

TP 1 : Introduction aux réseaux de l'Internet : utilisation du réseau

Ouvrez une fenêtre de terminal (dans le menu Applications/Outils Système). Ce programme permet d'interagir avec l'ordinateur en mode ligne de commandes (textuel).

I. Quelques commandes associées aux réseaux

Utiliser la commande `ifconfig` pour afficher les informations relatives aux cartes réseaux (interfaces de communication). Quels types d'informations récupérez-vous ? Repérez les informations relatives à l'interface notée `eth0` ou `e0`. Notez l'adresse IP de cette interface ainsi que le nombre de paquets transmis et reçus par cette interface.

La commande `ping` permet d'envoyer une requête vers un ordinateur donné pour savoir si celui-ci est actif (allumé par exemple). La syntaxe est `ping adr-ip` ou `ping nom-de-machine`. Essayer de faire un `ping` vers l'ordinateur de votre voisin. Faites aussi un `ping` sur www.univ-pau.fr. Quelles sont les informations affichées sur l'écran (essayer de déduire le plus de chose)?

Refaites la commande `ifconfig` et notez le nombre de paquets transmis et reçus. Que remarquez vous ? Comment pensez vous que le protocole `ping` fonctionne ? Fonctionne t-il en mode connecté ou non-connecté ?

Débranchez votre câble réseau et essayez de faire la même chose ? Que se passe t-il ? Laisser le `ping` fonctionner et rebranchez votre câble réseau. Que se passe t-il ?

Faites maintenant un `ping` sur ftp.univ-pau.fr, www.labri.fr, www.univ-pau.fr, www.amazon.com, www.meteo.fr, www.cela.com, www.cestlavie.com. Que constatez vous ? Avez vous une explication ? Vérifiez par un autre moyen que ces machines (ou services <http://www.amazon.com>) fonctionnent bien.

Ouvrez maintenant un navigateur web (Firefox par exemple) et allez sur le site <http://ping.eu>. Quelle est l'adresse IP qui est affichée comme étant votre adresse ? Avez-vous une explication ?

Sélectionnez le bouton radio `Ping` pour pouvoir faire des pings. Recommencez les pings avec les machines précédemment mentionnées ? Que constatez vous ? Avez-vous une explication ?

II. Utiliser le réseau pour travailler à distance

Nous allons utiliser le réseau pour nous connecter sur une autre machine distante. Pour cela nous utiliserons la commande et le protocole `ssh`. `ssh` signifie `Secure Shell`, traduit cela veut dire *terminal sécurisé* : les échanges entre ordinateurs sont cryptés afin que les mots de passe ne passent pas sur le réseau en texte clair. Tout d'abord, faites `which sshd` pour savoir si le service `ssh` est installé. Si la réponse est `/usr/bin/sshd`, alors c'est installé, sinon, appelez le professeur.

Utiliser `ssh` pour vous connecter sur la machine de votre voisin avec `ssh adr-ip`. S'il vous demande si vous acceptez la connexion, répondez par `yes`. Un mot de passe vous est demandé, c'est le mot de passe associé à votre login. Une fois connecté, vérifiez que vous êtes bien sur la machine du voisin (par exemple faites `ifconfig` pour voir l'adresse IP de la machine qui devrait être différente de la machine sur lequel vous êtes en train de taper le texte). Toutes les commandes que vous lancez sont en fait exécutées sur la machine distante sur laquelle vous vous êtes connecté avec la commande `ssh`. **Faites `exit` pour vous déconnecter.**

Utiliser maintenant `ssh` pour vous connecter sur la machine `sciences.univ-pau.fr` avec comme login `tpres` et comme mot de passe `tpres08`.

```
>ssh -l tpres sciences.univ-pau.fr
```

Une fois connecté, refaites les `ping` sur ftp.univ-pau.fr, www.labri.fr, www.univ-pau.fr, www.amazon.com, www.meteo.fr, www.cela.com, www.cestlavie.com. Que constatez vous ? Pouvez-vous compléter votre explication précédente ? **Faites exit pour vous déconnecter.**

III. Les noms symboliques

Vous avez manipulé des noms symboliques tels que www.amazon.com. Au niveau du réseau, ce nom symbolique est traduit en une adresse IP. Essayer d'utiliser `ping` pour trouver l'adresse IP de la machine www.univ-pau.fr. Essayer ensuite de trouver l'adresse IP de www.cestlavie.com

En fait, des serveurs spéciaux appelés serveurs de noms (Domain Name Server, DNS) sont utilisés pour traduire les noms symboliques (appelé des noms de domaine) en adresse IP. Ces aspects seront précisés au cours. Tout le monde peut acheter pour pas très cher un nom de domaine. Par exemple dupont.pierre.org. Voir le site

<http://www.commentcamarche.net/web/webdomain.php3> et le site

<http://www.lerelaisinternet.com> onglet Nom de Domaine.

Nous allons de nouveau utiliser le site <http://ping.eu> en utilisant le service DNS `lookup`. Entrez tous les noms de domaine que vous connaissez et essayer de trouver leur adresse IP.

IV. Transférer des fichiers

Un protocole très connu pour le transfert de fichier à distance est FTP (File Transfer Protocol). Nous allons d'abord l'utiliser avec l'interface graphique fournie avec Linux Ubuntu. Sélectionner `Raccourci/Se connecter à un serveur`, et entrer ftp.univ-pau.fr comme nom de serveur FTP auquel vous voulez vous connecter. Cliquez sur `Connecter`. Une icône devrait apparaître sur votre écran, double-cliquez dessus pour l'ouvrir, vous devriez voir des fichiers et des répertoires. Affichez en mode liste si vous préférez.

Qui est le serveur et qui est le client ? Entrez dans le répertoire `pub/select`, récupérez le fichier `produits.xls` et déconnectez cette connexion. Effacer le fichier téléchargé.

Un autre moyen avec lequel on se rend mieux compte de l'interaction entre le client FTP et le serveur FTP est de passer par la ligne de commande. Pour cela, ouvrez un terminal, créer un répertoire FTP à la racine de votre arborescence et entrez à l'invite du prompt la commande :

```
>ftp ftp.univ-pau.fr
```

Entrez `anonymous` pour le nom d'utilisateur (login) et le mot de passe. Une fois la connexion établie, entrez la commande `ls`. Que fait cette commande ? Entrez `help`. Entrez `help get`, puis `help cd`. Essayez de récupérer le même fichier que précédemment. Quitter la commande `ftp` en entrant `quit`.

Avec ces exemples, pouvez-vous dire quels sont les avantages du mode connecté. Représentez aussi un chronogramme d'une connexion FTP entre une machine A et une machine B sur laquelle on lance une commande `ls`. La machine A sera le client et la machine B, le serveur. Si besoin, refaites la connexion avec `ftp` ftp.univ-pau.fr pour bien voir les différentes étapes.

V. Les commandes associées au routage

La commande `route` permet d'afficher la table de routage utilisé par l'ordinateur pour accéder aux ressources (machines) distantes. Lancez `route` et essayez d'interpréter le résultat. Si la commande `route` bloque, utilisez `route -n`. Utilisez la commande `man route` pour savoir ce que fait l'option `-n`.

Voyez vous une relation entre l'adresse IP que vous pouvez voir affichée par `route` et votre propre adresse IP ?

La commande `traceroute` permet en spécifiant une adresse IP de destination ou un nom symbolique de machine de savoir par quelles étapes passent les paquets IP qui sont envoyés. Essayez de voir par où passent les paquets pour la destination www.univ-pau.fr en faisant :

```
>traceroute www.univ-pau.fr
```

Si cela bloque, faites CTRL-C (maintenez appuyée la touche CTRL et ensuite appuyer sur la touche C). Faites de même pour www.amazon.com, www.google.com, allspice.lcs.mit.edu, ftp.inria.fr et www.labri.fr.

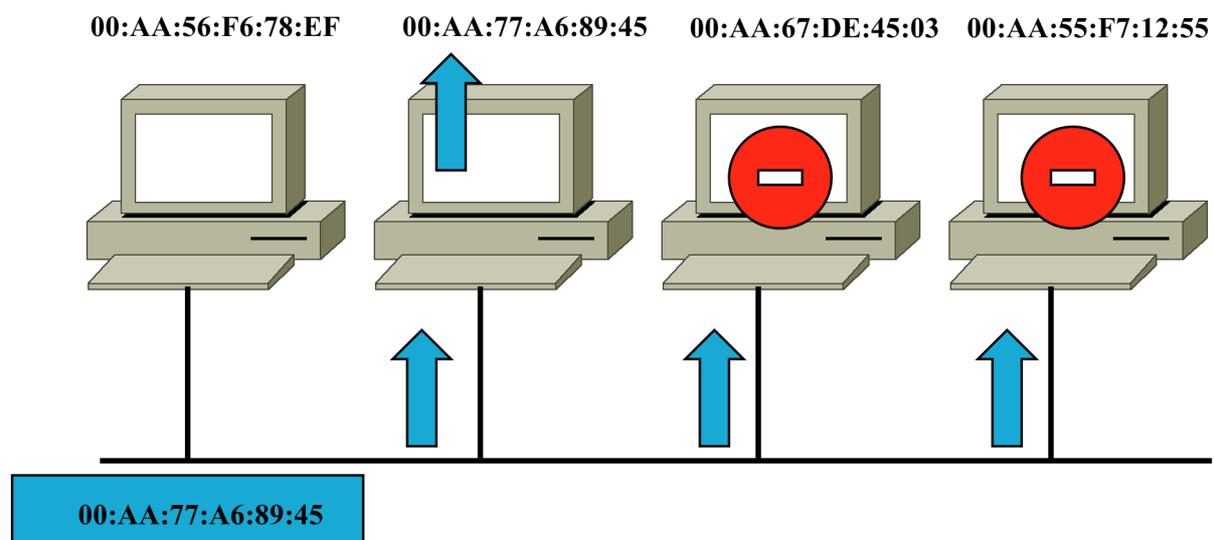
Le `traceroute` semble t-il fonctionner ? Si non, allez sur le site <http://ping.eu> et utiliser le service `traceroute` disponible. Que pouvez vous remarquer (pour www.univ-pau.fr par exemple) ?

Connectez vous maintenant sur la machine `sciences.univ-pau.fr` avec `ssh` comme précédemment indiqué. Utilisez la commande `traceroute` avec les machines indiquée ci-dessus. Que remarquez-vous ?

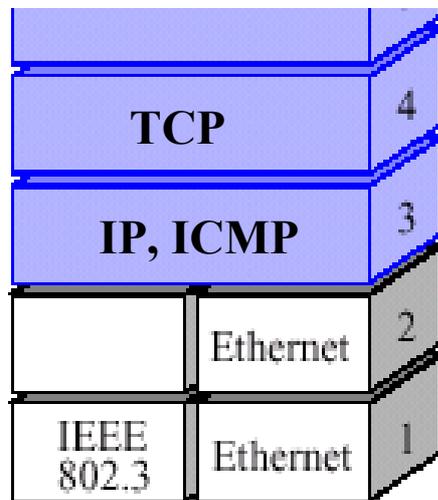
VI. Notion de protocole

Nous allons utiliser un outil spécifique pour pouvoir « voir » tous les paquets qui sont transmis sur un réseau. Normalement sur un réseau de type Ethernet, la carte réseau filtre les paquets qui ne sont pas destinés à la machine en se basant sur l'adresse Ethernet (adresse MAC) de la machine et en comparant avec l'adresse destination trouvé dans le paquet. Cette adresse est différente de l'adresse IP, on peut considérer que l'adresse MAC est une adresse plus « rudimentaire » ou « de plus bas niveau » qu'une adresse IP. L'adresse MAC est codé avec 6 octets, au format haxadécimal, ex :

00:AA:77:A6:89:45. La figure suivante résume le filtrage qui est réalisé :



Sur un réseau, les informations sont mis dans des paquets qui contiennent les informations de contrôle (qui sont mis dans ce que l'on appelle un entête) permettant le bon acheminement de ces paquets (exemple d'une lettre avec son adresse postal). De manière schématique, les paquets IP sont mis dans des paquets Ethernet. De manière générale, le principe d'architecture en couche et le principe d'encapsulation fait que les paquets d'un protocole d'une couche N sont mis dans des paquets d'un protocole de couche N-1. Sur un réseaux Ethernet avec IP, la structure des couches est la suivante :



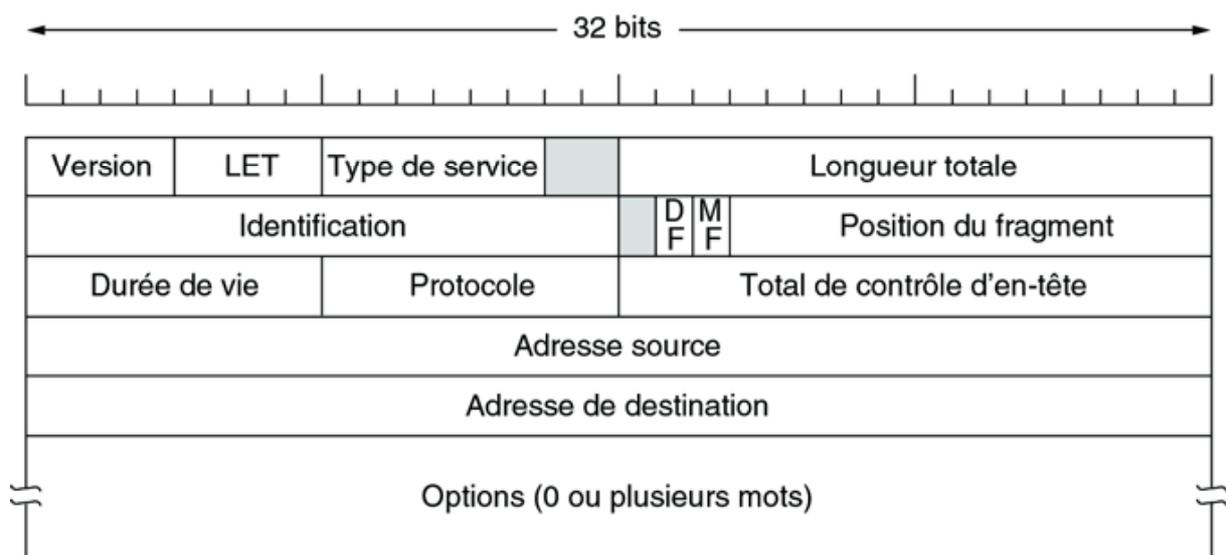
Ethernet, le format des paquets est le suivant :

FORMAT D'UNE TRAME ETHERNET

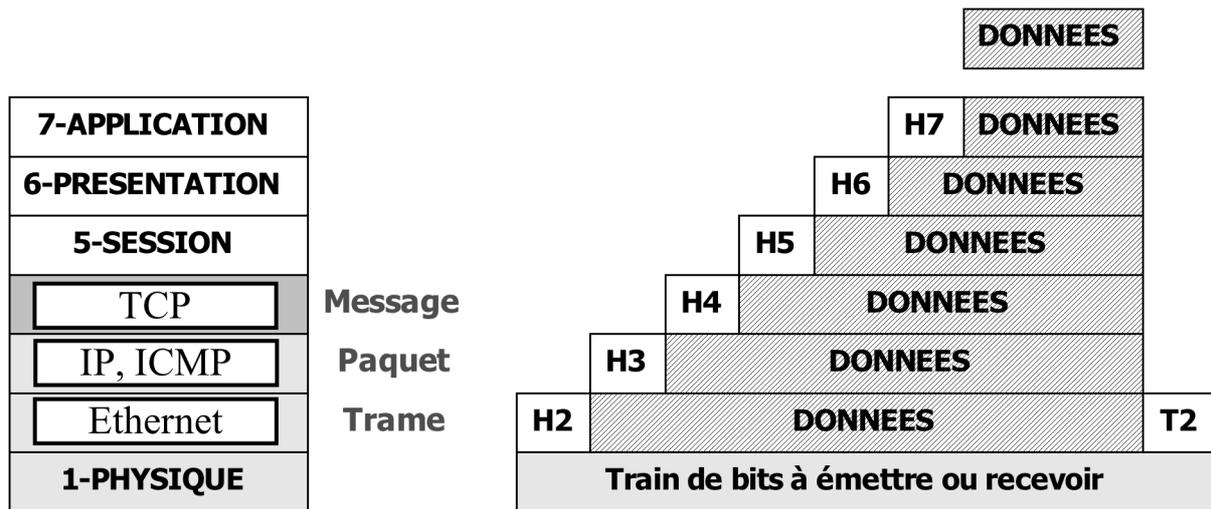


7x10101010 10101011

Le format d'un paquet IP est le suivant :



On peut donc avoir la vue logique suivante si on envoie un paquet depuis une application



Pour en revenir à la capture des paquets ou des trames qui sont transmises sur le réseau, il est possible de programmer sa carte réseau pour qu'elle accepte les paquets reçus, même si le paquet n'est pas pour elle. L'outil que nous allons utiliser est `wireshark`.

Lancer `wireshark` et essayer de capturer tous les paquets reçus sur l'interface réseau `eth0`. Essayer de reconnaître ce que vous pouvez.

Faites des ping entre vous et essayez de voir ces paquets avec `wireshark`.

Essayer de faire un filtre dans `wireshark` pour ne voir que les paquets ping qui sont de type ICMP.

Essayer de décoder un tel paquet en sachant que les paquets ping sont des paquets du protocole ICMP. La figure suivante montre le format d'un paquet de type ICMP, avec l'entête IP de 20 octets indiqué.

