

2021

Cours réseau : Comment séparer son réseau avec les VLAN



Donat FUZELLIER –

<http://reussirsonccna.fr/comment-separer-son-reseau-avec-les-vlan-2/>.

Donat FUZELLIER

Seo-webranking

17/12/2021

Table des matières

Comment séparer son réseau avec les VLAN	3
Définition	3
Les différentes utilisations de VLAN	4
Appartenance à un VLAN	4
Remarques	5
Configuration d'un VLAN sur un switch	6
Attribution d'un port dans un VLAN	6
Astuce.....	6
Important	7
A savoir aussi pour le CCNA	7

Comment séparer son réseau avec les VLAN

0



Aujourd'hui, il est plus que fréquent de voir l'utilisation de VLAN au sein d'un réseau d'entreprise.

Quand on branche tous les PC, imprimantes, serveurs sur un switch, ils peuvent communiquer entre eux sans même pré-configurer le switch. C'est du plug & play, "on branche, ça fonctionne". On dit que toutes les entités font parties du même **LAN – Local Area Network**, ou **réseau local** en français.

Au contraire, si vous souhaitez interdire la communication entre certaines entités, par exemple, que certains PC de R & D ne puissent pas communiquer avec les PC de production, vous avez 2 solutions:

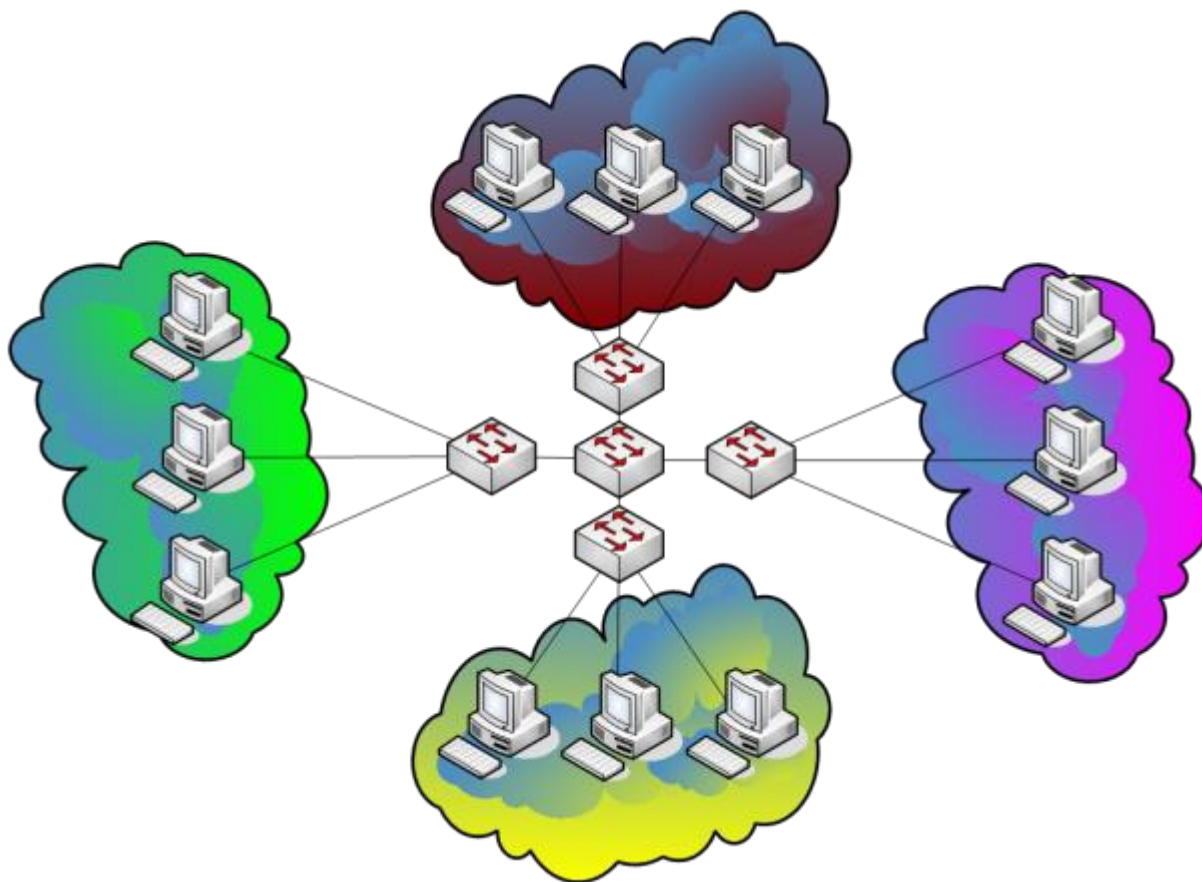
- brancher les PC de R & D sur un second switch
- ou découper "virtuellement" votre switch en deux switches logiques → C'est le **VLAN**

Définition

Selon [wikipedia](https://fr.wikipedia.org/wiki/VLAN), "un réseau local virtuel, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau."

Par exemple, les entités branchés sur les ports du switch qui sont configurés dans le VLAN 2 **pourront communiquer** entre eux et c'est tout. Tous les autres ports du switch qui n'appartiennent pas au VLAN 2 **ne pourront pas communiquer** avec ceux du VLAN 2.

Dans le schéma ci dessous, on a segmenté les PC par groupe de 3. La communication entre PC appartenant au VLAN vert est possible mais aucune communication ne pourra sortir de ce VLAN vert pour atteindre d'autres PC du réseau.



Les différentes utilisations de VLAN

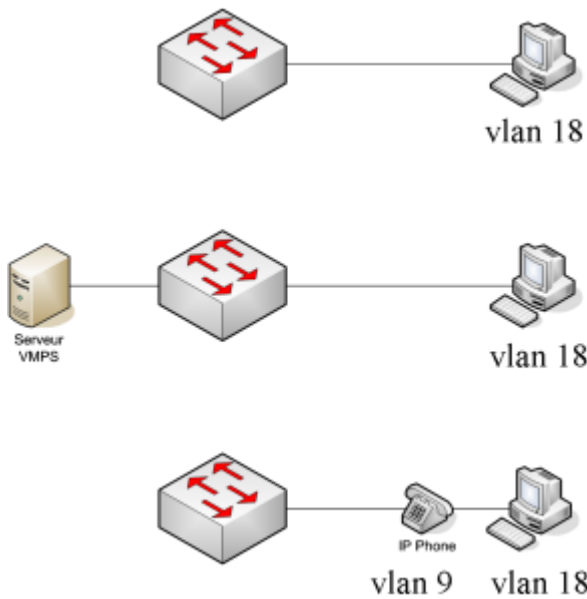
Maintenant qu'on sait à quoi sert le VLAN, on peut l'utiliser en fonction de nos besoins. On peut lister les différents VLANs qu'on aura besoin dans un réseau d'une entreprise classique:

- 1 VLAN pour le service commercial, 1 VLAN pour le service administratif, 1 VLAN pour le service ingénierie...
- 1 VLAN pour le service de téléphonie sur IP
- 1 VLAN pour le service de visioconférence
- 1 VLAN pour l'administration réseau (important, on va mettre les équipements réseau, switch, routeur... dans un VLAN dédié uniquement accessible aux stations des administrateurs réseau)
- ...

Appartenance à un VLAN

Comment configurer un VLAN et attribuer des entités dans ce VLAN?

Il y a plusieurs solutions dont voici les 3 principales:



La **première solution** est celle la plus utilisée: On crée le VLAN sur le switch puis on attribue ce VLAN sur les ports souhaités. Par exemple sur le 1er schéma, le port du switch qui est branché au PC est configuré pour être dans le VLAN 18.

Seconde solution beaucoup moins utilisée: On configure le switch pour qu'il récupère l'adresse MAC qu'il voit transiter sur le port, puis envoie cette adresse MAC vers un serveur **VMPS** (VLAN Membership Policy Server) qui fait le lien entre l'adresse MAC et le VLAN attribué via une base de données. Le serveur VMPS indique au switch quel VLAN il faut attribuer au port. Le principal inconvénient vient de la fragilité du serveur; s'il tombe en panne, tout le réseau est bloqué !

Dernière solution très utilisée dans le cas d'un réseau avec téléphonie sur IP. On utilise la 1ère solution pour attribuer le VLAN au PC. Pour le téléphone sur IP, on utilise le protocole **CDP** (Cisco Discovery Protocol) pour attribuer le VLAN voix uniquement au trafic voix.

Remarques

- Le nombre maximum de VLAN que l'on peut créer dépend du type de switch (64, 128, 1024, 4096)
- **Le VLAN 1 est créé par défaut et tous les ports du switch appartiennent à ce VLAN**
- Il faut d'abord créer l'identifiant du VLAN puis attribuer des ports dans ce VLAN
- On peut donner un nom à un VLAN (optionnel), par exemple:
 - VLAN 1 – Management
 - VLAN 2 – Commerciaux
 - VLAN 3 – Voix
 - VLAN 4 – Finance

De plus, certains VLAN sont réservés (donc non utilisables) et d'autres sont créés par défaut:

Plage de VLAN	Utilisation
0, 4095	Réservé pour le système, non utilisable
1	VLAN par défaut
2–1001	VLAN Ethernet
1002–1005	VLANs créés par défaut pour les technologies FDDI et Token Ring
1006–4094	VLAN Ethernet – plage étendue (attention aux switchs anciens)

Configuration d'un VLAN sur un switch

Rien de plus facile... créons le VLAN n°2 que l'on va nommer "finance"

```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name finance
SwitchX(config-vlan)#end
```

Attribution d'un port dans un VLAN

On identifie le port du switch (par exemple l'interface **fastethernet 0/1**) qui doit être dans le VLAN 2 précédemment créé :

```
SwitchX# configure terminal
SwitchX(config)# interface fastethernet 0/1
SwitchX(config-if)# switchport access vlan 2
SwitchX(config-if)# end
SwitchX# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2
2	finance	active	Fa0/1

On voit avec la commande **show vlan** que le port Fa0/1 est désormais dans le VLAN 2, nommé **finance**.

La commande **switchport access vlan 2** permet de mettre le port Fa0/1 dans le vlan 2. Le port **Fa0/1** n'appartient plus au VLAN précédent qui par défaut est le VLAN 1.

Astuce

Pour configurer plusieurs ports (exemple avec les ports 0/2 à 0/7) dans un VLAN, on peut utiliser la variable **range** pour configurer en une seule fois tous les ports:

```
SwitchX# configure terminal
SwitchX(config)# interface range fastethernet 0/2 - 7
SwitchX(config-if)# switchport access vlan 2
SwitchX(config-if)# end
SwitchX# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1
2	finance	active	Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7

Important

Le fait de mettre un port dans un VLAN dépend du mode du port. Je m'explique: dans un switch Cisco, le port peut être dans 2 modes:

- mode **Access**
- mode **Trunk**

J'explique les 2 modes dans un autre chapitre à venir.

Revenons à notre sujet, le port sera donc dans le VLAN **que s'il est en mode Access**. Pour savoir si le port est en mode **Access** ou **Trunk**, vous pouvez utiliser la commande suivante:

```
SwitchX# show interfaces fa0/2 switchport Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (finance)
Trunking Native Mode VLAN: 1 (default)
...
```

On voit que le port est en **static access** donc c'est bon!

A savoir aussi pour le CCNA

Pour le CCNA, il est important de savoir que les VLAN permettent de **limiter la propagation** des messages de broadcast (c'est à dire j'envoie un message à tout le monde dans le réseau). En effet, si tout le monde s'amuse à envoyer des messages de broadcast alors le réseau va vite saturer.

De même, pour l'examen CCNA mais aussi pour établir un design correct de son réseau, il faut retenir qu'à un VLAN créé, on attribue bien évidemment des ports de switch dans ce VLAN **mais surtout** que les PC branchés sur ces ports doivent être dans le même plan d'adressage IP. En effet, si on segmente au niveau 2 par des VLANs, il est primordial d'être cohérent avec le niveau 3.

Donc à retenir pour le CCNA:

- **VLAN = un domaine de broadcast**
- **à un VLAN créé, on attribue un sous-réseau IP dédié**