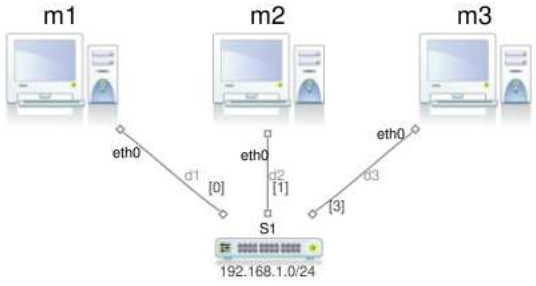
Travaux Pratiques
Encapsulation ICMP/IP/Ethernet, rôle du protocole ARP et fragmentation IPv4

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

Prérequis. Avoir suivi le cours magistral sur le sujet.

1 Câblage et configuration de base

Définissez un réseau local avec trois machines, m_1, m_2 et m_3, branchées à un commutateur S_1. En ajoutant une machine virtuelle dans le réseau, choisissez comme distribution GNU/Linux *debian* ou *mandriva* pour avoir la possibilité, par la suite, de lancer des applications graphiques (notamment `wireshark`).



La plage d'adresses attribuée au réseau est, en notation CIDR, 192.168.1.0/24. La machine m_i prendra l'adresse 192.168.1.i. Configurez les interfaces réseaux avec la commande `ifconfig` en utilisant la notation CIDR. Testez ensuite le bon fonctionnement des liaisons par la commande `ping`. Pendant qu'un `ping` tourne en boucle entre deux machines :

- essayez d'enlever (ou de débrancher) un câble impliqué dans la liaison,
- observez l'attente du programme `ping`,
- rebranchez et observez le `ping` qui repart : votre réseau présente à nouveau une configuration physique et logicielle correctes.

2 Configuration des noms symboliques

Sous Unix il est possible d'utiliser des noms de machines symboliques à la place des numéros IP sans passer par un serveur de noms (DNS), mais en modifiant simplement un fichier nommé `/etc/hosts`, dont les lignes sont de la forme :

```
<IP> <NOM> <NOM>*
```

Par exemple :

```
127.0.0.1 localhost
10.10.10.1 self this me
74.125.43.106 www.google.fr moteur
```

Il faut lire ces lignes de la droite vers la gauche : tous les noms symboliques (séparés par des blancs) seront traduits dans le numéro IP spécifié tout à gauche.

Modifiez donc ce fichier (avec un éditeur de texte tel que `vi`, `emacs`, `nano`, `kate`) sur les 3 machines de façon à pouvoir par la suite exprimer toute adresse de façon symbolique depuis n'importe quel poste du réseau. **Remarque** : après ce travail, effectué sur 3 machines, vous pourrez facilement constater les limites de cette approche pour des réseaux plus grands et donc l'intérêt des serveurs de noms.

Testez la résolution de noms, que vous avez mis en oeuvre sur votre réseau, par des `ping` "singuliers" (pas en boucle, un seul aller-retour, voir le sens de l'option `-c` dans le manuel de `ping`) :

```
m1# ping -c 1 m2
m1# ping -c 1 m3
m2# ping -c 1 m1
m2# ping -c 1 m3
m3# ping -c 1 m1
m3# ping -c 1 m2
```

3 ARP (Address Resolution Protocol)

Pour les exercices de cette section, vous utiliserez la commande `arp` qui permet d'afficher et de modifier la table ARP d'une machine. Pour obtenir de l'aide sur cette commande, comme pour la majorité des commandes sous Unix, vous pouvez utiliser l'option "h" (help) : `arp -h` ou le manuel Unix : `man arp`.

Placez-vous sur la machine m_1 :

- affichez le contenu de la table ARP de m_1
  - si la table est vide, relancez les deux commandes `ping` ci-dessus depuis m_1, puis affichez à nouveau le contenu de la table de m_1
- affichez maintenant le contenu de la table avec les adresses IP au lieu des noms de machines
- quelle sont les adresses Ethernet (MAC) de m_2 et m_3 ? En utilisant la commande `ifconfig`, vérifiez sur m_2 et m_3 l'exactitude de l'association (IP,MAC) relevée sur la table ARP de m_1.

3.1 Capture de trames ARP

- effacez le contenu de la table ARP de m_1
- lancez une instance du programme `wireshark` sur m_2, puis lancez une capture de trames sur l'interface `eth0`
- relancez un `ping` singulier depuis m_1 vers m_2 :

  ```
  m1# ping -c 1 m2
  ```

- depuis m_2 arrêtez la capture et analysez les trames (une ligne = une trame) ; vous devez constater la présence de 4 trames, deux ARP et deux ICMP :
  - quel est la valeur du champ `type` à l'intérieur des trames Ethernet contenant la requête et la réponse ARP ?
  - quel est, en revanche, la valeur du champ `type` à l'intérieur des trames Ethernet contenant la requête ECHO ICMP et la réponse ECHO ICMP ?
  - par le biais de `wireshark`, combien de niveaux d'encapsulation observez-vous pour chaque ligne (trame) ? Est-il différent selon le protocole (ARP vs ICMP) encapsulé ?

4 Fragmentation

La commande `ping` permet d'envoyer des requêtes ECHO ICMP d'une taille (en octets) paramétrable. Pour chacun des points suivants, vous constaterez avec `wireshark` la fragmentation des paquets survenue :

- provoquez une fragmentation avec des paquets de taille supérieure au MTU qui, par défaut, est fixé à la taille 1500
- provoquez une fragmentation avec des paquets de taille 1200 et un MTU que vous fixerez (par la commande `ifconfig`) à la valeur 1000 sur toutes les machines

– provoquez la fragmentation d'un seul message ECHO ICMP en 10 fragments. À quel niveau, ICMP, IP ou Ethernet, se trouvent les informations permettant au destinataire de reconstituer le message ICMP d'origine ?