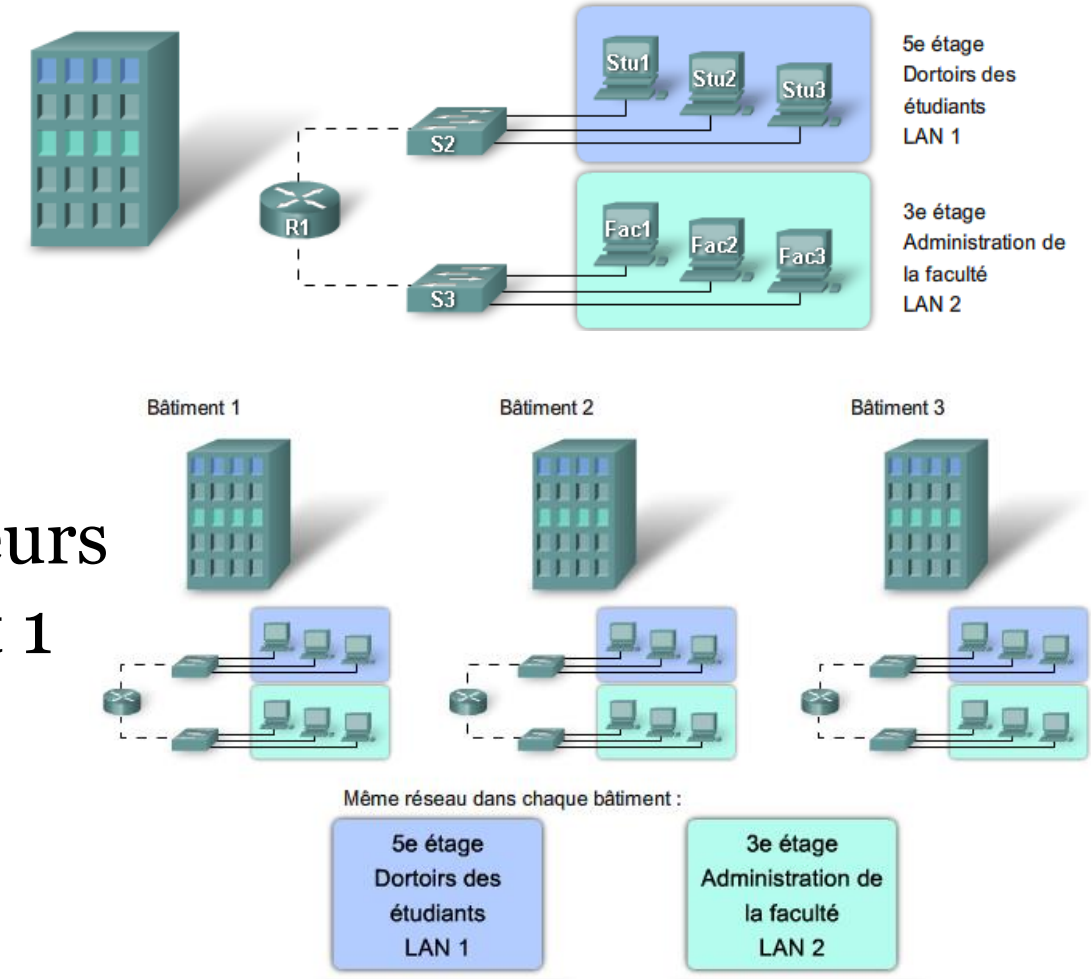
VLAN: Virtual Local Area Networks

Réseaux d'entreprise

Marouane SEBGUI

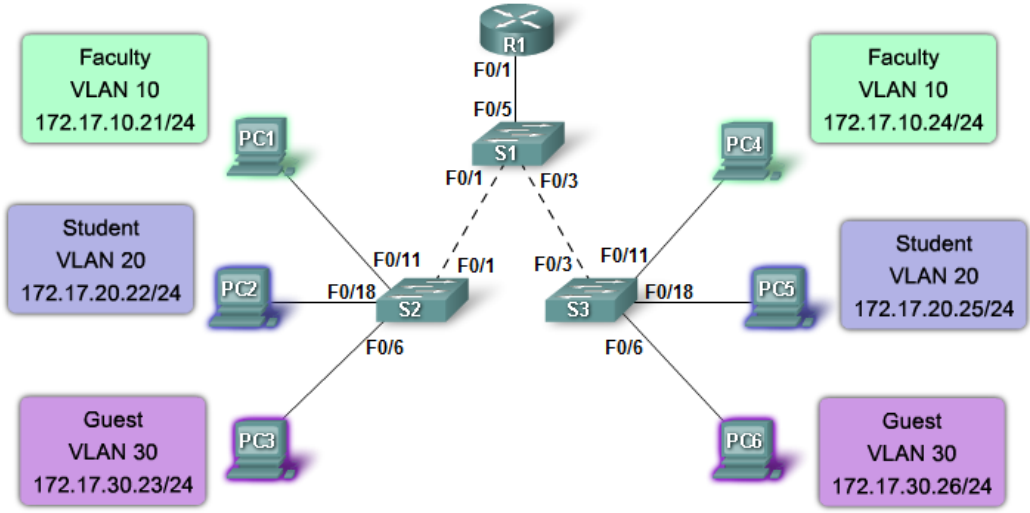
Avant les VLANs

- Si un utilisateur de l'administration se trouve dans le 5ème étage ?
- Connecter les utilisateurs étudiants du bâtiment 1 avec les étudiants des bâtiments 2 et 3 ?



Séparation par VLANs

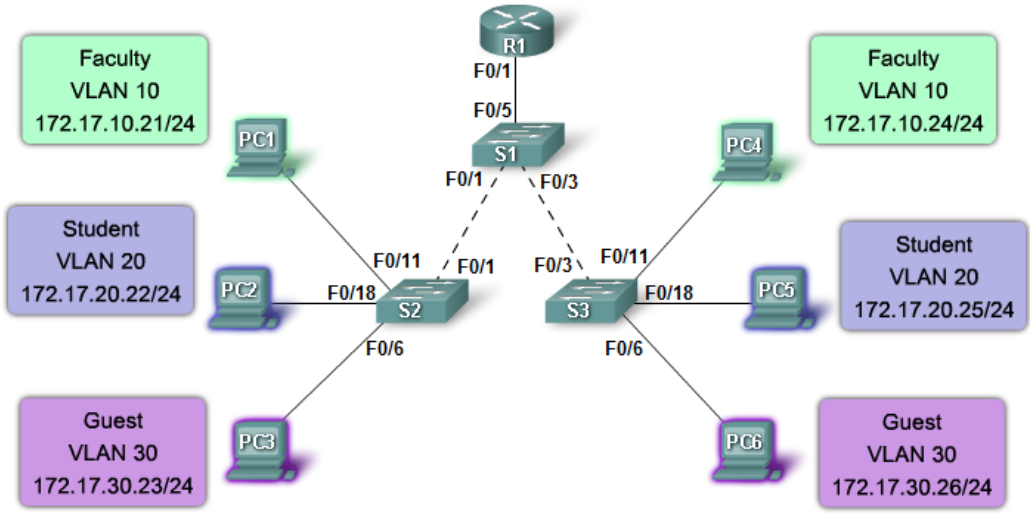
- Un VLAN c'est un réseau local indépendant. C'est une séparation logique des réseaux couche 2 qui permet à l'administrateur de grouper les utilisateurs selon des bases logiques quelque soit leurs dispositions physiques.
- Les utilisateurs dans des VLANs différents sont invisibles les uns par rapport aux autres.
- Un VLAN est un domaine de broadcast et doit être lié à un réseau couche 3.
- Les équipements n'ont pas conscience de leur appartenance aux VLANs, la séparation se fait au niveau du Switch



- Sur le Switch :
  - Créer et configurer les VLANs
  - Attribuer le port au VLAN
- Sur l'équipement
  - Attribuer une adresse IP convenable

Avantages des VLANs

- Permet à l'administrateur plus de flexibilité dans l'organisation du réseau en groupes.
- Facilite la mise en place des ACL et des mécanismes de sécurité
- Réduit les coûts
- Limite les domaines de diffusion
- Améliore l'efficacité de :
  - La gestion
  - La maintenance
  - Les nouveaux projets
  - …



- Le VLAN c'est :
  - Meilleure organisation
  - Plus de visibilité
  - Performance accrue

ID du VLAN

- Adresse sur 12 Bits permet d'identifier chaque VLAN de façon unique dans l'infrastructure

- Plage normale
  - ID compris entre 1 et 1005
  - VLAN 1 déjà créé et contient tous les ports
  - VLANs de 1002 à 1005 réservés pour VLAN Token Ring et FDDI

- Plage étendue
  - ID compris entre 1006 et 4094
  - Conçu pour les fournisseurs de services
  - Moins d'options que les VLANs de la plage normale

Nombre de VLANs supportés

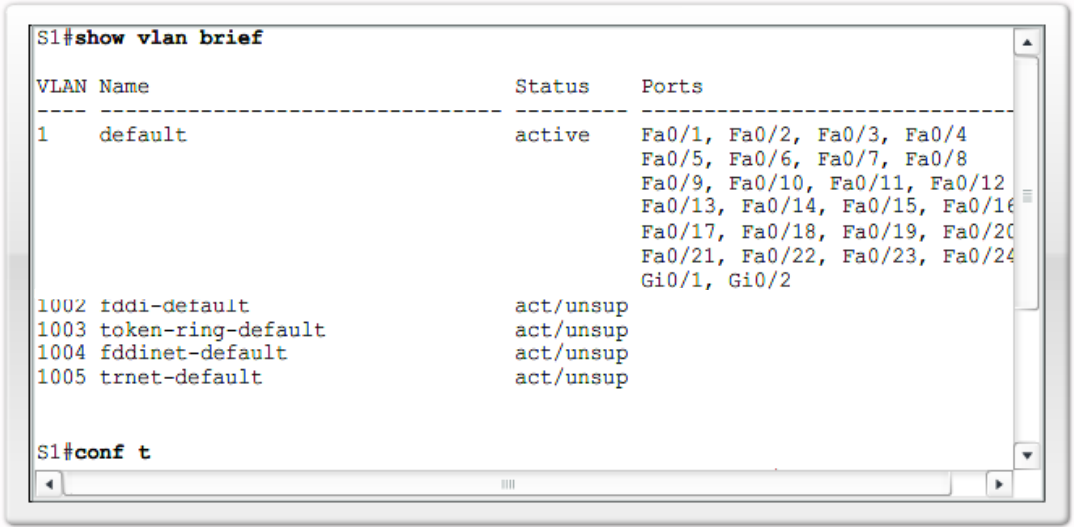
- Un commutateur peut être limité en terme de réseaux locaux virtuels qu'on peut créer.

Type of Switch	Maximum Number of VLANs	VLAN ID Range
Catalyst 2940	4	1–1005
Catalyst 2950/2955	250	1–4094
Catalyst 2960	255	1–4094
Catalyst 2970/3550/3560/3750	1005	1–4094
Catalyst 2848G/2980G/4000/4500	4094	1–4094
Catalyst 6500	4094	1–4094

- Attention : n'importe quel ID

Stockage des VLANs

- Les VLANs 1, 1002, 1003, 1004 et 1005 sont créés par le système, il n'est pas possible de les modifier ou de les supprimer
- Les VLANs de la plage normale sont créés et stockés dans le fichier vlan.dat qui se trouve dans la mémoire flash

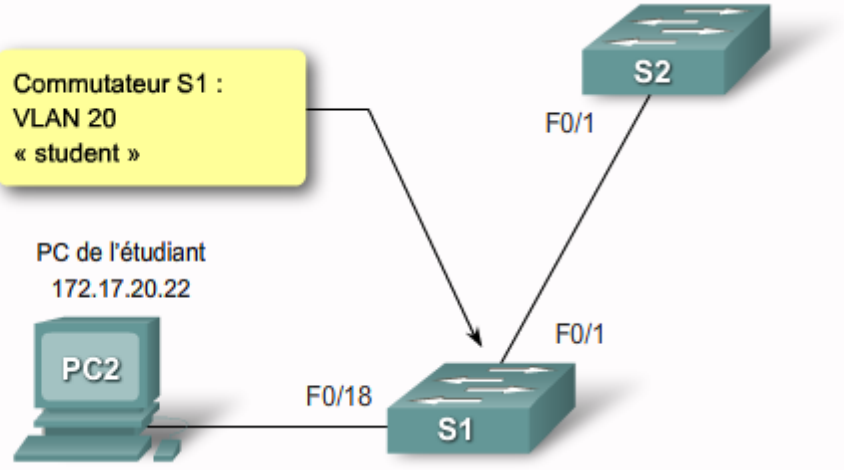


- Les VLANs étendus sont créés dans le fichier running-configuration (peuvent être copiés dans le startup-configuration)

Création des VLANs : Catalyste Cisco

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	`S1#configure terminal`
Créer un VLAN. « id de vlan » est le numéro de VLAN à créer. Passe en mode de configuration de VLAN pour l'ID de VLAN du VLAN.	`S1(config)#vlan id de vlan`
(Facultatif) Spécifier un nom de VLAN unique pour identifier le VLAN. Si aucun nom n'est entré, le numéro de VLAN, complété par des zéros, est ajouté au mot « VLAN », comme par exemple VLAN0020.	`S1(config-vlan)#name nom_vlan`
Revenir au mode d'exécution privilégié. Vous devez terminer votre session de configuration pour que la configuration soit enregistrée dans le fichier vlan.dat et pour qu'elle soit appliquée.	`S1(config-vlan)#end`

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



Vérification des VLANs (1)

`show vlan` Command

Cisco IOS CLI Command Syntax	
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

```
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#conf t
```

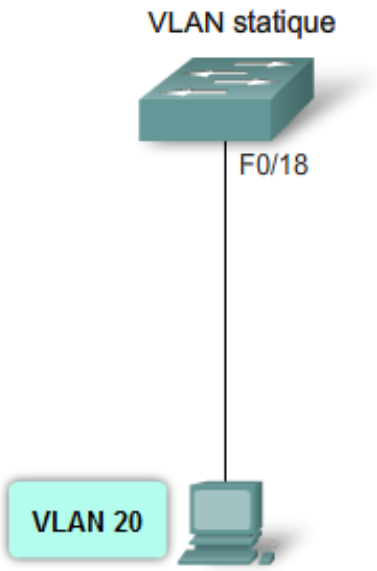
Vérification des VLANs (2)

`show vlan` Command

Cisco IOS CLI Command Syntax	
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs            : 7
Number of existing VTP VLANs        : 7
Number of existing extended VLANS   : 0

S1#
```

Affectation des Interfaces : Catalyste



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer en mode de configuration globale.	`S1#configure terminal`
Entrer dans l'interface pour affecter le réseau local virtuel.	`S1(config)#interface` *id_interface*
Définir le mode d'appartenance du port à un réseau local virtuel.	`S1(config-if)#switchport mode access`
Affecter le port à un réseau local virtuel.	`S1(config-if)#switchport access vlan` *id de vlan*
Repasser en mode d'exécution privilégié.	`S1(config-if)#end`

```
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
```

Vérification de l'affectation

```
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, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
20   student                           active    Fa0/18
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1#
```

HPE Comware

- Créer les VLANs 100 (Student) et 200 (Staff)
  - <core1> system-view
  - [core1] vlan 100
  - [Core1-Vlan100] name Student
  - [core1] vlan 200
  - [Core1-Vlan200] name Staff

- Affecter l'interface Giga 1/0/12 au VLAN 100
  - <core1> system-view
  - [core1] interface GigabitEthernet1/0/12
  - [Core1-GigabitEthernet1/0/1] port link-type access
  - [Core1-GigabitEthernet1/0/1] port access VLAN 100

HP ProCurve (Aruba)

- Créer les VLANs 100 (Student) et 200 (Staff)
  - SW1# conf t
  - SW1(config)# vlan 100
  - SW1(config-Vlan100)# name "Student"
  - SW1(config)# vlan 200 name "Staff"

- Affecter les interfaces e1, e12, e13, … e20 au VLAN 100
  - SW1# conf t
  - SW1(config)# vlan 100
  - SW1(config-Vlan100)# untagged e1
  - SW1(config-Vlan100)# untagged e12-e20

Changer une affectation

- Au niveau de l'interface (exemple fa0/11 déjà dans le VLAN 10)
  - SW(Config-if)#switchport access VLAN 20
- L'interface est affectée au nouveau VLAN

```
S1# config t
S1(config)# interface F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
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, Fa0/12, 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     F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Supprimer une affectation

- Au niveau de l'interface (exemple fa0/18)
  - SW(Config-if)#no switchport access VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Remove the VLAN assignment from the port.	S1(config-if)# **no switchport access vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

- L'interface est ré-affectée au default VLAN

```
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#
```

Supprimer un VLAN

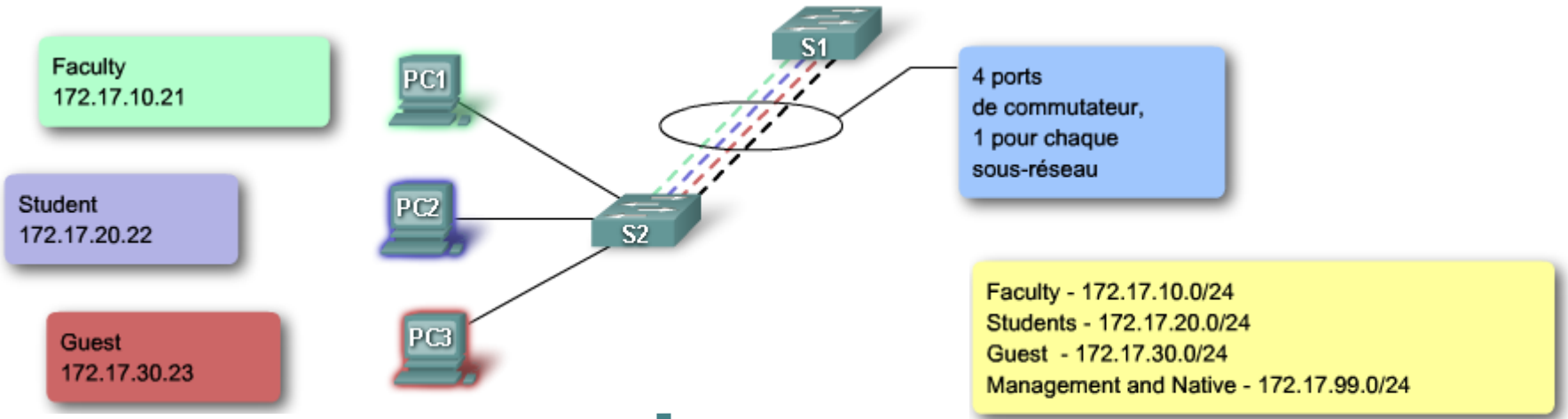
- En mode configuration globale
  - SW(config)#no VLAN 20
- En mode utilisateur privilégié
  - SW#delete flash:vlan.dat
  - SW# delete vlan.dat est possible aussi

```
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#
```

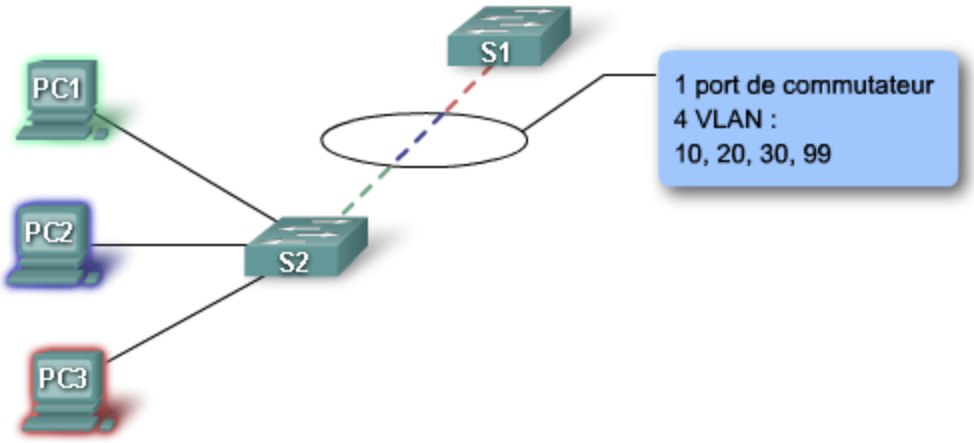
```
S1# config t
S1(config)# interface F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

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, Fa0/12, 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    F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

- Attention à l'interface F0/11

Agrégation des VLANs – Port Trunk

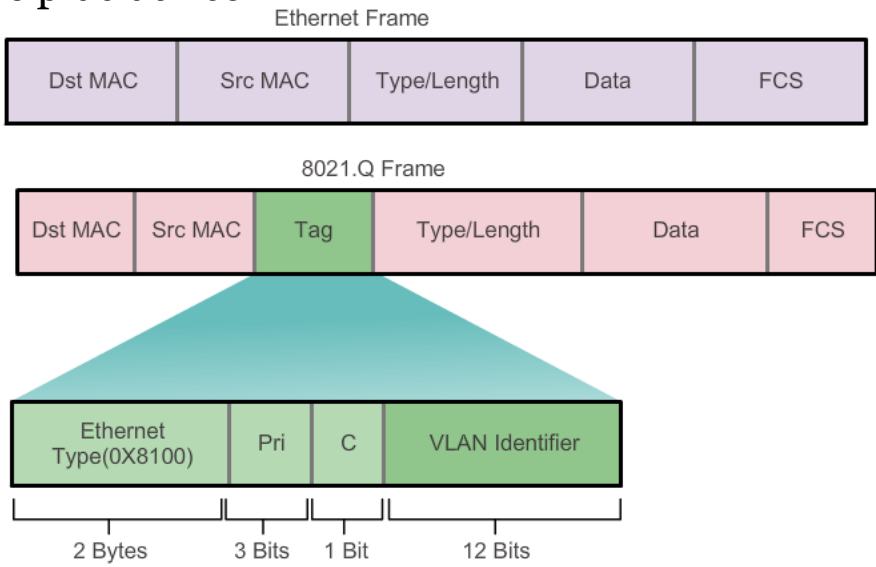


- L'agrégation permet de :
  - Relier les équipements du même VLAN qui sont sur des SW distants
  - Véhiculer le trafic de plusieurs VLANs dans un même lien
  - Économiser sur le nombre de ports et de liens
  - Distinguer les trafics en ajoutant des étiquettes (tags) qui seront ajoutées à l'entrée du lien Trunk et supprimées avant la redistribution



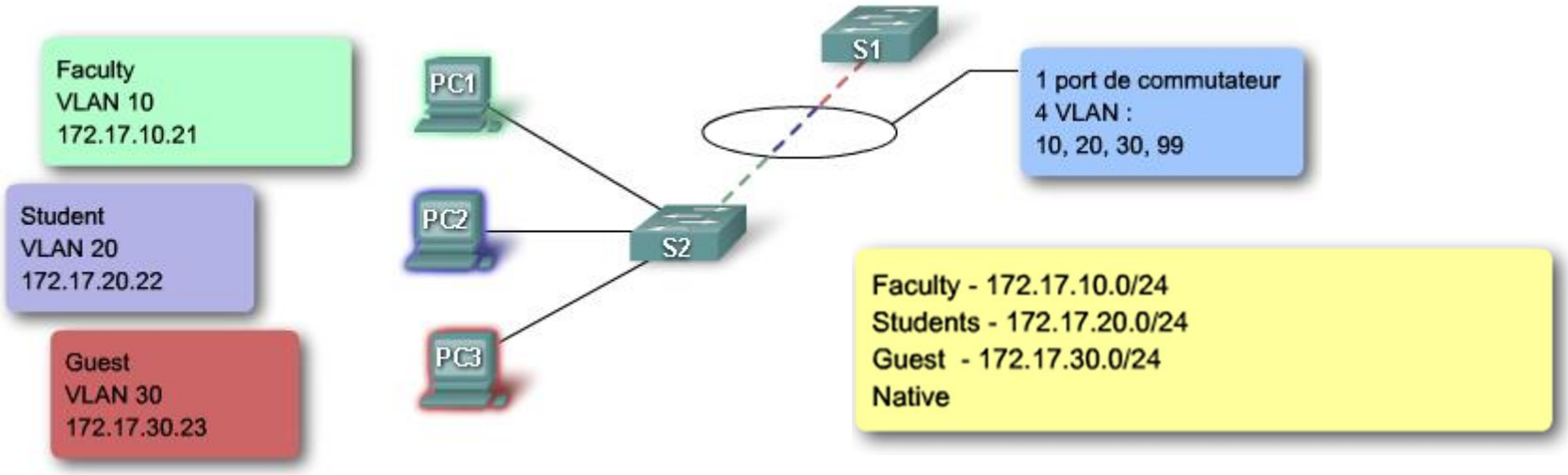
Agrégation des VLANs – encapsulation

- Il existe plusieurs protocoles d'agrégation. Le plus utilisé est le standard 802.1Q. Il permet de
  - Conserver la structure de la trame
  - Ajouter un champs de 32 bits (4oct) pour identifier le protocole lui-même et identifier le VLAN



- 1 champs 2oct : ID du protocole 802.1Q
  - Valeur en hexadécimal = 0x8100
- 1champs 2oct : les données 802.1Q
  - 3bit de priorité : utilisé par le protocole 802.1p pour faire de la Qualité de Service QoS.
  - 1bit de compatibilité avec Token Ring. Il est aussi utilisé pour notifier le Drop Eligibility de la trame
  - 12bit pour l'ID du VLAN

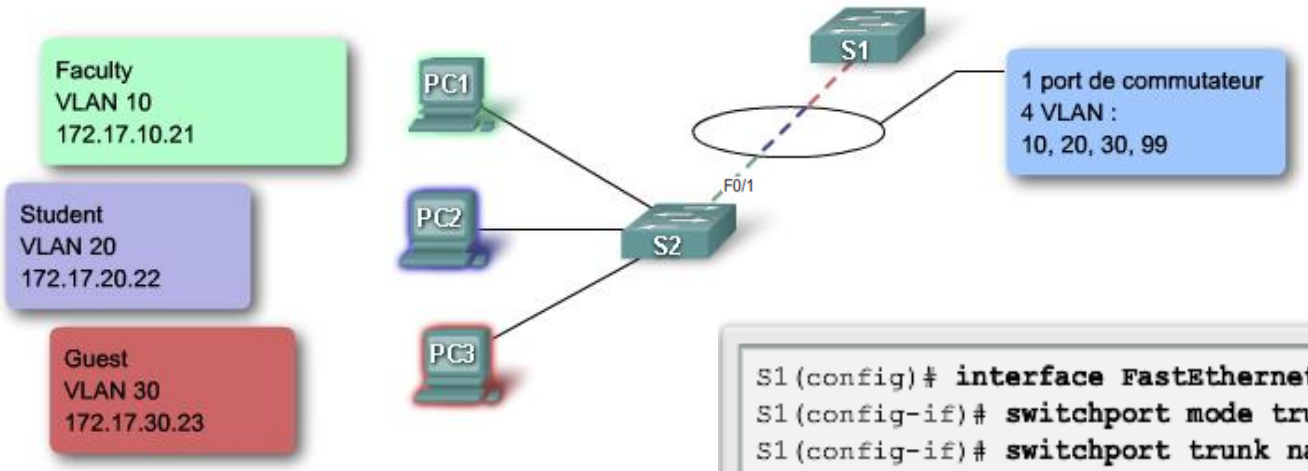
Agrégation des VLANs – VLAN Natif



- Un VLAN natif permet de véhiculer le trafic non-taggué sur un lien Trunk:
  - Un trafic reçu non étiqueté (sur un lien trunk) doit être retransmis non étiqueté
  - Le VLAN natif ne doit pas être utilisé comme VLAN de donnée
  - Par défaut (si aucune intervention) le VLAN natif est le VLAN 1

Agrégation – Configuration Catalyste

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer en mode de configuration globale.	`S1#configure terminal`
Entrer dans le mode de configuration d'interface pour l'interface définie.	`S1(config)#interface` *id d'interface*
Forcer la liaison reliant les commutateurs à devenir une liaison agrégée.	`S1(config-if)#switchport mode trunk`
Spécifier un autre VLAN en tant que VLAN natif pour le trafic non étiqueté pour les agrégations IEEE 802.1Q.	`S1(config-if)#switchport trunk native vlan` *id de vlan*
Repasser en mode d'exécution privilégié.	`S1(config-if)#end`




```
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
```

Agrégation – Configuration HP

- HPE ProCurve (Aruba)
  - SW1# **conf t**
  - SW1(config)# **vlan 100**
  - SW1(config-Vlan100)# **untagged e1-e12**
  - SW1(config-Vlan100)# **tagged e23-e24**
  - SW1(config)# **vlan 200**
  - SW1(config-Vlan200)# **untagged e13-e20**
  - SW1(config-Vlan200)# **tagged e23-e24**

- HPE Comware
  - <core1> **system-view**
  - [core1] **interface GigabitEthernet1/0/24**
  - [Core1-GigabitEthernet1/0/24] **port link-type trunk**

Agrégation – Vérification

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Agrégation – Correction

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Return Port to Access Mode

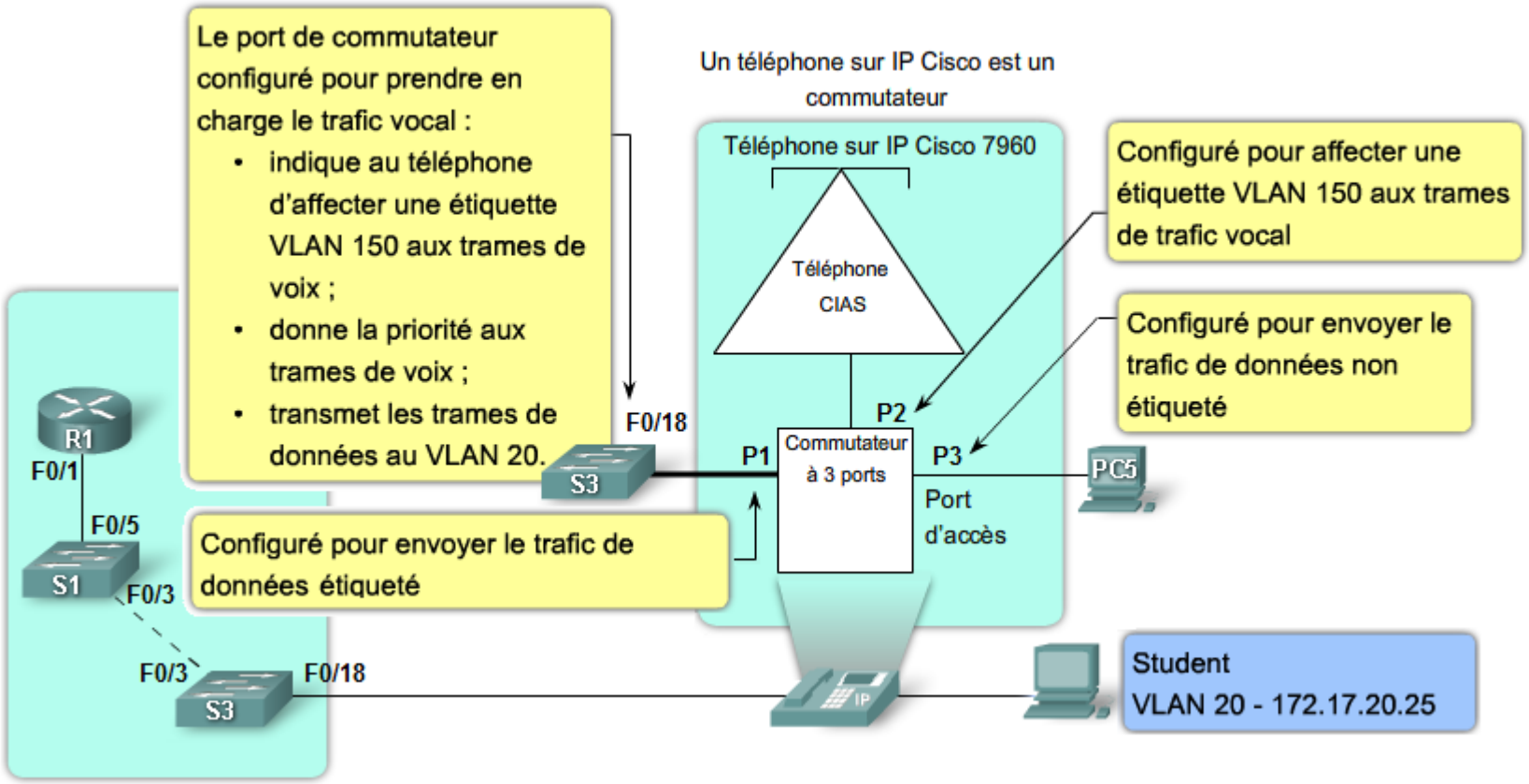
```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Agrégation des VLANs – Protocole DTP

- Le protocole DTP (Dynamic Trunking Protocol) est un protocole propriétaire développé par Cisco.
- L'objectif est que les ports des switches négocient s'ils passent en mode Trunk ou si ils restent en mode Access.
- DTP est activé par défaut (en mode dynamic auto) sur la plupart des Catalystes

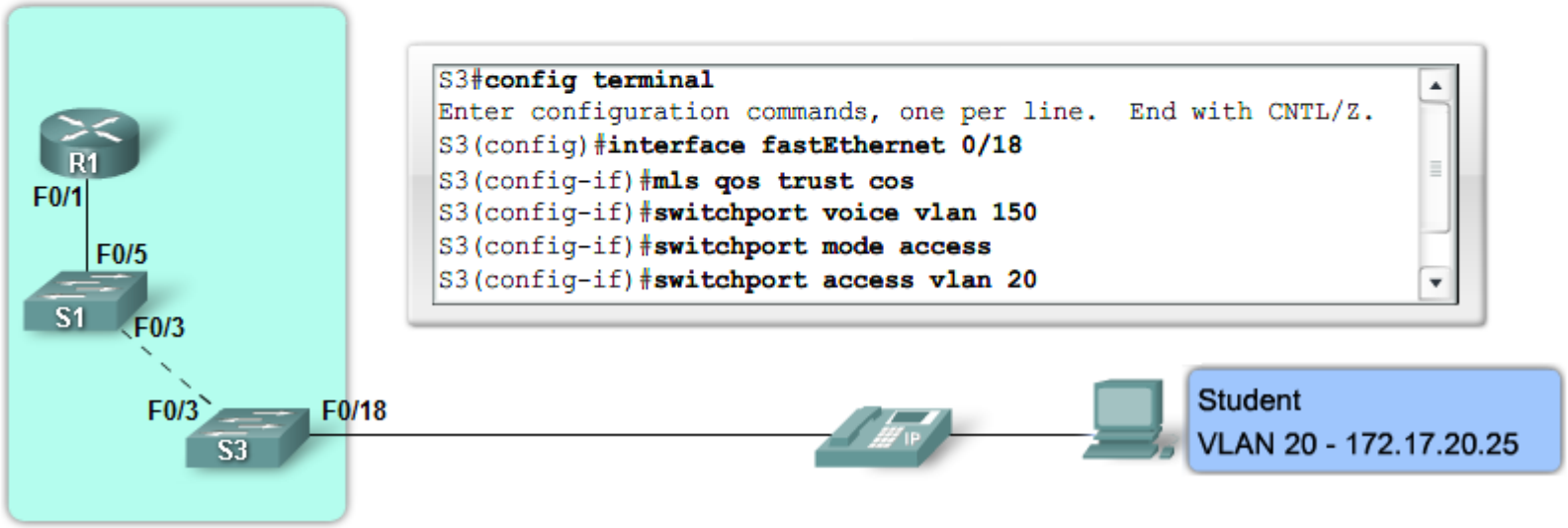
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

VLAN Voix - IP phones (VoIP)



VLAN Voix – Configuration

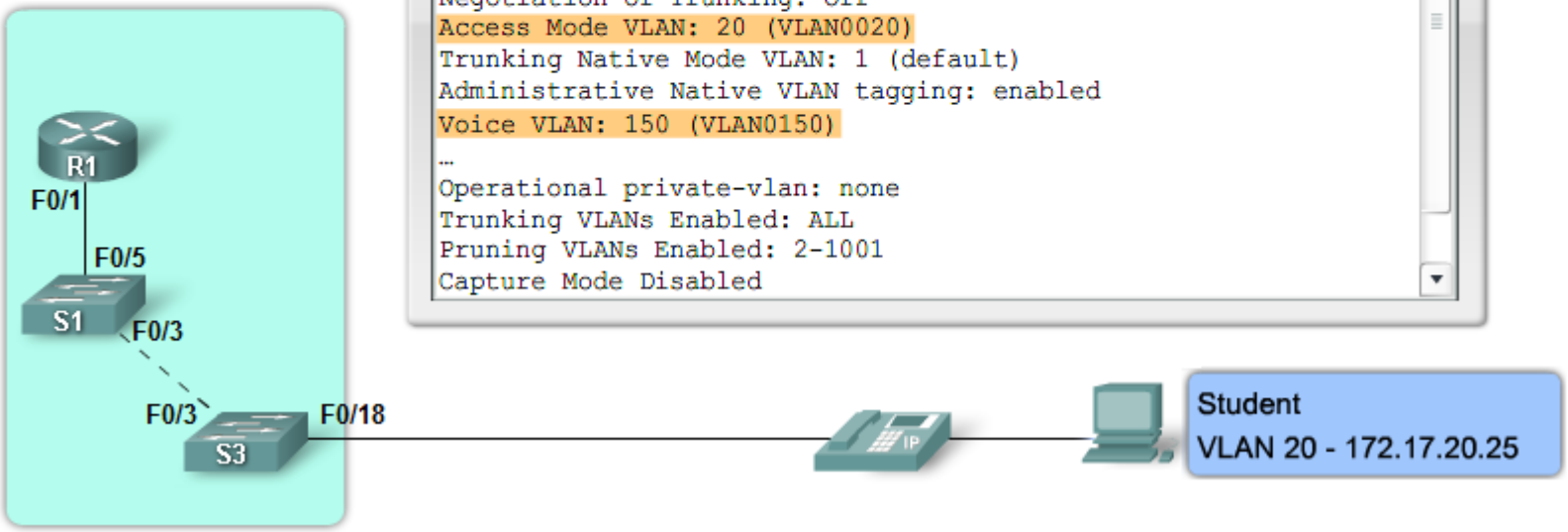
- Le port F0/18 doit logiquement être Trunk pour véhiculé les deux VLAN. Toutefois ce n'est pas le cas pour deux raisons principales:
  - Surcharge Administrative : Il faut changer la configuration (Access/Trunk) chaque fois que le téléphone est débranché/branché
  - Vulnérabilité majeure : Le port peut être utilisé pour connecter un autre switch



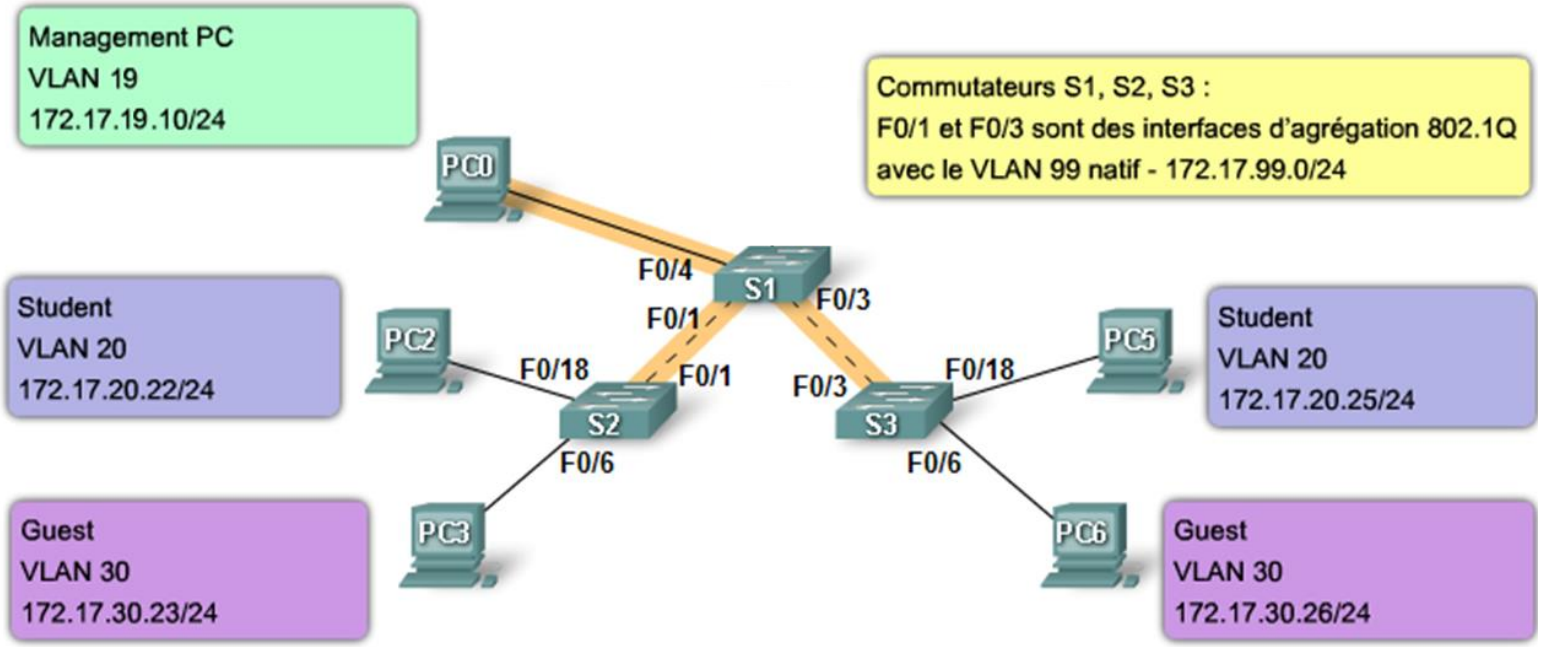

```
S3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface fastEthernet 0/18
S3(config-if)#mls qos trust cos
S3(config-if)#switchport voice vlan 150
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
```

VLAN Voix – Vérification

```
S3#show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
…
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```



VLAN de Gestion - configuration




```
Switch#
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 19
Switch(config-if)#ip address 172.168.19.102 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 172.168.19.1
Switch(config)#
```

VLAN de Gestion -Vérification

```
Switch#show running-config
Building configuration...

Current configuration : 1198 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan19
 ip address 172.168.19.102 255.255.255.0
!
ip default-gateway 172.168.19.1
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```