Université de Toulon

IUT de Toulon

Département Génie Electrique et Informatique Industrielle (GEII)

Réseaux Cybersécu Wireshark

Rapport de TP

écrit le 15 décembre 2023

par

Bruno HANNA

Encadrant universitaire : Stephane PIGNOL

Table des matières

Introduction

Ce document présente une série d'expérimentations pratiques visant à approfondir la compréhension des protocoles fondamentaux qui régissent les communications dans les réseaux informatiques. À travers l'application de méthodes d'analyse de trames réseau telles que Wireshark et l'usage de commandes comme `nslookup` et `dhclient`, ce rapport détaille les observations et les analyses relatives aux protocoles ARP, ICMP, TCP, DNS, et DHCP. L'objectif est double : examiner le comportement de ces protocoles en conditions réelles et démontrer l'utilisation d'outils de diagnostic réseau pour interpréter les résultats de ces interactions protocolaires.

Partie WireShark

1.1 Préliminaires

1.1.1 Configuration IP dynamique et vérification du paramétrage réseau

Dans cette partie, le mode de configuration IP dynamique a été sélectionné. La vérification du paramétrage réseau a été réalisée en utilisant la commande `ifconfig`.

Adresse MAC et IP de la machine

Les informations suivantes ont été obtenues :

— Adresse MAC de la machine : `50:64:2B:LA:73:CF`

— Adresse IP attribuée : `192.168.0.71`

1.2 Captures ARP et ICMP

1.2.1 Gestion de la table ARP

La commande `arp` a été utilisée pour visualiser et modifier la table des entrées ARP. La table a été purgée avec l'exception de l'entrée correspondant à la passerelle.

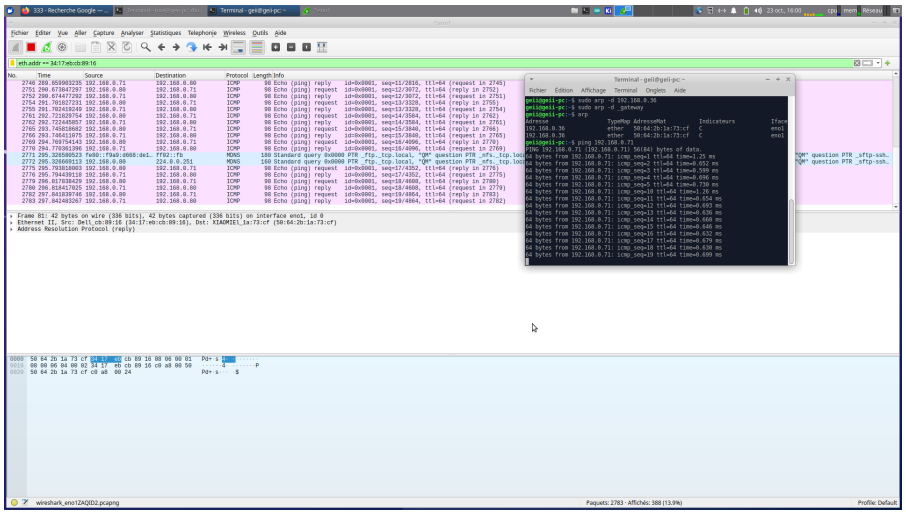

Figure 1.1 – La table ARP après la purge des entrées.

1.2.2 Capture ARP

Une capture de trames ARP a été initiée en filtrant sur l'adresse MAC de la machine. Une requête ARP a été générée par un ping vers une autre machine du réseau. Cette requête est illustrée dans la figure suivante.

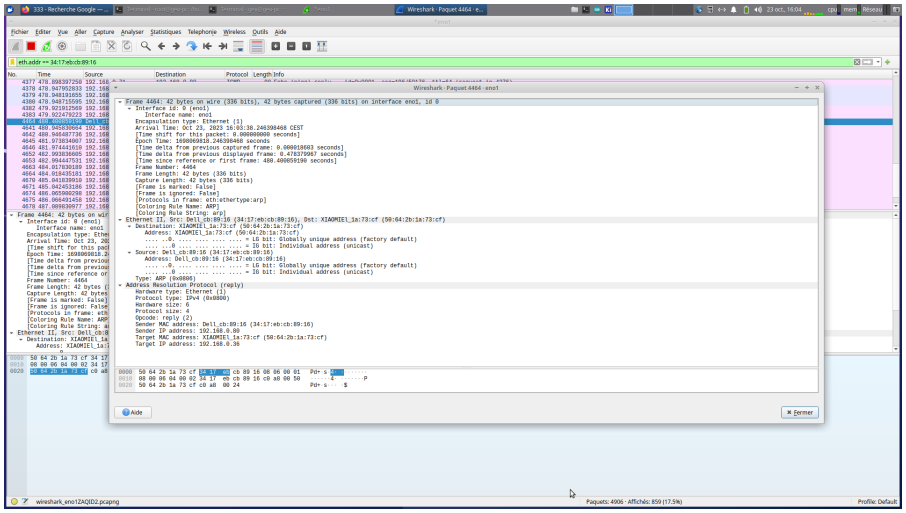

Figure 1.2 – Requête ARP et sa réponse correspondante.

1.2.3 Capture ICMP

La capture ICMP a permis d'analyser les trames générées par les commandes ping. Les données transférées lors d'un ping sont illustrées ci-dessous.

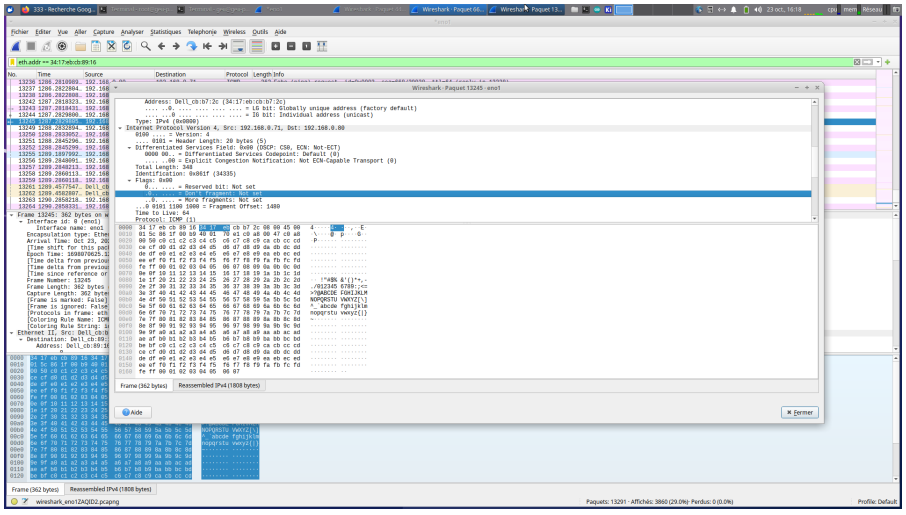

Figure 1.3 – Détail des trames ICMP générées par un ping standard.

1.2.4 Ping avec une grande taille de données

Les paquets ICMP résultant d'un ping de 1800 octets ont été fragmentés. Cette fragmentation est illustrée dans la capture d'écran suivante.

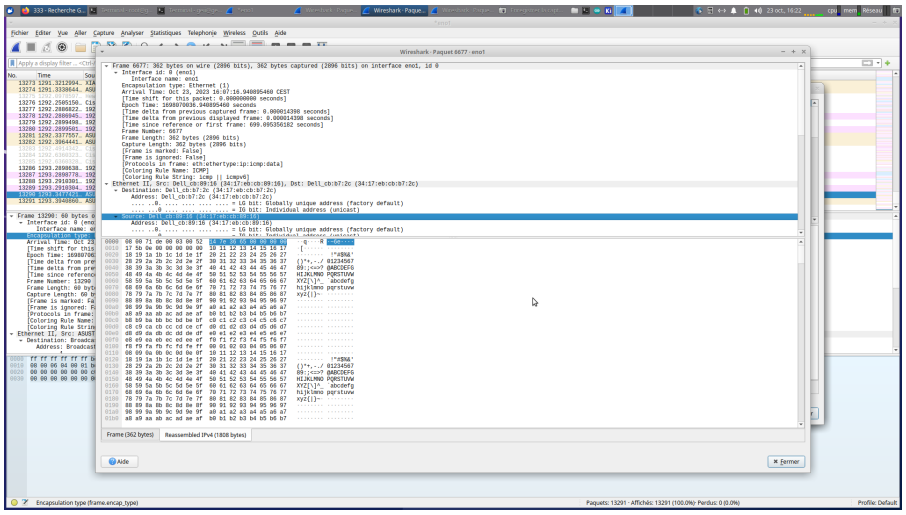

Figure 1.4 – Fragmentation observée lors d'un ping avec une taille de données de 1800 octets.

1.3 Observation des Ports et Connexions TCP

1.3.1 État des Services en Écoute

La commande `netstat -tlp` a révélé les services en attente de connexions sur divers ports. Ces services comprennent le serveur d'impression `cupsd` et le serveur SSH `sshd`, indiquant que la machine est prête à accepter les connexions pour ces services.

```
# Extrait des resultats de 'netstat -tlp'
tcp   0   0 0.0.0.0:ssh      0.0.0.0:*    LISTEN   1271/sshd
tcp   0   0 0.0.0.0:ipp      0.0.0.0:*    LISTEN   1219/cupsd
```

1.3.2 Connexions TCP Actives

La commande `netstat -tnp` a permis d'identifier une connexion TCP établie, signalant un échange de données actif avec un serveur distant sur le port 10000, généralement associé à des applications réseau personnalisées.

```
# Extrait des resultats de 'netstat -tnp'
tcp   0   0 192.168.0.80:55278   192.168.0.200:10000   ESTABLISHED 6857/telnet
```

1.4 Analyse Complète des Connexions Réseau

L'exécution de `netstat -tanp` a fourni une vue d'ensemble des connexions TCP, montrant à la fois les services en écoute et les connexions établies. Le remplacement de l'option '-t' par '-u' nous a permis d'examiner les connexions UDP, soulignant leur utilisation dans les communications nécessitant un transfert rapide de données.

1.5 Informations Réseau et Routage

La commande `netstat -rn` a révélé la table de routage, qui dirige les paquets vers les destinations appropriées. En parallèle, `netstat -ie` a offert un aperçu des configurations des interfaces réseau, similaire aux informations fournies par `ifconfig`.

 # Extrait des resultats de 'netstat -rn'

Destination	Passerelle	Genmask	Indic	MSS	Fen tre	irtt	Iface
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eno1
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eno1

1.6 Résolution de Nom de Domaine avec nslookup

1.6.1 Requête DNS pour www.meteo.fr

En utilisant la commande `nslookup`, nous avons déterminé l'adresse IP associée au nom de domaine www.meteo.fr, ce qui a permis d'observer l'échange DNS qui a suivi.

```
# Resultat de la commande 'nslookup www.meteo.fr'
Non-authoritative answer:
Name:    www.meteo.fr
Address: 137.129.43.129
```

1.6.2 Analyse de la Capture DNS

Une capture DNS a été réalisée avec le filtre `udp and port 53`, mettant en évidence les ports et les protocoles utilisés durant la résolution de nom de domaine. Le port 53, standard pour le service DNS, a été utilisé pour cette communication UDP.

1.7 Correspondance IP à URL

Une autre utilisation de `nslookup` a permis de relier l'adresse IP 77.73.245.170 à l'URL correspondante, vérifiée ultérieurement avec un navigateur.

```
# Resultat de la commande 'nslookup 77.73.245.170'
Non-authoritative answer:
170.245.73.77.in-addr.arpa    name = meteoblue.com.
```

1.7.1 Suppression du Cache DNS

L'exécution de la commande `sudo resolvectl flush-caches` a permis de vider le cache DNS pour observer les adresses retournées par le serveur DNS, même après de multiples demandes.

1.8 Captures de Trafic DHCP

1.8.1 Initialisation de la Capture

Une capture de paquets a été démarrée avec un filtre spécifique aux ports utilisés par DHCP, soit les ports 67 et 68. Cela a été réalisé pour observer les échanges DHCP lors de la libération et du renouvellement de la configuration IP.

1.8.2 Libération et Renouvellement de l'Adresse IP

Les commandes `sudo dhclient -r` et `sudo dhclient` ont été utilisées pour libérer l'adresse IP actuelle de la machine et ensuite renouveler la demande d'une adresse IP auprès du serveur DHCP.

```
# Liberation de l'adresse IP
sudo dhclient -r

# Renouvellement de l'adresse IP
sudo dhclient
```

1.8.3 Analyse du Trafic DHCP

Ceci nous a montré une série de messages DHCP typiques, y compris les requêtes et les offres, ainsi que les messages de renouvellement et d'acquisition d'adresse. Ces échanges illustrent la négociation entre le client et le serveur pour obtenir une adresse IP valide et les informations de réseau associées.

Conclusion

En conclusion, ce compte rendu a mis en place le fonctionnement interne et l'importance des protocoles ARP, ICMP, TCP, DNS, et DHCP dans la gestion quotidienne des réseaux informatiques. Les expériences menées ont permis de mettre en lumière les subtilités de la communication réseau, de la résolution des adresses IP aux mécanismes de transfert de données. En particulier, la capture et l'analyse des paquets avec Wireshark et l'usage des commandes réseau ont permis de comprendre le rôle et l'efficacité de chaque protocole.