TP1 - correction

I. Connaître sa machine

a) Quel est le nom de votre machine ?

```
env #pour connaitre la commande. Rappels sur les variable
d'environnement.

echo $HOSTNAME
```

b) Qu'est-ce qu'une interface réseau ? Avec la commande **/sbin/ifconfig**, donnez les interfaces réseaux actives sur votre PC. A quoi correspondent-elles ?

```
eth0 : interface ethernet. Elle permet à des machines connectées
sur un réseau ethernet de communiquer par envoi de trames
ethernet.

lo : boucle locale Elle permet à toutes les applications d'une
même machine de communiquer entre elles via le réseau.
```

c) Quelle est l'adresse ethernet (MAC) de votre pc ? Quelles sont les 2 parties de l'adresse MAC ? Quel est le constructeur de votre PC (http://www.coffer.com/mac_find/) ?

```
HWaddr 00:19:e0:0e:5b:02

LES 3 premiers octets sont l'adresse du constructeur. 0019E0 correspond
à TP-link Technologies,
```

d) Est-il possible de faire de la diffusion ou du multicast sur ce réseau local ? Quelle est la taille maximale autorisée pour un paquet Ethernet(http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit) ?

```
eth0      Link encap:Ethernet  HWaddr 00:19:e0:0e:5b:02

          inet adr:134.157.105.152  Bcast:134.157.105.255
Masque:255.255.255.0

          adr inet6: fe80::219:e0ff:fe0e:5b02/64 Scope:Lien

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

          RX packets:8307001 errors:0 dropped:0 overruns:0 frame:0

          TX packets:6021135 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 lg file transmission:1000

          RX bytes:3548712042 (3.3 GiB)  TX bytes:1798806030 (1.6 GiB)

          Interruption:17 Adresse de base:0xc800
```

II. Observer les trames ethernet

A) Format de trames Ethernet (II)

a) Donnez le format d'une trame Ethernet

En octets

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14 ... 1513	1514	1515	1516	1517
Adresse MAC destination													Adresse MAC source		Taille ou Type de protocole		Données sur 1500 octets max, 46 min.	FCS/CRC

Chaque octet est donné sous sa forme hexadécimale (2 caractères hexadécimaux).

Le type de protocole est codé sur 2 octets. Il faut consulter une table de correspondance.

Les données applicatives sont brutes et de taille limitée. La taille minimale des données est de 46 octets. Si nécessaire, des octets de bourrage (0) sont ajoutés.

Les 4 derniers octets correspondent à la séquence de contrôle -FCS ou Frame Control Sequence) de la trame qui permet de détecter d'éventuelles erreurs.

b) Identifier la source, le destinataire et le protocole applicatif encapsulé dans la trame ethernet ci-dessous :

```
ff  ff  ff  ff  ff  ff  00 30  48 56 2b c8 08 06 00 01
08 00 06 04 00 01 00 30  48 56 2b c8 86 9d 69 15
00 00 00 00 00 00 86 9d  69 c0 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00
```

```
ff  ff  ff  ff  ff  ff  00 30  48 56 2b c8 08 06 00 01
08 00 06 04 00 01 00 30  48 56 2b c8 86 9d 69 15
00 00 00 00 00 00 86 9d  69 c0 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00

jaune = destination = broadcast ; bleu = source ; 0806=ARP
```

B) Wireshark

Wireshark (anciennement *Ethereal*) est un analyseur réseau très populaire. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau. Un manuel utilisateur se trouve ici :

http://david.roumanet.free.fr/serendipity/uploads/reseaux/Manuel_WireShark.pdf

c) Démarrer **wireshark** (dans les raccourcis ou en ligne de commande). et charger la capture http://webia.lip6.fr/~lepape/ens/resap/tp/TP1/capture_arp.pcap Dans le menu **View>Name Resolution**, décochez les options de résolution de noms si elles sont sont cochées. Que voyez-vous ? Identifiez la fenêtre de résumé, la fenêtre d'arborescence de protocoles et la fenêtre de vue des données.

```
Wireshark capture toutes les trames ethernet qui passent sur le même réseau local,
en particulier celles qui sont en rapport avec le PC, mais aussi toutes les
autres.

Dans la fenêtre du haut (fenêtre de résumé), on a pour chaque tramet ethernet :
- le numéro de la trame
- l'estampille de capture
- l'adresse MAC de la source
- l'adresse MAC de la destination
- le protocole de plus haut niveau encapsuté dans la trame
- les infos principales sur le contenu applicatif

Dans la fenêtre centrale  (fenêtre des protocoles) on a le détail des piles de
protocoles encapsulés dans la trame et des données applicatives

Dans la fenêtre du bas  (fenêtre des données) on a la trame elle-même.
```

d) Pour limiter le nombre de données, l'utilisateur peut spécifier un filtre d'affichage (http://openmaniak.com/fr/wireshark_filters.php#display) . Filtrer les paquets en ne gardant que les trames **arp**.

```
Mettre arp dans le filtre
```

e) Pour cet exercice, il faut savoir qu'une machine n'est connue par son adresse MAC que sur le réseau local. Sur Internet, une machine est connue par une adresse globale, appelée adresse IP**. Que fa**it le protocole ARP ?

```
Un ordinateur connecté à un réseau informatique souhaite émettre une
trame ethernet à destination d'un autre ordinateur dont il connaît l'adresse IP et
placé dans le même sous-réseau. Le protocole ARP effectue  la traduction d'une
adresse de protocole de couche réseau (typiquement une adresse IPv4) en
une adresse MAC (typiquement une adresse ethernet).
```

f) Consulter la table ARP de votre PC avec la commande **/usr/sbin/arp -n**
Que contient-elle ?

```
   La conversion entre les adresses IP et les adresses MAC (HWaddress)

   Address                  HWtype  HWaddress           Flags Mask
   Iface

   134.157.105.59           ether   b8:ac:6f:89:b7:5a   C                     eth0
```

```
134.157.105.21           ether   00:30:48:56:2b:c8   C                     eth0

134.157.105.45           ether   00:e0:81:c5:81:c4   C                     eth0

134.157.105.254          ether   00:1d:71:71:b5:c0   C                     eth0

134.157.105.50           ether   00:16:3e:00:00:50   C                     eth0

134.157.105.57           ether   00:16:3e:00:00:12   C                     eth0
```

g) Analyser les trames 70 et 71..

```
trame 70 : 20:cf:30:81:30:8d broadcast à tous les équipements du réseau local
la demande de conversion de l'adresse IP 134.157.105.31 et indique sa propre
adresse

trame 71 : réponse de 00:23:54:bf:50:71 qui correspond à l'adresse IP
recherchée
```

h) La table ARP sur pc32 ne contenait pas pc31.polytech.upmc.fr et l'utilisateur exécute la commande
ping pc31.polytech.upmc.fr
Quelle nouvelle entrée doit être enregistrée dans la table ARP de pc32 ?

```
L'adresse IP de pc32 et son adresse MAC.
```

IV. Sécurité des trames ethernet

1. Ouvrez l'url suivante . http://pc84.polytech.upmc.fr/~lepape/resap/TP1/coucou.html . Le site demande un login (**test**) et un mot de passe (**soleil**). La capture de cette opération est ici : http://pc84.polytech.upmc.fr/~lepape/resap/captures/capture_htaccess. Filtrez les messages HTTP uniquement. Quelle opération HTTP a été effectuée ? Que lui a répondu le serveur ?

```
Seules les trames 311, 340, 679 et 680 nous intéressent.

311 : client : GET /~lepape/resap/TP1/coucou.html HTTP/1.1

340 : serveur : il manque l'authentification

679 : client : GET /~lepape/resap/TP1/coucou.html HTTP/1.1 avec
authentification dans le champ  Authorization

680 : serveur : retourne le contenu de la page
```

2. Dans la fenêtre de protocoles de la trame 679, chercher le champ d'authentification (Authorization). Avec l'outil en ligne http://www.dolcevie.com/js/converter.html, retrouver le codage hexadecimal correspondant à cette information et vérifier la correspondance dans la trame de wireshark.

```
    Authorization: Basic dGVzdDpzb2xlaWw=
```

```
Le code hexadecimal est identique à l'info de la trame:
41:75:74:68:6f:72:69:7a:61:74:69:6f:6e:3a:20:42:61:73:69:63:20:64:47:56:7a:
64:44:70:7a:62:32:78:6c:61:57:77:3d
```

3. Parmi ces informations de description se trouve les informations d'authentification. Sachant que ces informations sont codée en base 64 et à l'aide de l'outil en ligne http://www.hcidata.info/base64.htm, retrouver le login et le mot de passe.

```
en HEXA : 20:64:47:56:7a:64:44:70:7a:62:32:78:6c:61:57:77:3d

en ASCII :  dGVzdDpzb2xlaWw=

en base64 : test:soleil
```

4. Recommencer la même manipulation cette fois en utilisant un serveur web sécurisé (https) qui se trouve sur pc41 (*https://pc41.polytech.upmc.fr/ens/resap/TP1/test.html*).
La capture de cette opération est ici : http://pc84.polytech.upmc.fr/~lepape/resap/captures/capture_htaccess_securise. Attention : le filtre http ne fonctionne plus et le filtre https n'est pas reconnu. Il faut filtrer avec le filtre `tcp.port == 443`. Que constatez-vous ?

```
https = http + tls (le flux http est encapsulé dans une session sécurisée
où les données de l'application sont encryptées (cf
http://www.authsecu.com/ssl-tls/ssl-tls.php). On ne peut donc plus voir le
contenu des données applicatives.
```