


Chapitre 4

Les Réseau Locaux Virtuels

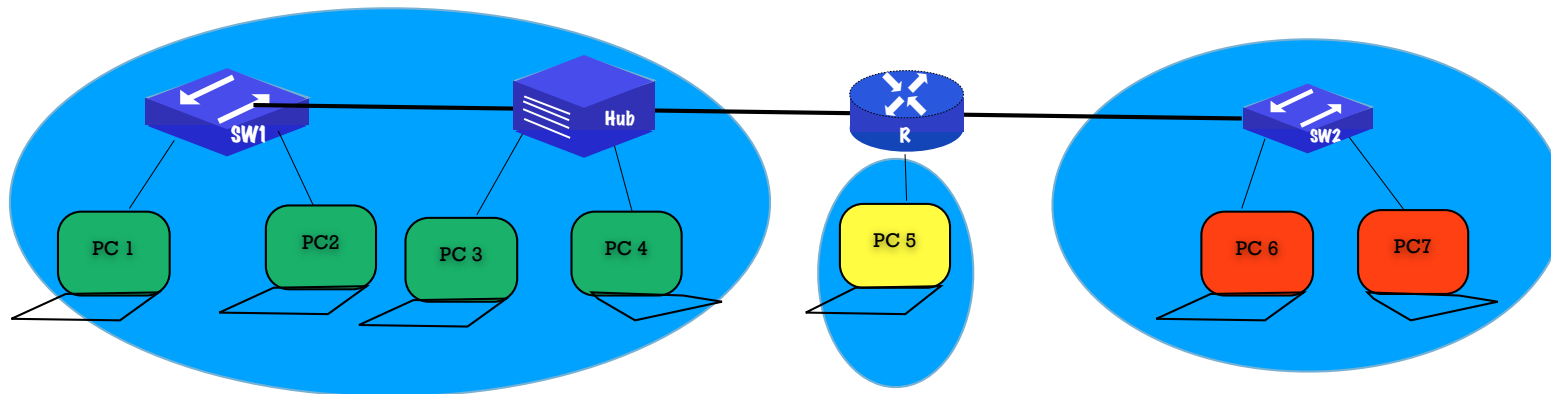


Objectifs

- Expliquer les fonctions des VLAN
 - Expliquer le transfert des trames dans un environnement de commutateurs avec VLAN
 - Attribution d'un port de commutateur à un VLAN
 - Configuration de port trunk
- 

Problématique

© Domaine de collision et domaine de diffusion



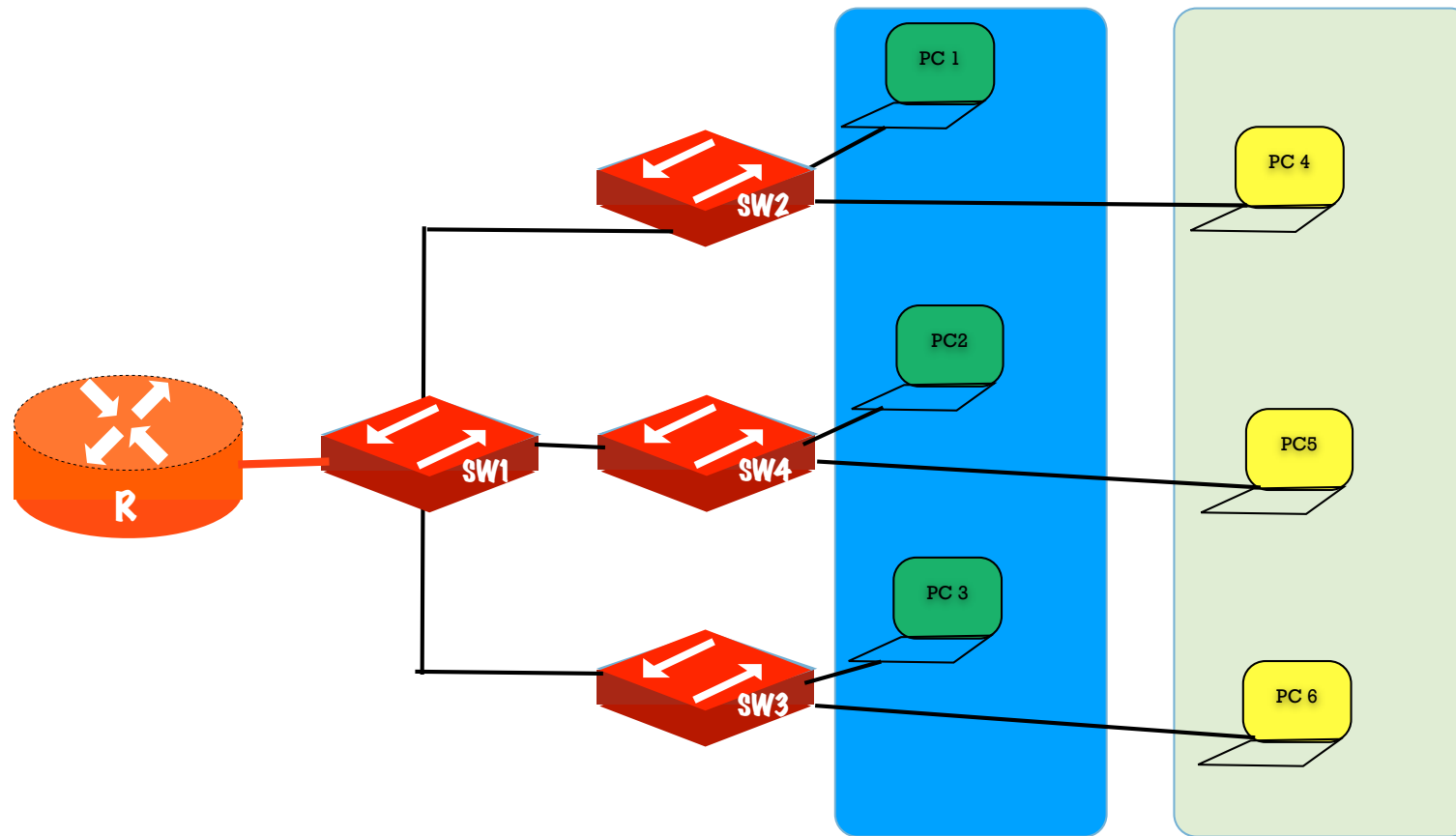
- Segmentation en sous réseau (niveau 3): plusieurs routeurs pour interconnecter les sous réseaux
- Un VLAN peut être créé sur un commutateur de couche 2 pour réduire la taille des domaines de diffusion



Présentation

- Les VLAN permettent la segmentation d'un réseau au niveau 2
 - Les périphériques d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant,
 - Chaque VLAN est considéré comme un réseau logique distinct, Les VLAN reposent sur des connexions logiques, et non des connexions physiques.
 - Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique.
 - Les paquets monodiffusion, de multidiffusion et de diffusion sont transférés et diffusés uniquement à des stations finales dans le VLAN dont proviennent les paquets.
 - La segmentation du réseau peut être effectuée en fonction des utilisateurs du même service, d'une même équipe etc.
-

Architecture des VLAN



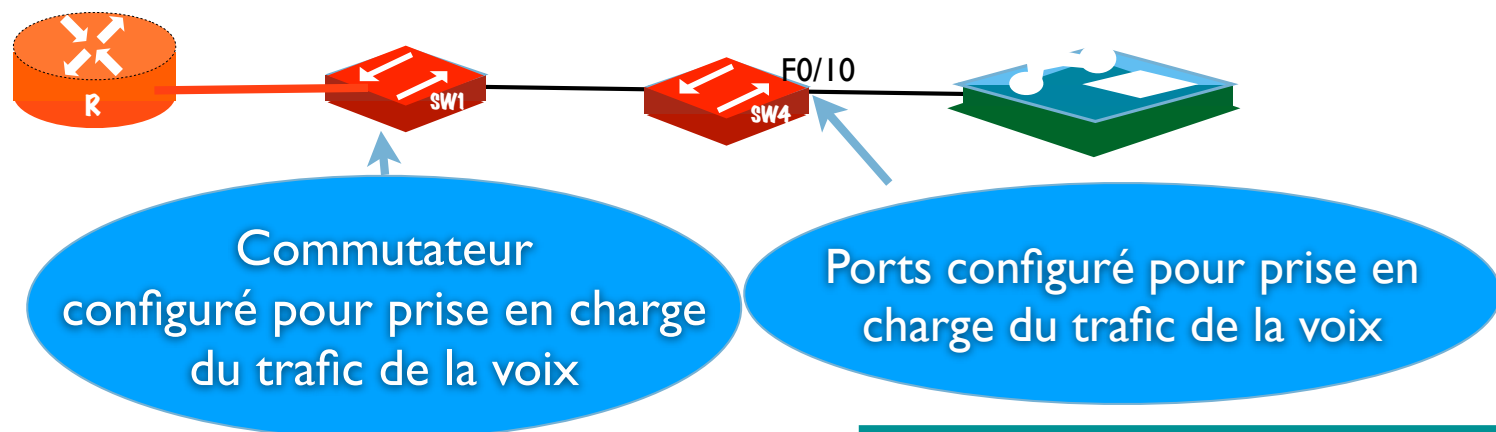
Types de VLAN: le VLAN par défaut

- VLAN par défaut: par défaut, tous les ports de commutateur font partis du VLAN par défaut. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques d'autres commutateurs. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1
- Le VLAN 1 dispose de toutes les fonctions de n'importe quel VLAN, à l'exception du fait qu'il ne peut pas être renommé ni supprimé.
- Avec la commande Switch# **show vlan brief** on visualise que tous les ports sont assignés au VLAN1 par défaut

Types de VLAN: le VLAN défini par le trafic

Il est d'usage de séparer le trafic de voix et de gestion du trafic de données

- * VLAN de données: les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques (appelé VLAN utilisateur)
 - * VLAN PER,
 - * VLAN Etudiants,
 - * VLAN PATS.
- * VLAN de voix: un VLAN est nécessaire pour prendre en charge la voix sur IP (VoIP) qui requiert:
 - * 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 ;
 - * Garantir un délai sur tout le réseau.



Types de VLAN: le VLAN défini par leur fonction

● **VLAN natif:**

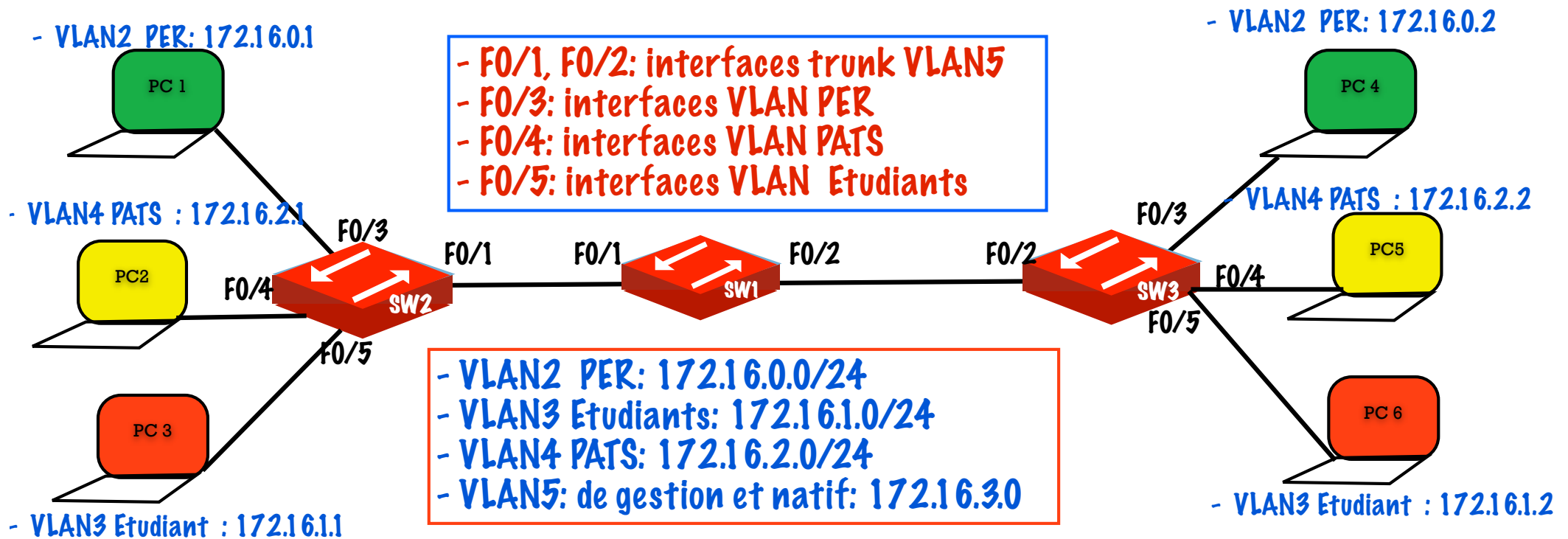
- Un port trunk prend en charge le trafic associé à plusieurs VLAN (trafic étiqueté i.e une étiquette de 4 octets ajoutée dans l'en-tête de trame Ethernet originale et spécifiant le VLAN auquel la trame appartient), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté)
- Le port trunk 802.1Q place le trafic non étiqueté sur le VLAN natif, qui par défaut est le VLAN 1.
- Il est recommandé de:
 - Configurer le VLAN natif comme VLAN inutilisé distinct du VLAN 1 par défaut et des autres VLAN
 - Dédier un VLAN fixe jouant le rôle de VLAN natif pour tous les ports trunk du domaine commuté.

Types de VLAN: le VLAN défini par leur fonction

- Le VLAN de gestion: c'est un VLAN configuré pour accéder aux fonctionnalités de gestion d'un commutateur
 - Par défaut le VLAN 1 est le VLAN de gestion
 - Pour créer un VLAN de gestion, il faut attribuer une adresse IP et un masque de sous-réseau à l'interface virtuelle du commutateur (SVI), ce qui permet de gérer le commutateur via HTTP, Telnet, SSH ou SNMP.
 - Puisque initialement un commutateur Cisco utilise le VLAN 1 par défaut, il n'est pas judicieux de le choisir comme VLAN de gestion.
-

VLAN sur plusieurs commutateurs

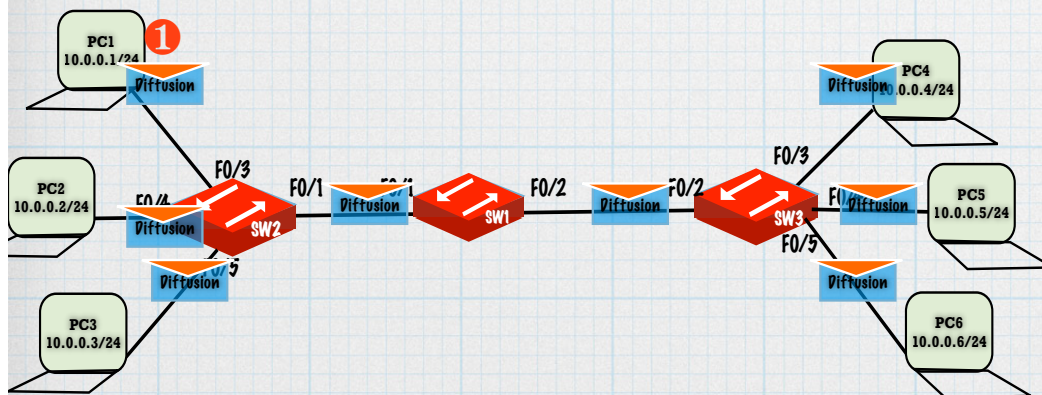
- * Un trunk: c'est une liaison point à point entre deux périphériques réseau qui transporte plusieurs VLAN.
- * Le trunk permet aux périphériques du même VLAN connectés à différents commutateurs de communiquer sans l'intervention d'un routeur.
- * Les liaisons entre SW1, SW2 et SW3 sont configurées pour transmettre le trafic des VLAN 2, 3, 4, 5 sur tout le réseau.



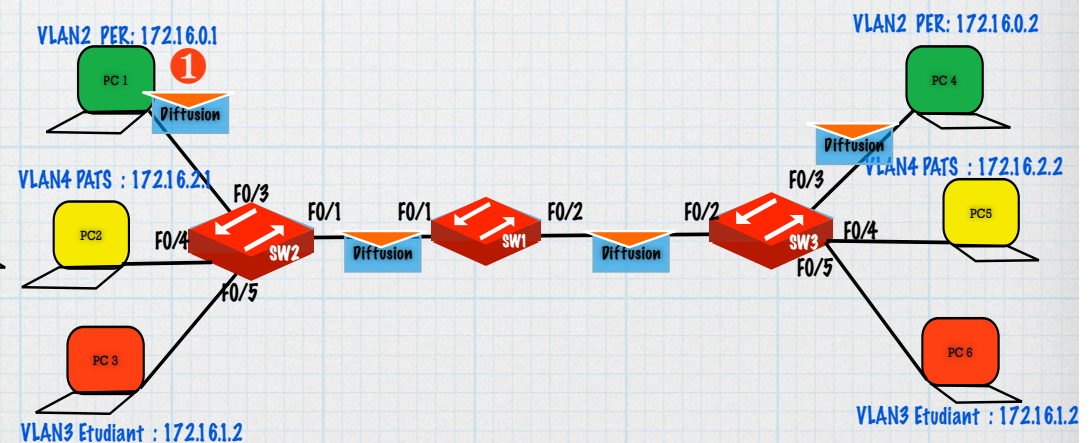
Diffusion et VLAN

* Normalement quand un commutateur reçoit une trame de diffusion, il la transfère par tous les autres ports, à l'exception du port de réception.

* Réseau sans VLAN: dans le sous réseau 10.0.0.0/24, PC1 envoie un message de diffusion qui sera reçu par tous les PC: un seul domaine de diffusion

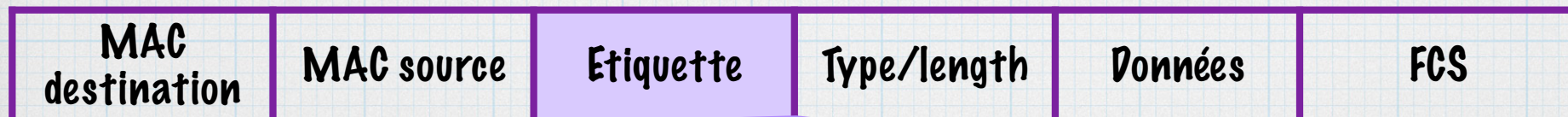
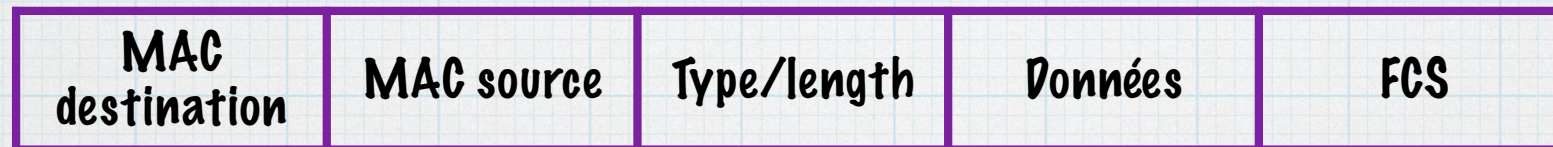


* Réseau avec VLAN: PC1 envoie un message de diffusion qui sera reçu par PC4 du même VLAN PER: plusieurs domaines de diffusion



Etiquetage

- * Pas de table de routage
- * Lorsque le commutateur reçoit une trame sur un port configuré en mode d'accès et associé à un VLAN, il ajoute les informations relatives au VLAN dont elle dépend (c'est l'étiquetage) puis envoie la trame étiquetée sur un port trunk.
- * **Etiquetage**: une étiquette de 4 octets indiquant le VLAN auquel appartient la trame est insérée dans l'entête d'origine de la trame. Ce processus s'effectue à l'aide de l'en-tête IEEE 802.1Q



- * CFI: Canonical Format Identifier pour activer les trames token ring à transmettre sur des liaisons ethernet
- * Priorité utilisateur: relative au service

- * Après insertion de l'étiquette, le FCS est recalculé

Etiquetage et VLAN de voix

- * Un port d'accès utilisé pour connecter un téléphone IP Cisco peut être configuré pour utiliser deux VLAN séparés
- * La liaison entre un commutateur et le téléphone IP fait office de trunk pour acheminer à la fois le trafic du VLAN voix et le trafic (d'un appareil connecté au téléphone IP) du VLAN de données.
- * Un port d'accès peut appartenir à un seul VLAN à la fois. La seule exception à cette règle consiste en un port connecté à un téléphone IP.
- * Dans ce cas, deux VLAN sont associés au port : un pour la voix et l'autre pour les données.

Implémentation de VLAN (1)

- * Les switches de la gamme Catalyst 2960 et 3560 sont compatibles avec plus de 4 000 VLAN dont les VLAN à plage normale sont numérotés de 1 à 1 005 et les VLAN à plage étendue, de 1 006 à 4 094.
- * **Réseaux locaux virtuels à plage normale:** pour les réseaux de petites, moyennes et grandes entreprises.
 - * L'ID de VLAN compris entre 1 et 1 005.
 - * Les ID de 1 002 à 1 005 réservés aux VLAN Token Ring et FDDI.
 - * Les ID 1 et 1 002 à 1 005 sont automatiquement créés et ne peuvent pas être supprimés.
 - * Les configurations sont stockées dans un fichier nommé **vlan.dat** se trouvant dans la mémoire Flash
 - * Le protocole VTP (VLAN Trunking Protocol), qui permet de gérer les configurations VLAN entre les commutateurs, peut uniquement découvrir et stocker les VLAN à plage normale.

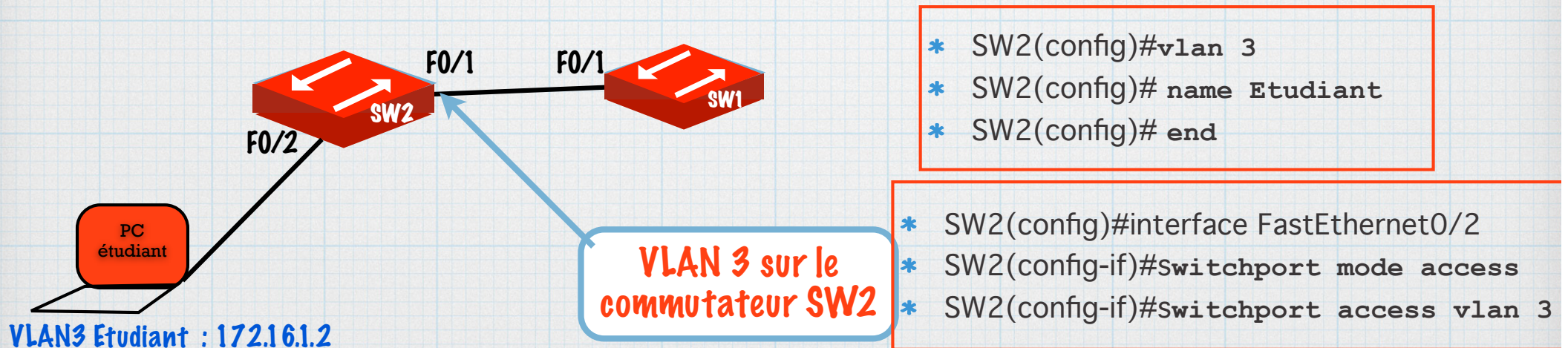
Implémentation de VLAN (2)

* VLAN à plage étendue

- * Certaines multinationales peuvent être suffisamment grandes pour avoir besoin d'une plage étendue d'ID de VLAN.
- * L'ID de VLAN compris entre 1006 et 4094.
- * Les configurations ne sont pas écrites dans le fichier vlan.dat mais dans le fichier de configuration en cours.
- * Le protocole VTP ne prend pas en compte les VLAN à plage étendue.
- * Remarque : 4096 est le nombre maximum de VLAN disponibles sur les commutateurs Catalyst car il y a 12 bits dans le champ d'ID de VLAN de l'en-tête IEEE 802.1Q. le premier ID VLAN disponible 0 et le dernier 4095 sont réservés et ne peuvent donc pas être utilisés.

Implémentation de port d'accès (1)

- * La commande `vlan vlan_id` permet d'ajouter un vlan à un commutateur
- * La commande `vlan vlan_name` permet de nommer le vlan
- * La commande `vlan vlan_id1,vlan_id2,vlan_idn` permet d'ajouter plusieurs VLAN à un commutateur
- * Après création du VLAN, on lui attribue des ports, un port d'accès peut appartenir à un seul VLAN à la fois sauf un port connecté à un téléphone IP
- * La commande `Switchport mode access` définit le port en mode accès
- * La commande `Switchport access vlan_id` met le PC connecté au port dans le vlan `vlan_id`



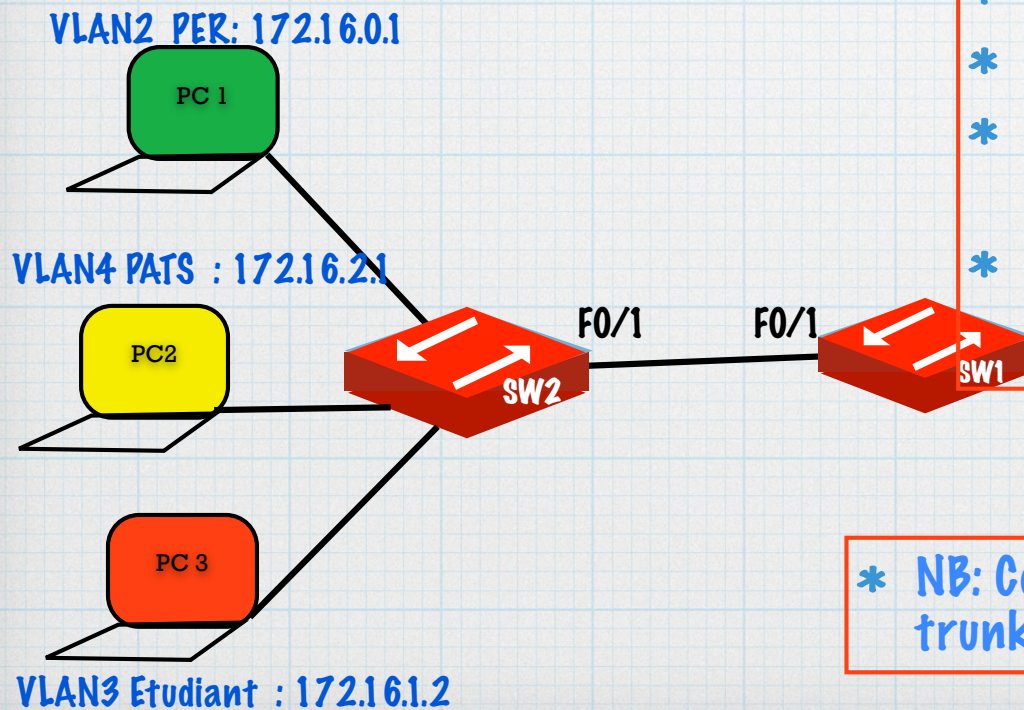
* Attention: 2 PC doivent être dans le même réseau logique, pour communiquer dans le même VLAN

Implémentation de port d'accès (2)

- * La commande (en mode config-if) `no switchport access vlan` fait passer un port du switch en appartenance VLAN 1
 - * L'affectation vers un autre VLAN modifie l'appartenance du port sans besoin de mettre la commande `no switchport access vlan`
 - * La commande `no vlan vlan-id` permet de supprimer le VLAN `vlan-id` du commutateur
 - * La commande `delete flash:vlan.dat` (en mode d'exécution privilégié) supprime le fichier `vlan.dat` et après le redémarrage du commutateur, les VLAN configurés disparaissent
- * SW2(config)#interface FastEthernet0/2
 - * SW2(config-if)#no switchport access vlan
 - * SW2(config)# end
- * Attention : avant de supprimer un VLAN, réattribuez d'abord tous ses ports. Sinon tous les ports non déplacés vers un VLAN actif ne pourront plus communiquer avec d'autres hôtes une fois le VLAN supprimé.
 - * Pour ramener un commutateur à ses réglages d'usine par défaut, utilisez les commandes `delete flash:vlan.dat` et `erase startup-config`.

Implémentation de port trunk (1)

- * Pour activer les liaisons trunk, configurez les ports sur chaque extrémité de la liaison physique
- * la commande `switchport mode trunk` configure un port du switch sur l'extrémité d'une liaison trunk et force la liaison à devenir une liaison trunk même si l'interface connectée n'est pas configurée
- * Par défaut, tous les VLAN sont autorisés sur une liaison trunk, la commande `switchport trunk allowed vlan vlan-list` précise la liste des VLAN à autoriser sur la liaison trunk.
- * Le VLAN natif doit également être changé, et ne plus être le VLAN 1, mais n'importe quel autre VLAN: `switchport trunk native vlan vlan id`



- * SW1(config)#interface FastEthernet0/1
- * SW1(config-if)#switchport mode trunk.
- * SW1(config-if)#switchport trunk native vlan 5
- * SW1(config-if)#switchport trunk allowed vlan 2,3,4,5

* NB: Configurez toujours les deux extrémités d'une liaison trunk avec le même VLAN natif.

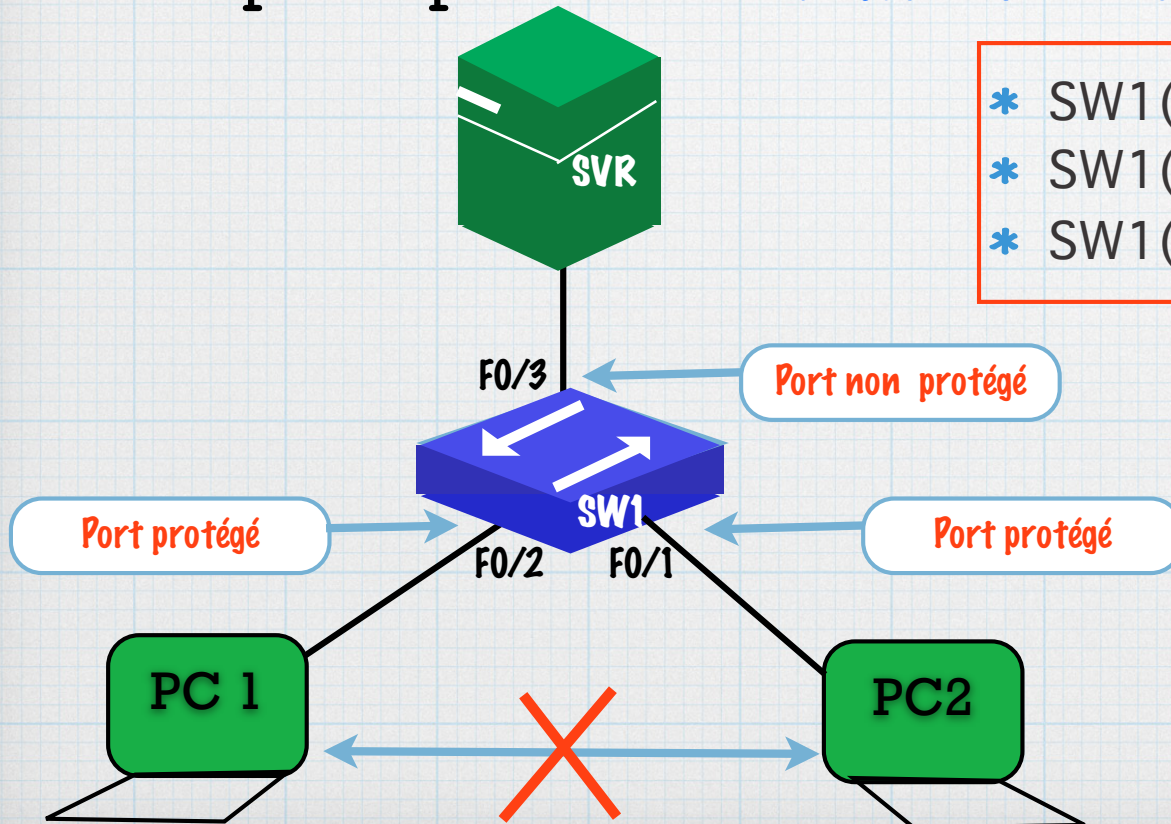
Implementation de port trunk (2)

- * La commande `no switchport trunk allowed vlan` supprimer les VLAN autorisés
- * La commande `no switchport trunk native vlan` réinitialiser le VLAN natif du trunk.
- * Une fois réinitialisée sur l'état par défaut, le trunk autorise tous les VLAN et utilise le VLAN 1 comme VLAN natif.
- * La commande `switchport mode access` supprime la fonctionnalité de trunk d'un port
- * la commande `show mac address-table` afficher la table d'adresses MAC et vérifie que les adresses ont été apprises sur le VLAN auquel le port est attribué.

```
* SW1(config)#interface FastEthernet0/1
* SW1(config-if)#no switchport trunk allowed vlan 2,3,4,5
* SW1(config-if)# no switchport trunk native vlan 5
* SW1(config-if)#no switchport mode access trunk
```


Implémentation de port protégé

- * Pour certaines applications le trafic généré par un PC ne doit pas être accessible par un autre PC du même commutateur
- * L'utilisation de la fonction Périphérie PVLAN (Private VLAN), appelée « **ports protégés** », garantit qu'il n'existe aucun échange de trafic monodiffusion, diffusion ou multidiffusion entre ces ports sur le commutateur.
- * Un port protégé ne transmet aucun trafic à aucun autre port étant également un port protégé, sauf pour le trafic de contrôle
- * La commande (en mode de config-if) `switchport protected` et `no switchport protected` active ou de désactive un port protégé.



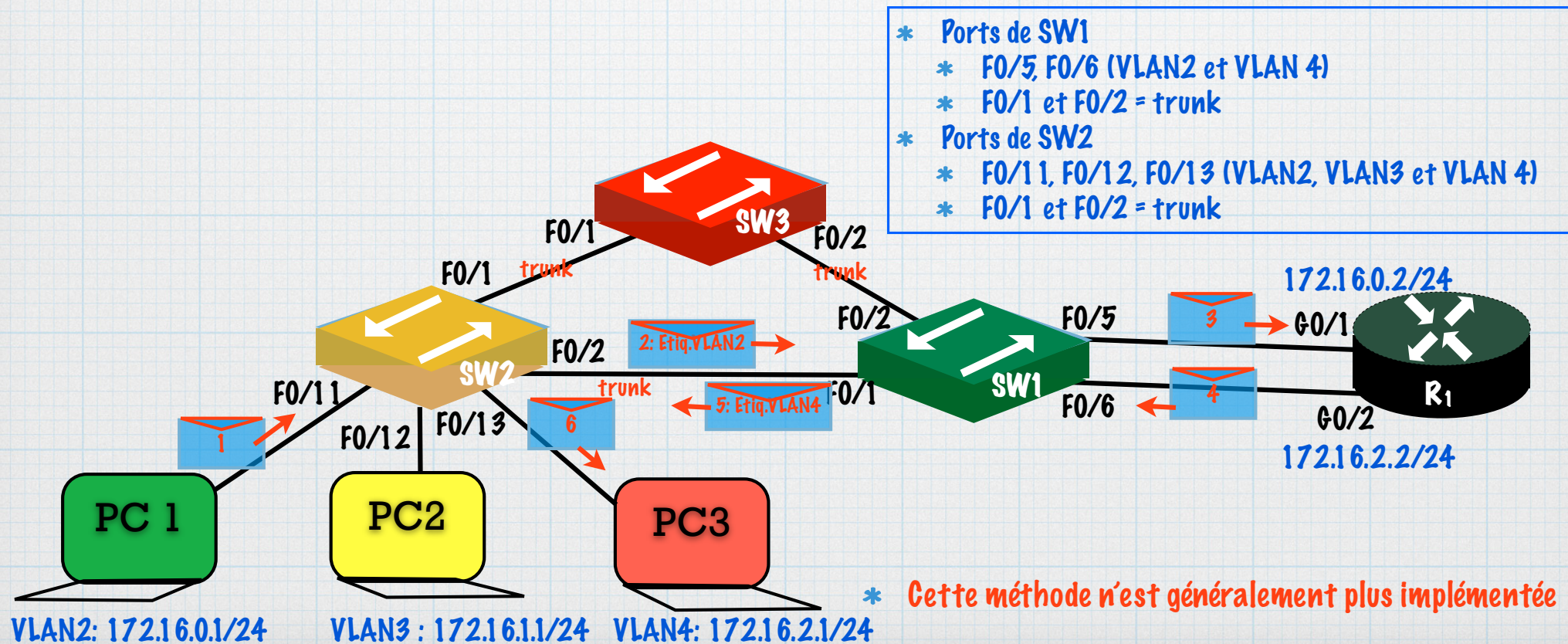
- * `SW1(config)#interface FastEthernet0/1`
- * `SW1(config-if)#switchport protected`
- * `SW1(config-if)#end`

Routage inter-VLAN

- * Étant donné que les VLAN ont segmenté le réseau, un processus de couche 3 est requis pour permettre au trafic de se déplacer entre VLAN
- * Les commutateurs cisco de couche 2 ont des fonctionnalités IPv4 et IPv6 très limitées et ne peuvent pas exécuter la fonction de routage dynamique des routeurs
- * Le processus de routage de couche 3 peut être mis en œuvre avec un routeur ou un commutateur de couche 3

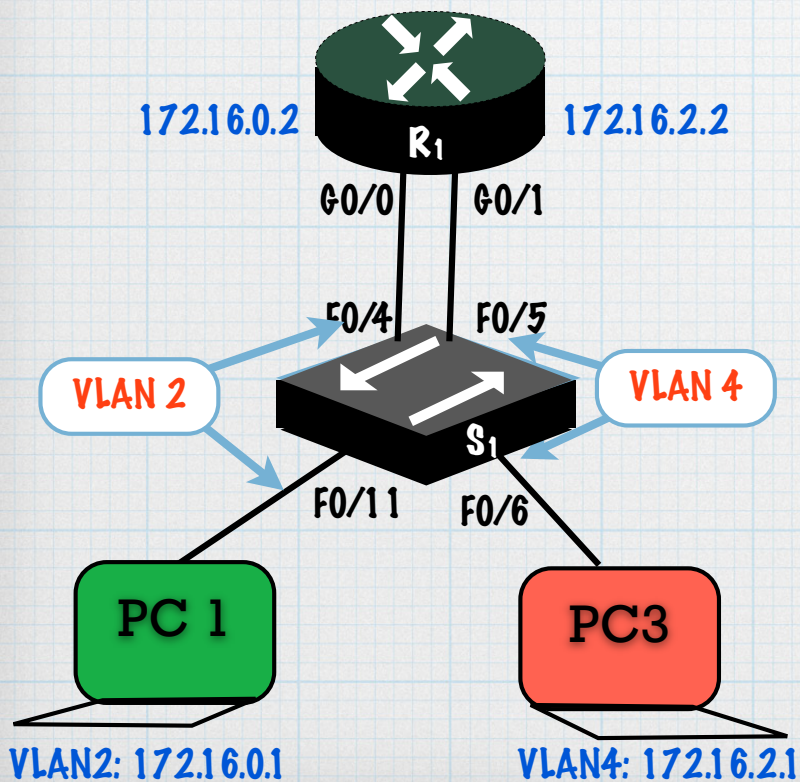
Routage inter-VLAN: Solution 1

- * Solution traditionnelle avec un routeur dont les interfaces sur des sous réseaux distincts sont connectées à des **port d'accès** de commutateur
- * Chaque interface physique du routeur est affectée à un VLAN distinct et accepte le trafic du VLAN associé à l'interface du commutateur à laquelle elle est connectée
- * **Exemple: PC1 du VLAN2 communique avec PC3 du VLAN4**



Configuration: Solution 1

- * Les ports F0/4 et F0/5 sont à configurer respectivement pour les VLAN 2 et 4.
- * Les interfaces F0/4 et F0/11 ont été affectées au VLAN 2 et F0/5 et F0/6 au VLAN 4
- * Pour la **configuration du routeur**, on attribue les adresses 172.16.0.2 et 172.16.2.2 respectivement à G0/0 et G0/1
- * Les PC doivent avoir une adresse IP un masque de sous-réseau et une gateway

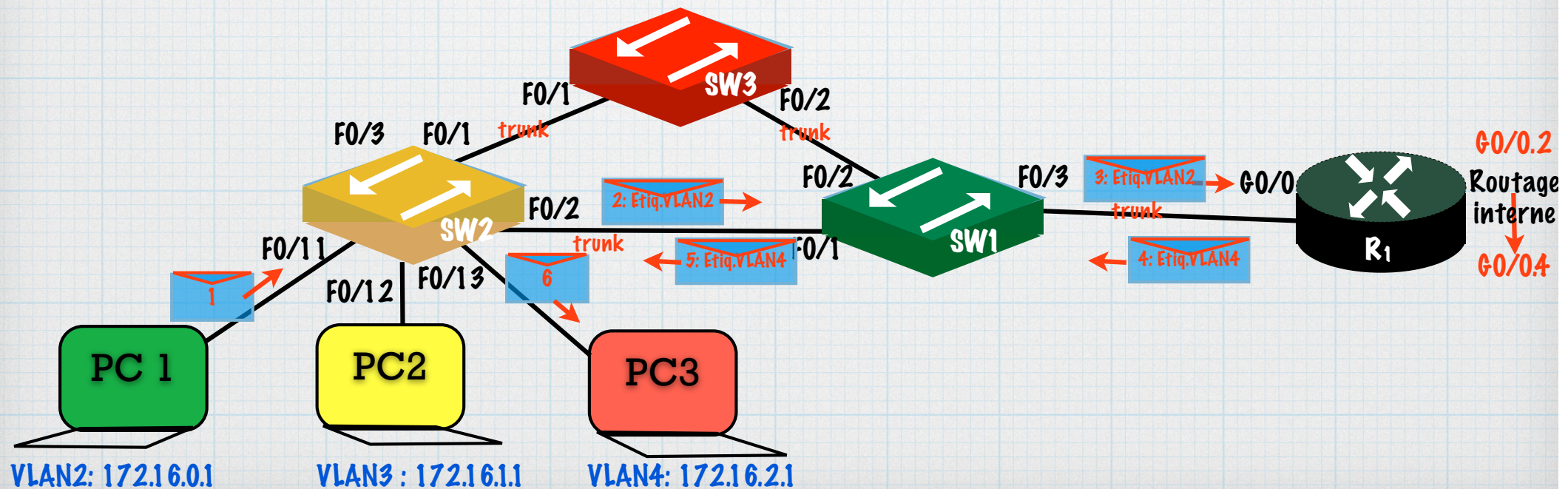


* Configuration du switch

- * S1(config)#vlan 2
- * S1(config-vlan)#vlan 4
- * S1(config-vlan)# interface F0/11
- * S1(config-if)#switchport access vlan 2
- * S1(config-if)# interface F0/4
- * S1(config-if)#switchport access vlan 2
- * S1(config-vlan)# interface F0/5
- * S1(config-if)#switchport access vlan 4
- * S1(config-if)# interface F0/6
- * S1(config-if)#switchport access vlan 4
- * S1(config-if)#end

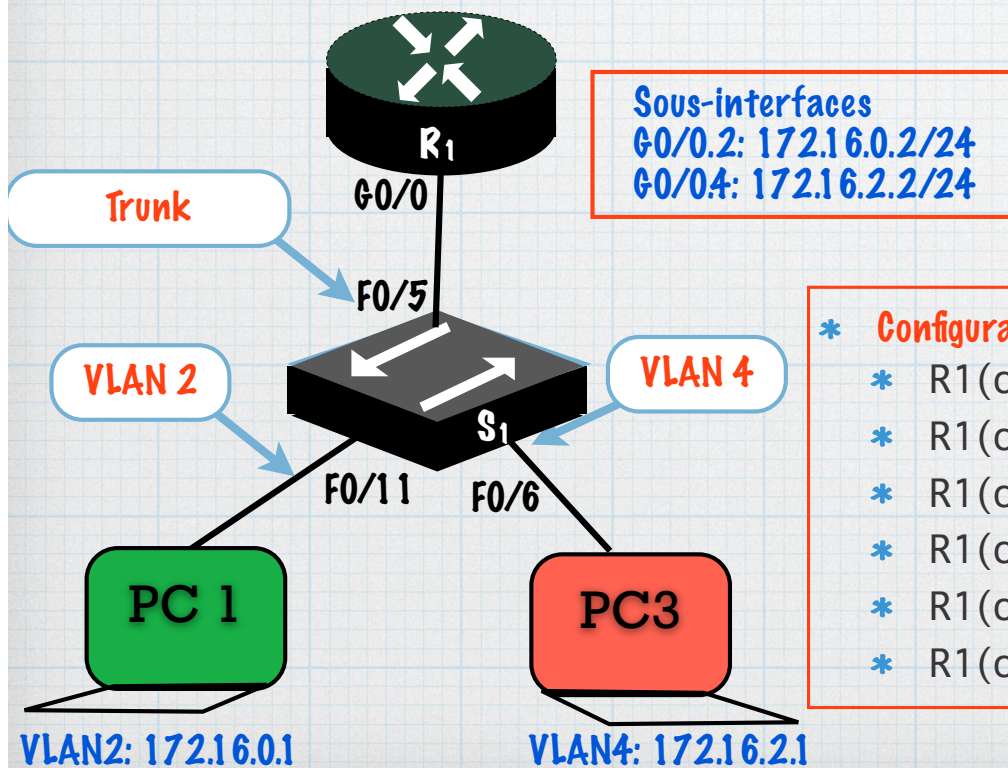
Routage inter-VLAN: Solution 2 (Router on a stick)

- * **Router-on-a-stick** est équivalent au modèle de routage inter-VLAN de la solution 1, mais au lieu d'interfaces physiques, il utilise les sous-interfaces d'une seule interface physique pour effectuer le routage.
- * L'interface du routeur est configurée en tant que liaison trunk avec une interface du commutateur pour acheminer les paquets entre VLAN.
- * Le routeur accepte le trafic étiqueté sur l'interface trunk provenant du switch et procède ensuite au routage interne entre-VLAN à l'aide de sous-interfaces (interfaces virtuelles) associées à une interface physique.
- * Les sous-interfaces sont configurées avec une adresse IP appartenant à des sous-réseaux différents et affectées (de par leur IP) aux VLAN.
- * **Exemple: PC1 du VLAN2 communique avec PC3 du VLAN4:**



Configuration du Router on a stick

- * Activer le trunking sur le port F0/5 du switch connecté au routeur, le trunk n'a pas besoin d'être attribuée à un VLAN
- * Création des sous-interfaces pour chaque VLAN unique sur le réseau et chaque sous-interface reçoit une adresse IP de son sous-réseau de VLAN
- * La commande de mode de configuration globale **interface** `interface_id subinterface_id` crée une sous interface.
- * Avant de recevoir une adresse IP, une sous-interface doit être configurée pour fonctionner sur un VLAN spécifique à l'aide de la commande **encapsulation dot1q** `vlan_id`



* Configuration du switch

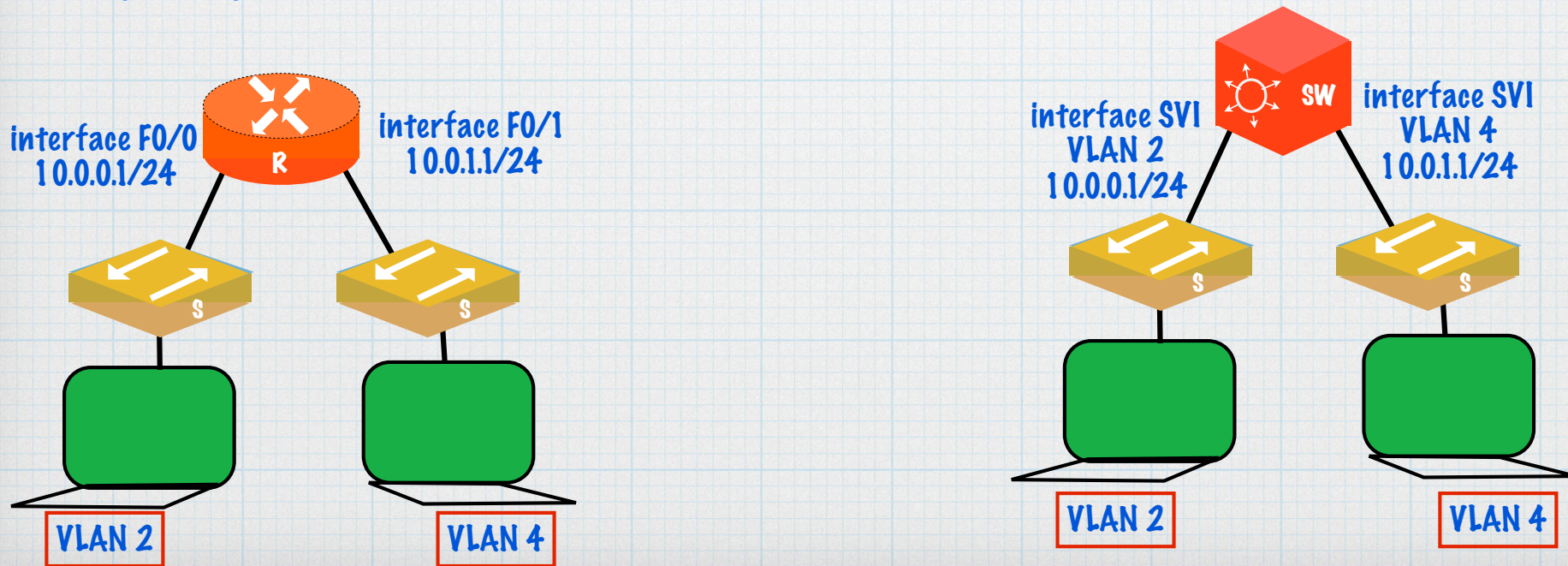
- * R1(config)# interface G0/0.2
- * R1(config-subif)#encapsulation dot1q 2
- * R1(config-subif)#ip address 172.16.0.2 255.255.255.0
- * R1(config)# interface G0/0.4
- * R1(config-subif)#encapsulation dot1q 4
- * R1(config-subif)#ip address 172.16.2.2 255.255.255.0

Commutateur de couche 3

- Les commutateurs de couche 3 offrent généralement plus de débits que les routeurs.
- Ils peuvent être configurés en tant que passerelles de couche 3 pour les utilisateurs de chaque VLAN de commutateur d'accès.
- Ils prennent en charge les types d'interfaces de couche 3 suivants:
 - * **Port routé** : interface de couche 3 pure similaire à une interface physique sur un routeur Cisco IOS.
 - * **Interface virtuelle de commutateur (SVI)**
 - * Peut assurer les mêmes fonctions pour le VLAN qu'une interface de routeur et peut être configurée à peu près de la même manière (adresse IP, listes de contrôle d'accès, etc.).
 - * Par défaut, une interface SVI est créée pour le VLAN par défaut (VLAN 1) pour l'administration à distance du commutateur

Routage inter-VLAN via SVI

- * Des utilisateurs de VLAN différents constituent généralement des sous-réseaux distincts. Par conséquent, il est logique de configurer les commutateurs de distribution en tant que passerelles de couche 3 pour les utilisateurs de chaque VLAN de commutateur d'accès.
- * Ainsi chaque commutateur de distribution doit avoir des adresses IP qui correspondent à chaque VLAN de commutateur d'accès.



Routage inter-VLAN via ports routés

- * Contrairement à un port d'accès, un port routé n'est pas associé à un VLAN spécifique. Un port routé se comporte comme une interface de routeur normale.
- * Les ports routés sur un commutateur Cisco IOS ne prennent pas en charge les sous-interfaces.
- * Pour configurer des ports routés, utilisez la commande en mode de configuration d'interface `no switchport` sur les ports appropriés

* Création des SVI sur SW1

- * `S1(config)# interface vlan 2`
- * `S1(config-if)# ip address 10.0.0.2 255.255.255.0`
- * `S1(config)# interface vlan 3`
- * `S1(config-if)# ip address 10.0.1.2 255.255.255.0`

* Activation du routage sur SW1

- * `SW1(config)# ip routing`

VLAN 2

VLAN 3

ports routés

Liaisons Trunk

* Ports routés

- * `SW2(config)# interface F0/1`
- * `SW2(config-if)# no switchport`
- * `SW2(config-if)# ip address 10.0.10.1`
- * Idem pour F0/1 de SW1

* Création SVI sur SW2

- * `S2(config)# interface vlan 4`
- * `S1(config-if)# ip address 10.0.2.2 255.255.255.0`

* Activation du routage sur SW2

- * `SW2(config)# ip routing`

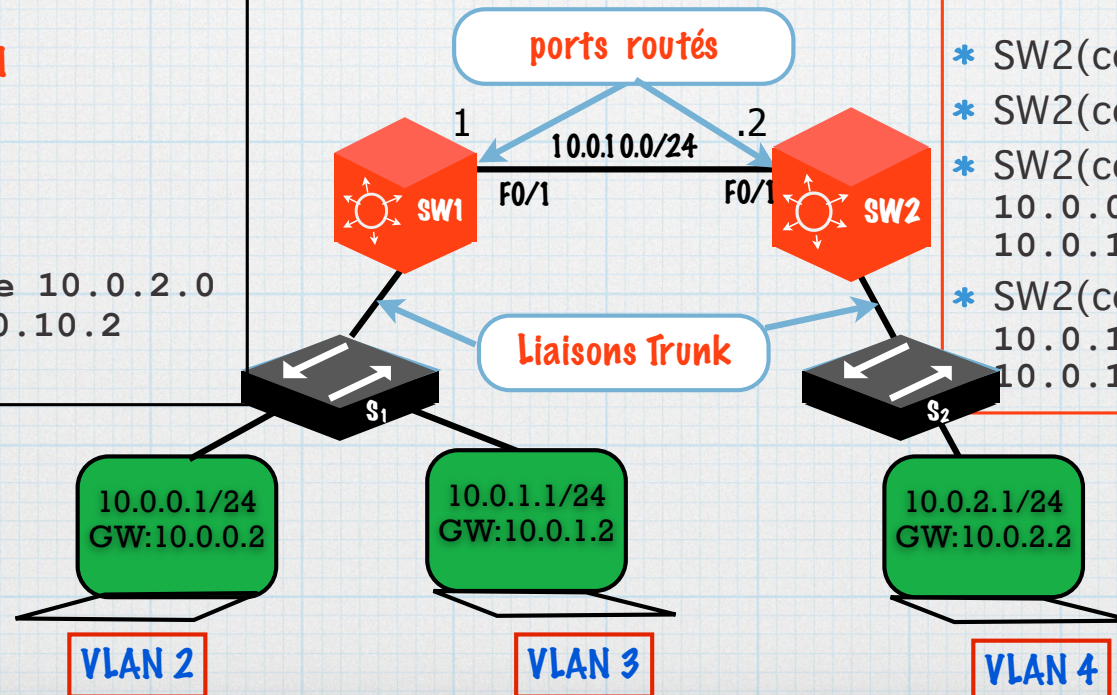
VLAN 4

Routage inter-VLAN via ports routés

- * Les VLANs 2 et 3 doivent être créés sur le SW1 et le VLAN4 sur le SW2.
- * Le routage statique ou dynamique (comme dans le cas d'un routeur) doit être configuré sur SW1 et SW2 pour que le VLAN 4 puisse communiquer avec les VLAN 2 et 3.
- * Sans le routage (statique ou dynamique), le routage entre le VLAN2 et le VLAN 3 est assuré par le SW1.

* Création des SVI sur SW1

```
* S1(config)#  
* S1(config)# vlan 2  
* S1(config)# vlan 3  
* S1(config)# ip route 10.0.2.0  
255.255.255.0 10.0.10.2
```



```
* SW2(config)#  
* SW2(config-if)#vlan 4  
* SW2(config-if)#ip route  
10.0.0.0 255.255.255.0  
10.0.10.1  
* SW2(config-if)#ip route  
10.0.1.0 255.255.255.0  
10.0.10.1
```