2ème année 2009-2010

Les réseaux locaux virtuels

Octobre 2009

Objectifs

Réseaux virtuels : Nous allons partitionner un réseau local à l'aide d'un matériel spécifique supportant la notion de VLAN (réseaux locaux virtuels). Ce partitionnement est un partitionnement virtuel de niveau 2.

1 Les réseaux virtuels

Le but de cette partie est de partitionner un réseau local à l'aide de VLAN.

Les VLAN (**V***irtual* **L***ocal* **A***rea* **N***etwork* ou réseau local virtuel) sont un système de segmentation de réseau particulièrement flexible (bien plus, par exemple, que les réseaux à base de hub ou même de switch).

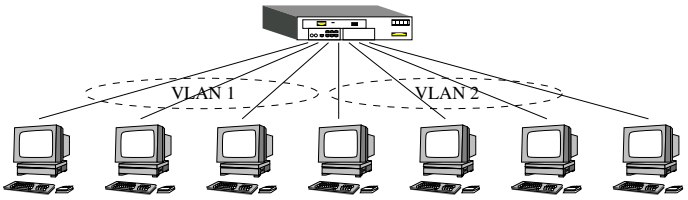

FIG. 1 – Définition de deux réseaux virtuels.

Ils présentent en particulier les avantages suivants :
- ils facilitent le changement et le déplacement des postes de travail au sein du réseau ;
- ils fournissent une sécurité supplémentaire car suppriment les communications inter-VLAN en l'absence de routage spécifique ;
- ils optimisent l'utilisation de la bande passante notamment par le partage des domaines de broadcast.

Ainsi dans la figure 1, deux réseaux virtuels ont été créés. Ils peuvent être considérés comme deux réseaux physiques traditionnels (à base de switch).

1.1 Mise en place des VLAN

La définition de réseaux virtuels fait partie de l'administration d'un switch (tout au moins d'un switch intégrant la notion de VLAN). Un VLAN par défaut est défini sur le switch et toutes les machines (le switch y compris) font partie de ce VLAN.

L'administration du switch peut se faire grâce à une connexion HTTP établie depuis un browser tel que Netscape lancé sur une machine située dans le VLAN par défaut (l'adresse IP du switch vous sera fournie en TP, ainsi qu'un *login* et un *passwd*).

Mais cette configuration peut également se faire depuis un terminal connecté physiquement au commutateur ou au travers du réseau grâce au protocole *telnet* :

```
# telnet 192.168.198.7
Connected to 192.168.198.7...
Escape character is '^]'.

User Access Verification

Password :****
c308-2750> enable
Password :****
c308-2750# config terminal
c308-2750(config)#
```

Les commandes de création d'un VLAN sont alors les suivantes

```
c308-swb(config)# vlan database
c308-swb(vlan)# vlan 14 name toto
c308-swb(vlan)# exit
```

▷ **Exercice 1 : Création des** VLAN

Le switch sur lequel sont connectées toutes les machines de la salle permet de définir des VLAN. *La manipulation que vous allez à présent effectuer consiste à définir 4* VLAN *différents au niveau du switch de telle façon à créer un partitionnement virtuel de votre réseau (les adresses* IP *des machines ne doivent pas être changées).*
Connectez-vous sur le switch et créez des VLAN. ■

1.2 Insertion des machines dans les VLAN

L'appartenance d'une station de travail à un réseau virtuel relève aussi de l'administration du switch. Les stations peuvent être distribuées sur les VLAN en fonction, par exemple, de leur adresse MAC ou du port sur lequel elles sont branchées.

Les commandes permettant d'insérer un port donné dans un VLAN choisi sur un commutateur Cisco sont les suivantes

```
c308-swb(config)# interface Fastethernet 0/5
c308-swb(config-if)# switchport mode access
c308-swb(config-if)# switchport access vlan 1276
```

▷ **Exercice 2 : Construction des** VLAN

Configurez le switch de façon à intégrer vos machines dans les VLAN *que vous avez créé. Constatez le bon fonctionnement de chacun de ces réseaux et vérifier la perméabilité entre eux. Attention : si vous sortez toutes vos machines du* VLAN *par défaut, vous ne pouvez plus administrer le switch !*
Vérifiez ensuite que les machines de votre groupe pour lesquelles vous avez créé un VLAN *se voient mais qu'elles ne voient aucune des autres machines de la salle.* ■

1.3 Utilisation de plusieurs commutateurs Ethernet

Plusieurs commutateurs Ethernet peuvent être reliés entre eux (au travers d'une interface dédiée, généralement à "haut débit") de sorte à permettre l'interconnexion d'un nombre plus grand de machines.

Qu'advient-il des réseaux virtuels dans une telle situation ?

▷ **Exercice 3 : Utilisation d'un second commutateur Ethernet**

Utilisez un second commutateur, l'enseignant vous en décrira la configuration en termes de réseaux virtuels. Connectez le au premier, qu'observez-vous ? ■

Les commutateurs Ethernet sont pourtant capables de respecter la notion de VLAN même lorsque ces réseaux virtuels sont répartis sur plusieurs équipements. Pour cela, les commutateurs devront être reliés par un câble et les ports sur lesquels ce câble est branché doivent être configurés de la façon suivante

```
Switch(config)# interface Fastethernet 0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
```

▷ **Exercice 4 : Activation du lien**

Configurez les ports reliant les deux switch et observez à nouveau la communication entre deux machines appartenant à un même VLAN *mais sur deux switch différents.*

Que constatez-vous ? ■

Par quel mécanisme une telle gestion est-elle possible ? Pour le comprendre, nous pouvons essayer d'observer le trafic qui circule sur le lien entre les deux commutateurs Ethernet.

Pour cela, les commutateurs Ethernet Cisco nous permettent de définir des sessions d'observation, par exemple de la façon suivante

```
Switch(config)# monitor session 1 source interface fastEthernet 0/5 both
```

Ici la session 1 est utilisée pour observer le trafic entrant et sortant (`both`) sur le port 5.

Cette session peut ensuite être redirigée sur un autre port de la façon suivante

```
Switch(config)# monitor session 1 destination interface fastEthernet 0/8
```

Une machine connectée sur ce port pourra alors observer le trafic avec un outil tel que `ethereal`.

▷ **Exercice 5 : Observation du trafic entre les commutateurs Ethernet**

Observez le trafic circulant entre les deux commutateurs Ethernet.

Quelles conclusions en tirez-vous ? ■

Les mécanismes utilisés entre les deux commutateurs Ethernet peuvent également être utilisés entre un commutateur Ethernet et un routeur IP. L'utilisation des réseaux virtuels ne peut plus alors être transparente à l'administrateur comme nous le verrons par la suite.