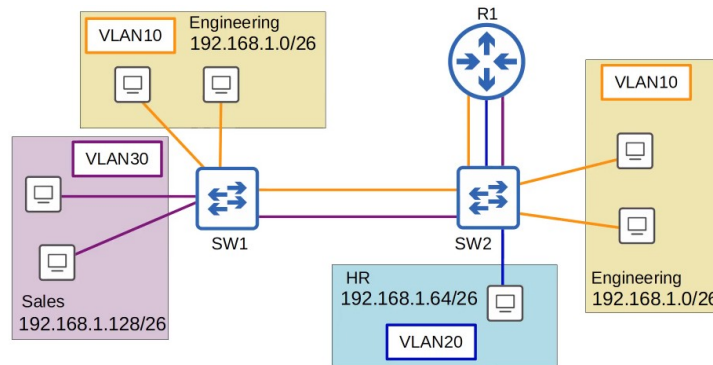


Cours 17 : Vlan

Dans ce cours nous allons continuer l'apprentissage à propos des Vlan (Virtual Local Area Network). Tout d'abord nous verrons ce qu'est qu'un port Trunk et son but, puis ce qu'est l'encapsulation 802.1Q, nous verrons ensuite comment configurer un port Trunk et ce qu'est « Router on a Stick » (ROAS).

Voici la topologie réseau que nous utiliserons dans ce cours :



Il n'y a pas de lien en Vlan20 entre SW1 et SW2. Ceci car il n'y a pas de PC dans le Vlan 20 connectés au SW1. Les PC dans le Vlan 20 peuvent tout de même joindre les PC connectés au SW1. R1 fonctionne avec un routage inter-vlan c'est à dire que lorsqu'un pc veut communiquer avec un pc se trouvant sur un autre vlan c'est le routeur qui va rediriger le trafic vers le vlan adapté.

Dans un petit réseau avec peu de Vlan il est possible d'utiliser des interfaces dédiées pour chaque Vlan lorsque l'on connecte des switchs entre eux, et les switchs aux routeurs.

Lorsqu'il y a beaucoup de vlan il n'est plus vraiment possible de connecter une interface par vlan car il n'y aura plus assez d'interface pour chaque Vlan.

Une solution est d'utiliser le Trunk pour que le trafic soit multiplié en plusieurs Vlans sur une seule interface.

Imaginons qu'un PC de Vlan 10 veuille envoyer un paquet vers un autre PC sur la Vlan 10, le trafic ne passera pas par le routeur obligatoirement il peut passer directement vers le SW1 pour distribuer le paquet mais une fois au SW1 comment le Switch saura t-il sur quelle interface distribuer le paquet ?

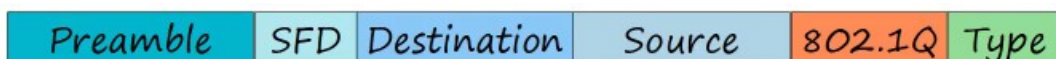
La réponse est en marquant la trame envoyé sur le lien trunk cela permet d'identifier et savoir à quelle Vlan la trame appartient.

Il existe deux principaux protocoles de trunk : ISL (Inter-Switch Link) et IEEE 802.1Q

ISL est un ancien protocole Cisco propriétaire crée avant le standard industrie : IEEE 802.1Q

IEEE 802.1Q est un protocole de standard industrie crée par le IEEE (Institute of Electrical and Electronics Engineers). On utilisera probablement jamais ISL dans le monde réel même si les Cisco moderne le supporte.

Le marquage du type de protocole de trunking est inséré dans l'entête Ethernet entre l'adresse IP source et le Type de paquet/longueur du paquet :



Le tag est de 4 bytes (32 bits) de longueur ; ce marquage consiste en deux parties principales :

- Tag Protocol Identifier (TPID) et le Tag Control Information (TCI)

Le TCI consiste en 3 sous parties.
Voici une capture du format 802.1Q :

802.1Q tag format			
16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

- Le TPID est de 16 bits (2 bytes) de longueur, la valeur indiquée est toujours : 0x8100 en hexadécimal. Cela indique la trame marqué par le 802.1Q.
 - Le PCP (priority Code Point) est de 3 bits de longueur. Et utilisé pour le Class of Service (COS) qui priorise le trafic important dans un réseau.
 - Le DEI (Drop Eligible Indicator) est de 1 bit de longueur et utilisé pour indiquer la trame qui peut être lâché si le trafic réseau est trop important.
 - Le VID est d'une longueur de 12 bits, il permet d'identifier le Vlan et à quelle trame il appartient. 12 bits de longueur = 4096 Vlan en tout (2^{12}), se qui fait un classement de 0 – 4095
Les Vlan 0 et 4095 sont réservés et ne peuvent pas être utilisés, le classement des Vlan se fait donc de 1 – 4094.
- Le protocole ISL Cisco à aussi un classement Vlan de 1 – 4094

Le classement des Vlan (1- 4094) est divisé en deux sections :
Normal Vlan : 1 – 1005
Vlan étendus : 1006 – 4094

Certains anciens appareils n'utilisent plus le classement Vlan, même s'il est plus sûr de s'attendre qu'un Switch moderne va supporter un classement Vlan étendu.

Donc si l'on reprend la question du départ avec notre topologie réseau et qu'un PC se trouvant dans le Vlan 10 veut envoyer une donnée à un autre PC se trouvant dans le Vlan 10, il va directement passer par le Switch sans passer par le routeur et le SW1 va distribuer le trafic directement au Vlan adapté grâce au marquage inscrit dans le l'entête Ethernet.

802.1Q à une fonctionnalité appelé native VLAN (ISL ne possède pas cette fonction) Le Vlan Natif est le Vlan 1 par défaut sur tous les ports trunk, il peut être configuré manuellement sur chaque port Trunk. Le Switch n'ajoute pas un tag 802.1Q à la trame native du Vlan. Lorsqu'un switch reçoit une trame non marqué dans un port trunk, il l'attribue au Vlan natif.
Il est donc important que les Vlan natif soient correspondant entre switchs sinon le paquet risque d'être mal distribué.

Voici à présent les commandes nécessaire pour la configuration d'un interface en mode trunk :

```
SW1(config)#interface g0/0  
SW1(config-if)#switchport trunk encapsulation dot1q  
SW1(config-if)#switchport mode trunk
```

Pour manuellement configurer une interface comme port trunk, il faut d'abord placé l'encapsulation en 802.1Q ou ISL. Sur les switchs qui supportent uniquement 802.1Q cela n'est pas nécessaire.
Une fois l'encapsulation mis en place il faut configurer l'interface en trunk.

On peut ensuite utiliser la commande suivante pour vérifier la configuration de l'interface en mode trunk :

```
SW1#show interfaces trunk
```

Voici les commandes pour ajouter la permission d'une vlan pour un trunk :

```
SW1(config)#int g0/0
```

```
SW1(config-if)#switchport trunk allowed vlan add 20
```

Pour supprimer la permission d'une Vlan sur un trunk on lance la commande :

```
SW1(config)#int g0/0
```

```
SW1(config-if)#switchport trunk allowed vlan remove 20
```

Pour ajouter la permission de toutes les vlan pour le trunk on lance la commande :

```
SW1(config-if)#switchport trunk allowed vlan all
```

On peut aussi excepter certains Vlan de la permission à toutes les Vlan en lançant la commande :

```
SW1(config-if)#switchport trunk allowed vlan except 1-5,10
```

On peut empêcher toute les Vlan d'utiliser le mode trunk en lançant la commande :

```
SW1(config-if)#switchport trunk allowed vlan none
```

Pour plus de sécurité il est conseillé de changer le Vlan natif à un Vlan inutilisé tout en étant sûr que le vlan native est la même entre les switches.

La commande pour changer le Vlan Natif est :

```
SW1(config-if)#switchport trunk native vlan 1001
```

Au lieu d'utiliser 3 interface différentes pour connecter le switch au routeur 1 comme dans la topologie, il est possible d'utiliser un seul câble interface et de configurer des « sub-interface » afin que le trafic soit redirigé vers les trois Vlan et fonctionner comme 3 interfaces séparés.

Voici les commandes pour configurer des « sub-interface » sur le routeur1 :

```
R1(config)#interface g0/0
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#interface g0/0.10
```

```
R1(config-if)#encapsulation dot1q 10
```

```
R1(config-if)#ip address 192.168.1.62 255.255.255.192
```

On peut vérifier la configuration des sub-interface avec la commande :

```
R1#show ip interface brief
```

ROAS est utilisé pour faire le routage entre plusieurs Vlan en utilisant une seule interface dans un routeur et un switch. L'interface switch est configuré comme un trunk regular. L'interface de routage est configuré utilisant des subinterfaces. On configure le marquage Vlan et l'adresse IP sur chaque subinterface. Le routeur à la trame qui arrive avec un certain marquage Vlan configuré avec le tag Vlan. Le routeur va marquer la trame envoyé vers la sub-interface avec le marquage Vlan configuré sur la sub-interface.