Comment séparer son réseau avec les VLAN

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 préconfigurer 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 les PC « Compta » ne puissent pas communiquer avec les PC « Secrétariat », vous avez 2 solutions :

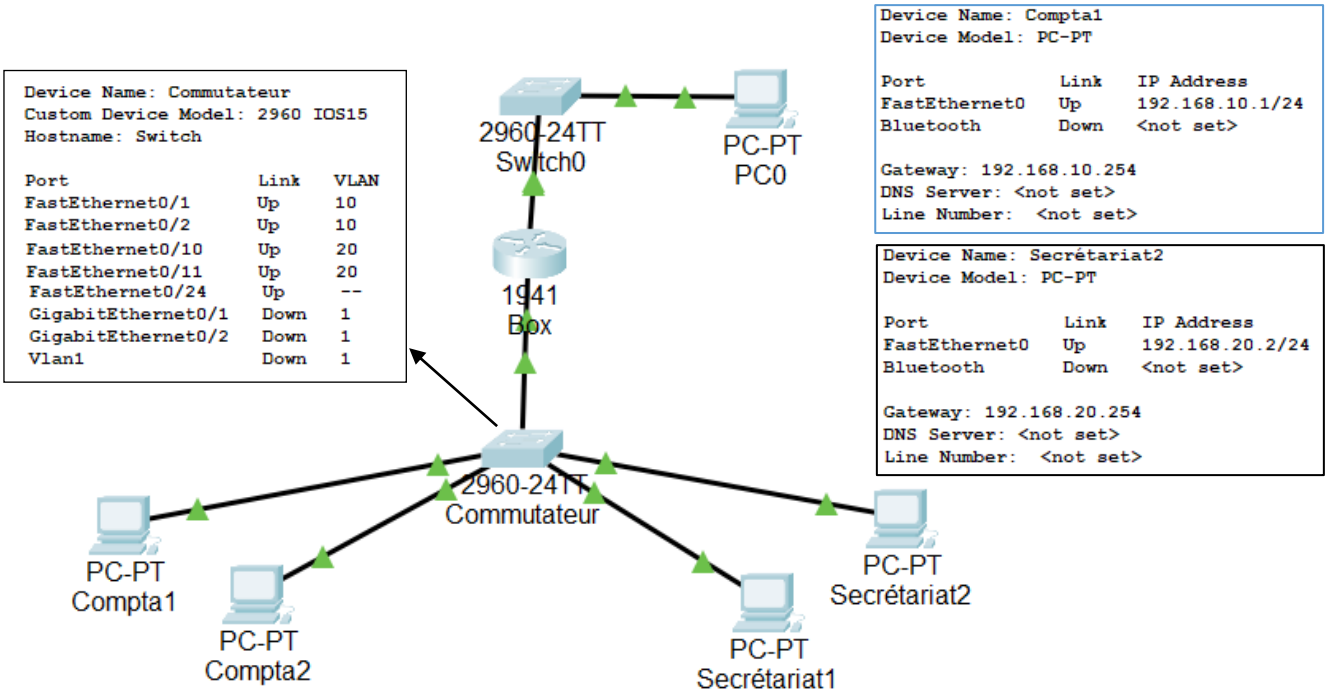
- brancher les PC « Secrétariat » sur un second switch
- ou découper « virtuellement » votre switch en deux switchs logiques –> C'est le VLAN

DEFINITION

Selon wikipedia, « 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 branchées 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 2. La communication entre PC appartenant au VLAN compta est possible mais aucune communication ne pourra sortir de ce VLAN pour atteindre d'autres PC du réseau, à part uniquement le PC0 (après la box).



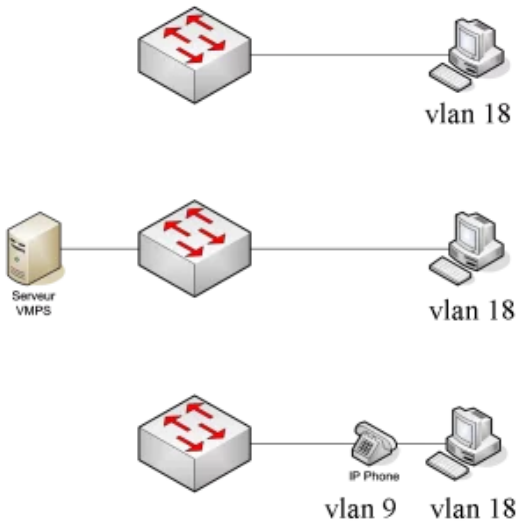
LES DIFFERENTES UTILISATIONS DE VLAN

Maintenant qu'on sait à quoi sert le VLAN, on peut l'utiliser en fonction de nos besoins. On peut lister les différents VLANs dont 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 comptabilité…
- 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)
- …

COMMENT CONFIGURER UN VLAN ET ATTRIBUER DES ENTITES DANS CE VLAN ?

Il y a plusieurs solutions dont voici les 3 principales :



La **première solution** est celle la plus utilisée : On créé 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 envoi 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 utilisé 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) : 0 et 4095

Et d'autres sont créés par défaut : 1, 1002-1005 (techno FDDI et Token Ring), 1006-4094 (Ethernet – plage étendue)

CONFIGURATION D'UN VLAN SUR UN SWITCH

Rien de plus facile… créons le VLAN n°10 que l'on va nommer « compta »

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name compta
Switch(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 10 précédemment créé :

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/2
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
Switch# show vlan

VLAN  Name              Status    Ports
----  ----------------  --------  ---------------------
10    compta            active    Fa0/1, Fa0/2
```

On voit avec la commande **show vlan** que le port Fa0/1 est désormais dans le VLAN 10, nommé **compta**.

La commande **switchport access vlan 2** permet de mettre les ports Fa0/1 et Fa0/2 dans le vlan 10. 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 :

```
Switch# configure terminal
Switch(config)# interface range fastethernet 0/2 - 7
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
```

Vous pouvez configurer le sous-réseau **secrétariat** de la même façon en **vlan 20**.

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

CONFIGURATION PORT SWITCH – ROUTER

Vu que nous sommes en présence que d'un seul lien montant du switch vers le routeur, nous devons créer un lien 802.1q, qui permet d'encapsuler le label du VLAN dans le paquet réseau : mode **Trunck**

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fastethernet 0/24
Switch(config-if)# switchport trunk allowed vlan 10,20
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

CONFIGURATION PORTS SWITCH - PC

Le port connecté au PC 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 :

```
Switch# show interfaces fa 0/2 switchport
Name: Fa0/2
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: 10 (compta)
Trunking Native Mode VLAN: 1 (default)
...
```

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

Sauvegarde de la configuration dans la NVRAM

```
Switch# copy running-config startup-config
```

CONFIGURATION COTE ROUTEUR

Comme notre routeur contient une seule interface physique reliée au switch, nous devons créer deux interfaces virtuelles afin de pouvoir adresser les deux passerelles de chaque réseau. 10 et 20 corresponde au numéro de VLAN.

```
Router> enable
Router# configure terminal
Router(config)# interface gig0/0.10                    # création de la 1er int virtuelle
Router(config-subif)# encapsulation dot1Q 10       # tj avant l'@ passerelle
Router(config-subif)# ip address 192.168.10.254 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gig0/0.20                    # création de la 2nd int virtuelle
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.254 255.255.255.0
Router(config-subif)# no shutdown
Router(config-subif)# end
Router# copy running-config startup-config       # sauvegarde
```

A partir du PC-Compta1 ou Compta2, test d'accès à la box

```
C:\>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255
Reply from 192.168.10.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

A partir du PC-Compta1, test d'accès au PC-Secrétariat1

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=127
Reply from 192.168.20.1: bytes=32 time<1ms TTL=127
Reply from 192.168.20.1: bytes=32 time<1ms TTL=127
Reply from 192.168.20.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dans l'état actuel la communication entre les VLAN est possible via le routeur. En effet vous pouvez vérifier que PC-Compta1 communique avec PC-Secretariat1 en passant par le routeur (commandes ping et tracert).

C'est normal : par défaut un routeur route le trafic entre les réseaux auxquelles il est directement connecté. Si nous voulons interdire le trafic entre les vlan, mais permettre l'accès à internet, il faut configurer des **ACL** (Access Control List).

CONFIGURATION DES ACL SUR LE ROUTEUR

Création de l'ACL 110 pour le réseau « Compta » et de l'ACL 120 pour le réseau « Secretariat »

- Blocage les adresses provenant de 192.168.10.0/24 vers 192.168.0.0/16 sauf la passerelle 192.168.10.254

```
Router> en
Router# configure terminal
Router(config)# access-list 110 remark Stoppe les adresses provenant de 192.168.10.0/24 vers
192.168.0.0/16 sauf la passerelle 192.168.10.254
Router(config)# access-list 110 permit ip 192.168.10.0 0.0.0.255 host 192.168.10.254
Router(config)# access-list 110 deny  ip 192.168.10.0.0 0.0.0.255 192.168.0.0 0.0.255.255
Router(config)# access-list 110 permit ip any any
```

- Blocage les adresses provenant de 192.168.20.0/24 vers 192.168.0.0/16 sauf la passerelle 192.168.20.254

```
Router> en
Router# configure terminal
Router(config)# access-list 120 remark Stoppe les adresses provenant de 192.168.20.0/24 vers
192.168.0.0/16 sauf la passerelle 192.168.20.254
Router(config)# access-list 120 permit ip 192.168.20.0 0.0.0.255 host 192.168.20.254
Router(config)# access-list 120 deny ip 192.168.20.0.0 0.0.0.255 192.168.0.0 0.0.255.255
Router(config)# access-list 120 permit ip any any
Router(config)# end
```

- Application les ACL sur chaque interface du routeur

```
Router(config)# interface interface gig0/0.10
Router(config-subif)# ip access-group 110 in
Router(config-subif)# exit
Router(config)# interface interface gig0/0.20
Router(config-subif)# ip access-group 120 in
```

- Désactivation du proxy-arp sur chaque interface du routeur

```
Router> en
Router# configure terminal
Router(config)# interface interface gig0/0.10
Router(config-subif)# no ip proxy-arp
Router(config-subif)# exit
Router(config)# interface interface gig0/0.20
Router(config-subif)# no ip proxy-arp
Router(config-subif)# no shutdown
Router(config-subif)#end
```

- Création de l'interface de sortie de la box

```
Router> en
Router# configure terminal
Router(config)# interface interface gig0/1
Router(config)# ip address 10.10.10.254 255.255.255.0
Router(config-subif)# no shutdown
Router(config-subif)#end
```

- Sauvegarde en mémoire NVRAM

```
Router> en
Router# copy run start
```

TESTS DE VERIFICATION

Réaliser des tests à partir de commandes « ping » pour vérifier les communications suivantes :

- D'un poste « Compta » vers un poste « Compta »
- D'un poste « Secrétariat » vers un poste « Secrétariat »
- D'un poste « Compta » vers un poste « Secrétariat »
- D'un poste « Compta » vers le poste PC0
- D'un poste « Secrétariat » vers le poste PC0

Conclure sur le bon fonctionnement du routage inter-VLAN.