Travaux Pratiques
VLAN (de type 1)

Séance de TP entièrement effectuée avec le logiciel Marionnet. Durée estimée : 2h - 2h30.

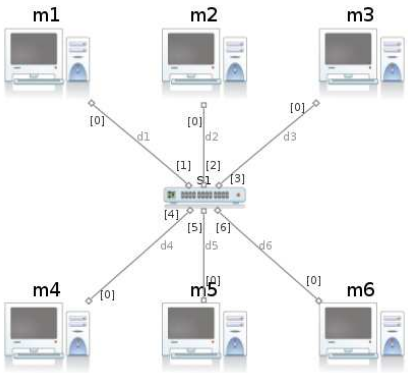
Prérequis. Avoir suivi le cours magistral sur les principes des VLAN. Attention : pour la version 0.90.6 ou inférieure de Marionnet il existe une probabilité faible mais non nulle d'inversion de deux leds voisins d'un commutateur (p.e. le port 4 fait clignoter le led 3 et viceversa le port 3 fait clignoter le led 4). Le bug est corrigé à partir de la version 0.91.0 (juin 2012).

Première partie
Partitionnement d'un commutateur

Nous commençons par le cas simple où l'ensemble des ports physiques d'un unique commutateur est partitionné en VLANs. Nul besoin du *trunking* et du protocole IEEE 802.1Q associé. Plus simplement, vous devrez définir une partition (au sens ensembliste) des ports physiques, c'est-à-dire affecter un identifiant de VLAN (une "partie" associée) à chaque port du commutateur.

1 Câblage et configuration de base

Définissez un réseau local avec 6 machines, m_1, m_2, m_3, m_4, m_5 et m_6, branchées à un commutateur avec au minimum 6 ports. Pour un démarrage rapide des machines virtuelles, choisissez la distribution GNU/Linux *pinocchio* : les éventuelles captures de trames se feront en modalité texte par la commande `tcpdump` (cf. `man tcpdump`).



Vous disposez de la plage d'adresses 195.12.56.0/21.

```
[0 jean@laptop ~]$ ipcalc 195.12.56.0/21
Address:   195.12.56.0          11000011.00001100.00111 000.00000000
Netmask:   255.255.248.0 = 21   11111111.11111111.11111 000.00000000
Wildcard:  0.0.7.255            00000000.00000000.00000 111.11111111
=>
Network:   195.12.56.0/21       11000011.00001100.00111 000.00000000
HostMin:   195.12.56.1          11000011.00001100.00111 000.00000001
HostMax:   195.12.63.254        11000011.00001100.00111 111.11111110
Broadcast: 195.12.63.255        11000011.00001100.00111 111.11111111
Hosts/Net: 2046                  Class C
```

Segmentez cette plage en deux partie d'égale capacité (i.e. 1022 hôtes) et configurez donc deux sous-réseaux locaux IP indépendants "slash 22" : $LAN_1 = \{m_1, m_3, m_5\}$ (réseau "impair") et $LAN_2 = \{m_2, m_4, m_6\}$ (réseau "pair").

Astuce : par simplicité, la machine m_i prendra l'adresse `_._._.`i dans son réseau d'appartenance, et sera connecté au commutateur par le port numéro i (comme dans l'image ci-dessus).

Configurez toutes les interfaces réseaux avec la commande `ifconfig` en utilisant la notation CIDR et testez ensuite le bon fonctionnement des liaisons par la commande `ping`.

2 Constater la non étanchéité

En supposant les deux réseaux opérationnels, observez leur non étanchéité en provoquant une diffusion (broadcast) ARP et une diffusion DHCP (voir feuille de TP n°2) que toutes les machines écouteront.

Exemple-rappel de configuration DHCP basique. Les lignes suivantes (typiquement dans `/etc/dhcpd.conf`) :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.51  192.168.1.99;
}
ddns-update-style none;
```

instruisent le serveur à répondre avec un numéro IP qu'il choisira dans la plage `192.168.1.51` - `192.168.1.99` en fournissant le masque réseau `255.255.255.0` (`/24`). **Adaptez cet exemple à vos plages réseau**.

3 Configurer les VLANs

Certains commutateurs peuvent être configurés pour découper un réseau physique en plusieurs réseaux logiques en fonction des **ports** utilisés (VLAN 1) ou des **adresses MAC** utilisés (VLAN 2), voire même des **adresses IP** utilisées (VLAN 3). Le composant commutateur (switch) de Marionnet permet de simuler la fonctionnalité VLAN de type 1 (en pilotant le logiciel sous-jacent `vde_switch` du projet *virtualsquare*). Pour pouvoir configurer les VLANs, il faut alors préciser vouloir un terminal de configuration au moment de l'ajout d'un nouveau commutateur ou au moment de la modification (*Propriétés*) d'un commutateur existant (modification qui est permise seulement si le commutateur est éteint, donc éteignez-le). La fenêtre de dialogue *Ajout*/*Propriétés* des commutateurs contient à cet effet une case à cocher "Show VDE terminal".

Si l'on coche cette case puis on démarre le commutateur, on observera apparaître un terminal de configuration du commutateur en plus de la fenêtre de leds habituelle :

Or, dans le terminal du commutateur la commande `help` nous permettra d'avoir un aperçu rapide des possibilités de configuration du commutateur :

```
VDE switch V.2.2.1
(C) Virtual Square Team (coord. R. Davoli) 2005,2006,2007 - GPLv2
vde$ help
0000 DATA END WITH '.'
COMMAND PATH       SYNTAX          HELP
------------       --------------  ------------
ds                 ============    DATA SOCKET MENU
ds/showinfo                        show ds info
help               [arg]           Help (limited to arg when specified)
logout                             logout from this mgmt terminal
shutdown                           shutdown of the switch
showinfo                           show switch version and info
load               path            load a configuration script
debug              ============    DEBUG MENU
...
...
fstp/print         [N]             print fst data for the defined vlan
port               ============    PORT STATUS MENU
port/showinfo                      show port info
port/setnumports   N               set the number of ports
port/sethub        0/1             1=HUB 0=switch
port/setvlan       N VLAN          set port VLAN (untagged)
port/create        N               create the port N (inactive|notallocatable)
port/remove        N               remove the port N
port/allocatable   N 0/1           Is the port allocatable as unnamed? 1=Y 0=N
port/epclose       N ID            remove the endpoint port N/id ID
port/resetcounter  [N]             reset the port (N) counters
port/print         [N]             print the port/endpoint table
port/allprint      [N]             print the port/endpoint table (including inactive port)
vlan               ============    VLAN MANAGEMENT MENU
vlan/create        N               create the VLAN with tag N
vlan/remove        N               remove the VLAN with tag N
vlan/addport       N PORT          add port to the vlan N (tagged)
vlan/delport       N PORT          add port to the vlan N (tagged)
vlan/print         [N]             print the list of defined vlan
vlan/allprint      [N]             print the list of defined vlan (including inactive port)
.
1000 Success
vde$
```

En particulier, concernant les fonctionnalités VLANs, d'une part, la commande `vlan/create` permet de créer un VLAN en lui affectant une étiquette numérique (ce qui dans l'help est appelé `tag`)

N. D'autre part, la commande `port/setvlan` permet d'associer un port (non "taggé") au VLAN dénoté par son étiquette.

Remarque : ne pas utiliser la commande `vlan/addport` qui ajoute un port "taggé", c'est-à-dire un port faisant partie du "trunking" (infrastructure de liaison inter-commutateurs).

Exercice : Configurez deux VLANs de façon à avoir une étanchéité parfaite des réseaux $LAN1$ et $LAN2$. Testez en provoquant à nouveau des diffusions ARP et/ou DHCP et observez, pendant ces diffusions, le clignotement d'une partie seulement des leds dans la fenêtre de leds du commutateur.

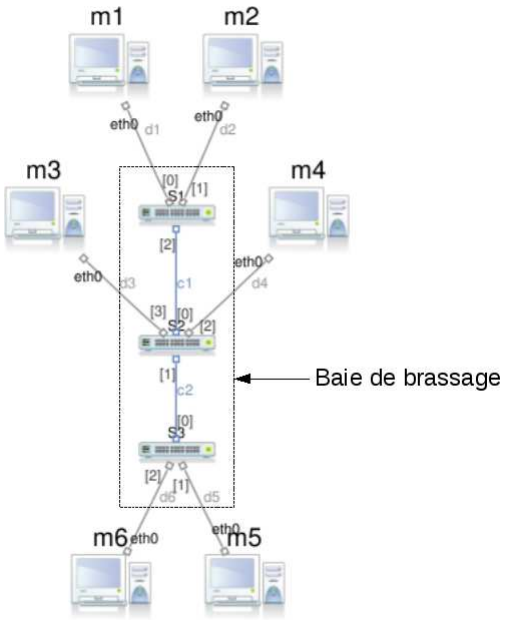
Deuxième partie

Partitionnement d'un ensemble de commutateurs reliés (trunking)

Il est courant de réaliser un ou plusieurs réseau non par un seul appareil de liaison mais plutôt par un ensemble d'appareils (commutateurs et/ou concentrateurs) reliés entre eux par des câbles croisés (en cas de ports n'ayant pas la fonctionnalité *Auto MDI-X*, ce qui est le cas des appareils simulés dans Marionnet). Dans ce cas, les ports d'interconnexion entre commutateurs doivent être "taggés" et constituent le "trunking". Le but est essentiellement économique : il s'agit de partager une seule connexion (une seule paire de ports physiques et un seul câble) pour l'ensemble des VLANs utilisées. La simplicité et l'économie au niveau physique sera payée en ajoutant un niveau d'encapsulation supplémentaire entre la couche Ethernet 802.3 et la couche IP ou autre (ARP, etc). Les trames IEEE 802.3 transporteront des trames du protocoles IEEE 802.1Q (annoncées par le type $0x8100$) qui, elles, véhiculeront de l'IP ou autre.

4 Câblage

Remplacez l'unique commutateur par un ensemble de trois commutateurs reliés.



5 Configuration

Configurez les deux VLANs sur l'ensemble des commutateurs de façon à obtenir à nouveau une étanchéité parfaite des réseaux $LAN1$ et $LAN2$. Pensez encore une fois à observez les leds des commutateurs pendant les diffusions pour vérifier le bon partitionnement. Vous devez à présent utiliser aussi la commande `vlan/addport` qui ajoute un port "taggé", c'est-à-dire un port faisant partie du trunking, à une VLAN.

6 Capture des trames IEEE 802.1Q

Pour capturer ce type de trames vous allez intercepter les trafic circulant sur n'importe quel câble croisé du trunking. Pour ce faire, il suffit de remplacer le câble en question par deux câbles en interposant un répéteur (hub) et une machine *espion* branché au répéteur. Sur la machine *espion* vous lancerez une instance de `wireshark` pour observer l'encapsulation (IP, ARP ou DHCP)/802.1Q/802.3.