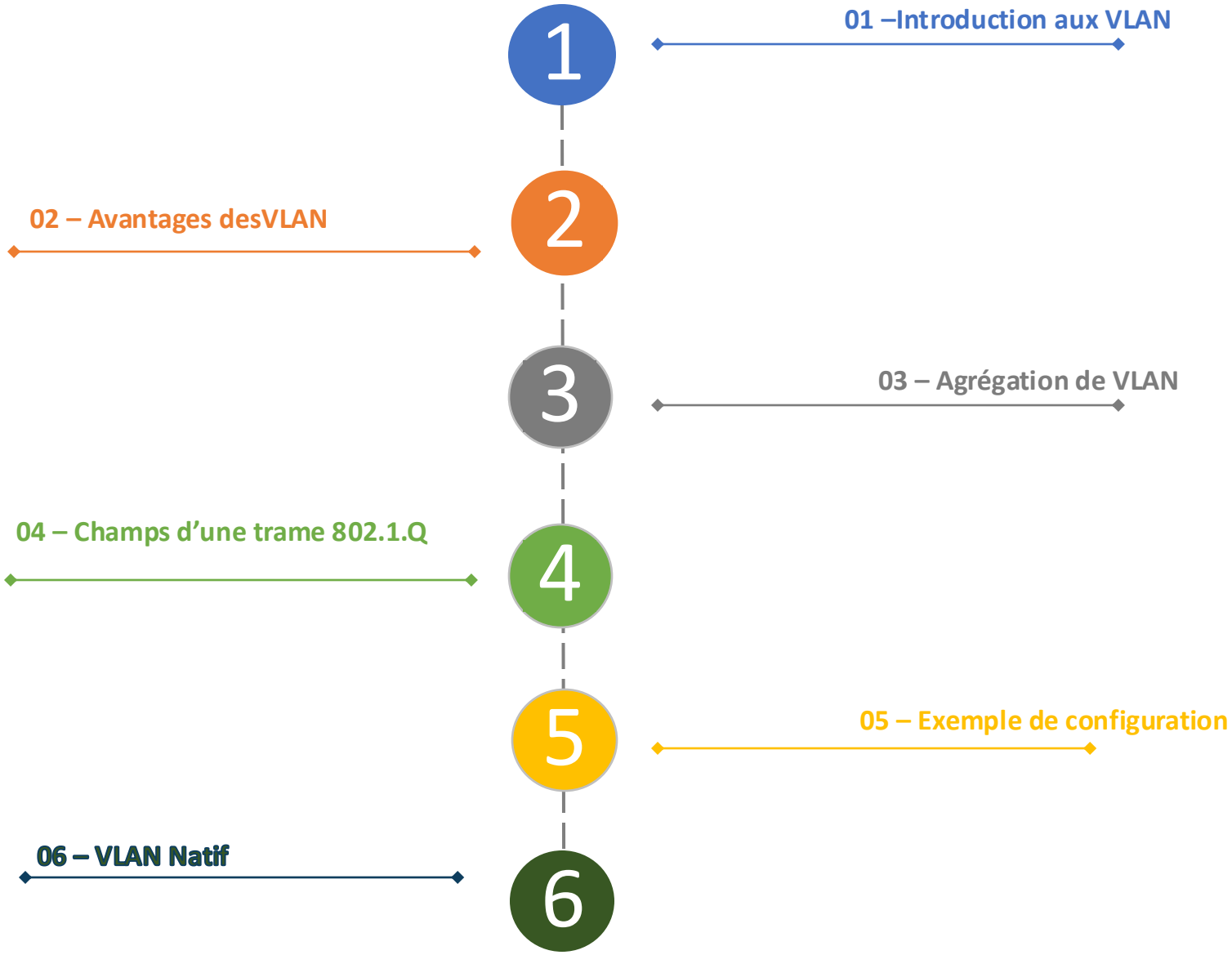
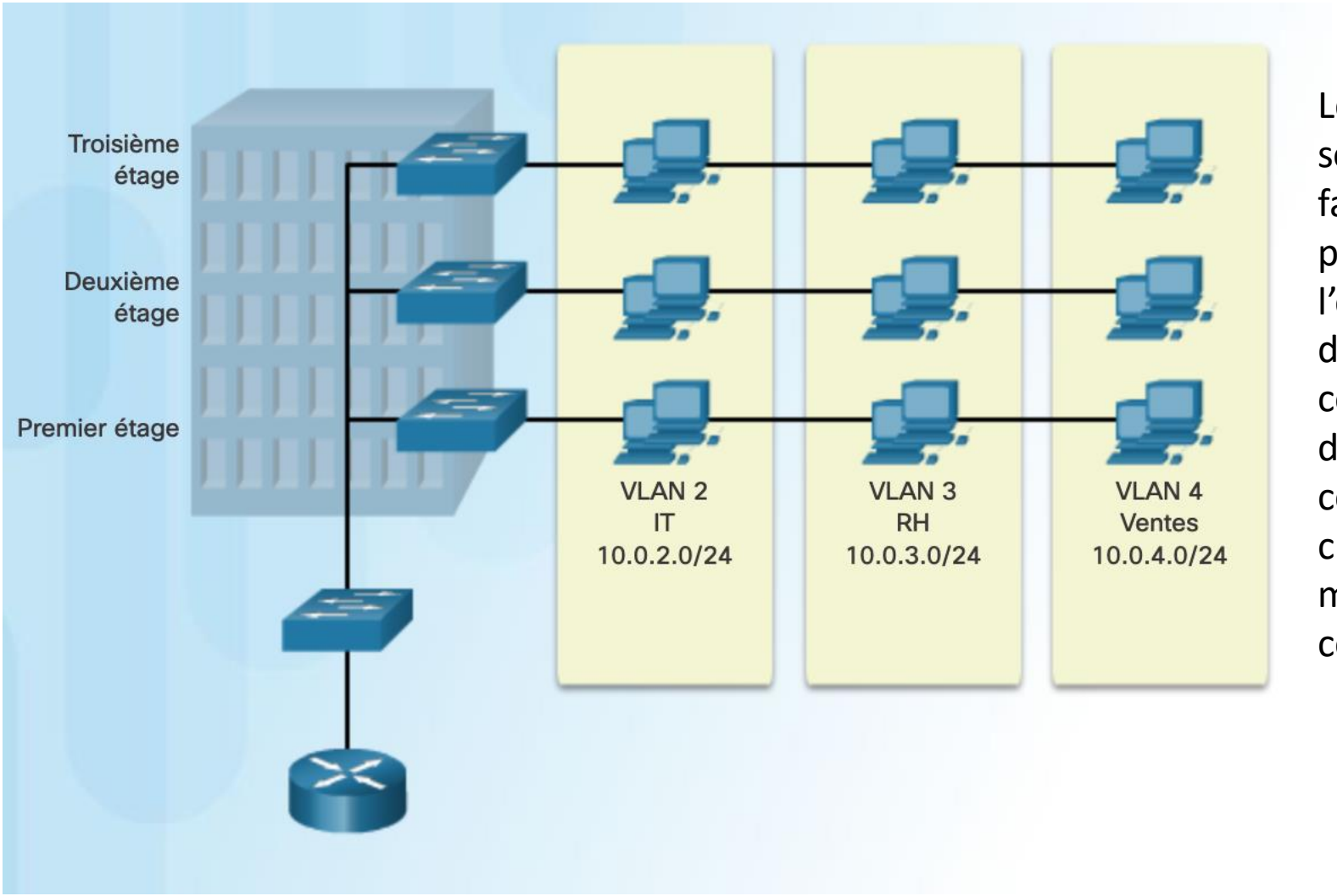
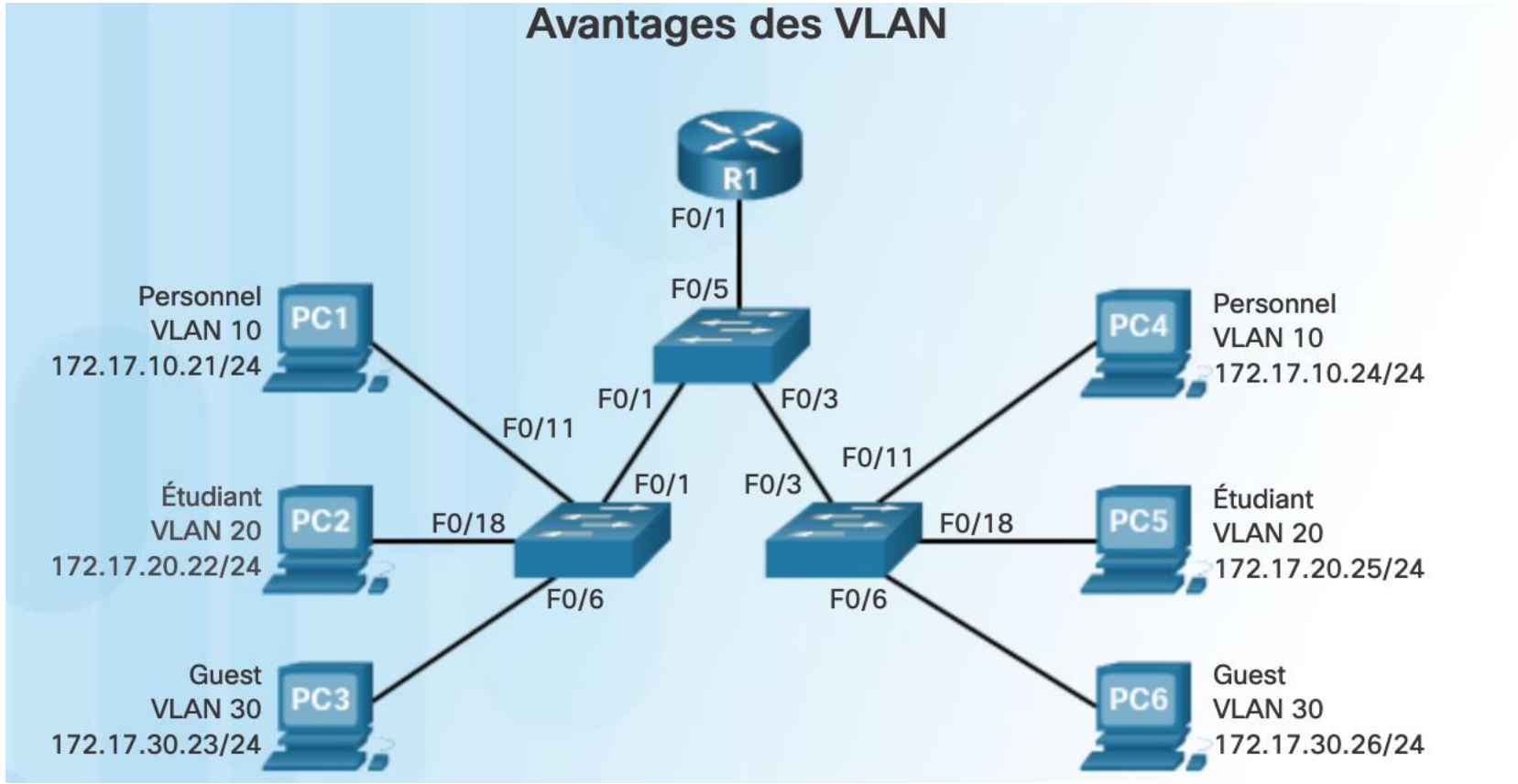
PLAN :


1
01 –Introduction aux VLAN
2
02 – Avantages desVLAN
3
03 – Agrégation de VLAN
4
04 – Champs d’une trame 802.1.Q
5
05 – Exemple de configuration
6
06 – VLAN Natif

Les VLANs



Les VLAN 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. Les appareils d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN.



Les principaux avantages des VLAN sont les suivants :

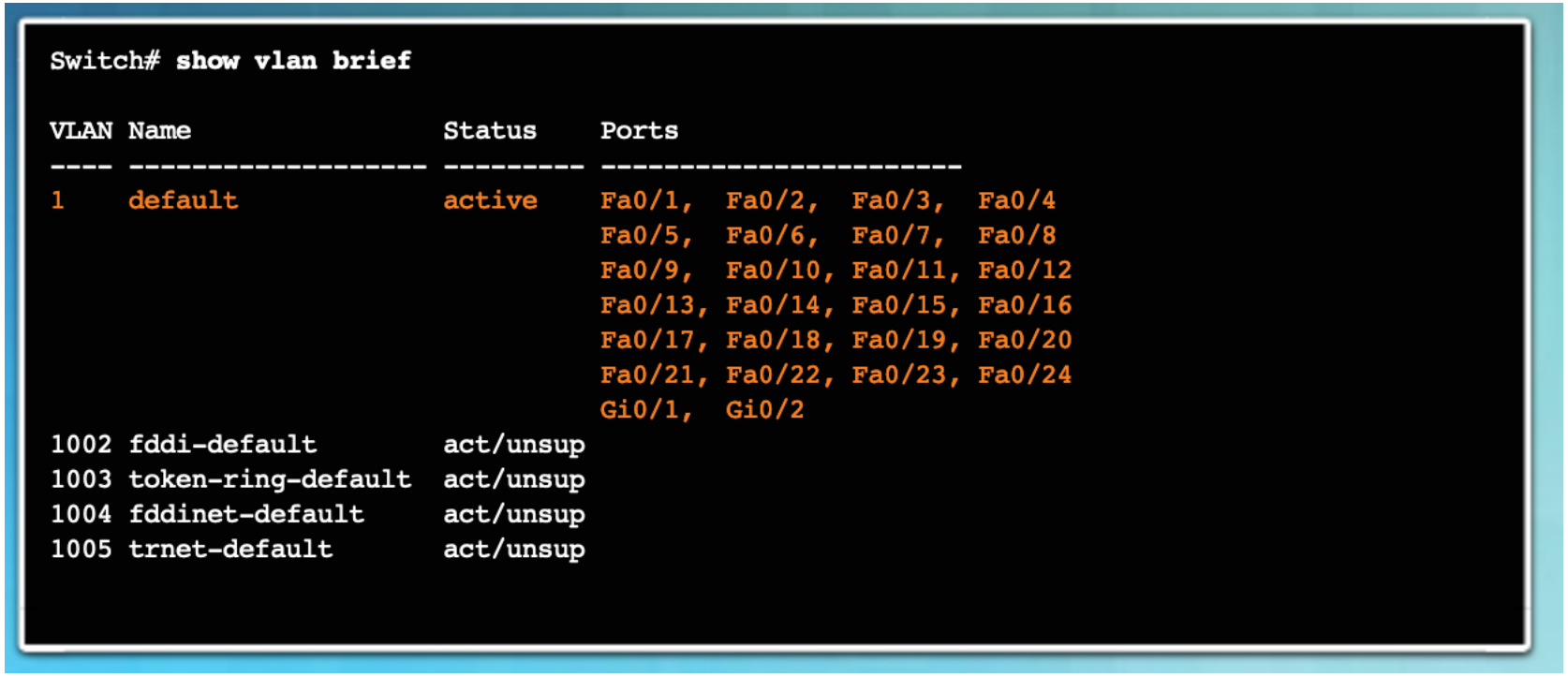
Sécurité

Réduction des coûts

Meilleures performances

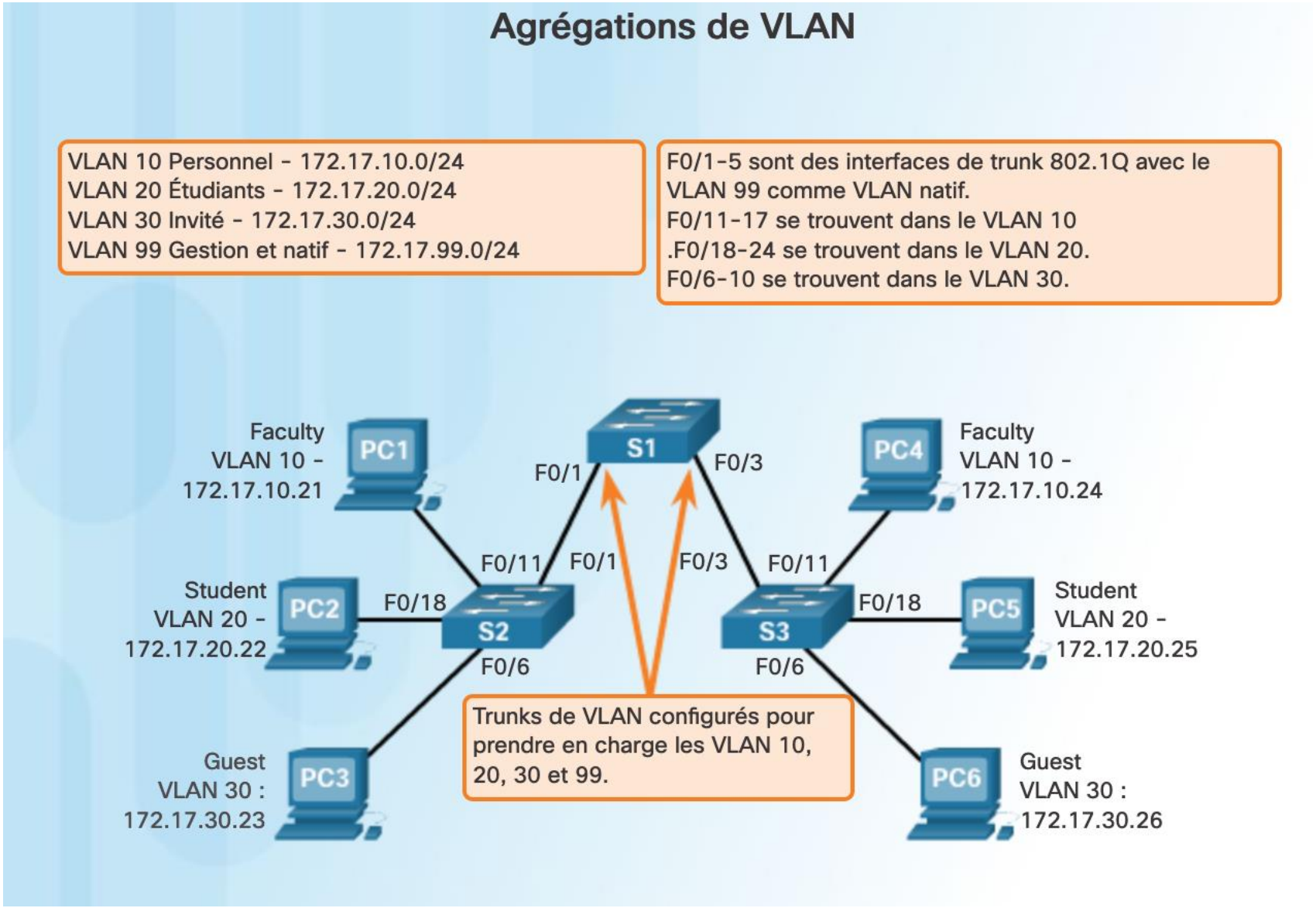
Réduction de la taille des domaines de diffusion

Efficacité accrue du personnel informatique



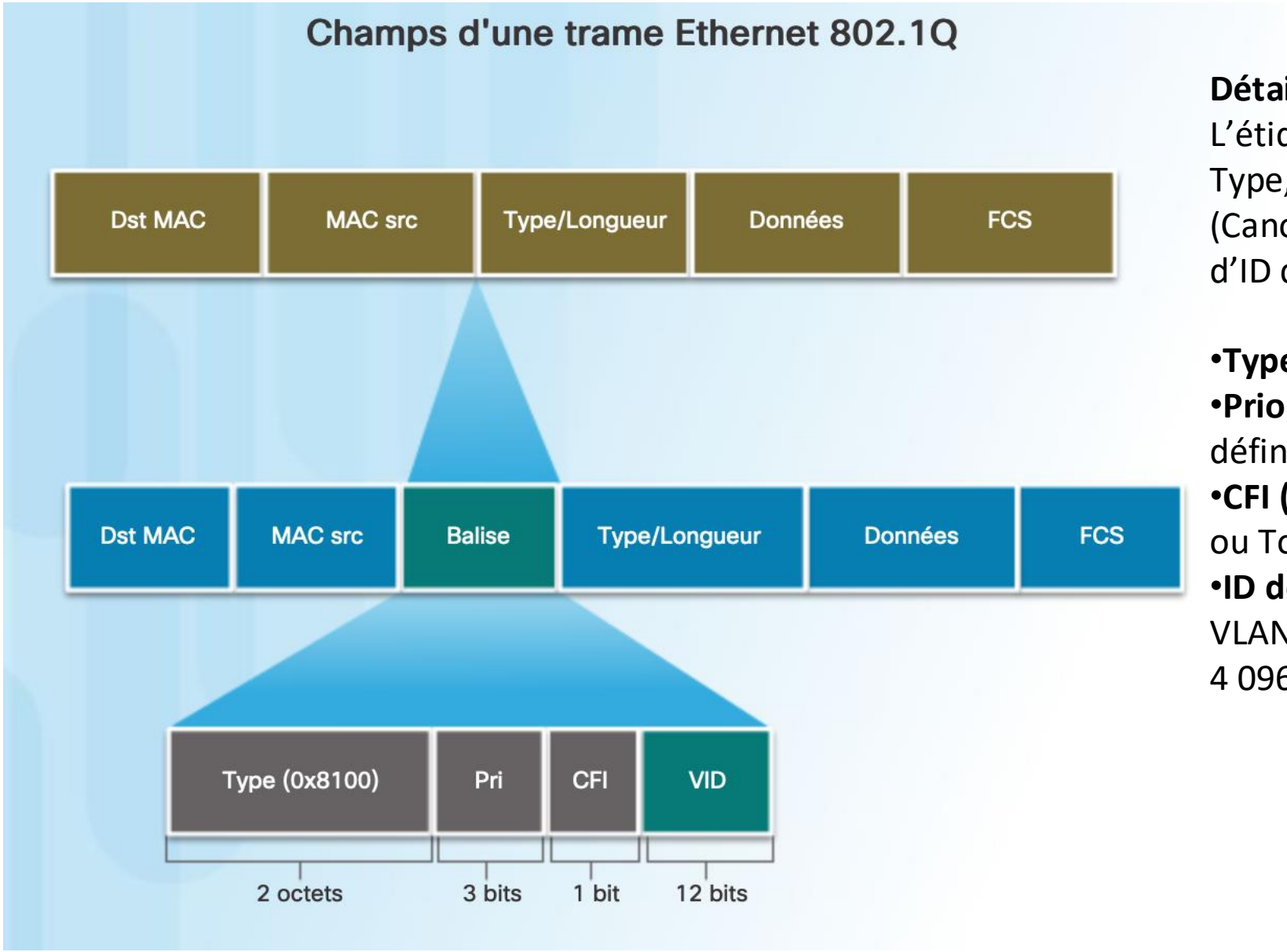
VLAN par défaut

Tous les ports de commutateur font partie du VLAN par défaut 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. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1. Dans la figure, la commande **show vlan brief** a été émise sur un commutateur utilisant la configuration par défaut. Notez que tous les ports sont assignés au VLAN 1 par défaut.



Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN. Un trunk de VLAN permet d'étendre les VLAN à l'ensemble d'un réseau. Cisco prend en charge la norme IEEE 802.1Q pour la coordination des trunks sur les interfaces Fast Ethernet, Gigabit Ethernet et 10 Gigabit Ethernet.

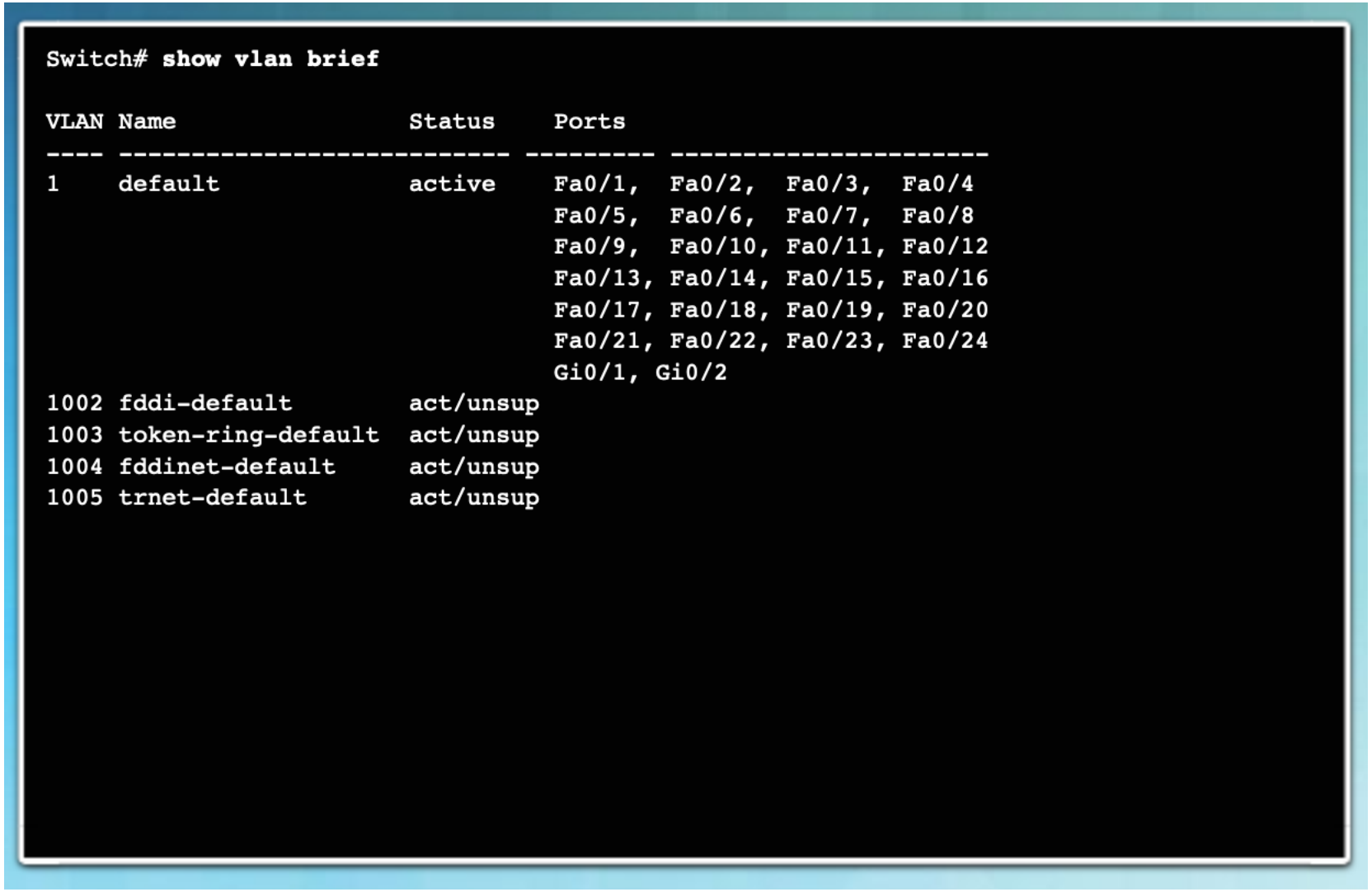
Un trunk de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour plusieurs VLAN entre les commutateurs et les routeurs. Un trunk peut également être utilisée entre un périphérique réseau et un serveur ou un autre périphérique équipé d'une carte réseau 802.1Q appropriée.



Détails du champ de l'étiquette VLAN
L'étiquette VLAN se compose d'un champ Type, d'un champ Priorité, d'un champ CFI (Canonical Format Identifier) et d'un champ d'ID de VLAN :

- **Type** : type de tag, 0x8100 pour 802.1q.
- **Priorité utilisateur** : niveau de priorité définit par l'IEEE 802.1p.
- **CFI (Canonical Format Identifier)** : Ethernet ou Token-ring
- **ID de VLAN (VID)** : numéro d'identification VLAN de 12 bits qui prend en charge jusqu'à 4 096 ID de VLAN.

Réseaux locaux virtuels à plage normale



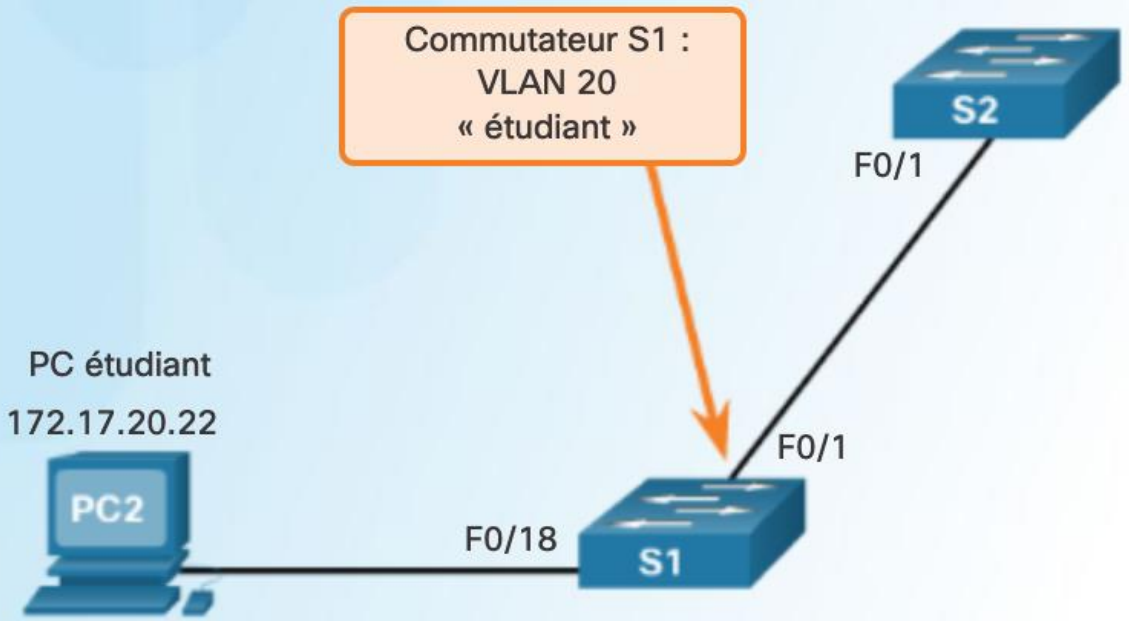
```
Switch# show vlan brief

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
```

- Identifiés par un ID de VLAN compris entre 1 et 1005.
- Les ID 1002 à 1005 sont réservés aux VLAN Token Ring et FDDI (Fiber Distributed Data Interface).
- Les ID 1 et 1002 à 1005 sont automatiquement créés et ne peuvent pas être supprimés.
- Les configurations sont stockées dans un fichier de base de données VLAN nommé vlan.dat. Le fichier vlan.dat se trouve dans la mémoire Flash du commutateur.

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.

Exemple de configuration

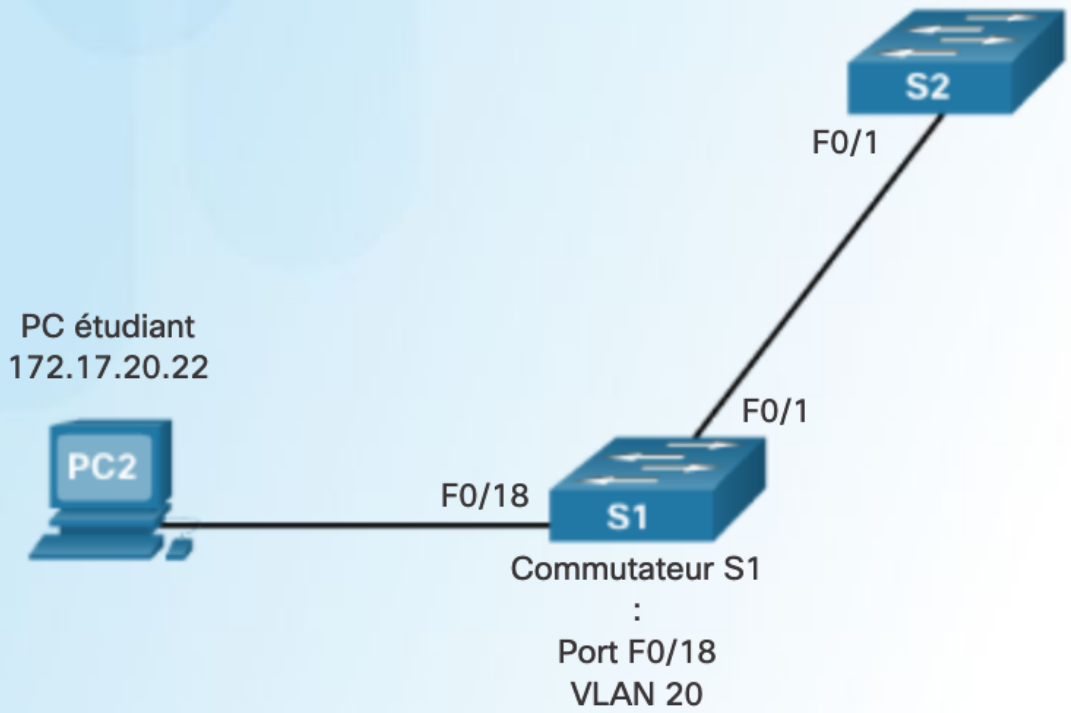
```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



Création d'un VLAN

Exemple de configuration

```
S1# configure terminal
S1(config)# interface F0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```



Affectation de ports à un VLAN

Exemple de configuration

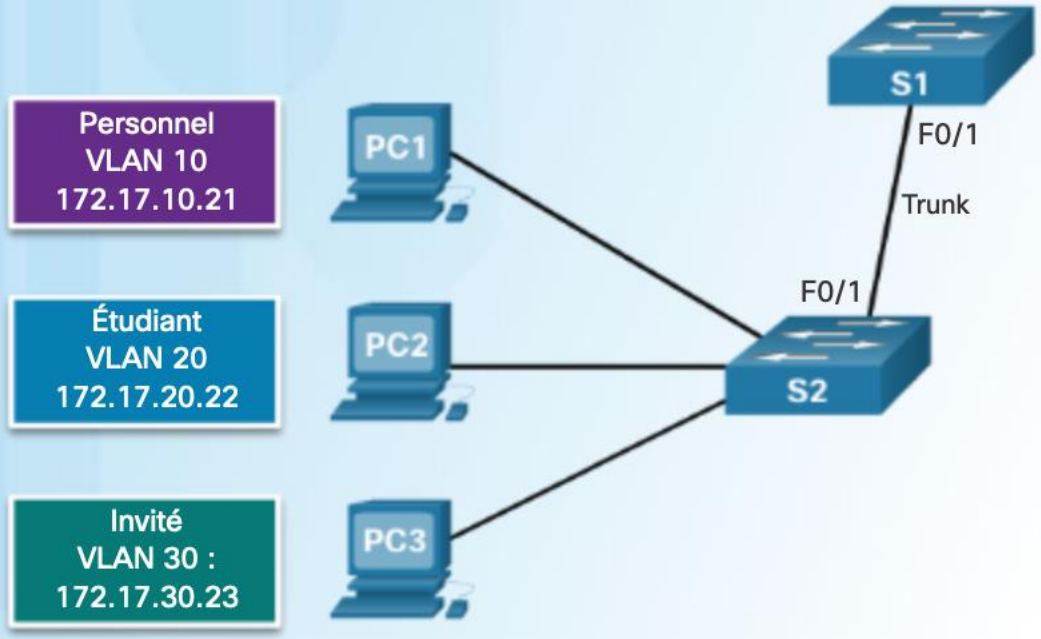
```
S1(config)# int F0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

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
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Suppression d'une affectation de VLAN

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, 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
S1#
```

Suppression de VLAN

```
VLAN 10 - Faculty/Staff - 172.17.10.0/24
VLAN 20 - Students - 172.17.20.0/24
VLAN 30 - Guest - 172.17.30.0/24
VLAN 99 - Native - 172.17.99.0/24
```



Création d'un trunk (agrégation de VLAN).

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

VLAN NATIF

Le VLAN natif est utilisé pour le trafic qui n'est pas associé à un VLAN spécifique par étiquetage VLAN (802.1Q). Lorsqu'un commutateur reçoit une trame **non marquée (untagged)** sur un port **trunk**, cette trame est automatiquement associée au VLAN natif.

Rôle du VLAN Natif :
Le VLAN natif sert à transporter les trames non marquées sur un lien trunk.
Il **ne doit pas être utilisé pour le trafic de gestion ou de données**. Son rôle est purement technique pour la compatibilité avec des équipements ne marquant pas leurs trames VLAN.

Sur de nombreux commutateurs (notamment Cisco), le **VLAN 1** est le VLAN natif par défaut.
Ainsi, si un commutateur reçoit une trame Ethernet non marquée, celle-ci est placée dans le VLAN 1, sauf configuration contraire.

Il est recommandé de **changer le VLAN natif par défaut** (par exemple VLAN 999) afin d'éviter toute confusion ou faille de sécurité.

SÉCURITÉ

Le VLAN 1 est souvent associé à du trafic de gestion par défaut.
Cela en fait une cible potentielle pour les attaques (ex. VLAN hopping).

Bonnes pratiques :

- Isoler le trafic de gestion dans un **VLAN dédié (ex. VLAN 99)**.
- Configurer un **VLAN natif inutilisé (ex. VLAN 999)**.
- Éviter d'autoriser le VLAN 1 sur les trunks.

```
interface gig0/1
switchport mode trunk
switchport trunk native vlan 999     ← isolé / blackhole
switchport trunk allowed vlan 10,20,30,99
```

```
interface vlan 99
ip address 192.168.99.10 255.255.255.0
```