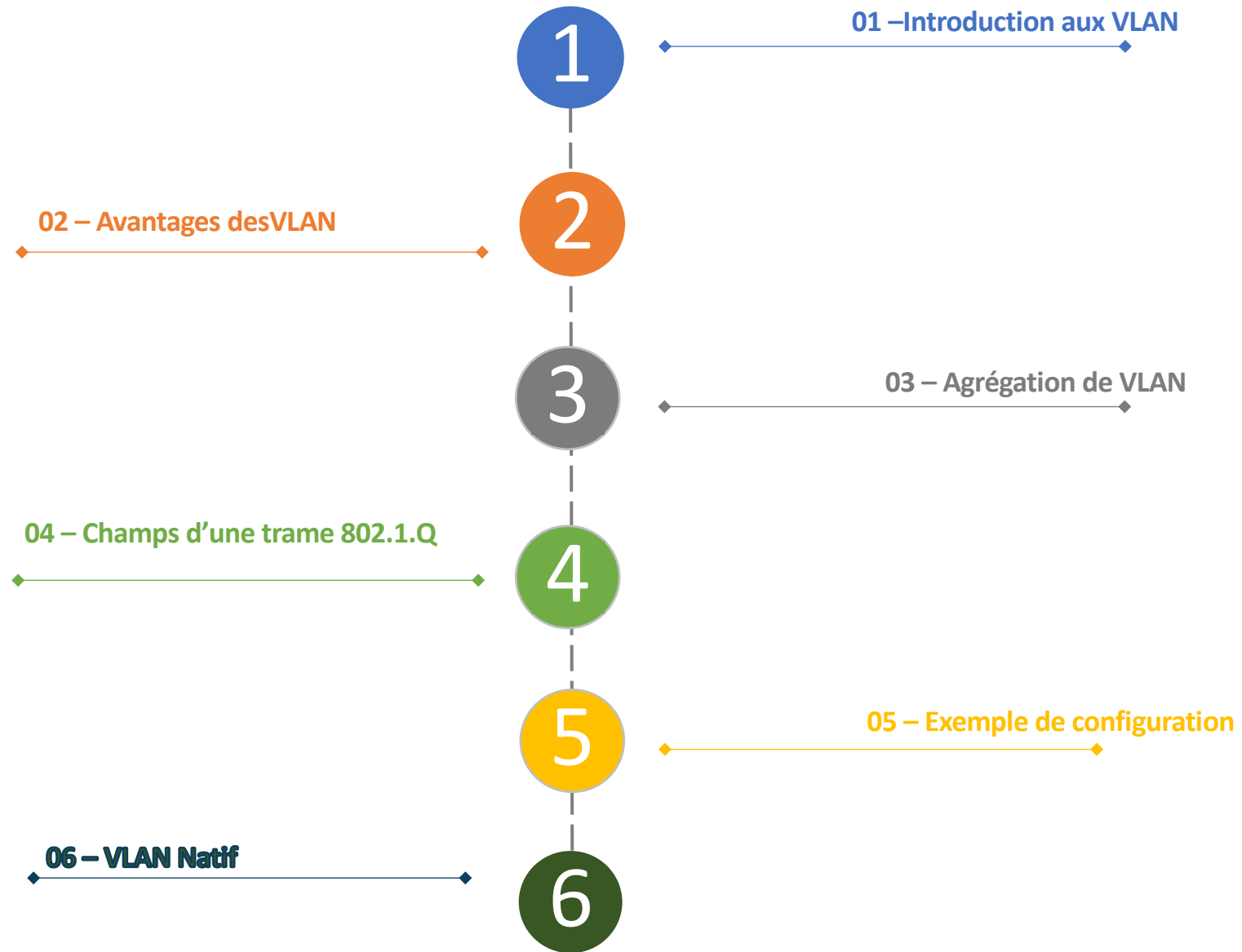
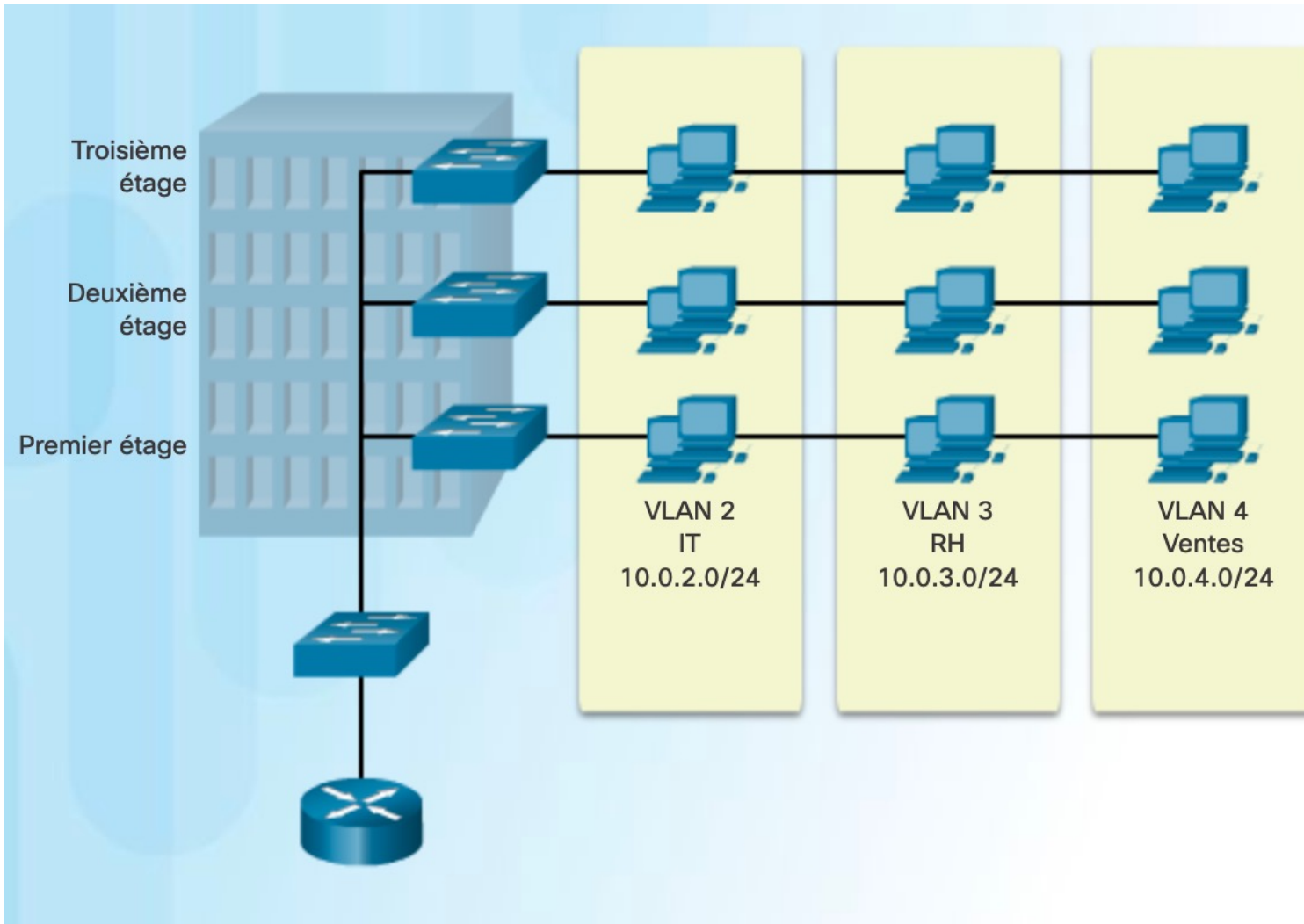


PLAN :

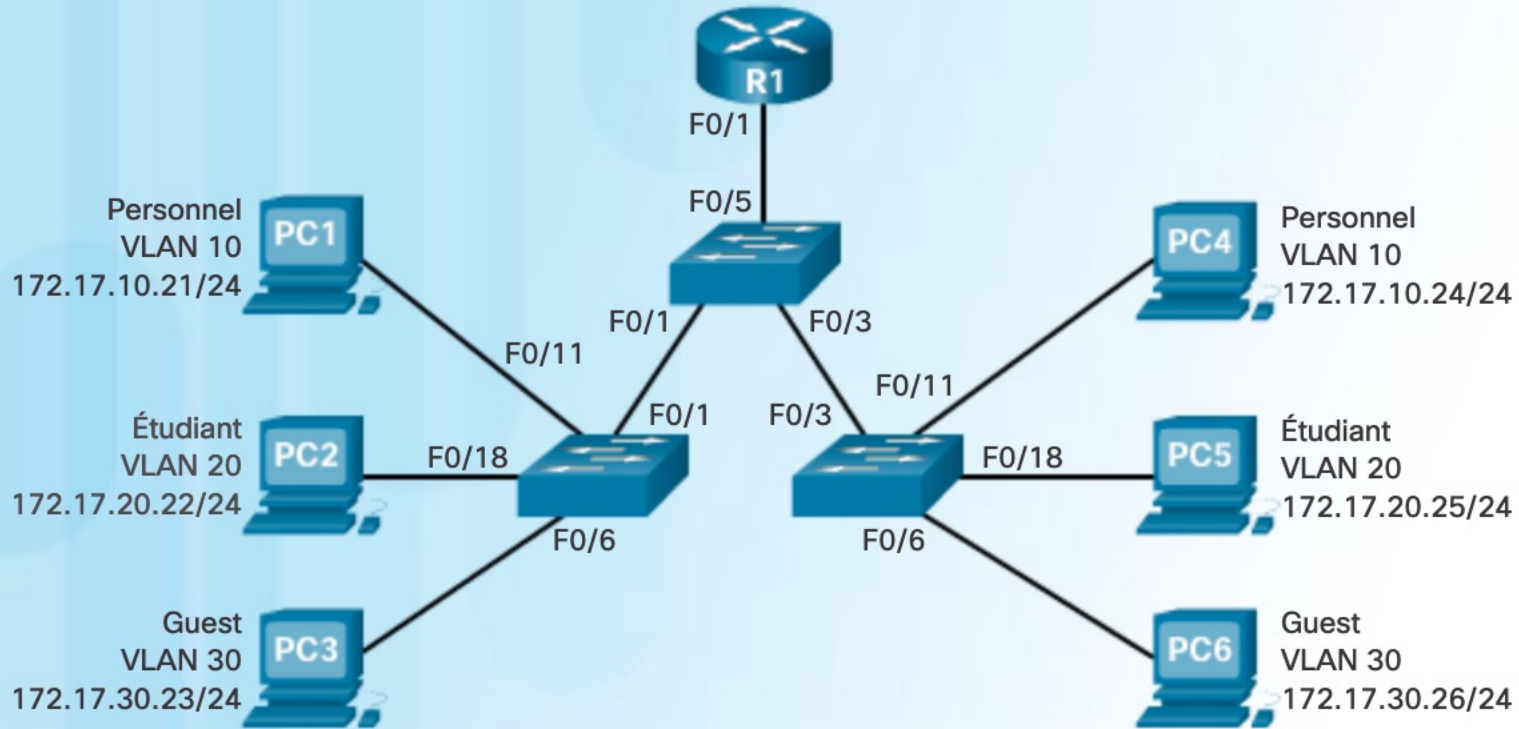


Les VLANs



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.

Avantages des 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

```
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	

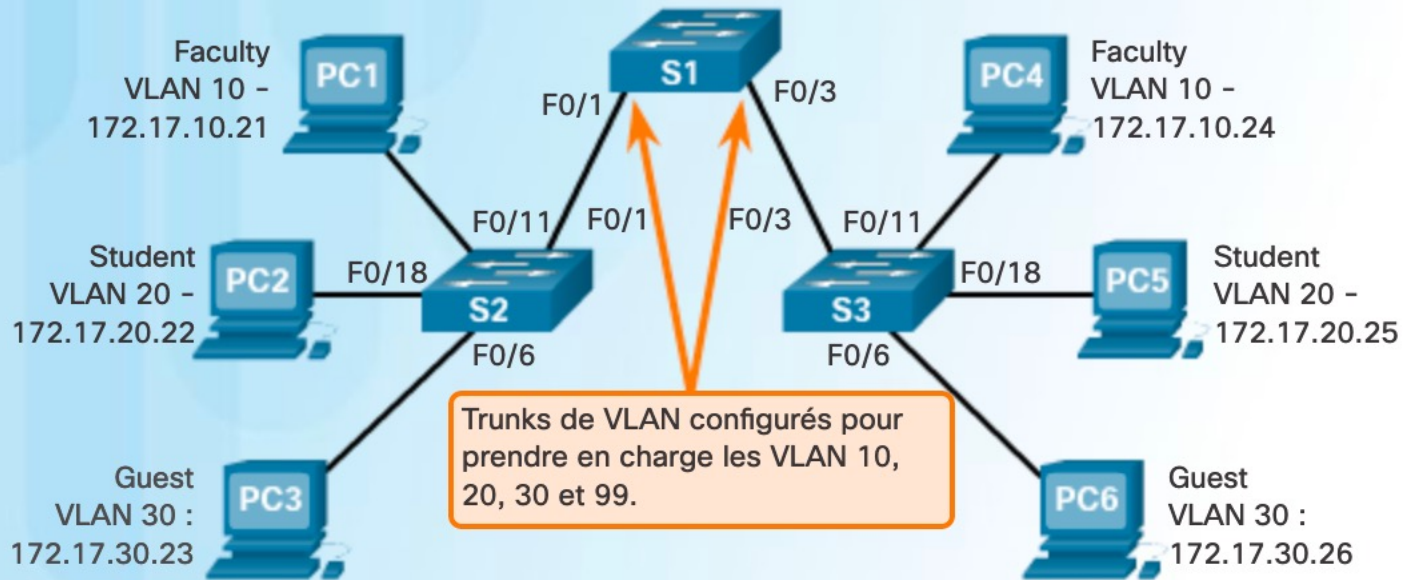
VLAN par défaut

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.

Agrégations 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

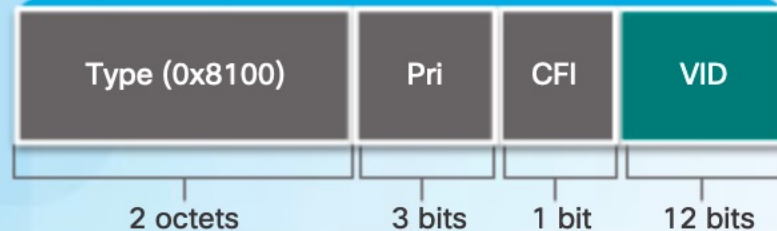
F0/1-5 sont des interfaces de trunk 802.1Q avec le VLAN 99 comme VLAN natif.
F0/11-17 se trouvent dans le VLAN 10
.F0/18-24 se trouvent dans le VLAN 20.
F0/6-10 se trouvent dans le VLAN 30.



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.

Champs d'une trame Ethernet 802.1Q



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 défini 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).

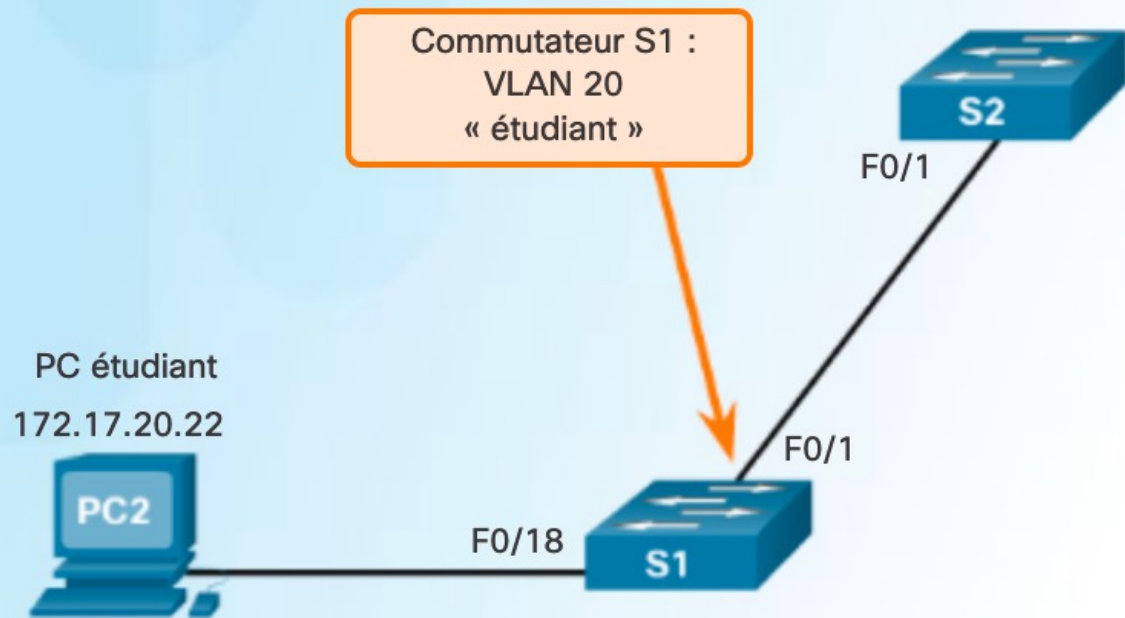
- Les ID 1 et 1002 à 1005 sont automatiquement créés et ne peuvent pas être supprimés.

- 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

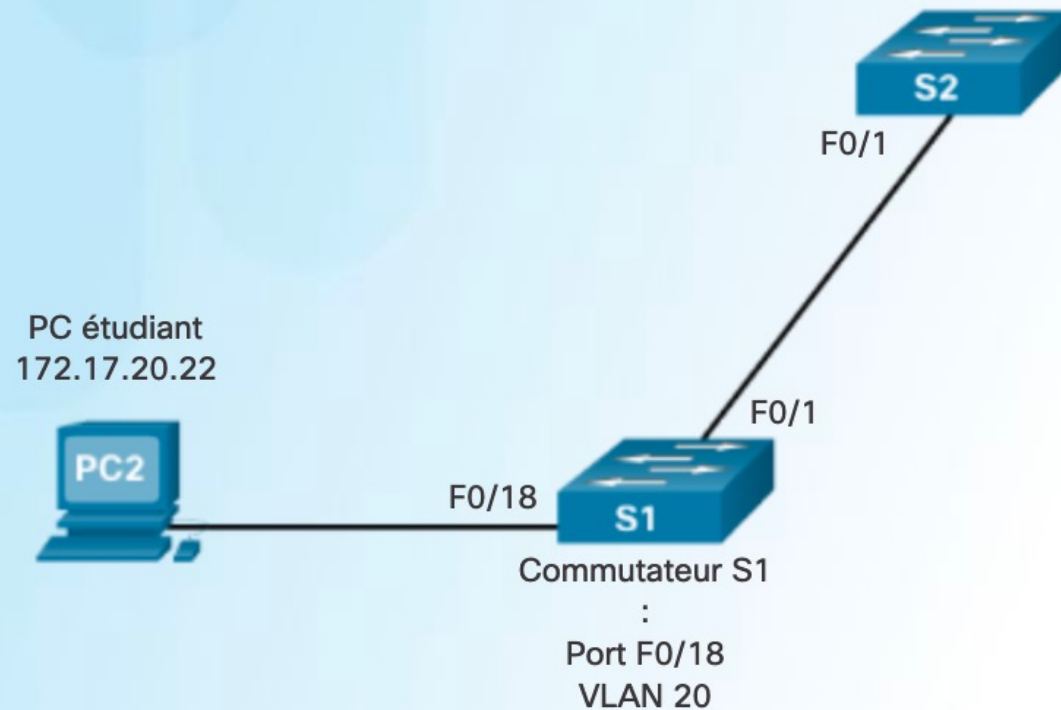
```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



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

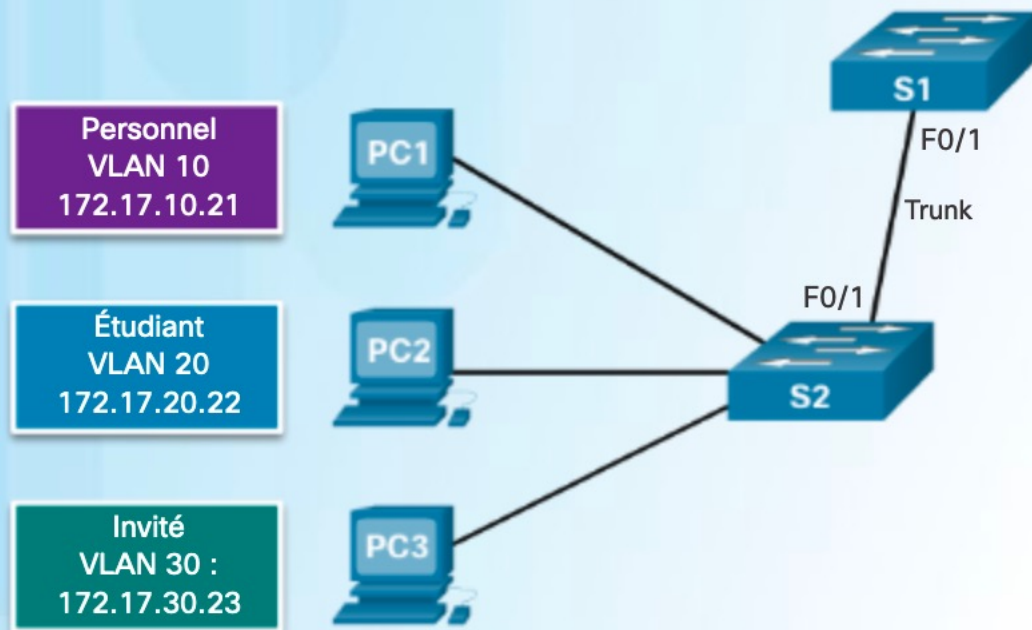
```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief
```

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 le biais de l'étiquetage VLAN. Lorsque des trames sont reçues sur un port de commutateur sans étiquette VLAN (trames non marquées), elles sont automatiquement attribuées au VLAN natif.

Rôle du VLAN Natif : Le VLAN natif est souvent utilisé pour le trafic qui ne nécessite pas de segmentation spécifique en VLANs. Il est couramment utilisé pour le trafic de gestion, tel que l'accès au commutateur lui-même via une interface d'administration.

Le VLAN natif **par défaut** sur de nombreux commutateurs Cisco est le VLAN 1. Cela signifie que si un commutateur reçoit des trames Ethernet non marquées (c'est-à-dire des trames sans étiquette VLAN), ces trames seront automatiquement placées dans le VLAN 1, à moins qu'il n'y ait une configuration spécifique pour utiliser un autre VLAN natif.

Sécurité : Le VLAN 1 (VLAN natif par défaut) est souvent utilisé par de nombreux commutateurs pour le trafic de gestion. Par conséquent, il peut être la cible d'attaques potentielles. En changeant le VLAN natif par défaut, vous pouvez réduire la surface d'attaque en isolant le trafic de gestion dans un VLAN distinct.