***
- Les LAN virtuels peuvent **assurer la sécurité des réseaux** en définissant quels nœuds réseaux peuvent communiquer entre eux, en restreignant le nombre d'utilisateurs dans un Vlan.
- Les LAN virtuels empêchent d'autres utilisateurs d'accéder **au réseau s'ils n'ont pas été autorisés**
  - Le trafic requiert un **périphérique de couche 3** pour se déplacer entre réseaux locaux virtuels.



Appartenance à un VLAN (types de VLAN's)

Types de VLANs

- **Dans un réseau commuté, un périphérique peut être affecté à un réseau local virtuel en fonction :**
  - ***De son emplacement,***
  - ***De son adresse MAC,***
  - ***De son adresse IP***
  - ***Ou des applications qu'il utilise le plus fréquemment.***
- Dans un réseau local virtuel, l'appartenance est affectée de **façon statique** ou **dynamique** par les **administrateurs.**

Appartenance à un VLAN (types de VLAN's) (cont.)

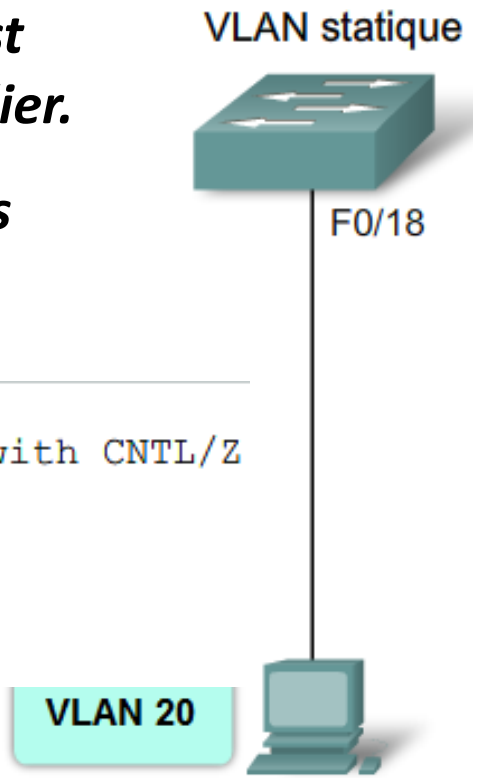
VLAN par port

- **L'administrateur configure de manière statique l'attribution des VLAN aux ports**

- **On parle de VLAN par port**
  - ***Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur à un VLAN particulier.***
  - ***C'est une solution simple, qui a été rapidement mise en œuvre par les constructeurs***

- **Exemple d'affectation**

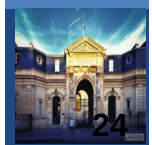
```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
S3(config)#interface fastEthernet0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```



Appartenance à un VLAN (types de VLAN's) (cont.)

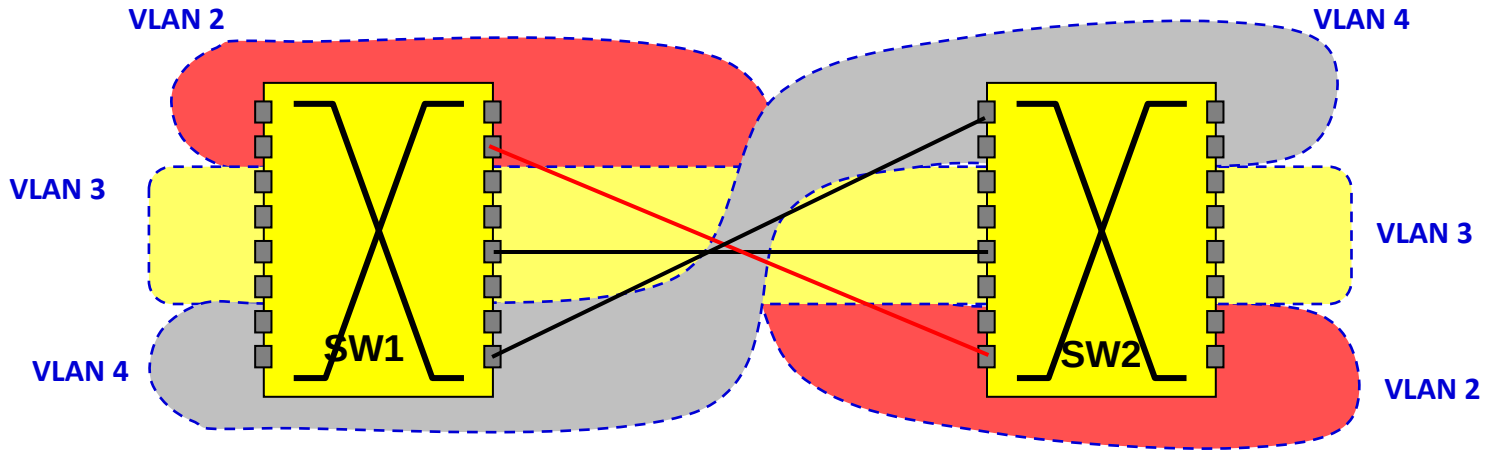
VLAN par port

- **Les VLAN par port manquent de souplesse,**
  - **Tout déplacement d'une station nécessite une reconfiguration des ports.**
  - **De plus, toutes les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN.**



Situation de base

- **Voici l'exemple suivant avec trois VLANs**
  - La question est : comment réaliser la communication entre les deux commutateurs : SW1 et SW2 Ou bien : comment le switch receveur d'une trame va arriver à aiguiller des trames vers tel ou tel VLAN ?

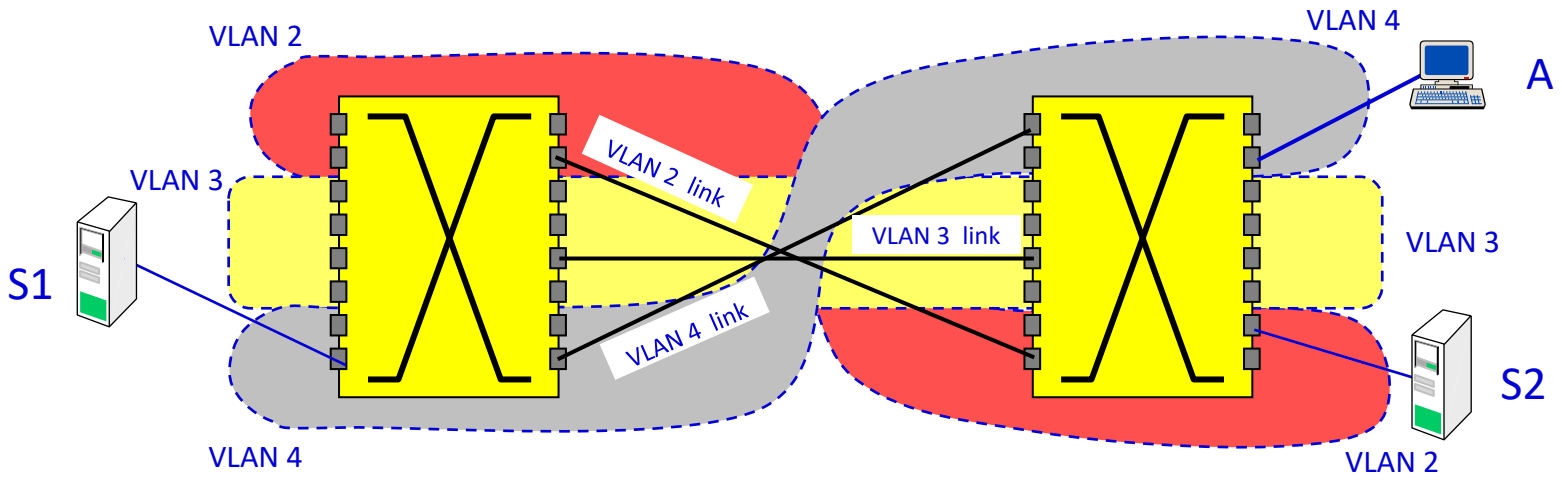


- **Deux solutions possibles :**
  1. *Utiliser un lien dédié entre les commutateurs pour chaque VLAN*
  2. *Utilise un **schéma de multiplexage basé sur les labels** sur les **liens inter-switch** ⇔ **solution Frame Tagging***

VLANs multi-switch (cont.)

Utiliser des liens indépendant pour chaque VLAN

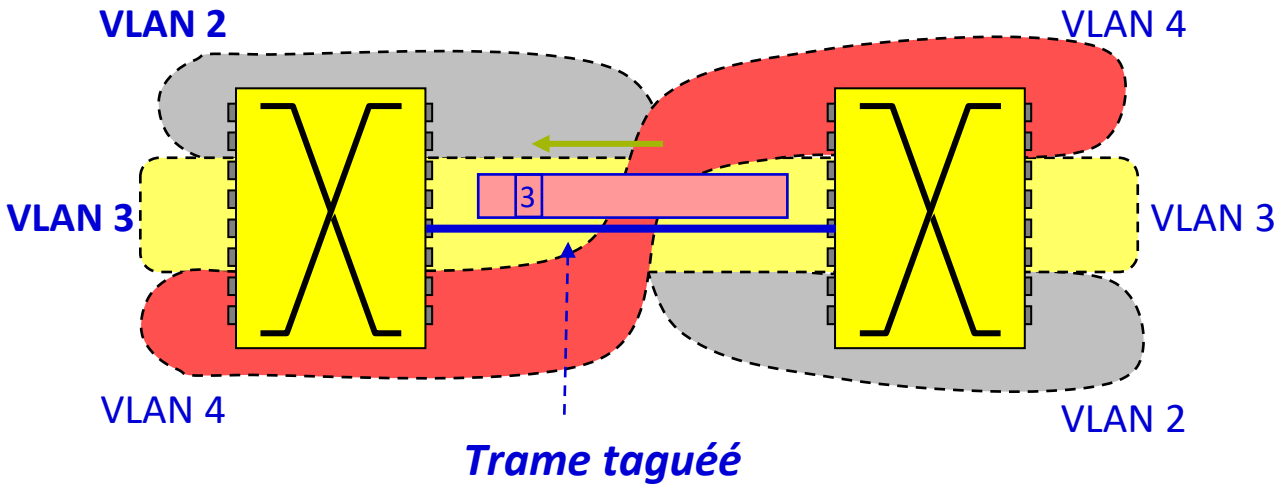
- **Cette méthode dédie un lien entre-switchs (inter-switch) pour chaque VLAN**
- **Fonctionne bien avec un nombre faible de VLANs,**
  - Manque de *scalabilité*
  - Fonctionne de moins en moins bien avec l'ajout des VLAN's
  - Besoin d'une paire de ports par VLAN avec les câbles associés



VLANs multi-switch (cont.)

Solution basée sur le VLAN tagging

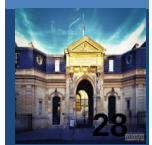
- **Meilleur scalabilité**
- **Les liens inter-switch sont configurés comme « trunks » multi-VLAN**
  - *Les trames sont tagguées lorsqu'elles traversent les trunks*
  - *Véhiculent une information supplémentaire dans l'entête renseignée par des informations spécifiques VLAN*
  - *Informent le switch receveur **de quel switch VLAN** ces trames proviennent*



VLANs multi-switch (cont.)

Frame Tagging

- **Standard internationale : Méthode qui ajoute 4 octets**
  - **Les quatre octets sont composés de deux champs**
    - *Identification de VLAN (IEEE 802.1Q)*
    - *Priorité des trame « Frame Priority » (pour supporter IEEE 802.1p)*
  - **Supporté par la plus part des OS des SWITCH**
    - *Pose un pb de taille max de trames*
    - ☞ *Dépasse le **1518 octets***

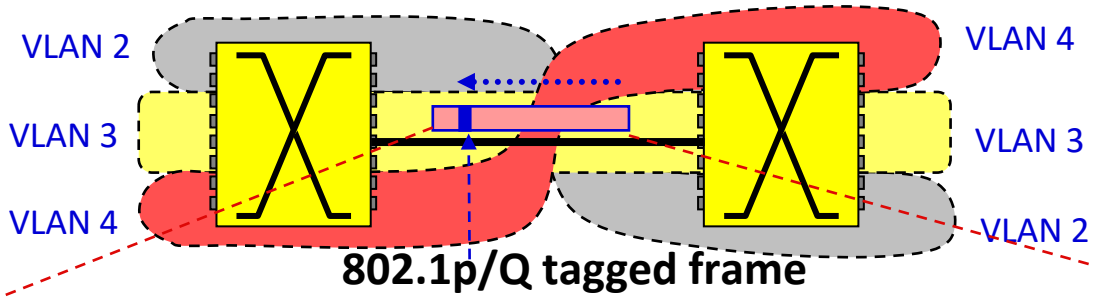


VLANs multi-switchs (cont.)

Frame Tagging

Length 1518 Bytes

6	6	2	1500	4
Destination Address	Source Address	Type / Length	Data Max of 1500 Bytes	FCS



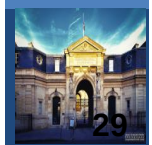
802.1p/Q tagged frame

TPID (16 bits)	TCI (16 bits)

- Tag Protocol IDentifier : TPID
- Tag Control Information : TCI

Length 1522 Bytes

6	6	2	2	2	1500	4
Destination Address	Source Address	802.1Q Tag		Type/ Length	Data Max of 1500 Bytes	New FCS
		8100	Tag			

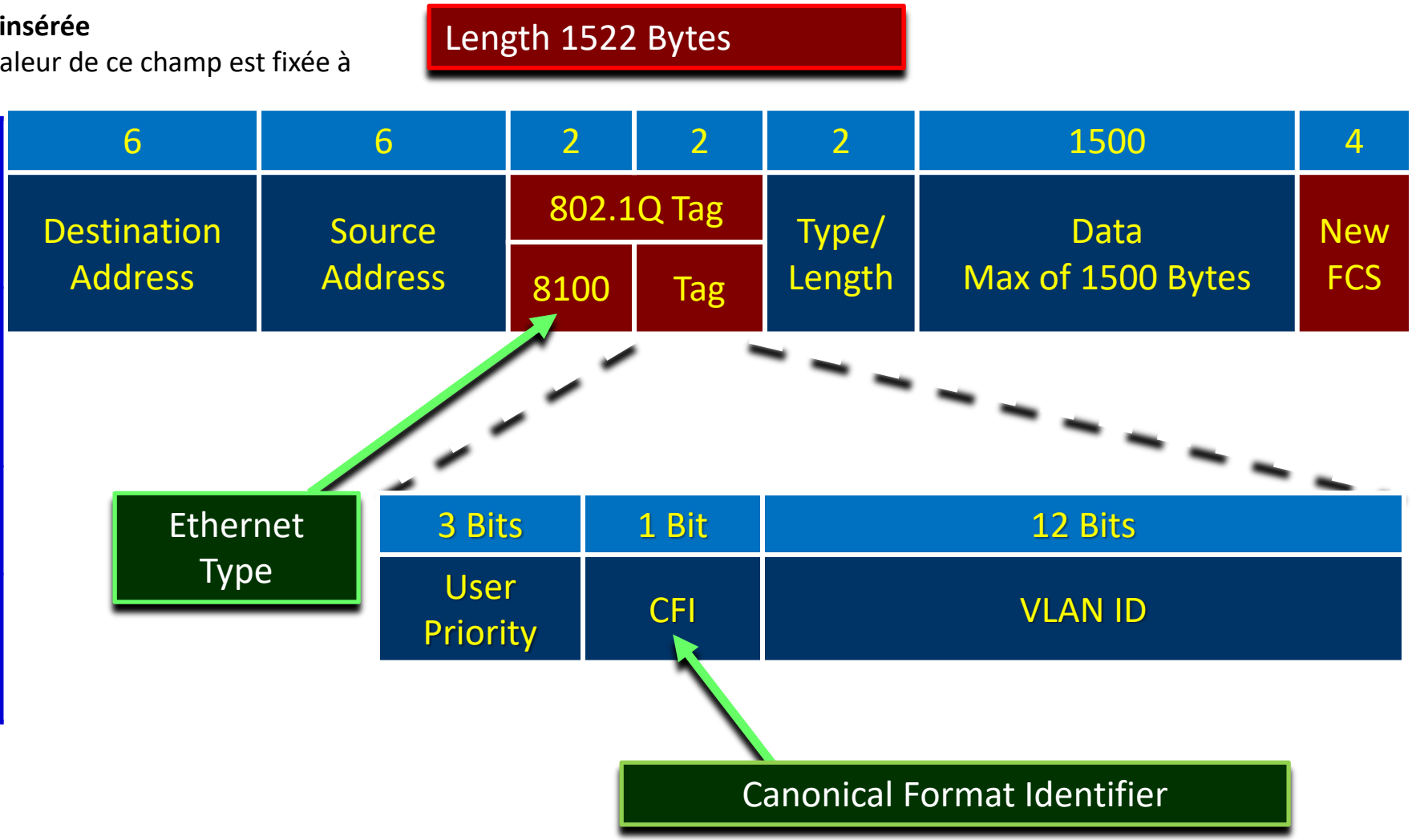


Frame Tagging

TPID :

- identifier **le protocole de la balise insérée**
- Dans le cas de la balise 802.1Q la valeur de ce champ est fixée à **0x8100.**

TPID	• **Tag Protocol Identifier (EtherType): 0x8100 trame est taguée avec le protocole 802.1Q-tagged (/Cisco : ISL).**
PRI	• **IEEE 802.1p : Champs priorité *(also called class of service, or CoS, field)* 7=highest priority,** • **0=lowest**
CFI	• **Canonical Format Identifier: 0 = CSMA/CD frame**
VLAN ID	• **12-bit VLAN IDentifier poss.** • **values 2 – 4094 0, 1 and 4095 are reserved**

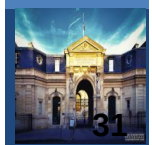


VLANs multi-switchs (cont.)

Frame Tagging : A quoi sert le TAG ?

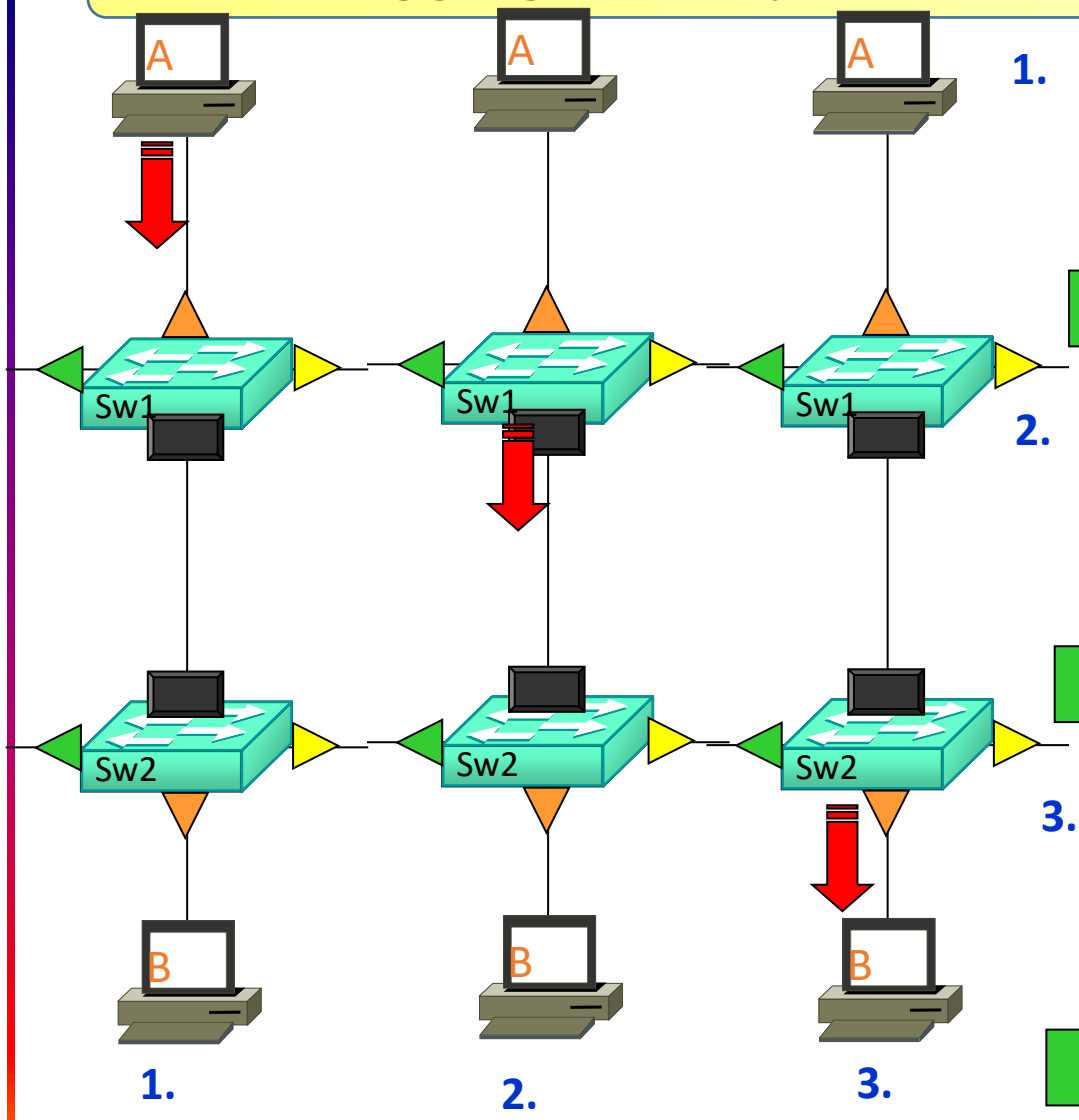
- Il permet d'indiquer au switch distant à quel VLAN appartient la trame envoyée.
- Le switch distant saura alors quelle table de Mac adresses utiliser pour forwarder cette trame.

☞N. B : chaque VLAN possède sa propre table d'adresse Mac.



VLANs multi-switchs (cont.)

Frame Tagging : Exemple

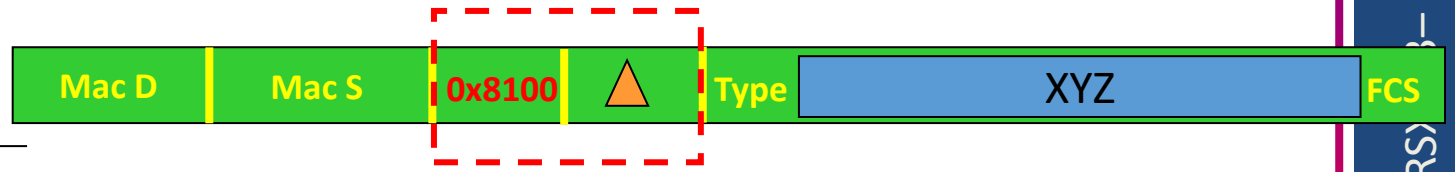


1.

- A envoie une trame à B.
- A génère cette trame.
- Elle n'est pas taggée :

2.

- Sw1 veut envoyer cette trame sur l'interface Trunk.
- Sw1 rajoute le TAG et recalcule la FCS :

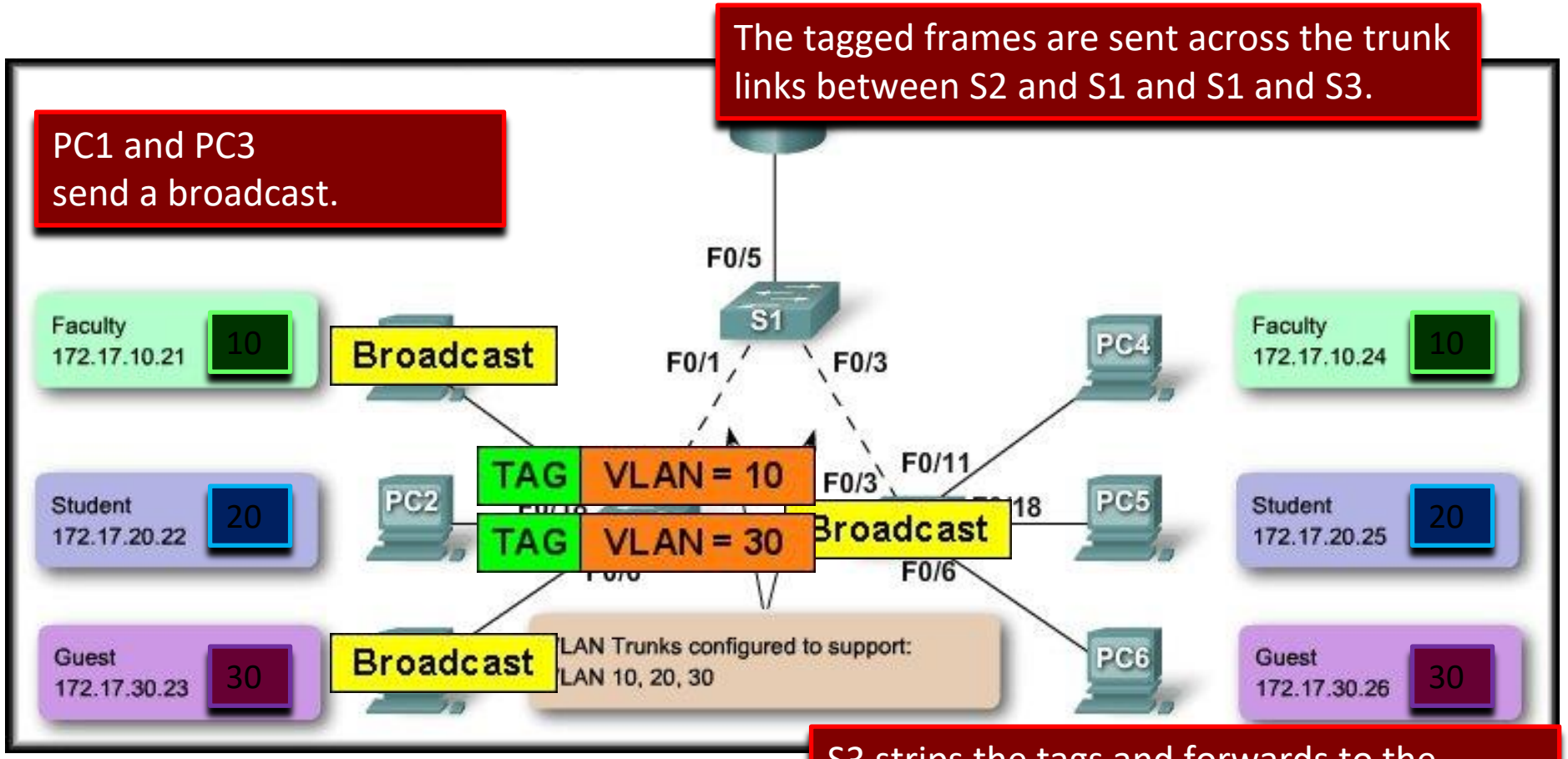


3.

- Sw2 reçoit une trame taggée.
- Sw2 retire le TAG, recalcule la FCS et envoie la trame à B :

VLANs multi-switchs (cont.)

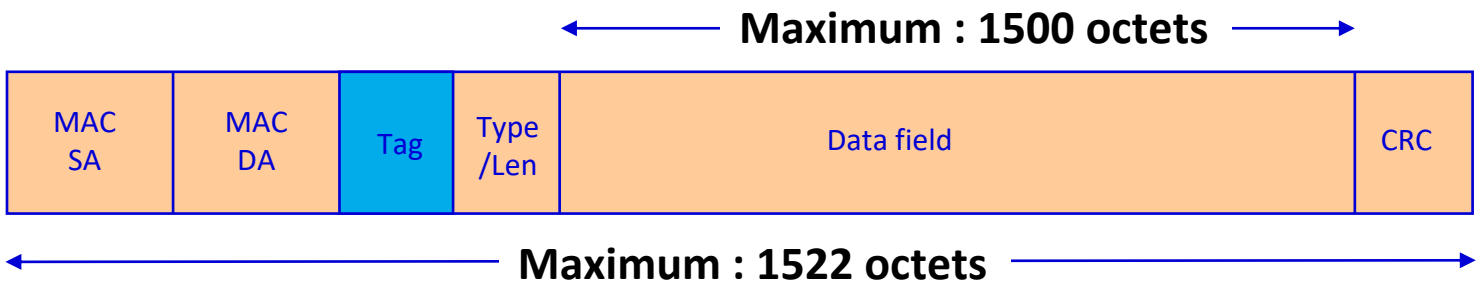
Exemple : le Truncking en Action



VLANs multi-switchs (cont.)

Problème potentiel

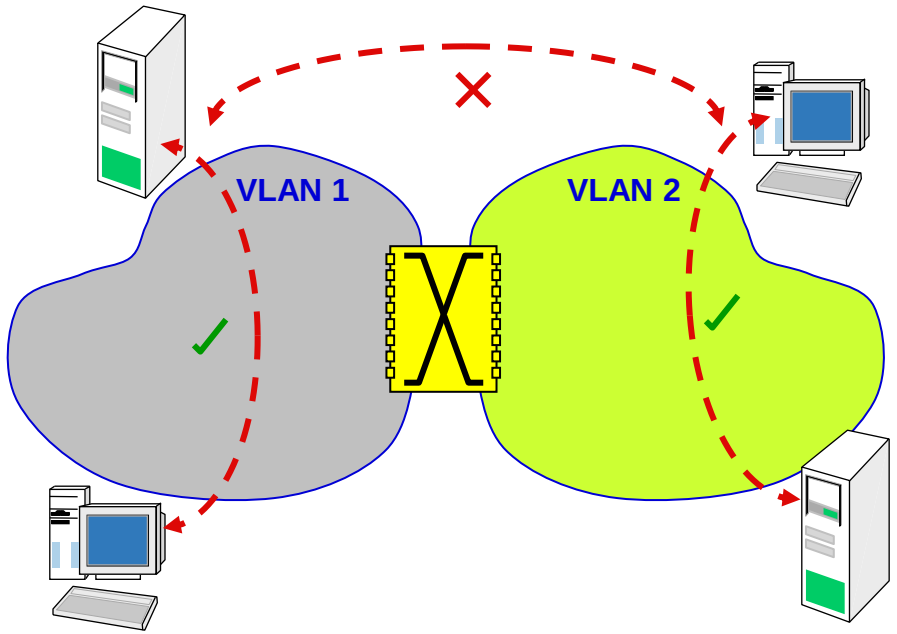
- **Taille max d'une trame CSMA/CD : 1518 octets**
  - **Entête : 14 octets , 1500 octets : charge utile, 4 octets : CRC**
- **Taille max d'une trame 802.1 Q taguée est 1522 octets**
  - **La norme IEEE 802.3ac étend officiellement la longueur de la trame CSM/CD à 1522 octets**
- **Ceci pourrait causer un pb d'interopérabilité avec les anciens équipements**
  - **La solution de contournement : était de modifier les config dans les OS pour limier la charge à 1448 octets (MSS au niveau transport)**

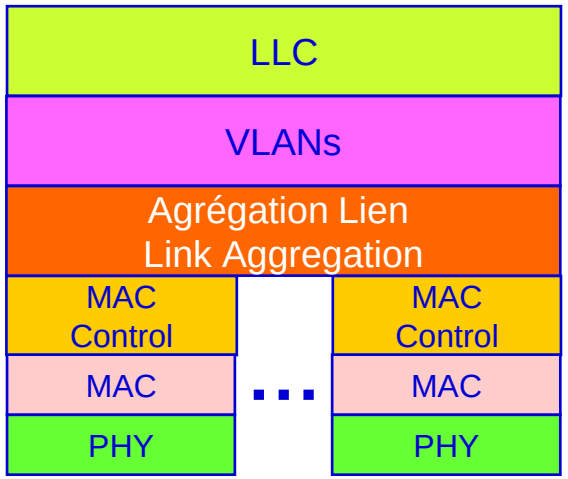


MSS = maximum segment size

Communication inter-VLANs

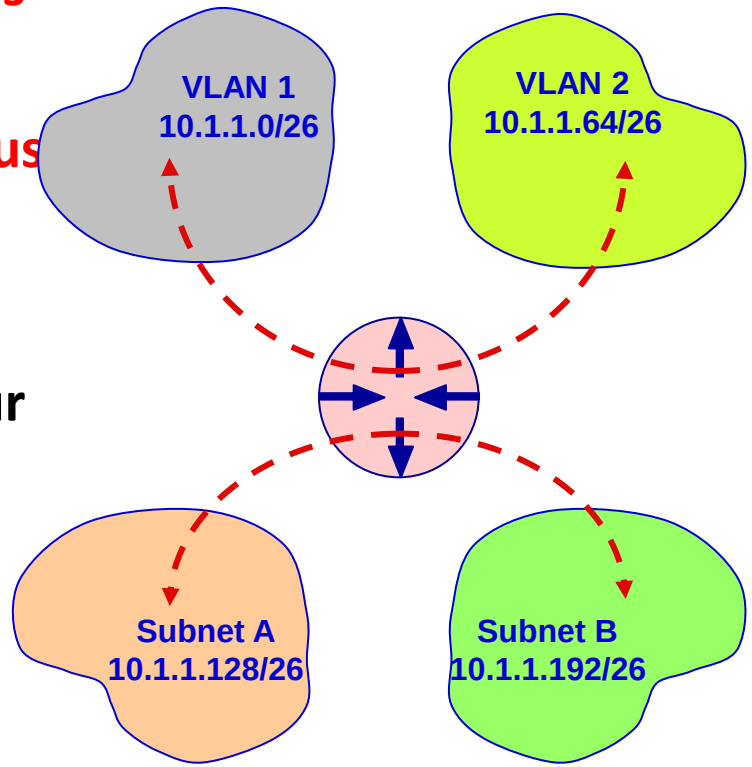
- **Les traitements VLAN empêchent la communication ente plusieurs VLANs**
  - **La couche deux ne forward pas les trames entre les VLANs**
- **Ils Empêchent les opérations au niveau de la couche 2 au delà de la zone d'un VLAN**
  - **Exemple : les broadcast ARP se terminent aux frontière du VLAN**





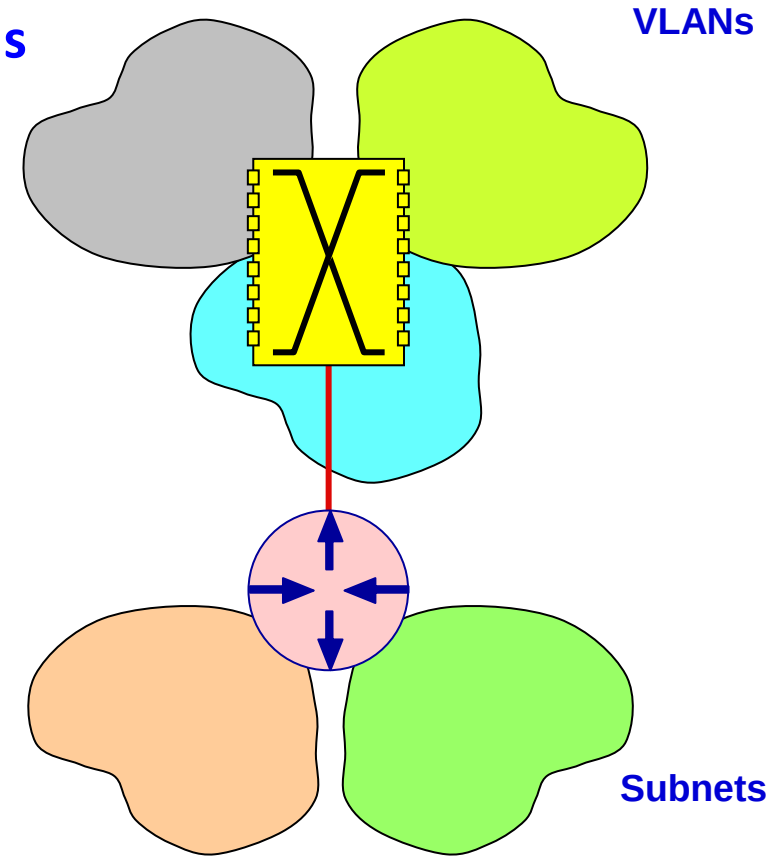
Communication inter-VLANs

- La communication entre VLAN's Nécessité d'utiliser des routeurs pour les communications inter-VLANs
  - Traité de la même manière que la communication entre sous réseaux
- Les VLANs se voient assignées des préfixes réseau
  - Comme s'ils étaient sur deux interfaces séparées du routeur
- Les hôtes comparent le préfixes réseaux (le sein avec celui du réseau de destination)
  - Envoie direct si les deux préfixes sont identiques
    - ⇔ Même VLAN ou sous réseau
  - Envoi via la passerelle (interface du routeur) si les deux préfixes réseau sont différents
- Activé en plaçant l'interface du routeur dans chaque VLAN



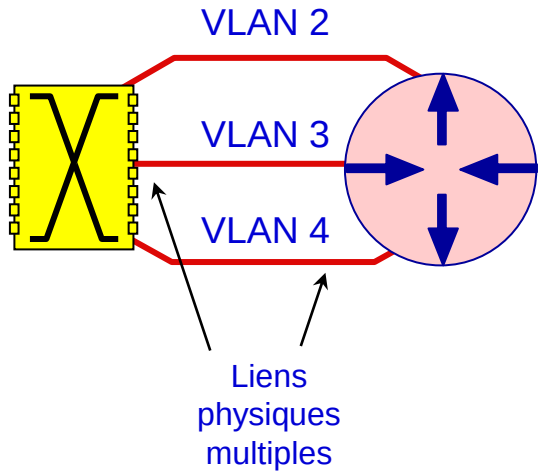
Le rôle du routeur

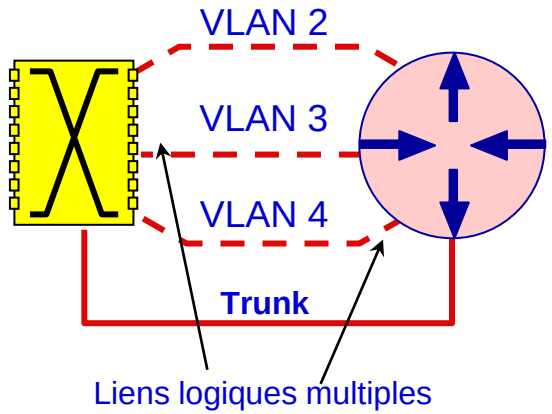
- **Trois Solutions populaires pour la communication inter-VLANs**
  1. **Routeur externe avec des liens multiples**
  2. **Routeur externe avec un seul lien**
  3. **Routeur interne intégré au switch**



Solutions pour la communication inter-VLANs

- **Multiples connexions physiques entre le routeur et le switch**
  - Une connexion physique pour chaque VLAN
  - Logiquement, c'est la même chose que de connecter plusieurs switchs à des ports séparés du routeur
  - Solution nécessaire pour les anciens routeurs
- **Plusieurs connexions logiques sur un seul lien physique Switch – routeur**
  - Décrit comme : «router-on-a-stick»
  - Nécessite une amélioration du système d'exploitation du routeur
- **Connexions logiques multiples sur un lien commutateur-routeur interne**
  - Topologiquement équivalent à la liaison externe commutateur-routeur





Résumé

- **Les VLANs sont devenus de plus en plus populaires**
  - **Et de plus en plus complexe**
- **Plusieurs critères possibles pour la création de VLAN**
  - **Couche 2 : ports de commutation, adresses MAC, groupes multicast**
  - **Couche 3 : type de protocole, adresse L3**
- **Appuie large et préférence pour les VLAN couche 2**
- **Les VLAN multi-switch exigent que les trames MAC soient complétés par des informations VLAN**
  - **Les normes IEEE 802.1p et 802.1Q précisent la méthode de marquage des trames**
- **La communication inter-VLAN nécessite certain type de de routeur**
  - **VLAN traités comme des sous-réseaux à des fins d'adressage et de routage**

Fin du chapitre

Pause-réflexion sur le chapitre

Avez-vous des questions ?