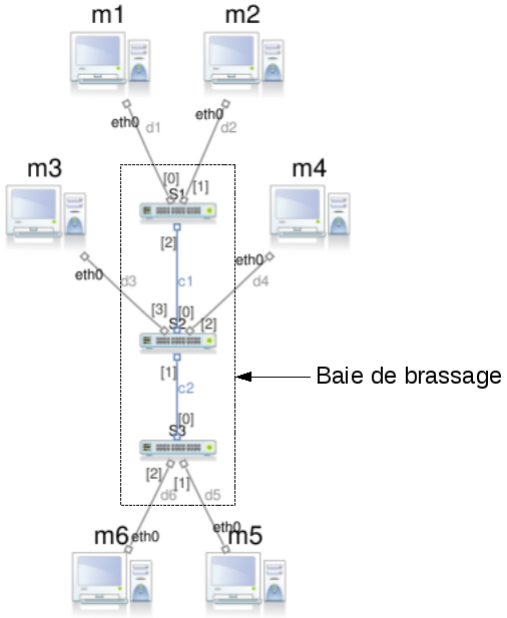
Travaux Pratiques
Segmentation d'une plage réseau, MDI/MDI-X, Adresses IP multiples sur baie de brassage, Vers les VLAN.

Séance de TP entièrement effectuée avec le logiciel Marionnet. Durée estimée : 1h30 - 2h.

Prérequis. Avoir suivi le cours magistral sur les adresses IP (v4) et la segmentation.

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 une baie de brassage constituée de 3 commutateurs S_1, S_2 et S_3. Choisissez la distribution GNU/Linux *debian-wheezy* pour les machines : la capture de trames se fera en modalité texte par la commande `tcpdump` (cf. `man tcpdump`) ou en modalité graphique par `wireshark`.



La plage d'adresses attribuée au réseau est, en notation CIDR, 194.85.40.0/21.

```
$ ipcalc 194.85.40.0/21
Address:   194.85.40.0          11000010.01010101.00101 000.00000000
Netmask:   255.255.248.0 = 21   11111111.11111111.11111 000.00000000
Wildcard:  0.0.7.255            00000000.00000000.00000 111.11111111
=>
Network:   194.85.40.0/21       11000010.01010101.00101 000.00000000
HostMin:   194.85.40.1          11000010.01010101.00101 000.00000001
HostMax:   194.85.47.254        11000010.01010101.00101 111.11111110
Broadcast: 194.85.47.255        11000010.01010101.00101 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 : $LAN_1 = \{m_1, m_3, m_6\}$ (partie gauche de la figure) et $LAN_2 = \{m_2, m_4, m_5\}$ (partie droite). Dans le jargon des ingénieurs réseau, nous dirons avoir découpé la plage en deux sous-réseaux "slash 22".

1.1 Utilisation des alias de carte

Il est possible d'affecter plusieurs adresses IP à une même carte réseau. Cela permet de réaliser plusieurs réseaux avec la même infrastructure de niveau 1 ou 2 (hub ou switch). Mais ce qui en IPv6 serait très naturel, est plus compliqué en IPv4. En effet, pour attribuer plusieurs adresses IPv4 à une même interface réseau, la syntaxe de la commande `ifconfig` demande de choisir **arbitrairement** un "**alias**" de carte (cf. `man ifconfig`). **Par exemple**, pour ajouter l'adresse 10.10.10.4 à l'interface

`eth0` de m_4 nous choisirons l'alias "lan3" (tout comme on aurait pu choisir "toto") et nous utiliserons donc une commande du genre :

```
m4# ifconfig eth0:lan3 10.10.10.4
```

Configurez donc un troisième un réseau, cette fois en utilisant des adresses privées, $LAN_3 = \{m_5, m_6\}$ en 10.10.10.0/24 (partie basse de la figure). La machine m_6 appartiendra ainsi à la fois au LAN_1 et au LAN_3, et la machine m_5 appartiendra ainsi à la fois au LAN_2 et au LAN_3.

Par simplicité, la machine m_i prendra l'adresse $\_.\_.\_.i$ sur tous les réseaux sur lesquels elle doit être présente. 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 Polarité MDI/MDI-X

Pendant qu'un `ping` traversant 2 commutateurs tourne en boucle entre deux machines (p.e. m_1 et m_3) :

— essayez de remplacer dans la baie de brassage un câble croisé connectant deux commutateurs par un câble droit : deux ports ayant la **même** polarité (à l'occurrence MDI-X) seront ainsi mal connectés ;

— observez l'attente du programme `ping`,

— rebranchez le bon type de câble et observez le `ping` qui repart.

3 Constater la non étanchéité

En supposant les trois réseaux opérationnels, vous allez observer dans cette dernière section que l'étanchéité entre les réseaux LAN_1, LAN_2 et LAN_3 n'est pas complète.

Broadcast ARP. Provoquez un broadcast ARP sur un réseau (p.e. LAN_1) et observez-le avec `tcpdump` depuis une machine ne faisant pas partie de ce réseau (p.e. m_4).

Broadcast DHCP. Si le broadcast ARP provoque une perte de bande passante (tous les réseaux sauf un sont concernés à chaque broadcast), le broadcast DHCP peut être bien plus grave. En effet, on ne peut imaginer de configurer des serveurs DHCP comme si le découpage était réel (physique), et c'est ce que nous allons constater. Le protocole DHCP permet à des clients sans adresses IP de "demander" sur un réseau sur lequel ils sont branchés si quelqu'un a autorité pour leur affecter une adresse IP. Sous GNU/Linux la commande qui permet de faire cette demande est `dhclient`. Par exemple, la machine m_4 pourrait tenter de configurer son interface `eth0` par la commande :

```
m4# dhclient eth0
```

D'autre part, pour qu'une machine ait autorité à délivrer des adresses IP, il suffit de lancer sur elle un serveur DHCP, typiquement par une commande du type :

```
m1# /etc/init.d/dhcpd start
```

cela après avoir éditer son fichier de configuration `/etc/dhcpd.conf` (cf. `man dhcpd.conf`), fichier où l'on donne des instructions sur la façon dont le serveur doit répondre à ses clients.

Par exemple, les lignes suivantes :

```
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`).

La dernière ligne (`ddns-update-style none;`) est géneralement obligatoire : sans cette ligne le serveur risque ne pas accepter le fichier de configuration et donc de ne pas se lancer.

Exercice : configurez et lancez un serveur sur m_1 pour servir les requêtes du LAN_1 (une sous-plage de `194.85.40.0/22` au choix) et un serveur m_2 pour servir les requêtes du LAN_2 (une sous-plage de `194.85.44.0/22` au choix). Essayez ensuite d'ajouter une nouvelle machine pour chacun des commutateurs déjà présents de la baie de brassage (donc au total 3 nouvelles machines), et de les configurer toutes par DHCP. Vous devriez constater une sorte de "course" entre les serveurs : les nouvelles machines appartiendront au LAN_1 ou au LAN_2 selon la rapidité de réponse des serveurs...

Solution : les VLAN. 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). Cela permet d'obtenir une étainchéité complète des réseaux logiques réalisés.