TD 4 – Le protocole TCP et autres protocoles réseaux

Ce TD a pour objectif de vous faire découvrir ce qui se passe au niveau du réseau lorsque vous réalisez des échanges entre différentes applications. Sera étudié le fonctionnement du protocole TCP, mais aussi des autres protocoles présents sur un réseau, ainsi que les interactions qui existent entre-eux.

I - Exercice d'introduction à TCP

La commande ipconfig exécutée sur une machine donne le résultat suivant :

```
Adresse physique . . . . . .    00-60-08-61-04-7b
Adresse IP. . . . . . . . . . . :    110.10.111.2
Masque de sous-réseau . . .    255.255.0.0
Passerelle par défaut . . . . .    110.10.1.0
Serveurs DNS . . . . . .    110.10.1.1
```

1. Quelle est le contenu « minimal » de la table de routage de la machine 110.10.111.2

Sur cette même machine vous installez et activez un analyseur de trames afin d'observer les échanges réalisées. Vous lancez ensuite un navigateur et tapez dans la zone adresse : http://www.monsite.fr
Suite à une erreur de manipulation vous récupérez l'ensemble des trames échangées, mais dans le désordre.

Protocole	Source	Destination	Options
TCP	110.10.111.2 : 1234	163.34.45.1 : 80	Flag=fin,ack Seq=615 Ack=145 Win=64240 Len=0
TCP	110.10.111.2 : 1234	163.34.45.1 : 80	Flag=syn Seq=0 Ack=0 Win=64240 Len=0
DNS	110.10.1.1 : 53	110.10.111.2 : 1234	
HTTP	163.34.45.1 : 80	110.10.111.2 : 1234	HTTP/1.1 304 Not Modified
ARP	000102aff5e2	00600861047b	
HTTP	110.10.111.2 : 1234	163.34.45.1 : 80	Get /http://…
TCP	163.34.45.1 : 80	110.10.111.2 : 1234	Flag=ack Seq=1 Ack=615 Win=6754 Len=0
ARP	00600861047b	ffffffffffff	
TCP	110.10.111.2 : 1234	163.34.45.1 : 80	Flag=ack Seq=615 Ack=145 Win=64240 Len=0
DNS	110.10.111.2 : 1234	110.10.1.1 : 53	
TCP	110.10.111.2 : 1234	163.34.45.1 : 80	Flag=ack Seq=1 Ack=1 Win=64240 Len=0
TCP	163.34.45.1 : 80	110.10.111.2 : 1234	Flag=ack, syn Seq=0 Ack=1 Win=5840 Len=0

2. Remettez dans l'ordre chronologique les trames ci-dessus, en justifiant vos choix
3. Expliquez le rôle des options qui figurent dans les lignes TCP
4. Quelle est la longueur des données transmises dans les lignes HTTP . Justifiez vos réponses.

II - Analyse de trames TCP et autres protocoles avec Wireshark (Version Linux)

A – Découverte des échanges entre votre navigateur et un site Web

1 - Présentation

Wireshark est un analyseur de trafic réseau, ou "sniffer" qui est installé sur les machines linux. Il utilise une interface graphique basée sur GTK+, il est basé sur la bibliothèque libpcap, qui fournit des outils pour capturer les paquets réseau.

2 - Utilisation de Wireshark

Pour lancer ce logiciel, il suffit d'utiliser un terminal et d'y taper la commande : **sudo wireshark.**

Pour plus d'informations sur l'utilisation même du produit, tapez **man** Wireshark à l'invite de commande d'un shell.

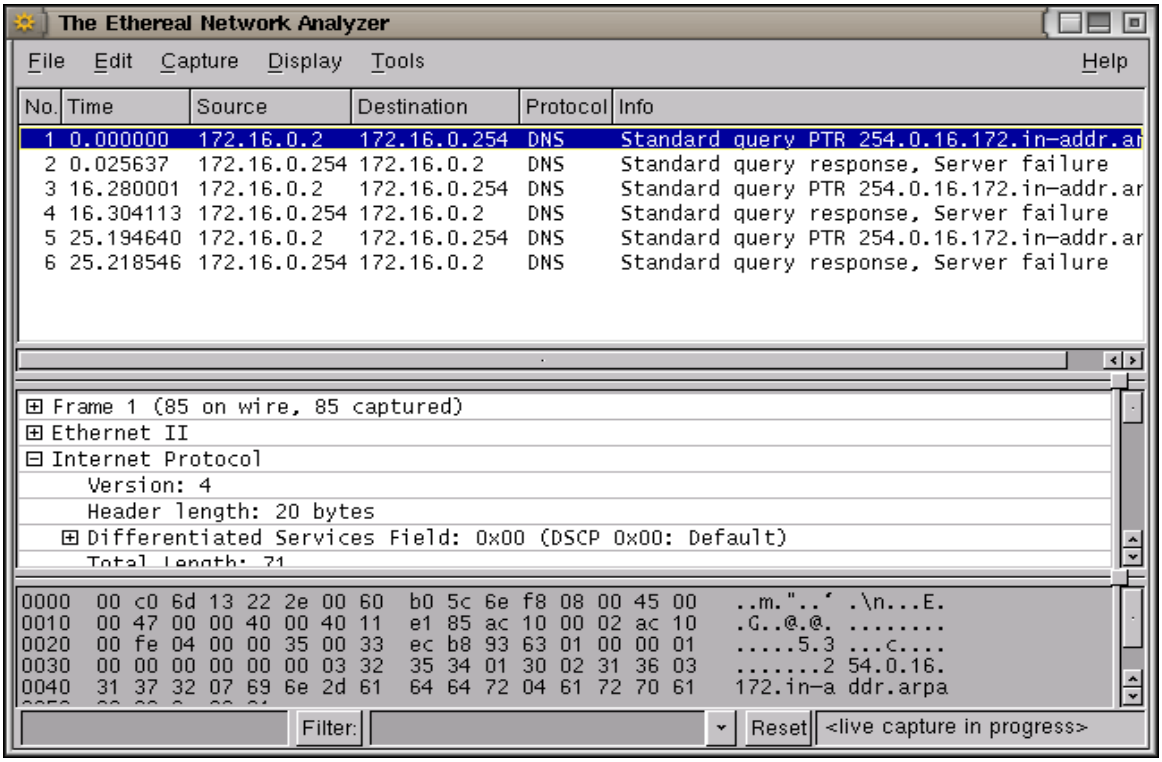
Le principe est simple, vous lancez une session de capture à l'aide du menu **Capture**. Cette session peut être interactive ou pas. En d'autres termes, les paquets capturés peuvent être affichés au fur et à mesure ou à la fin de la capture.

Pour lancer une session de capture, il faut accéder au menu **Capture** puis cliquer sur l'option **Interface...**.

Apparaît la boîte de dialogue qui permet de spécifier sur quelle interface vous souhaitez « écouter » les paquets.

Il est préférable d'opter pour l'option « any » qui écoute tous les interfaces en même temps.

Durant la capture, une boîte de dialogue récapitule les paquets qui sont conservés. En même temps les paquets apparaissent dans la fenêtre principale. L'appui du bouton Stop de l'interface permet d'arrêter la capture. Les paquets deviennent disponibles dans la fenêtre principale s'ils n'étaient pas déjà disponibles



3 - Analyse des échanges

1 – Lancer simplement la capture de paquets et attendez quelques instants. Couper la capture et observer tous les paquets capturés :

- Quels protocoles étaient actifs dans le réseau ?

- Lesquels connaissez-vous ?
- Arrivez-vous à déterminer qui a effectué une requête vers qui ?

2 – Lancer la capture de paquets, puis lancer un navigateur et allez à l'adresse : http://ffctlr.free.fr

- Combien de requêtes http ont-elles été faites ? Pourquoi ?
- Pour toutes ces requêtes combien de connexion du protocole TCP ont-elles été créées ?
- Identifier les paquets relatifs à cette connexion.
- Identifier les différentes phases d'un échange TCP. Quelles sont les adresses IP et les ports utilisés ?

4 - Analyse du protocole TCP

Dans l'analyse des entêtes des messages TCP on peut observer une zone nommée « Flags ». A l'aide du filtre de Wireshark afficher une session TCP complète (connexion, échange, déconnexion). Pour cela TCP utilise à chaque session un nouveau port, il suffit donc de mettre un filtre sur un port local donné et demander l'affichage.

- Relevez dans chaque message les valeurs des indicateurs « flags » utilisés. Quel est le rôle de chaque indicateur ?
- Analysez le paramètre « len » (longueur des données), pourquoi certains messages ont une longueur = 0 et d'autres non ?
- Analysez le paramètre « sequence number », comment évoluent les valeurs au cours de cet échange ? A quoi sert cette donnée ?

5 - Manipulation amusante :

- Réinitialiser la capture des paquets et aller à l'adresse : http://ffctlr.free.fr/formulaire.html
- Remplir les champs du formulaire, mot de passe compris et le « soumettre »
- Arrêter la capture, repérez les paquets relatifs à la connexion et essayez d'identifier votre login (nom + mot de passe).

B - Analyse et comportement des applications utilisant TCP (Question bonus)

Téléchargez 2 programmes C qui , a l'exécution, se comportent comme un « chat ».

Vous avez un programme « serveur.c » qui active un port de communication par lequel il pourra recevoir et envoyer des messages .

Vous avez un programme « client.c » qui se connecte au port de communication du serveur par lequel il peut envoyer et recevoir des messages :

Travail à faire :

- Télécharger depuis Moodle , sur votre machine les programmes : client.c et /serveur.c
  Vous devez pour cela ouvrir un editeur de texte (exemple **kwrite**), copier puis coller les programmes et les sauvegarder sur le Bureau (par exemple)
- En mode « console » : modifiez le programme client en mettant comme adresse serveur l'adresse IP de votre machine ou de la boucle locala (SERV 127.0.0.1) puis compiler ces programmes :
  gcc serveur.c –o serveur puis gcc client.c –o client
- Ouvrez une console et activez « Wireshark » en demandant d'écouter toutes les interfaces.
- Ouvrez une nouvelle console et exécutez le programme « ./serveur »
- Ouvrez une troisième console et exécutez le programme « ./client »
- Ouvrez en fin une dernière console et exécutez la commande « netstat »
- Combien de connexion sont actives ?

- Echangez quelques messages entre le client et le serveur et terminer en tapant le mot « fin ».
- Arrêtez la récupération des trames sous « Wireshark » et analysez les échanges.
- Que s'est-il passe au moment de la connexion entre les deux programmes.
- Comment se réalisent les échanges ?
- Comment se matérialise la fin de l' échange ?

- Recommencez tout cela en exécutant cette fois plusieurs clients dans plusieurs fenêtres.
- Recommencez tout cela en exécutant des clients qui se connectent à des processus serveurs actifs sur d'autres machines (n'oubliez pas de changer l'adresse IP).

Remarque : Si Wireshark récupère trop de trames parasites, mettez un filtre sur le protocole TCP