
TD n°2

Les réseaux locaux virtuels (VLAN)

Exercice 1 *Utilité des VLANs*

1. Rappelez pourquoi les VLANs sont utiles
2. Pourquoi sont-ils un élément important de la sécurité d'un réseau ?
3. Quels matériels sont mis à contribution pour faire fonctionner un réseau de VLANs ?
4. Quels paramètres sont à régler sur une station de travail pour qu'elle puisse participer à un VLAN ?
5. Comment rendre possible la communication entre VLANs ?
6. Dans le cas où on attribue un sous-réseau IP par VLAN, cette technique ne devient-elle pas équivalente à la simple segmentation en sous-réseaux ?
7. Quels sont les protocoles mis en oeuvre pour faire fonctionner un réseau de VLANs ?
8. Pouvez-vous donner des exemples des situations réelles où l'utilisation des VLANs est indispensable ?

Exercice 2 *Les différents méthodes d'attribution de VLANs*

1. Rappelez quels sont les différents méthodes d'attribution de VLAN
2. Discutez des avantages de ces différentes méthodes
3. Laquelle vous semble la plus intéressante ?

Exercice 3 *Fonctionnement des switches*

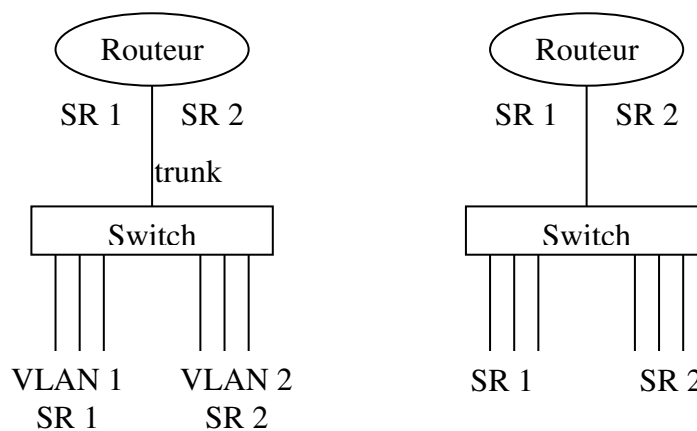
1. Combien y-a-t-il de tables d'adresses MAC dans un switch ?
2. A quel VLAN appartient un port en mode trunk ?
3. Que se passe-t-il quand un switch reçoit un broadcast de niveau 2 sur un port appartenant à un VLAN ?
4. Que se passe-t-il quand un switch reçoit un broadcast de niveau 2 sur un port appartenant à plusieurs VLAN ?
5. Que se passe-t-il quand un switch reçoit un broadcast de niveau 2 sur un port utilisé en mode trunk ?
6. Que se passe-t-il quand un switch reçoit un broadcast de niveau 3 sur un port appartenant à un VLAN ?

Exercice 4 Topologie

Vous disposez d'un routeur avec deux ports série et un port Ethernet. Vous devez le connecter à un lien WAN vers votre fournisseur d'accès Internet et à quatre VLANs internes.

1. Que devez-vous vérifier sur le routeur avant de faire quoi que ce soit d'autre ?
2. Quel type de configuration allez-vous donner à l'interface Ethernet ?
3. Vous avez choisi le marquage des trames 802.1q. Il n'y a aucune erreur dans la configuration du routeur, tous les cordons de brassage sont correctement positionnés, et pourtant, rien ne marche. Quel est la cause probable de l'erreur ?

Exercice 5 VLAN versus sous-réseaux



1. Comparez les deux architectures ci-dessus. Pourquoi n'obtient-on pas le même fonctionnement ?
2. Laquelle des solutions vous semble la meilleure du point de vue de la sécurité ?

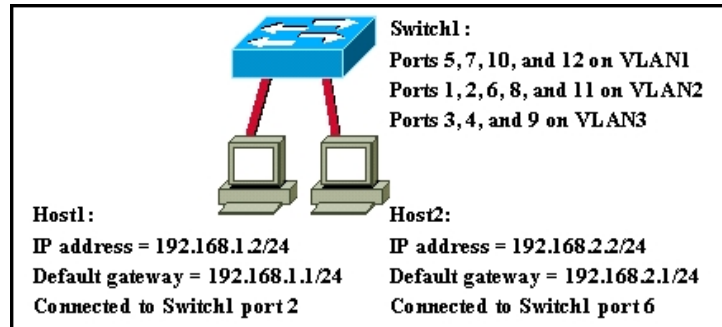
Exercice 6 Configuration

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#exit
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
```

Un switch a été configuré comme il est montré dans la figure ci dessus. L'hôte 1 est connecté au port 0/4 avec l'adresse IP 192.168.1.22/28. L'hôte 2 est connecté au port 0/5 avec l'adresse IP 192.168.1.33/28. L'hôte 3 est connecté au port 0/6 avec l'adresse IP 192.168.1.30/28.

1. L'hôte 1 peut-il faire un ping sur l'hôte 2 ?
2. L'hôte 1 peut-il faire un ping sur l'hôte 3 ?
3. L'hôte 2 peut-il faire un ping sur l'hôte 3 ?

Exercice 7 Topologie



1. Pourquoi les hôtes 1 et 2 ne peuvent-ils pas communiquer entre eux ?

Exercice 8 Configuration

```
RA(config)#interface fastethernet 0/1
RA(config-if)#no shutdown
RA(config-if)#interface fastethernet 0/1.1
RA(config-subif)#encapsulation dot1q 10
RA(config-subif)#ip address 192.168.1.49 255.255.255.240
RA(config-if)#interface fastethernet 0/1.2
RA(config-subif)#encapsulation dot1q 60
RA(config-subif)#ip address 192.168.1.65 255.255.255.192
RA(config-if)#interface fastethernet 0/1.3
RA(config-subif)#encapsulation dot1q 120
RA(config-subif)#ip address 192.168.1.193 255.255.255.224
RA(config-subif)#end
```

Le routeur RA a été configuré selon la figure ci dessus.

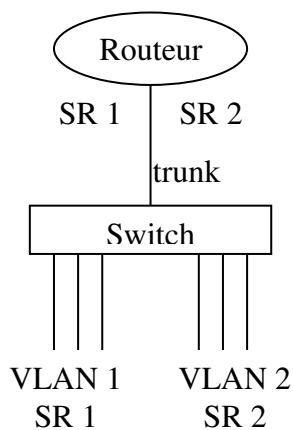
1. A quoi peut correspondre cette configuration (faites un schéma) ?
2. Un paquet arrive sur l'interface physique FastEthernet 0/1 du VLAN 10. Le paquet est à destination de l'adresse 192.168.1.120. Que va faire le routeur avec ce paquet ?

Réponses

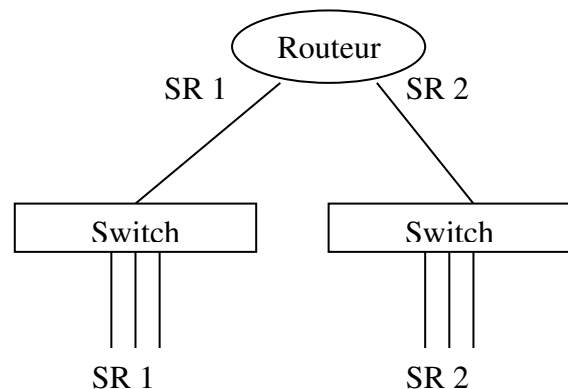
Exercice 1 :

1. Ils permettent de s'affranchir du lieu de connexion des postes, pour pouvoir les grouper en domaines de broadcast selon leur fonction. Cela permet de concentrer les communications à l'intérieur des VLANs.
2. La technique des VLANs est une technique de segmentation. Une fois séparés en groupes de travail, les ordinateurs se voient autorisés, par l'administrateur réseau, uniquement les communications utiles au sens de la politique de sécurité.
3. Switchs et routeurs
4. Aucun, les postes ne connaissent pas leur appartenance à un VLAN.
5. En les interconnectant avec un routeur
6. Non
 - exemple1: dans le cas de l'utilisation d'un seul switch, on utilise les VLAN pour économiser des interfaces et des switches :

Avec VLANs :
1 seule interface du routeur
1 seul switch

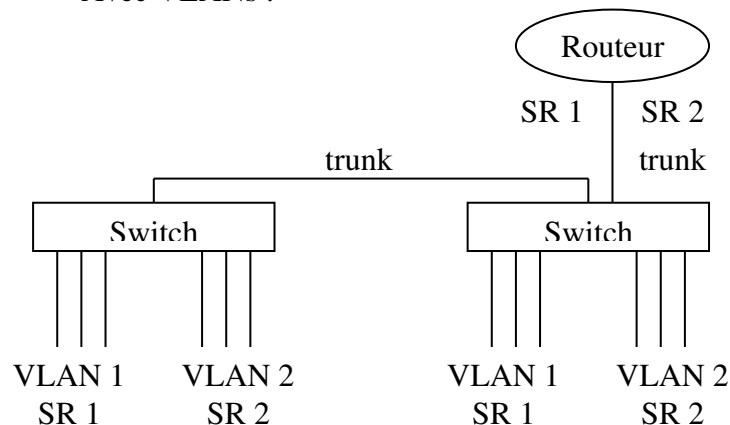


Sans VLAN :
2 interfaces du routeur
2 switches

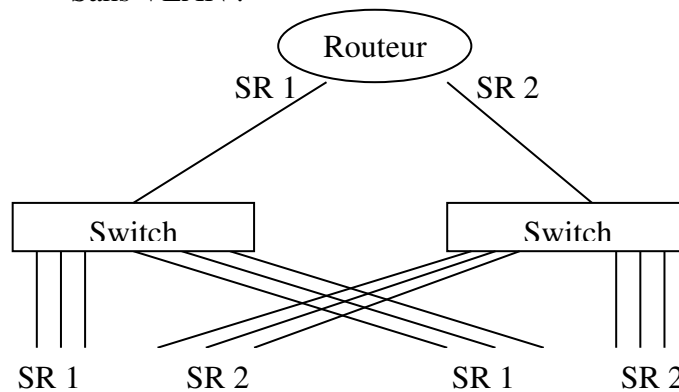


- exemple2: dans le cas de machines dispersées, on utilise plusieurs switches, et l'apport des VLANs permet de s'affranchir des contraintes de câblage

Avec VLANs :



Sans VLAN :



7. Protocoles d'étiquetage des trames : ISL (Inter-Switch Link ou 802.1q)

8. Exemples :

- quand un domaine de broadcast est trop grand, il faut le segmenter, les VLANs sont une bonne solution
- partout où le câblage doit rester figé alors que la fonction des postes peut changer en fonction des l'utilisateur à qui on attribue ces postes

Exercice 2 :

Méthodes d'attribution de VLAN :

- statiques ou VLAN par port : facile à mettre en oeuvre, difficile à maintenir, peu sécurisant, sauf si vos ordinateurs sont absolument inamovibles
- dynamiques ou VLAN par adresse MAC : plus difficile à mettre en route (tables d'adresses MAC à construire), mais plus facile à maintenir. Plus sécurisant car les machines peuvent bouger.
- il existe des VLAN dynamiques par adresse IP, ou VLAN de niveau 3, ils sont peu utilisés car peu sécurisant puisque l'@IP est facilement paramétrable sur un ordinateur.

Ce sont les VLANs dynamiques par adresse MAC qui sont, de loin, les plus utilisés.

Exercice 3 :

1. Il y a une table MAC par VLAN
2. A aucun, ils sont utiles pour « propager » tous les VLAN entre deux switch ou entre un switch et un routeur
3. Il renvoie la trame uniquement aux ports participants au même VLAN (y compris les ports trunk, après étiquetage)
5. Une trame de broadcast de niveau 2 provenant d'un port trunk porte l'identification d'un seul VLAN. Après l'étiquetage, la trame est retransmise vers tous les ports trunk et les ports participants à ce VLAN (mais sans l'étiquetage)

Exercice 4 :

1. Il faut vérifier que le routeur dispose d'une carte Fastethernet, sinon la définition de sous-interfaces sera impossible. Il faut aussi que l'IOS du routeur supporte les fonctions attachées à l'utilisation des VLANs
2. Il faudra obligatoirement mettre l'interface Ethernet en mode trunk

Exercice 5 :

Sans VLAN :

- Les trames de broadcast de niveau 2 sont visibles par toutes les machines, même si elles ne sont pas dans le même réseau IP.
- Il suffit de changer d'@IP pour changer de réseau
- L'architecture n'est pas propre, en ce sens que on ne s'attend pas à trouver des réseaux différents interconnectés par un switch !

Exercice 6 :

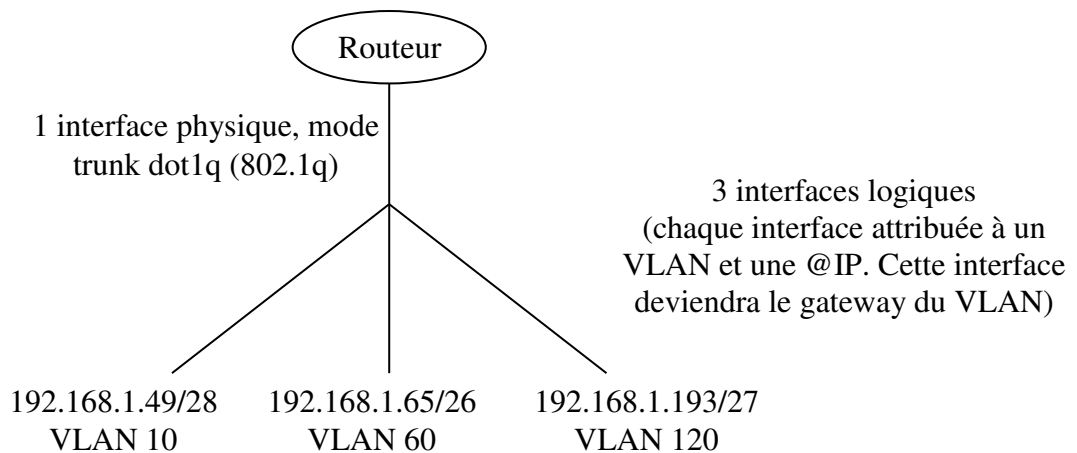
1 peut faire un ping sur 3 car ils sont dans le même VLAN **et dans le même réseau**

Exercice 7 :

Les ports 6 et 2 sont affectés au VLAN 2 mais les deux machines ne peuvent communiquer, car ils ne sont pas dans le même réseau (la première fait partie du réseau 192.168.1 et la deuxième fait partie du réseau 192.168.2)

Exercice 8 :

1)



2) Le routeur routera le paquet vers la même interface, mais avec l'étiquette du VLAN 120

NB. pour configurer la sous interface 0/0.x :

- Router(config)#int fastEthernet 0/0.X
- Router(config-subif)#encapsulation dot1Q X
- Router(config-subif)#ip address adresse--ip masque

Pour cet exemple l'interface 0/0.1 est attribuée au VLAN 10 avec adresse réseau 192.168.1.49 et masque 255.255.255.240. Ceci peut être représenté par 192.168.1.49/28