Université Toulouse III – Paul Sabatier
L3 Informatique

Réseau
20 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.

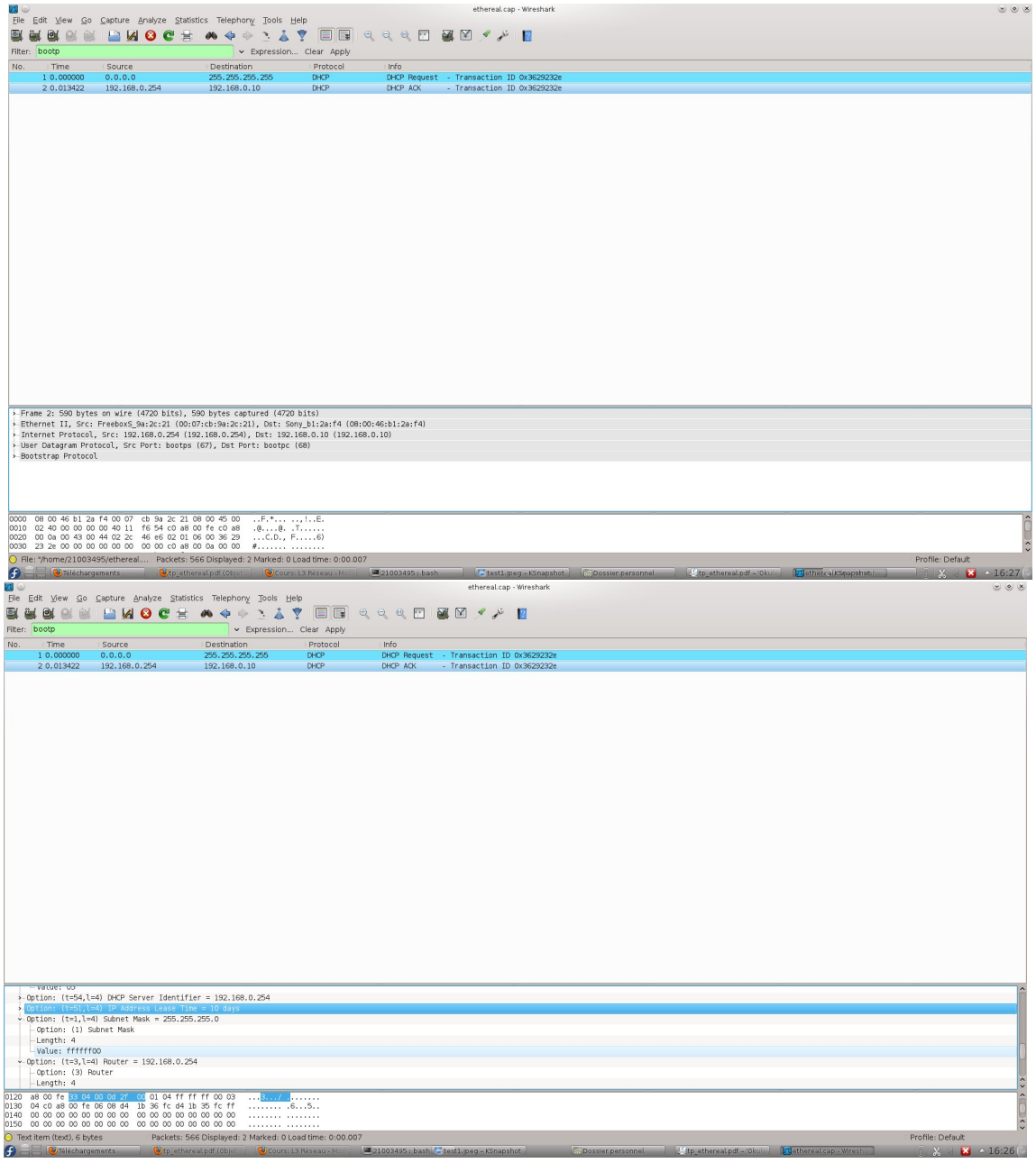

Figure 1 – Messages DHCP

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

Le message N° 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 2.

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`.

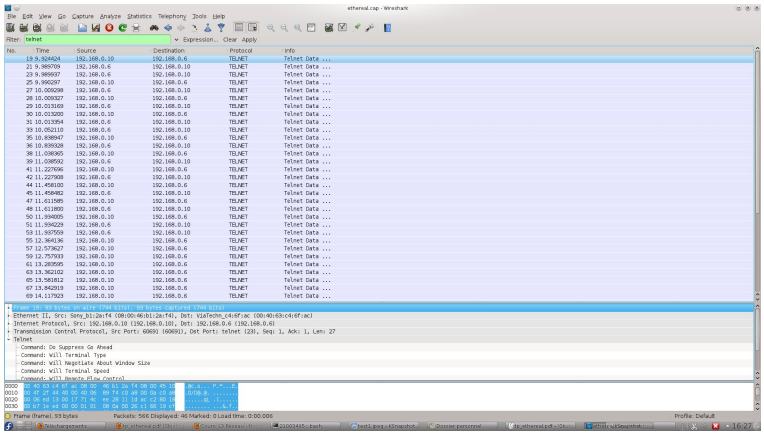

Figure 2 – Messages telnet

Figure 3 est disponible le diagramme temporel d'échange.

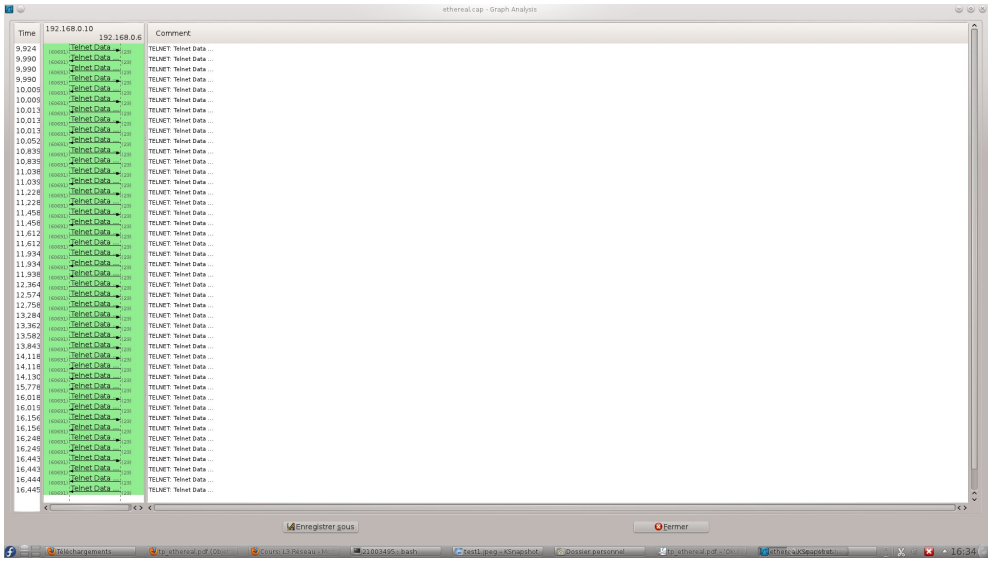

Figure 3 – Diagramme temporel d'échange

R C'est le fait que le protocole telnet ne soit pas sécurisé qui nous permet de pouvoir analyser le login et le mot de passe de l'utilisateur, ainsi l'utilisation d'un autre protocole tel que SSH permettrai que personne utilisant un analyseur réseau puisse obtenir ces informations

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 5.

Le protocole DNS permet de faire le lien entre un domaine (ftp.kernel.org) et une adresse ip (204.152.191.37).

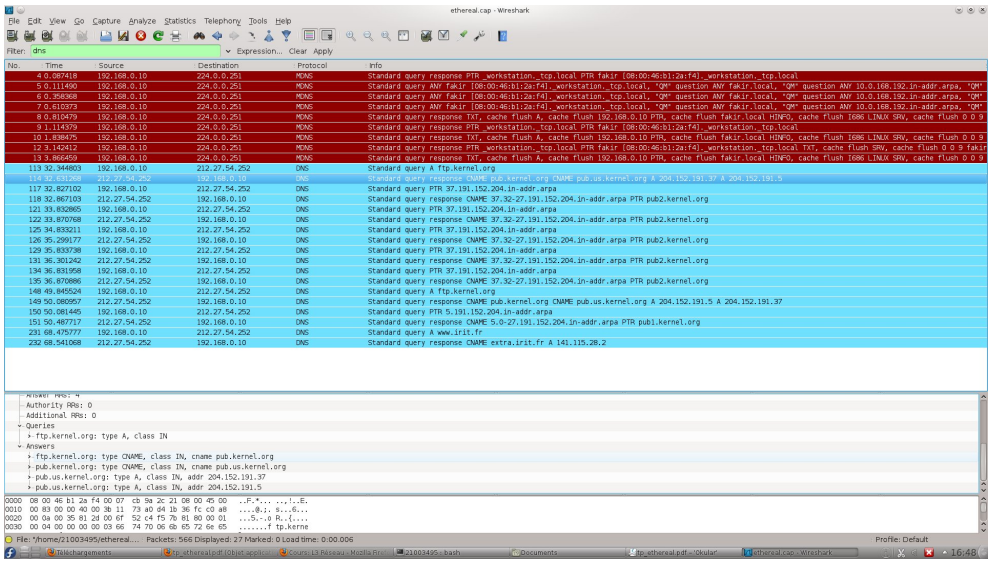

Figure 4 – Les messages DNS

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.

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

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 « Welcome to the... »

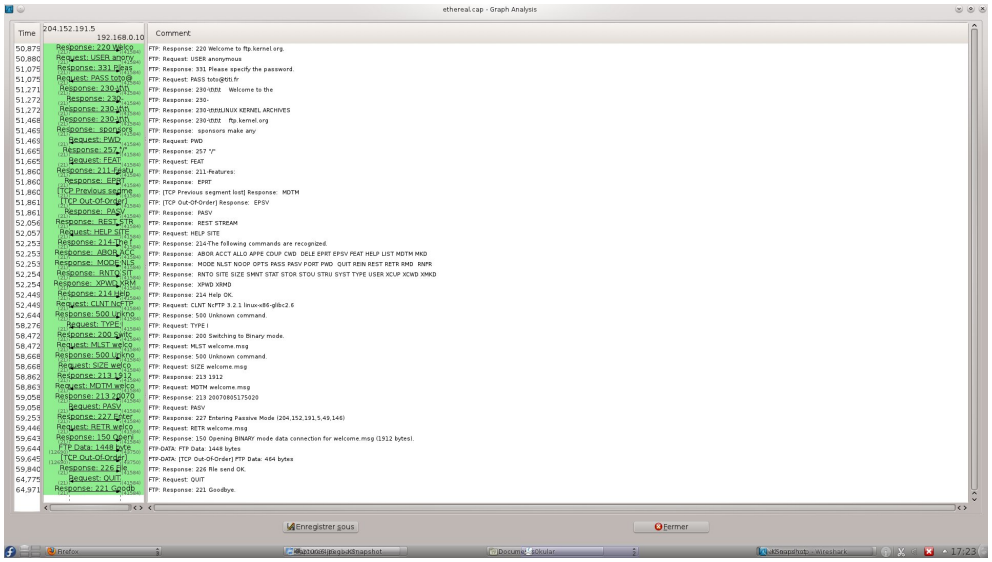

Figure 5 – Diagramme temporel d'échange FTP

> R De la même manière que Telnet, FTP n'est pas un protocole sécurisé, ainsi l'utilisation du protocole FTP encapsulé dans du SSH (utilisation de sftp) semblerai meilleur. Ainsi il n'aurai pas été possible d'obtenir le contenu des échanges et les logins et mot de passe.

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.

Le fichier est grand, ainsi lors de la demande du fichier par l'utilisateur, le serveur HTTP envoie

un acquittement, et découpe le fichier en 36 trames[2]. Pour chaque trame, le serveur envoie la trame numérotée, et le client un acquittement (protocole TCP), une fois que toutes les trames sont envoyées et acquittées, le serveur peut envoyer `HTTP/1.1 200 ok` afin de signaler la fin de la communication et le bon envoie du fichier.

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.

6.3 Traceroute

Traceroute envoie des messages aux serveurs jusqu'à que ceux-ci atteignent un TTL de 1, ainsi les messages envoyés ont un TTL de plus en plus grand afin de passer de plu en plus de routeurs. Une fois qu'un routeur atteind le TTL de 1, celui-ci envoie « time to lie excedeed ».

A *

Table des figures

2. jusqu'à la trame 272