

# VLAN

---

# VLAN

---

## ***La notion de VLAN,***

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

# VLAN

---

## Intérêt des VLAN

Les VLAN présentent les intérêts suivants :

- Améliorer la gestion du réseau.
- Optimiser la bande passante.
- Séparer les flux.
- Segmentation : réduire la taille d'un domaine de broadcast,
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité.
- Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

# VLAN

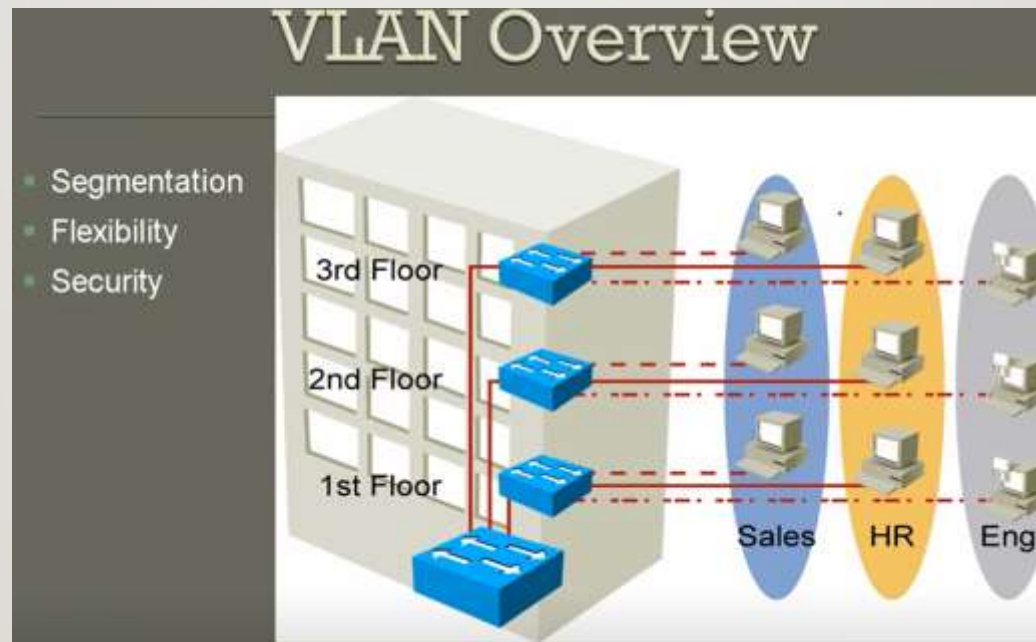
---

## ***POURQUOI CRÉER UN RÉSEAU VIRTUEL ?***

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

# VLAN

## POURQUOI CRÉER UN RÉSEAU VIRTUEL ?



# VLAN

---

## ***TYPOLOGIE DE VLAN (QUELS CRITÈRES)***

Trois méthodes sont généralement utilisées pour attribuer un équipement à un réseau VLAN :

**Les réseaux VLAN basés sur les ports;**

Les réseaux VLAN basés sur les adresses MAC;

Les réseaux VLAN basés sur les protocoles.



# VLAN

---

## **VLAN NIVEAU I**

Un VLAN de niveau I (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le switch ou commutateur.

Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

# VLAN

---

## **VLAN NIVEAU 2 L2**

Un VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations.

Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.



# VLAN

---

L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur.

Dans l'exemple du réseau VLAN composé d'imprimantes, imaginons qu'une imprimante soit retirée d'un port du commutateur pour être remplacée par un périphérique du service de comptabilité. Ce dernier dépendra désormais du réseau VLAN des imprimantes. Ceci risque de limiter l'accès du périphérique de comptabilité aux ressources du réseau.



# VLAN

---

Les réseaux VLAN basés sur les adresses MAC permettent de résoudre ce problème.

En effet, dans ce cas, l'appartenance au réseau VLAN dépend de l'adresse MAC du périphérique et non du port de commutation physique.

Lorsque le périphérique est retiré pour être connecté à un autre port, son appartenance au réseau VLAN le suit.

# VLAN

---

## Comprendre Mode Access && trunk

Les interfaces Ethernet peuvent être configurées en mode **accès** , mode **trunk**, ou **Auto** comme suit:

### Mode Accès

Un port d'accès ne peut avoir qu'un seul VLAN configuré sur l'interface;  
il ne peut transporter du trafic que pour un seul VLAN.

# VLAN

---

## **Port en mode Trunk:**

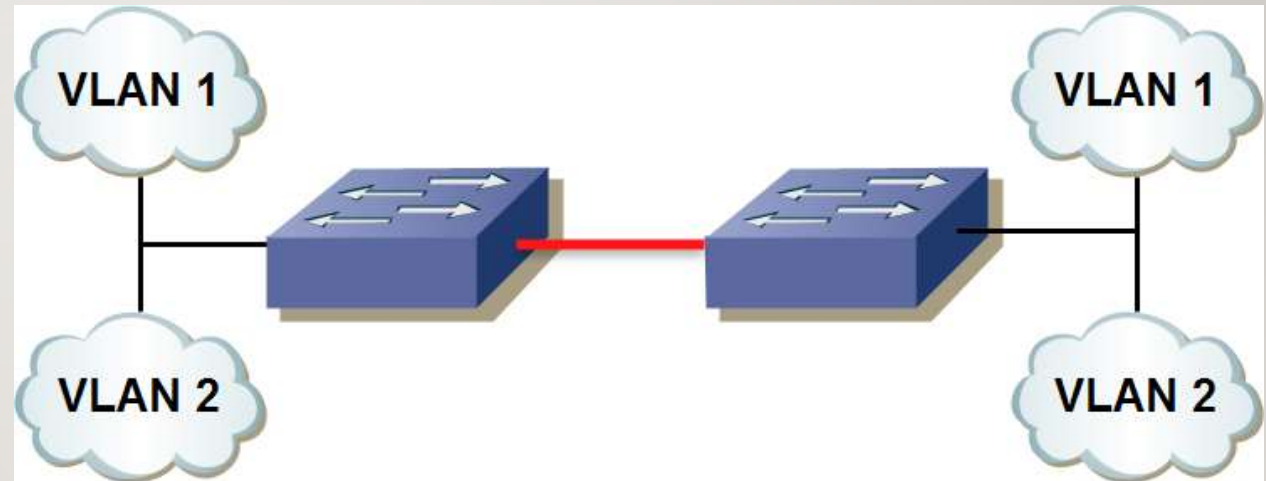
Un **trunk** est un lien entre deux équipements, le plus souvent entre deux switch, (Switch – routeur) configuré de telle sorte que l'on peut y faire circuler des trames Ethernet modifiées comportant des informations relatives au VLAN sur lequel elles transitent.

Prenons par exemple l'exemple où deux switch sont reliés l'un à l'autre, chacun ayant été configuré avec 2 VLANS, le VLAN 1 et le VLAN 2...

(Il peut avoir deux ou plusieurs VLAN configurés sur l'interface; il peut transporter du trafic pour plusieurs VLAN simultanément.)

# VLAN

## Trunk



Le but ici est que le **traffic** du VLAN1 de gauche puisse circuler sur le VLAN1 de droite et idem pour le VLAN2.  
Afin que cela soit possible, il faut configurer la liaison entre les deux switch en « **trunk** »



# VLAN

---

## **Trunk 802.1Q et ISL,**

Le **trunk** est le mécanisme qui permet d'insérer l'identifiant du **VLAN** sur une trame utilisateur.

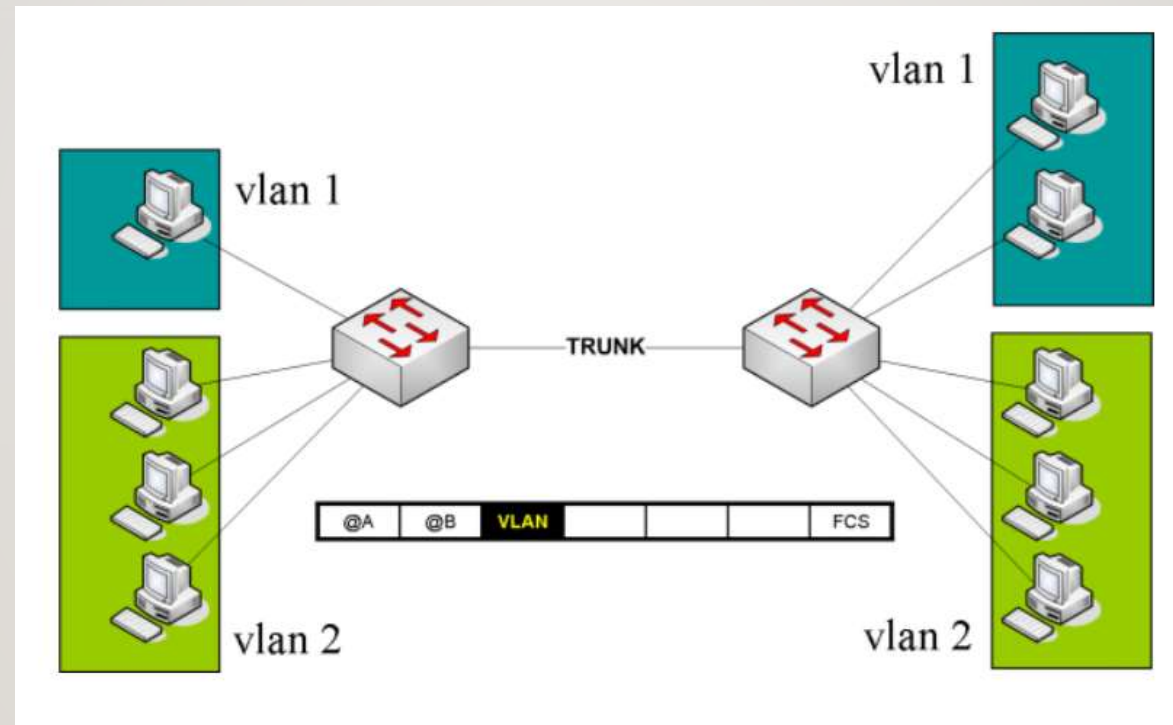
Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN.

Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN).

Cette configuration de lien **Trunk** s'effectue sur les liens entre switchs, (switch – routeur)



# VLAN



# VLAN

---

Dans le schéma ci dessous, on configure le lien inter-switch en **Trunk**.

Toutes les trames qui sortiront sur ce lien (switch de droite ou de gauche), se verront appliquer une étiquette supplémentaire qui contient l'identifiant du VLAN (en **noir** sur la trame).

Historiquement, Cisco avait créé son propre protocole de Trunk entre ses switches, nommé **ISL – Inter-Switch Link**.

La norme **Trunk 802.1Q** fut sortie et Cisco l'implémenta aussi dans ses switches.

D'où la possibilité sur certains switches Cisco de décider quel **trunk** on souhaite faire, ISL ou 802.1Q.

# VLAN

---

## Trunk ISL

Le trunk propriétaire Cisco ISL a la particularité **d'encapsuler toute la trame** de l'utilisateur dans une nouvelle trame, nommée trame ISL. Voici à quoi ressemble une trame ISL:

<b>Entête ISL</b> <b>26 octets</b>	<b>Trame Ethernet Utilisateur</b> <b>0 – 1500 octets</b>	<b>FCS</b> <b>4 octets</b>
---------------------------------------	---	-------------------------------

---

### 1- Inter Switch Link ( ISL ):

- It is a *Cisco* proprietary Trunking method that adds a *26-Byte header* and a *4-Byte trailer* to the original Ethernet frame.



# VLAN

---

**Remarque**: comme cette trame a un format particulier, il est obligatoire que le switch d'en face puisse comprendre ce formatage.

Il faut donc configurer le port du switch d'en face en trunk ISL.



# VLAN

---

## Configuration d'un VLAN,

*Switch>enable*

*Switch#Configure terminal*

*Swicth(conf)#Vlan (numéro)*

Pour afficher la configuration on tape la commande **show vlan** (Mode privilégié) ou **do show vlan** (Mode config)

```
Switch>enable
Switch#configu
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
```

**NB: Nombre max de vlan. (ca dépends de commutateur)**



# VLAN

---

## Attribution d'un port dans un vlan

###Mode privilégié###

Configure terminal (pour passer en mode config)

Interface (Numéro d'interface)

Switchport mode access

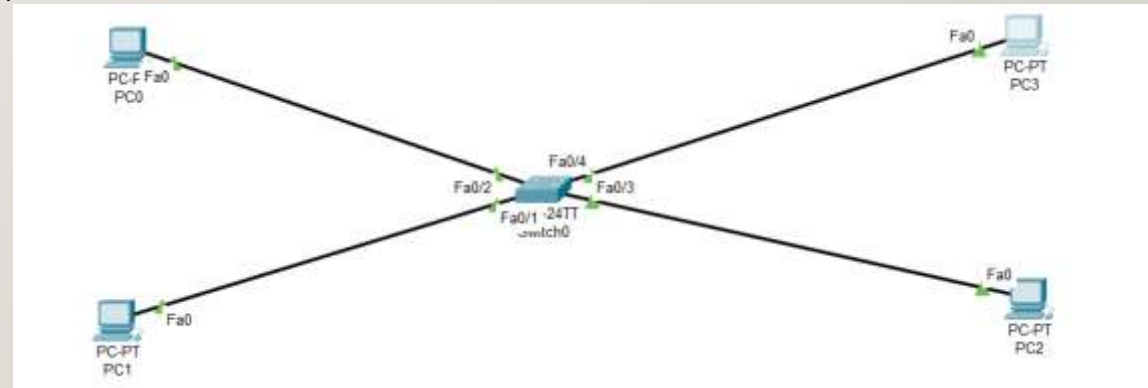
Switch accès vlan n°

# VLAN

---

Prenons l'exemple ci-dessous :

- Nous allons créer deux VLAN (VLAN 10 et VLAN 20)
- PC0 (branché sur F0/2 switch) VLAN 10
- PC1 (F0/2 switch) en VLAN 10
- PC3 (F0/4 Switch) VLAN 20 // PC2 (f0/3 switch)



# VLAN

- Nous allons créer deux VLAN (VLAN 10 et VLAN 20)

```
Switch(config-vlan)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#do show vlan
```

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 Gig0/1, Gig0/2
2	VLAN0002	active	
3	VLAN0003	active	
10	VLAN0010	active	
20	VLAN0020	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0

--More--

# VLAN

---

Mettre PC0 (branché sur F0/2 switch) VLAN 10 // PC1 (F0/2 switch) en VLAN 10

## SWITCH ##

```
Switch(config)#interface f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport acce
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

P-0

---

PC3(F0/4 Switch) VLAN 20 // PC2 (f0/3 swicth) Vlan 20

```
Switch(config-if)#interface f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

---

Pour faire communiquer les machines du mêmes VLAN, on doit configurer des IP pour les machines,

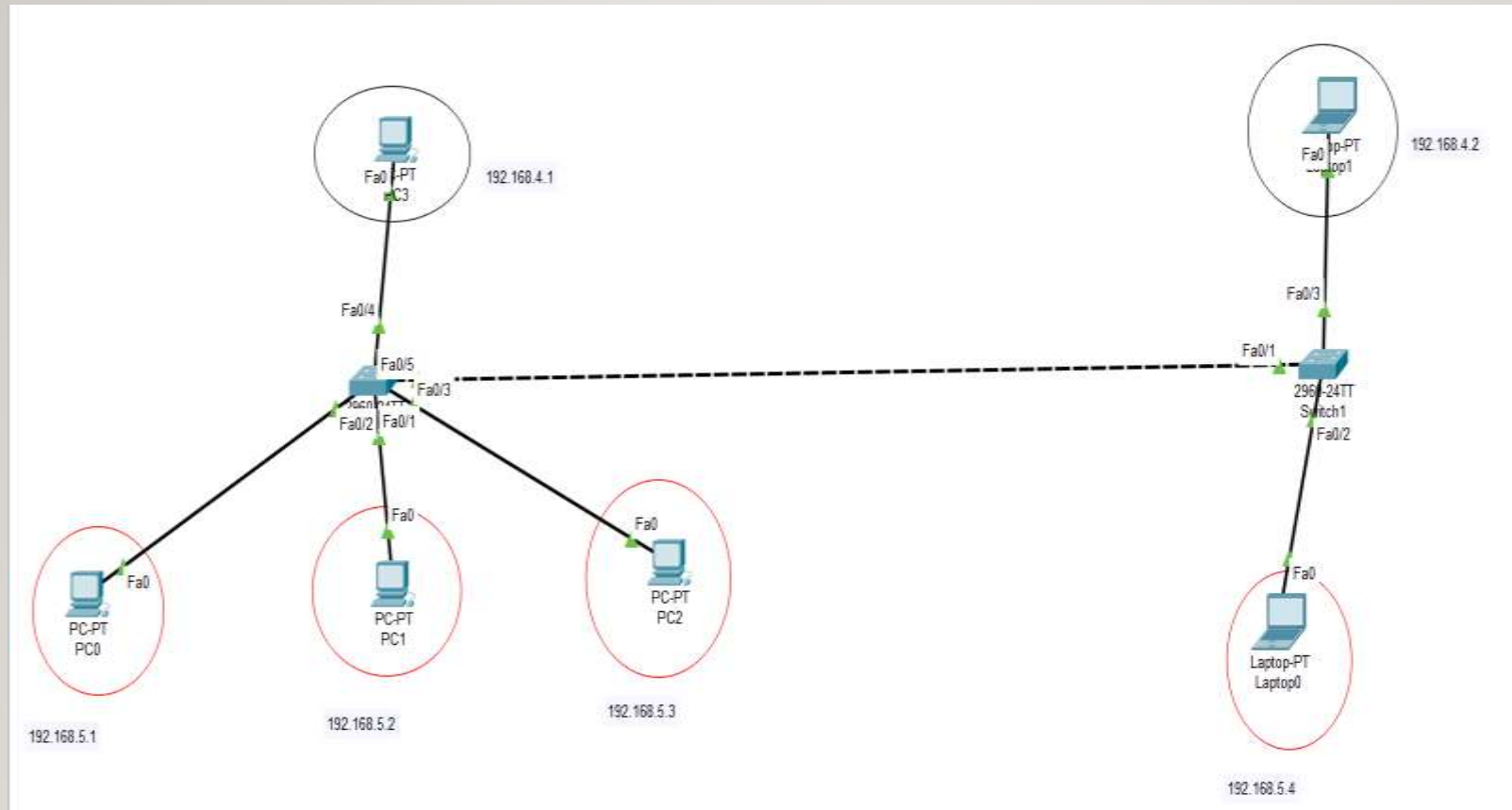
Pour VLAN 1 nous allons prendre le réseau : 10.1.1.0/24

VLAN 2 nous allons prendre l'adresse : 192.168.5.0/24



- 
- En : show interfaces f0/1 switchport //

```
SW1#sh interfaces f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```



ur exemple)