T.P. RTD 1/2

Olivier Fourmaux

Ce T.P. d'une journée doit être réalisé par **binômes**[1]. Vous devez rendre, à la **fin de la séance**, la présente feuille de sujet comprenant vos noms, prénoms, date et quelques renseignements[2] demandés dans les cadres ci-dessous avec le compte-rendu réalisé.

NOM, Prénom du premier étudiant		NOM, Prénom du second étudiant	

Date de la séance		Groupe de TP	
Adresse IP		Numéro de la machine	
Adresse MAC de la carte Ethernet		Numéro disque extractible	

1 Découverte de l'analyse de trames

1.1 Préliminaires

Les paramètres de base associés à votre machine (nom, adresse IP etc...) peuvent ne pas être corrects au démarrage. Votre encadrant vous les communiquera pour un fonctionnement adéquat.

Avec votre système **Debian GNU/Linux**, vous pouvez changer le nom avec la commande **hostname pc***xx* et les paramètres IP en éditant le fichier `/etc/network/interfaces`. Stoppez votre interface avec la commande `ifdown eth0` au préalable. Le fichier doit contenir une entrée du type :

```
iface eth0 inet static
                address 194.254.167.2xx
                netmask 255.255.255.0
                gateway 194.254.167.254
```

où 2xx désigne l'octet spécifique de votre adresse IP en correspondance avec le nom de votre machine (pc*xx*). Relancer votre interface avec la commande `ifup eth0`.

Pour modifier les ressources réseaux, vous avez à votre disposition le compte administrateur : *login* = `root` (*password* = `racine`).

Attention : Si vous réalisez la moindre modification de la configuration de votre machine, n'oubliez pas de réaliser une copie de sauvegarde des fichiers modifiés dans le même répertoire (`cp toto toto.old ; vi toto`). *Vos modifications peuvent altérer le bon fonctionnement du système, il est donc impératif de pouvoir restaurer l'état précédent celles-ci.*

Vous avez aussi accès à un compte utilisateur : *login* = `user` (*password* = `utilisateur`).

1.2 Introduction

Dans ce premier T.P., nous vous proposons d'analyser divers protocoles circulants dans les trames du réseau local. Pour cela, nous récupérons celles-ci à partir de votre interface. Le réseau étudié (*Ethernet*) étant de type à **médium partagé**, l'interface "voit" potentiellement tout le trafic échangé sur le réseau local. Pour lui demander de ne pas juste "voir", mais d' "enregistrer" le trafic pour transmettre ces trames observées au système d'exploitation (y compris celles qui ne lui sont pas destinées), un mode "promiscuité" est disponible. Ce mode ne perturbe ni le trafic du réseau, ni celui de votre machine, et permet de transformer celle-ci en analyseur multiprotocolaire avec un logiciel adéquat.

1.3 Exemple d'analyse

Pour les exercices suivants, lorsque l'on vous demande d'*analyser une trame*, vous devez recopier le contenu de la trame et réaliser sa segmentation en associant **toutes** les valeurs observées avec les différents champs protocolaires et leurs significations.

Exemple avec le début d'une trame ARP en représentation hexadécimale :

```
ff ff ff ff ff ff 08 00 11 0c 59 45 08 06 00 01
08 00 06 04 00 01 08 00 11 0c 59 45 c0 21 b6 b7
...
```

L'analyse attendue est la suivante :

La trame est de type *Ethernet* car la valeur du champ *type* est supérieure à 1500. Elle comporte les champs suivants :

- `ff ff ff ff ff ff` : adresse *Ethernet* destination sur 6 octets. Trame envoyée vers `FF:FF:FF:FF:FF:FF` (adresse de diffusion).
- `08 00 11 0c 59 45` : adresse *Ethernet* source sur 6 octets. Trame émise de la carte `08:00:1:0C:59:45`.
- `08 06` : type de données transportées par la trame sur 2 octets. 0x0806 correspond au protocole *ARP*.
- cette trame encapsule le paquet *ARP* avec les champs suivants :
  - `00 01` : type de medium sur 2 octets. 0x0001 spécifie un type d'adresse matérielle *Ethernet*.
  - `08 00` : type de protocole sur 2 octets. 0x0800 spécifie un type d'adresse de protocole *IP*.
  - `06` : taille des adresses medium sur un octet. Indique que la taille pour *Ethernet* est de 6 octets.
  - `04` : taille des adresses protocole sur un octet. Indique que la taille pour *IP* est de 4 octets.
  - `00 01` : code opération *ARP*. Indique que c'est un paquet requête codé avec la valeur 0x0001.
  - `08 00 11 0c 59 45` : adresse *Ethernet* de l'émetteur représentée en hexadecimal sur 6 octets (la même que le second champ de la trame).
  - `c0 21 b6 b7 ...` et ainsi de suite...

[1] Si le nombre d'étudiants du groupe est impair, **un monôme est autorisé** mais en aucun cas un trinôme.
[2] Voir la section 1.1 puis exécuter la commande `ifconfig eth0` et observez les champs `inet adr` et `HWaddr`.

1.4 Réalisation d'une capture : Ethereal

Le logiciel `ethereal`[3] est un analyseur de protocoles (*sniffer*). Celui-ci utilise directement l'interface *Ethernet* de votre machine pour réaliser la capture de toutes les informations circulant sur le réseau local sur lequel vous êtes connecté[4]. Avec la commande `man ethereal` vous obtiendrez les informations de base.

Exécutez `ethereal` **avec les privilèges administrateur.**

Initialement l'écran est vide car aucune capture n'a été réalisée. Cliquez sur le menu **Capture** et sélectionnez **Start**. La boîte de dialogue "*Ethereal : Capture Preferences*" apparaît.

– Activez : *Update list in packets in real time*,
– Désactivez : *Enable name resolution*.

Ne pas spécifier de filtres dans le champ *Filter*, nous y reviendrons plus loin. Cliquez finalement sur **Ok** : La capture de trafic commence... vous observez tout le trafic échangé localement.

Pour stopper la capture, il suffit de cliquer sur la boîte de dialogue "*Ethereal : Capture*" et sélectionnez **Stop**. Vous pouvez maintenant vous déplacer sur les différentes trames pour avoir des informations spécifiques à chacune d'elles. De plus, vous pouvez aussi sauver les captures réalisées (cliquez sur **File**, puis sélectionnez **Save Capture File**) pour pouvoir les réutiliser ultérieurement.

1. Sous quelles formes sont représentées les données échangées sur le réseau ?
2. Quels sont les différents protocoles que vous pouvez observer dans la capture réalisée ?

1.5 ARP

Nous nous intéressons à la résolution d'adresse ARP.

1. Décrivez le fonctionnement théorique du protocole ARP.
2. Comment sont gérées les correspondances des adresses au niveau du système d'exploitation ?
3. Quand une requête ARP est-elle émise ?
4. Comment fonctionne la commande `arp` (utilisez `man`) ?
5. A l'aide de la commande `arp`, effacez les entrées de la table locale pour générer une requête ARP lors d'un accès au réseau (exemple : `ping`). Analysez les deux trames échangées.

1.6 IP + ICMP

Nous analysons un échange de paquets ICMP.

1. Étudiez le fonctionnement de la commande `ping`. Quel est son utilisation la plus classique ? Donnez un exemple probant d'utilisation.
2. Analysez les deux trames échangées (transportant ICMP) lors de l'utilisation de la commande `ping` à l'aide du logiciel d'analyse de trames.
3. Quelle modification entraîne l'utilisation de l'option d'enregistrement de la route `RECORD_ROUTE` (`ping -R`).
4. Analysez la trame de retour pour une machine de la salle (`ping -R 194.254.167.yyy`).
5. Analysez la trame de retour pour une machine proche (`ping -R www.univ-paris13.fr`).
6. Analysez la trame de retour pour une machine éloignée (`ping -R www.umass.edu`).

1.7 Transmission FTP

Réalisez et analysez une transmission FTP. Ouvrez une connexion à partir de votre machine (commande `ftp`) vers une autre machine de la salle où vous vous connecterez en tant qu'utilisateur `user` et récupérez le fichier `/etc/services`.

1. Décrivez les fonctionnalité de l'application client `ftp`.
2. Quel protocole de la couche transport est utilisé ? Pourquoi deux ports sont utilisés ? A votre avis, quel est le principe de fonctionnement de FTP ?
3. Quelles sont les différentes commandes échangées par le protocole ?
4. Analysez l'échange complet de paquets que génère la commande `ls` sur le port FTP-DATA (étudiez seulement à partir de la couche transport).
5. A l'aide de l'outils `telnet`, réalisez une connection sur le port 21. Quel est l'intéret de cette manipulation ? Quelles informations pouvez vous obtenir. Quelles actions pouvez vous réaliser ?

1.8 Traces diverses

Dans cette dernière partie, nous nous intéressons à des situations que vous ne pouvez pas observer sur le réseau local de la salle. Nous allons donc nous baser sur des traces pré-enregistrées qui se trouvent sur votre machine dans `/usr/share/traces`. Cliquez sur **File**, puis sélectionnez **Open** pour charger celles que nous allons étudier dans la suite (ne pas oublier de désactiver : *Enable name resolution*).

1.8.1 Trace `dualhome.iptrace`

1. Quel est le nouveau type de trames que vous observez ?
2. Quelles sont les différences avec les trames *Ethernet* ?
3. Analysez la **N**ième[5] trame *Token Ring*.
4. Quelles différences notez-vous au niveau de la résolution d'adresse *Token Ring* ?

1.8.2 Trace `genbroad.snoop`

1. Quels sont les nouveaux types de protocoles de la couche réseau que vous observez ?
2. Décrivez les principaux échanges réalisés.
3. Dans quelle situation peut on observer un tel trafic ?

1.8.3 Trace `v6.pcap`

1. Quel est le nouveau type de protocols réseau ?
2. Analysez la **N**ième trame ICMPv6.
3. Analysez la **N**ième trame TCP/IPv6.

1.9 Nettoyage

Supprimez les configurations réalisées dans la machine. puis stoppez la en passant administrateur et en tappant `halt`.

[3] `ethereal` est un logiciel libre. Il est disponible sur un grand nombre de plate-formes matérielles et systèmes d'exploitation (outre les machines à architecture **i368** avec système **Debian GNU/Linux** que vous utilisez actuellement). Vous pouvez le télécharger sur `www.ethereal.org`.

[4] L'interface *Ethernet* doit être configurée par `ethereal` dans le mode "*promiscuous*" afin d'accéder à tout le trafic diffusé sur le segment où votre machine est connectée. Pour changer de mode, l'application doit être exécutée avec les privilèges de l'administrateur.

[5] **N** est votre numéro de disque extractible modulo 20.