

# TP8 - VLAN

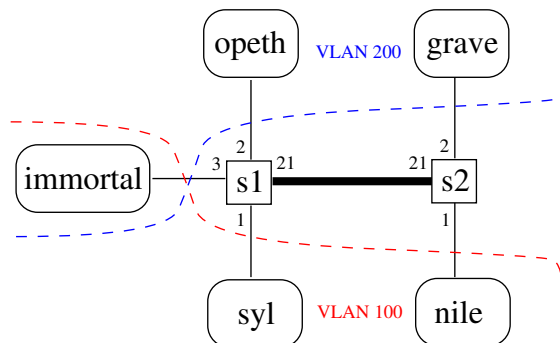
## 1 Avant de commencer

1. Lancez le script de démarrage `/net/ens/qemUNET/qemUNET.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initiale des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
/net/ens/qemUNET/qemUNET.sh -x -t /net/cremi/sathibau/Reseau/TPvlan/topology -y -v
```

L'option `-y` sert à lancer les consoles d'administration des switch. L'option `-v` quant à elle sert à activer le support des VLAN.

2. Regardez le contenu `/net/stockage/aguermou/AR/TP/4/topology` et observez la topologie de notre réseau. Elle est présentée dans la figure ci-dessous :



Vous pouvez disposer les nombreuses fenêtres qui s'ouvre de la même façon que cette figure pour vous y retrouver. En plus des 5 fenêtres Linux habituelle, vous avez les 2 fenêtres correspondant à la console d'administration des switches s1 et s2 du réseau virtuel. Pour l'instant, rien n'est configuré, seuls les câbles sont branchés entre les machines et les switches.

## 2 Premiers pas

Nous allons nous concentrer dans un premier temps sur les machines `immortal`, `opeth` et `sy1`. En consultant la description de la topologie, nous pouvons constater que l'objectif

est que machine `syl` (resp. `opeth`) fasse partie du VLAN 100 (resp. 200). Nous allons donc configurer un premier réseau IP contenant `immortal` et `syl` et un second contenant `immortal` et `opeth`, `immortal` faisant office de passerelle entre les deux réseaux/VLAN.

1. Configurer `syl` et `opeth` de telle sorte qu'elles soient dans deux réseaux IP différents.
2. Lancer un `tcpdump` sur `opeth`, puis lancer sur `syl` un ping vers une autre adresse de son propre réseau. Même si les réseaux sont différents, les deux machines étant pour le moment sur le même réseau Ethernet, `opeth` voit passer les trames de `syl` ! (du moins les broadcasts utilisés pour ARP).
3. On va donc commencer par isoler ces deux machines dans des VLANs différents 100 et 200. On utilise pour cela la console d'administration du switch `s1` pour configurer ces VLANs. Si vous souhaitez avoir la liste des commandes disponibles au niveau de la console d'administration, il suffit de taper la commande `help`. Dans un premier temps, il faut créer les VLAN 100 et 200 à l'aide de la commande `vlan/create` :

```
vlan/create      Num_VLAN (créer le VLAN Num_VLAN)
```

Il faut maintenant préciser que l'on veut placer les ports de nos deux machines à l'intérieur des VLANs. Les numéros de ports sur lesquels sont branchées les machines sont indiqués sur la figure plus haut, ou bien visibles avec `port/print`

```
port/setvlan    Num_PORT Num_VLAN (associer Num_PORT à Num_VLAN en mode untagged)
```

Relancez le ping, observez que `opeth` ne voit pas passer les trames.

4. Utilisez la commande `vlan/print`, on remarque que les ports sont en mode *untagged* : le trafic de ces ports ne contient pas le tag 802.1q, c'est de l'Ethernet classique. Le switch s'occupe d'ajouter le tag à la volée pour le trafic qui y entre et de l'enlever pour le trafic qui en sort.
5. La configuration d'`immortal` va être différente de celle des autres machines dans le sens où elle va devoir faire partie des deux réseaux IP/VLAN à la fois ! Pour ce faire, il est nécessaire de :

— Dire à l'interface réseau d'`immortal` qu'elle fait partie des deux VLANs. Ceci peut être fait en exécutant les commandes suivantes :

```
ifconfig eth0 up
```

```
vconfig add eth0 100 # pour ajouter le vlan 100
```

```
vconfig add eth0 200 # pour ajouter le vlan 100
```

Ceci a pour effet de créer deux interfaces réseaux `eth0.100` et `eth0.200` faisant partie des VLANs 100 et 200. `eth0` verra passer toutes les trames avec les tags, tandis que `eth0.100` et `eth0.200` ne verront passer que les trames des VLANs correspondants, sans les tags.

— Configurer les nouvelles interfaces réseau pour qu'elles fassent partie des bons réseaux IP.

```
ifconfig eth0.100 ...
```

```
ifconfig eth0.200 ...
```

Si vous voulez que la création et la configuration des interfaces réseaux associées aux VLAN soit faite automatiquement à chaque démarrage, il suffit d'éditer le fichier `/etc/network/interfaces` et d'y ajouter les sections suivantes :

```
#VLAN 100
auto eth0.100
iface eth0.100 inet static
address ...
netmask ...
```

```
#VLAN 200
auto eth0.200
iface eth0.200 inet static
address ...
netmask ...
```

Remarque : N'oubliez pas d'activer le mode passerelle sur `immortal` pour qu'elle puisse relayer les paquets allant de `syl` vers `opeth` et inversement.

6. Configurer `syl` et `opeth` de telle sorte qu'`immortal` soit leur passerelle. Cela ne fonctionne cependant pas encore...
7. Il faut en effet encore placer le port switch sur lequel `immortal` est branchée dans les deux VLANs. Pour qu'`immortal` puisse distinguer les deux VLANs, il faut que le port soit en mode *tagged* : le trafic sortant du switch doit conserver son tag 802.1q. Pour ce faire, on dispose de la commande suivante dans l'interface d'administration du switch `s1`.

```
vlan/addport    Num_VLAN Num_PORT (associer Num_PORT à Num_VLAN en mode tagged)
```

Vérifier la configuration avec `vlan/print` .

8. Faites communiquer `opeth` et `syl` en vous mettant en écoute sur `immortal`. Il s'agit d'analyser le trafic passant par `eth0`, `eth0.100` et `eth0.200` avec `tcpdump`. Vous pouvez ajouter l'option `-e` pour voir le tag vlan (dans le cas d'`eth0`) et les MAC source destination, pour vérifier que cela se comporte comme prévu.

### 3 Configuration avancée

Maintenant qu'`immortal`, `opeth` et `syl` sont configurées correctement et arrivent à communiquer les unes avec les autres, nous allons nous intéresser à la configuration de `nile`, `grave` et du switch `s2`.

1. Configurer `nile` (resp. `grave`) en lui donnant une adresse IP qui est dans le même réseau que `syl` (resp. `opeth`). De plus, il faudra considérer `immortal` comme passerelle par défaut.

2. Configurer le switch `s2` pour que `nile` (resp. `grave`) soit dans le même VLAN que `syl` (resp. `opeth`).
3. Configurez le lien de type *trunk* reliant les switches `s1` et `s2` pour faire en sorte qu'il transporte le trafic des VLAN 100 et 200. Il s'agit donc juste d'associer le port 21 (où est branché le lien trunk) aux différents VLANs en mode *tagged* pour qu'ils puissent faire le tri. Cette étape se fera sur les consoles d'administration de `s1` et `s2`.

De nouveau, vous pouvez maintenant observer avec `tcpdump` que les VLANs sont bien isolés et les paquets sont donc obligés de passer par le routeur `immortal` qui pourra donc mettre en œuvre des règles de firewall.