Université Toulouse III – Paul Sabatier
L2 Informatique

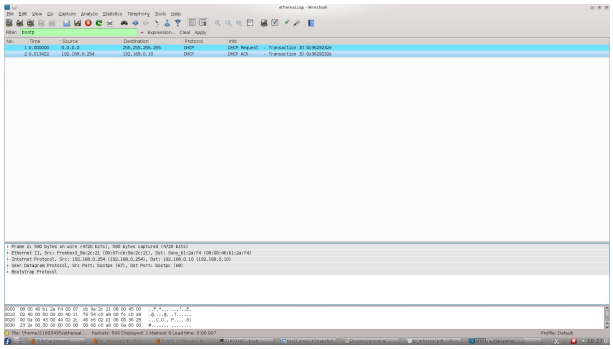
Réseau
7 octobre 2013
Semestre 5

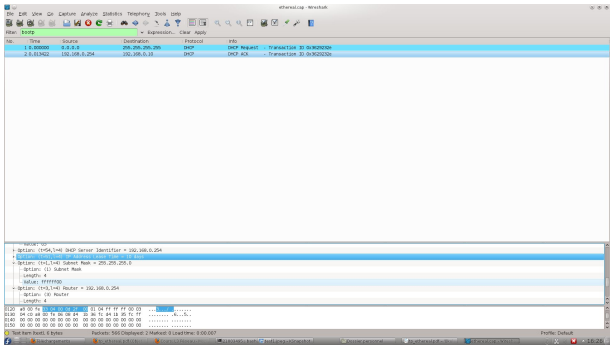
TP nº 1 — Observation bas niveau de protocoles

Antoine de Roquemaurel (Groupe 1.1)

1 DHCP

Les messages DHCP sont envoyés au dessus d'UDP, cf figure 1.





IP du serveur DHCP : 192.168.0.254, cela correspond à la source du second message, la réponse.

Le message Nº 2, à l'instant 0.013422 contient la nouvelle IP, il fait également office d'acquittement, cette IP est 192.168.0.10.

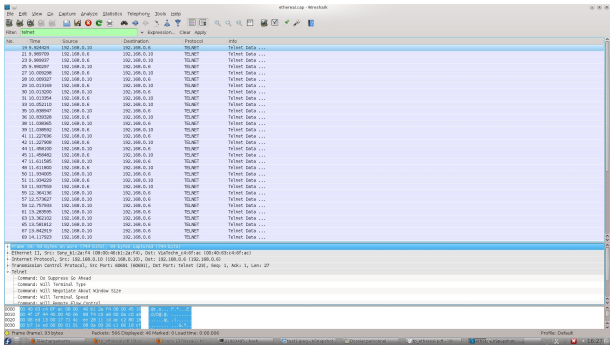
L'adresse IP à une durée de vie de 10 jours, cette durée de vie est transmise dans le protocole bootstrap via le champ *Address Lease Time*.

2 Telnet

Ils sont envoyés sur TCP. Cf figure **??**.

Le login est « guest » et le mot de passe est « trivial », cela permet de se connecter au serveur d'adresse IP 192.168.0.6.

La commande tapée est `pwd` ayant pour réponse `/home/guest`.



3 DNS

Les messages sont envoyés en UDP, c'est une requête de type « standad query A ».

Plusieurs réponses sont situées dans la requête 114, celle-ci répondant avec les adresses IP et sous domaines de kernel.org [1]. Cf figure **??**.

4 Ping

Le protocole du ping est le protocole ICMP.

Pour le second message, contrairement à la requête 101, le client ne connait pas l'adresse, ainsi avant d'effectuer le ping, il effectue une résolution de nom à l'aide du serveur DNS. Dans le premier cas, le ping s'effectue immédiatement.

Le protocole ICMP n'a pas de numéro de port car il est situé au même niveau que TCP et UDP.

5 FTP

Les échanges s'effectuent en TCP, j'utilise le filtre `ftp || ftp-data` afin d'avoir tous les échanges ftp, y compris les données.

L'utilisateur est « anonymous » et le mot de passe « toto@titi.fr », il a téléchargé le fichier welcom.msg d'une taille de 1912 octets.

Le message est dans l'échange 218, de protocole ftp-data, le message commence par « ‾Ŵelcome to the ‾...»

1. c'est à dire ftp.kernel.org, pub.kernel.org qui correspondent au adresses ip de pub.us.kernel.org, 204.152.191.37 et 204.152.191.5

6 HTTP

6.1 Image

Le client demande la version 1.1 de http, le serveur renvoit bien la version 1.1 avec le statut 200 (signifiant que tout est ok).

Le fichier a été modifié le Lundi 21 Janvier 2008 a 10h55 et 2 secondes.

La requête HTTP à une taille totale de 23754 octets.

6.2 Site Web

Le client est sur le système Linux(Debian 2.0).

Le nombre maximal de fichier demandé simultanément est

Cette image à été mise en cache dans le navigateur, elle n'est ainsi pas redemandée.