# M1 SIRIS – SR
# TP Analyseur Réseau

## Sujet : réalisation d'un analyseur réseau sous Linux

Les logiciels comme tcpdump utilisent la librairie pcap[1] afin de capturer les paquets circulant sur le réseau. Le but de ce TP est de récupérer cette librairie, de l'installer et de faire appel à ses primitives afin de capter les trames.

Une fois cette première étape franchie, il vous est demandé d'analyser les paquets et d'afficher le contenu de ces derniers de manière compréhensible.
Evidemment, il ne vous est pas demandé de réaliser tcpdump mais d'au moins être capable d'afficher sous une forme synthétique les informations des en-têtes des protocoles, et le contenu applicatif :

- ethernet,
- IP,
- UDP,
- TCP,
- ARP,
- applications vues en cours : BOOTP et DHCP, DNS, HTTP, FTP, SMTP, etc.

Votre programme, écrit en C standard, devra pouvoir analyser les trames capturées directement sur le réseau, ou bien obtenues à partir d'un fichier de capture créé par tcpdump (voir -w dans les manpages de tcpdump).

**Ce TP s'étale sur l'ensemble du semestre : après chaque nouveau protocole abordé en cours, il est conseillé de l'intégrer immédiatement dans votre programme (ne pas tenter de tout faire dans les dernières semaines du semestre !)**

## Contraintes d'implémentation

Les entrées de votre programme seront obligatoirement passées sur la ligne de commande (pas d'interaction avec l'utilisateur après le démarrage, sauf ^C pour quitter). Les commutateurs de la ligne de commande sont imposés :
-i <interface> : interface pour l'analyse live
-o <fichier> : fichier d'entrée pour l'analyse offline
-f <filtre> : filtre BPF (optionnel)
-v <1..3> : niveau de verbosité (1=très concis ; 2=synthétique ; 3=complet)

Le niveau de verbosité indique le niveau de détail de l'affichage :

- très concis : une ligne par trame
- synthétique : une ligne par protocole, soit quelques lignes par trame
- complet : la totalité des champs protocolaires et des contenus applicatifs, organisés de manière hiérarchique.

L'analyse doit se poursuivre jusqu'à l'arrêt par ^C. La capture concernera l'ensemble des octets présents dans les trames. Vous utiliserez impérativement les librairies des répertoires /usr/include/net et /usr/include/netinet pour lire les différents champs d'en-têtes ; il faudra rechercher bootp.h qui ne s'y trouve pas.
La liste des primitives de la librairie pcap a été vue en cours.

[1] http://www.tcpdump.org

Pour avoir le support des primitives liées à la librairie pcap, insérer la ligne suivante dans votre programme : `#include <pcap.h>`
Pour compiler : `gcc -o analyseur analyseur.c -lpcap`

## Informations complémentaires

Vous serez notés sur :

- l'écriture de votre programme (pas de warnings à la compilation, code commenté, programme clairement structuré en différentes fonctions/procédures ayant un objectif bien précis),
- la justesse des informations,
- l'affichage issu de l'analyse des trames : la présentation doit être synthétique, par exemple sous forme d'arborescence détaillant les différents protocoles encapsulés et leurs champs intéressants.

Il s'agit d'un travail individuel. Vous posterez finalement votre programme C sur moodle, impérativement accompagné d'un makefile et du fichier bootp.h utilisé. Les programmes qui ne passent pas l'étape de la compilation ne seront pas évalués.