

Services des réseaux



Ghazi Oueslati

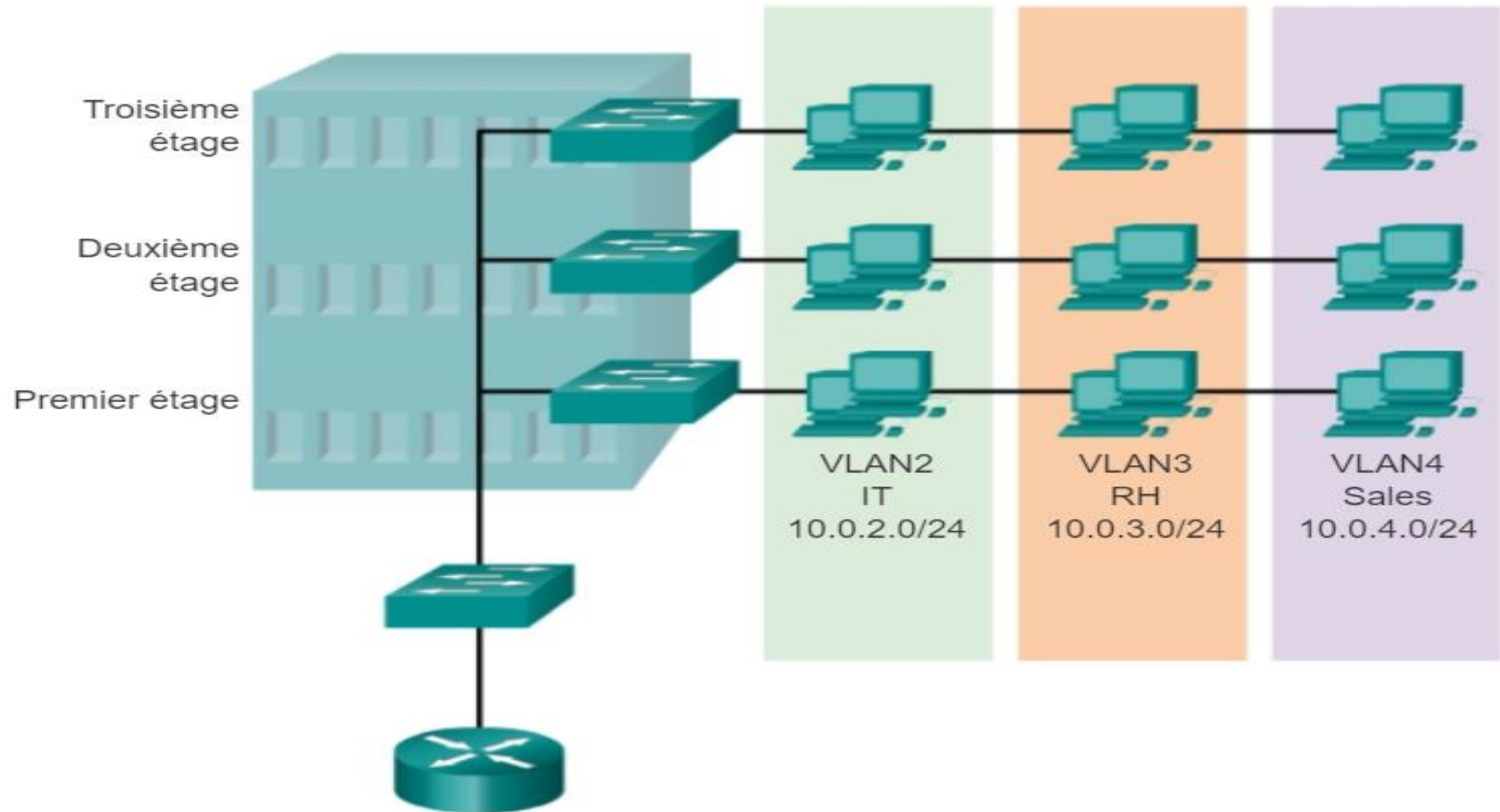
Ghazyoueslati@gmail.com

Chapitre 2: VLAN (Virtual Local Area Networks)

Vue d'ensemble des VLAN

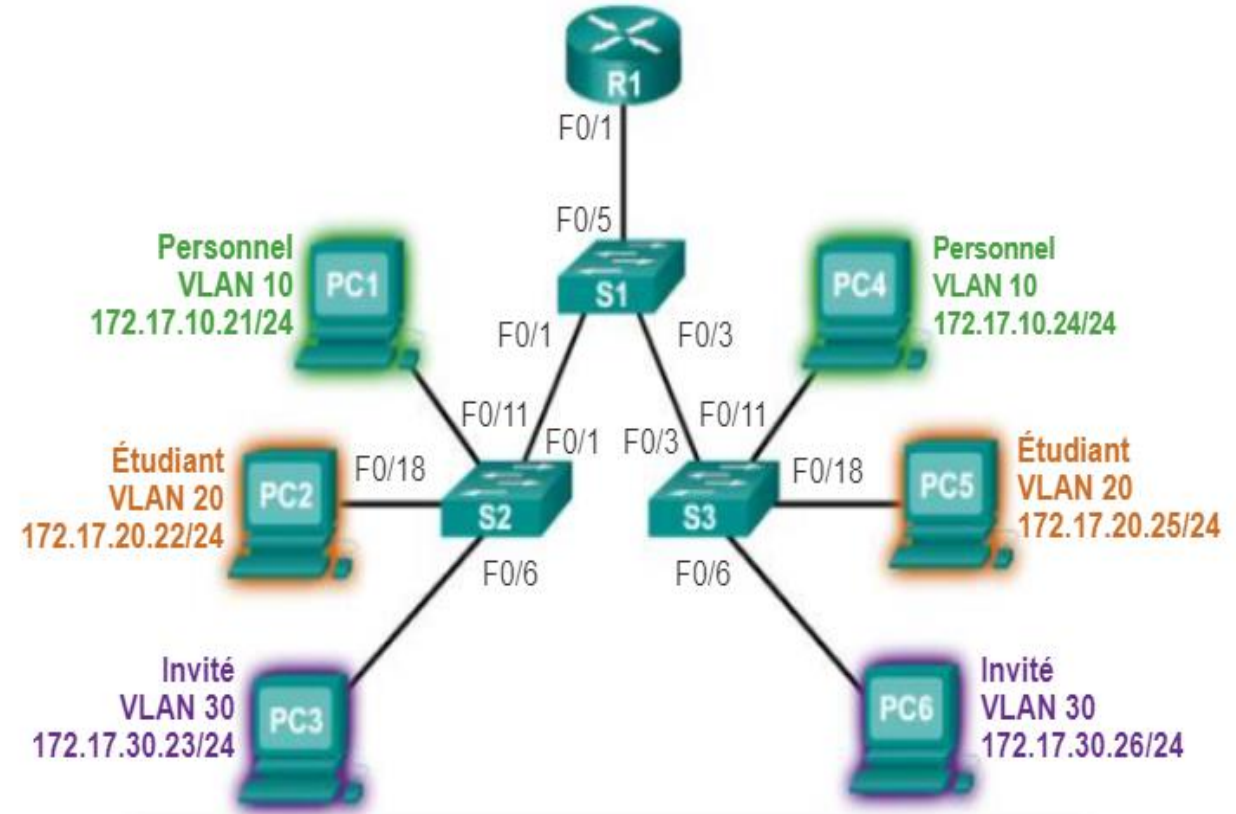
- Les VLAN (Virtual Local Area Networks) permettent de segmenter les réseaux physiques en sous réseaux-logiques.
- Un **Virtual Local Area Network (VLAN)** est un sous-réseau logique créé à l'intérieur d'un réseau physique.
- Contrairement à un réseau local traditionnel où tous les appareils sont sur le même segment de réseau, un VLAN permet de **regrouper des appareils en fonction de critères comme la fonction, le département ou la sécurité.**
- Chaque VLAN est indépendant des autres. Ceci permet de les configurer ou de les gérer de manière séparée.

Vue d'ensemble des VLAN



Vue d'ensemble des VLAN

- Les VLAN améliorent les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits.
 - Si un périphérique d'un VLAN envoie une trame Ethernet de diffusion, tous les périphériques du VLAN la reçoivent, mais pas les périphériques d'autres VLAN.
- Chaque VLAN d'un réseau commuté correspond à un réseau IP.
 - Le passage d'un VLAN à un autre nécessite un équipement N3.



Avantages des VLAN

- Sécurité optimisée
- Coût réduit
- Meilleures performances
- Efficacité IT

Vue d'ensemble des VLAN: Types de VLAN

- **VLAN de données**

- Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur.

- **VLAN par défaut**

- Par défaut, le VLAN 1 est celui qui est assigné à tous les ports d'un commutateur tant qu'ils n'ont pas été configurés autrement.

- **VLAN natif**

- La notion de VLAN natif n'intervient que lorsque l'on configure un port Trunk 802.1Q.
- Quand un port est configuré en mode Trunk, le commutateur insère une étiquette dans l'en-tête de la trame avec le numéro de VLAN approprié.
- Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou tagged traffic), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou untagged traffic).
- Le port trunk 802.1Q place le trafic non étiqueté sur le VLAN natif qui est par défaut le VLAN 1.

Vue d'ensemble des VLAN: Types de VLAN

- **VLAN de gestion**

- Le VLAN de gestion est un VLAN spécifique attribué aux commutateurs pour qu'ils soient accessibles via une adresse IP (ICMP, Telnet, SNMP, HTTP).

- **VLAN de voix (Voice VLAN)**

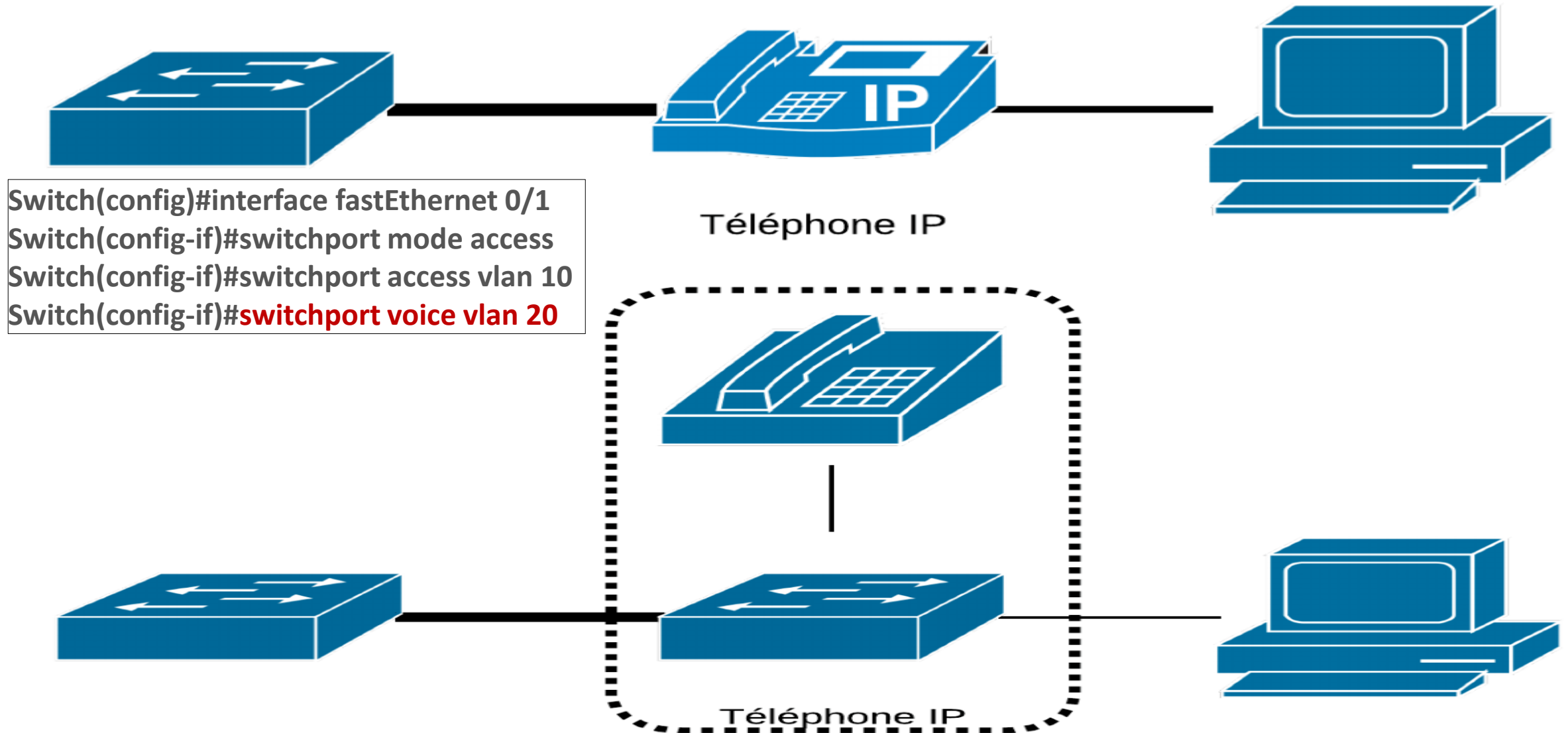
- Pour assurer la Qualité de Service (QoS) des communications vocales, le VLAN Voice se configure sur un port Access et crée une sorte de mini-Trunk vers un téléphone IP.

- **VLANs réservés**

- Puisque le VLAN ID est codé sur 12 bits dans les étiquettes 802.1q, offrant de la sorte 4096 possibilités, le premier ID VLAN disponible 0 et le dernier 4095 sont réservés et ne peuvent donc pas être utilisés.

Vue d'ensemble des VLAN: Types de VLAN

Voice VLAN



Vue d'ensemble des VLAN: Types de VLAN

VLAN 1

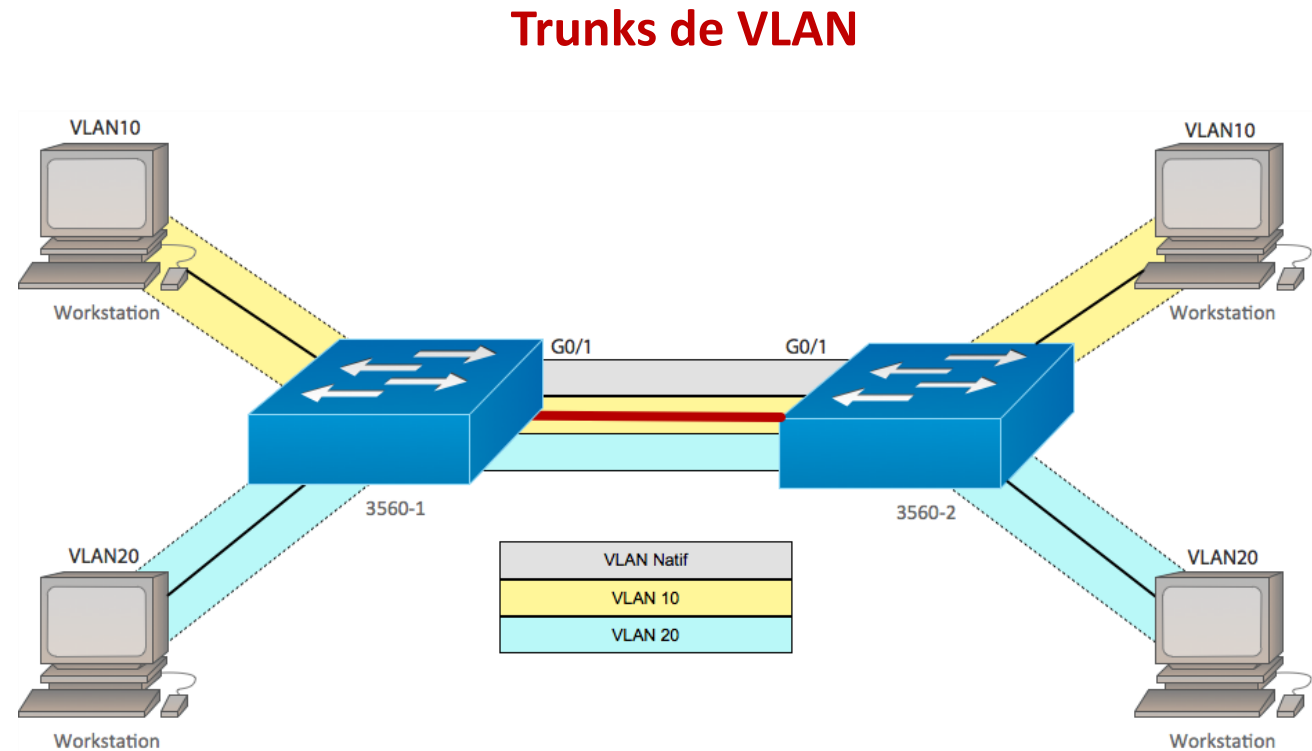
```
Switch# show vlan brief
```

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 dans un environnement à commutateurs multiples

- 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.
- 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.
- Les trunks de VLAN permettent à tout le trafic VLAN de se propager entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur.



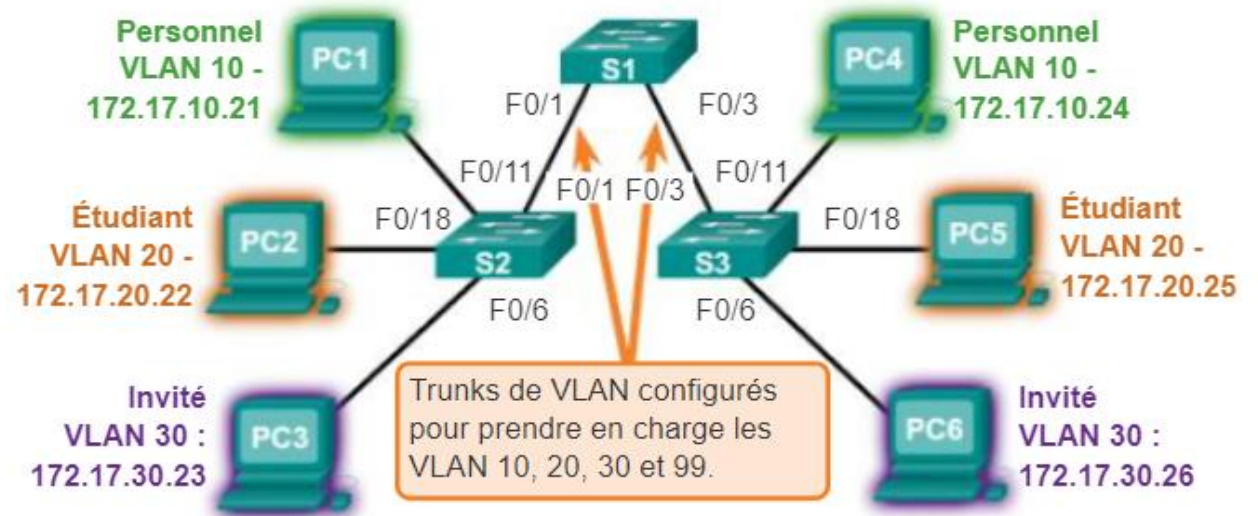
VLAN dans un environnement à commutateurs multiples

- 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.
- Par défaut, sur un commutateur Cisco Catalyst, tous les VLAN sont pris en charge sur un port trunk.

Trunks de VLAN

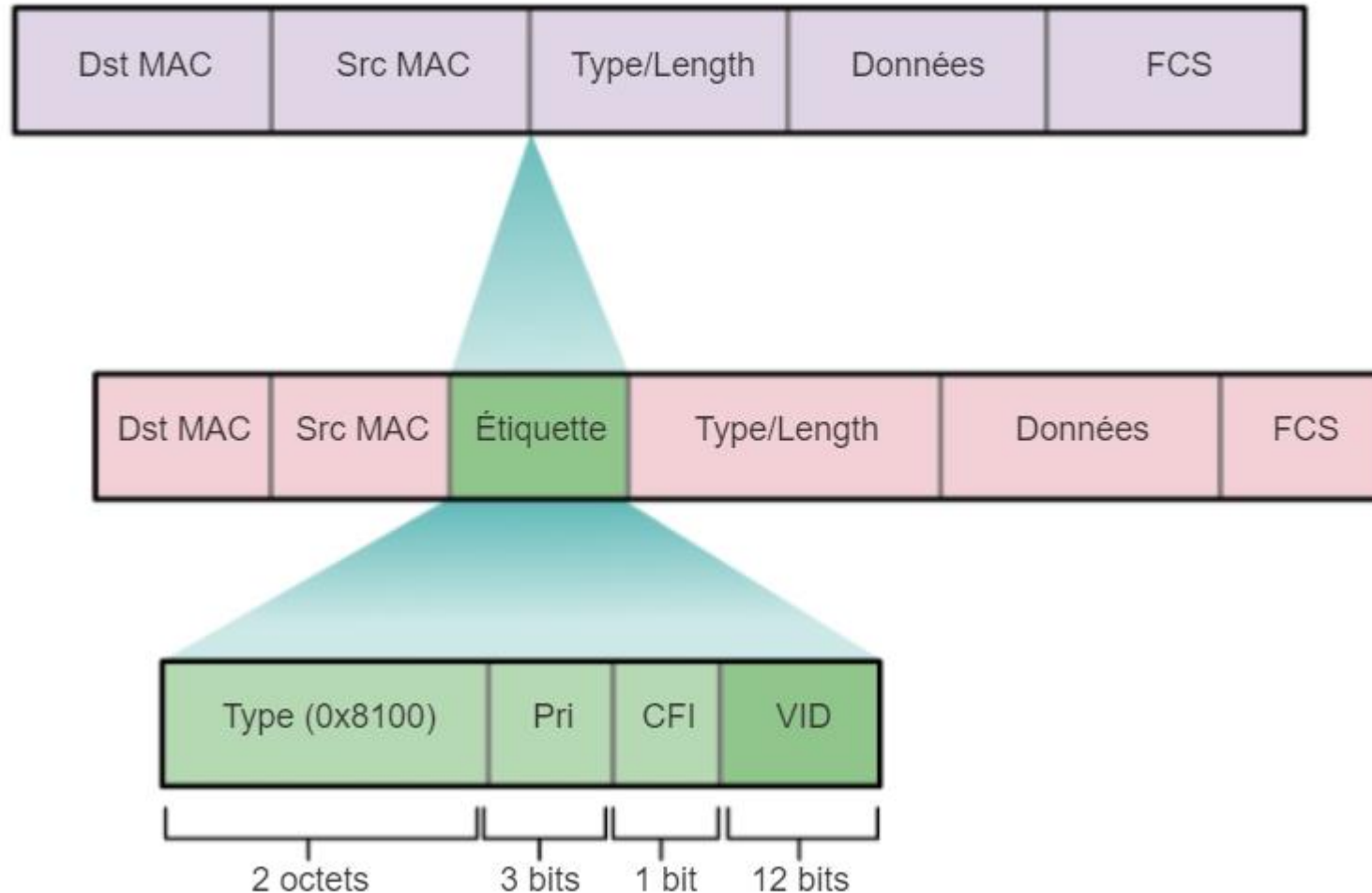
VLAN 10 Personnel - 172.17.10.0/24
VLAN 20 Étudiants - 172.17.20.0/24
VLAN 30 Invité - 172.17.30.0/24
VLAN 99 Gestion et natif - 172.17.99.0/24

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.



VLAN dans un environnement à commutateurs multiples

Champs d'une trame Ethernet 802.1Q



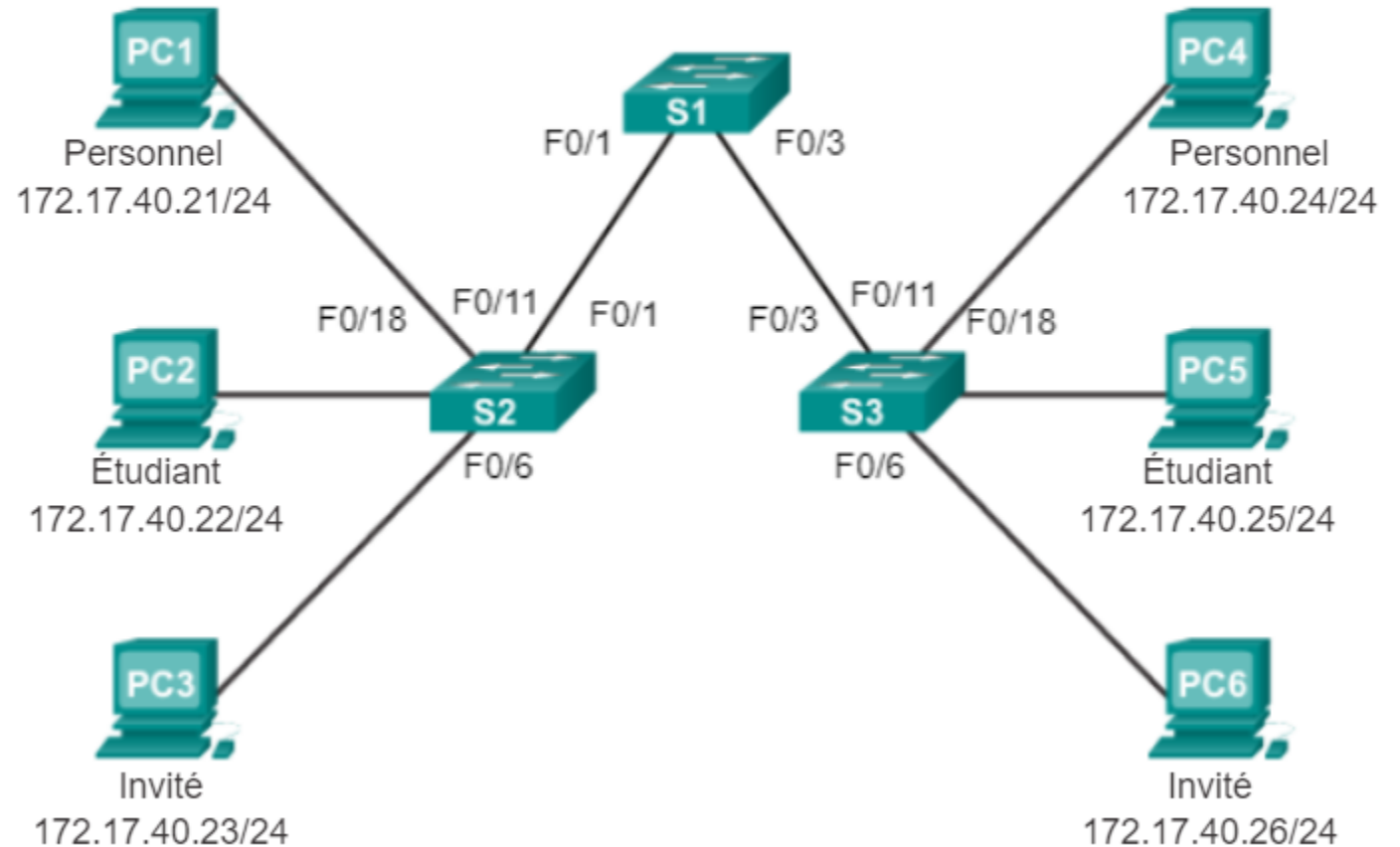
VLAN dans un environnement à commutateurs multiples

Aucune segmentation VLAN

■ Réseau sans VLAN

- Dans des circonstances normales, lorsqu'un commutateur reçoit une trame de diffusion sur l'un de ses ports, il la transfère par tous les autres ports, à l'exception du port de réception.
- Le réseau entier est configuré dans le même sous-réseau (172.17.40.0/24) et aucun VLAN n'est configuré. Par conséquent, lorsque l'ordinateur du personnel enseignant (PC1) envoie une trame de diffusion, le commutateur S2 l'envoie par tous ses ports. Par la suite, l'ensemble du réseau reçoit la diffusion, car il s'agit d'un seul domaine de diffusion.

PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion par tous les ports disponibles.



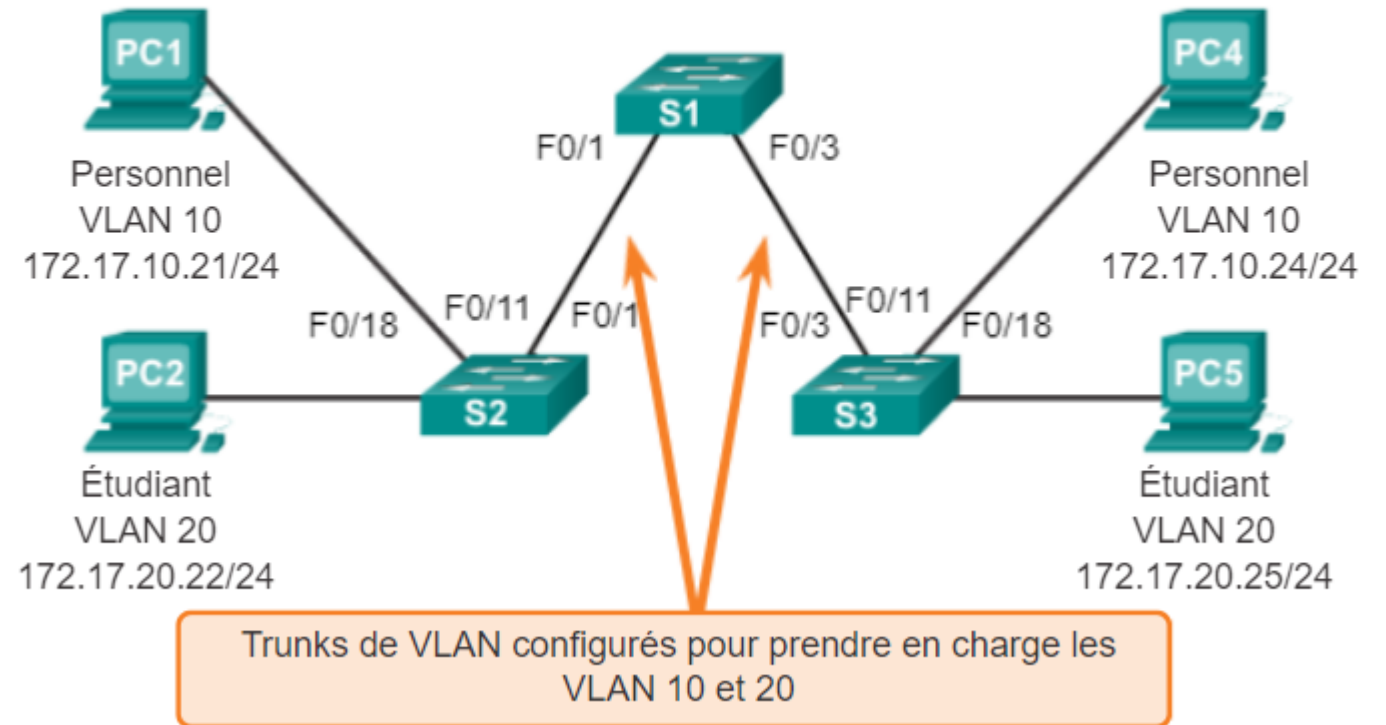
VLAN dans un environnement à commutateurs multiples

■ Réseau avec VLAN

- Comme le montre la Figure, le réseau a été segmenté en utilisant deux VLAN.
- Les périphériques du personnel enseignant sont affectés au VLAN 10 et les périphériques des étudiants au VLAN 20.
- Lorsqu'une trame de diffusion est envoyée de l'ordinateur du personnel enseignant (PC1) au commutateur S2, ce dernier transfère la trame de diffusion uniquement aux ports du commutateur configurés pour prendre en charge le VLAN 10.

Avec segmentation VLAN

PC1 envoie une diffusion de couche 2 locale. Les commutateurs transmettent la trame de diffusion uniquement par les ports configurés pour le VLAN 10.



Implémentation des VLAN

Attribution de ports aux VLAN

Création d'un VLAN

Commandes IOS de commutateur Cisco

Passez en mode de configuration globale.	S1# configure terminal
Créez un VLAN avec un numéro d'identité valide.	S1(config)# vlan <i>vlan-id</i>
Indiquez un nom unique pour identifier le VLAN.	S1(config-vlan)# name <i>vlan-name</i>
Repassez en mode d'exécution privilégié.	S1(config-vlan)# end

Commandes IOS de commutateur Cisco

Passez en mode de configuration globale.	S1# configure terminal
Passez en mode de configuration d'interface pour SVI.	S1(config)# interface <i>interface_id</i>
Définissez le port en mode d'accès.	S1(config-if)# switchport mode access
Affectez le port à un réseau local virtuel.	S1(config-if)# switchport access vlan <i>vlan_id</i>
Repassez en mode d'exécution privilégié.	S1(config-if)# end

Suppression d'une attribution de VLAN

Commandes IOS de commutateur Cisco

Passez en mode de configuration globale.	S1# configure terminal
Supprimez l'attribution VLAN du port.	S1(config-if)# no switchport access vlan
Repassez en mode d'exécution privilégié.	S1(config-if)# end

Implémentation des VLAN

Suppression d'un 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#
```


Implémentation des VLAN

Configuration de trunk

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	S1# configure terminal
Passer en mode de configuration d'interface pour SVI.	S1(config)# interface <i>interface_id</i>
Forcer la liaison à devenir une liaison trunk.	S1(config-if)# switchport mode trunk
Indiquer un VLAN natif pour les trunks 802.1Q non étiquetés.	S1(config-if)# switchport trunk native vlan <i>vlan_id</i>
Indiquer la liste des VLAN autorisés sur la liaison trunk.	S1(config-if)# switchport trunk allowed vlan <i>vlan-list</i>
Repasser en mode d'exécution privilégié.	S1(config-if)# end

Implémentation des VLAN

Réinitialisation de valeurs configurées sur des liaisons trunk

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	S1# configure terminal
Passer en mode de configuration d'interface pour SVI.	S1(config)# interface <i>interface_id</i>
Définir le trunk de sorte qu'il autorise tous les VLAN.	S1(config-if)# no switchport trunk allowed vlan
Redéfinir le VLAN natif sur les paramètres par défaut.	S1(config-if)# no switchport trunk native vlan
Repasser en mode d'exécution privilégié.	S1(config-if)# end