

TP Analyse de trames

L'objectif de ce TD est de mieux comprendre le fonctionnement des trames réseaux ainsi que le mécanisme de certains protocoles par l'utilisation de l'outil Wireshark. A la fin du TP, vous déposerez sur l'ENT un compte rendu de ce TP. Celui-ci pourra être rédigé à partir de n'importe quel éditeur. Comme tout rapport, vous serez évalué sur la clarté de votre compte rendu, votre capacité de synthèse et de rigueur.

La salle A214 est destinée à un usage pédagogique notamment pour des TP système et/ou réseaux, vous êtes root des machines donc attention à ce que vous faites mais pas de panique rien n'est irrémédiable, les machines sont facilement réinstallables.

login : root
mot de passe : gonfle !

1 Introduction

Pour communiquer, les machines échangent des informations sous forme de packets qui sont l'unité de données échangées sur le réseau. Il est possible d'écouter et capturer ce qui se passe quand on lance certaines requêtes sur le réseau.

Un premier outil permet d'observer le réseau, celui-ci s'appelle *tcpdump*. Par défaut *tcpdump* écoute en mode promiscuous, c'est à dire qu'il analyse les trames circulant sur le réseau même celles qui ne concernent pas la machine sur laquelle il tourne. Un deuxième outil : Wireshark est un utilitaire d'analyse de protocoles réseau (renifleur de packets) qui permet de capturer des packets sur le réseau en direct afin de les analyser, un peu plus convivial que *tcpdump* car il dispose d'une interface graphique.

Ces deux outils permettent d'établir des filtres de capture de packets de manière assez fine.

1.1 Information de configuration IP de votre ordinateur

Dans un premier temps, il est important de connaître la configuration réseau de votre ordinateur. Pour cela, vous devez ouvrir un terminal et taper :

ifconfig

Remplir les champs ci-dessous :

Adresse IP:

Adresse MAC:

Adresse IP de la passerelle:

Adresse IP du serveur DNS:

1.2 Quelques commandes pratiques, ainsi que des fichiers utiles à connaître

Penser à utiliser les pages de manuelles de linux RTFM

/etc/network/interfaces

/etc/hosts - permet de nommer symboliquement des machines

/etc/services - liste les services réseaux

ip route - permet de visualiser la table de routage d'une machine

ip n - permet de visualiser la table ARP d'une machine (équivalent à *arp*)

traceroute - permet de visualiser les routeurs rencontrés pour atteindre l'adresse indiquée

yum - pour installer un paquet sous centos/fedora

1.3 Wireshark

Démarrer Wireshark

Sélectionner une interface pour Wireshark afin de capturer des paquets.

Utiliser Interface List pour choisir l'interface associée à l'adresse IP et MAC de votre PC (voir ci-dessus)

Cliquer sur le bouton start pour commencer à capturer le trafic réseau. **Ce dernier point est à faire lors des prochaines étapes.**

2 Analyse de protocoles ICMP et ARP

Lancez Wireshark sur la machine. Sur cette même machine lancez un *ping* vers www.google.fr.

Une fois le ping terminé, arrêter la capture en cliquant sur l'icône adéquate.

Le résultat de la capture est le suivant :

L'affichage des résultats se décompose en trois parties :

1 - la liste des messages capturés avec un affichage synthétique du contenu

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Tools

Internals

Help

Filter:

▼

Expression...

Clear

Apply

No.	Source	Destination	Protocol	Length	Info
16	10.1.27.1	10.1.27.251	ICMP	74	Echo (ping) request id=
17	10.1.27.251	10.1.27.1	ICMP	74	Echo (ping) reply id=
18	10.1.27.1	139.124.1.2	DNS	82	Standard query PTR 3.27.
19	10.1.27.1	10.1.27.251	ICMP	74	Echo (ping) request id=
20	10.1.27.251	10.1.27.1	ICMP	74	Echo (ping) reply id=
21	10.1.27.1	139.124.1.2	DNS	82	Standard query PTR 3.27.
22	Cisco_76:9a:90	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/1/00:
23	10.1.27.1	10.1.27.251	ICMP	74	Echo (ping) request id=
24	10.1.27.251	10.1.27.1	ICMP	74	Echo (ping) reply id=
25	10.1.27.1	10.1.27.251	ICMP	74	Echo (ping) request id=
26	10.1.27.251	10.1.27.1	ICMP	74	Echo (ping) reply id=
27	10.1.27.1	139.124.1.2	DNS	82	Standard query PTR 3.27.

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Cisco_76:9a:90 (00:0e:38:76:9a:90), Dst: Cisco_76:9a:90 (00:0e:38:76:9a:90)

Configuration Test Protocol (loopback)

Data (40 bytes)

0000

00 0e 38 76 9a 90 00 0e 38 76 9a 90 90 00 00 00

..8v.... 8v.....

0010

01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

0020

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

0030

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

.....

FIGURE 1 – Capture Wireshark.

de chaque message.

2 - zone contenant la décomposition exacte du message actuellement sélectionné dans la liste précédente. Cette décomposition permet de visualiser les PDU de chaque couche qui s'affiche sous la forme d'une arborescence que vous pouvez développer ou réduire.

3 - zone contenant la capture affichée en hexadécimal et en ASCII.

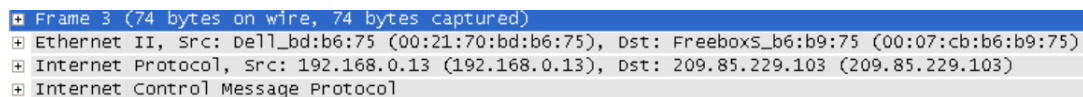
2.1 Analyse de la capture du ping

Observez la liste des messages et répondre aux questions suivantes :

Question 1. *Avez-vous capturé un échange avec le DNS dont l'adresse IP source est celle de votre machine ? Pourquoi votre ordinateur a-t-il interrogé le DNS ?*

Question 2. *En observant la colonne Info, donnez les deux types de messages ICMP que vous avez capturés ?*

Sélectionnez dans la première fenêtre un message contenant une requête **Echo ping request**. Le volet du milieu affiche des informations détaillées sur le message semblables à celles-ci



```
Frame 3 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Dell_bd:b6:75 (00:21:70:bd:b6:75), Dst: FreeboxS_b6:b9:75 (00:07:cb:b6:b9:75)
Internet Protocol, Src: 192.168.0.13 (192.168.0.13), Dst: 209.85.229.103 (209.85.229.103)
Internet Control Message Protocol
```

FIGURE 2 – Trame

Ce que vous voyez correspond à l'encapsulation des protocoles utilisés. Ici dans une trame Ethernet, il y a un paquet IP, qui lui-même contient un message ICMP. Nous pouvons schématiser cela par écrit de la sorte [Ethernet[IP[ICMP]]].

Comme vous pouvez le constater, il est possible de développer encore chaque section et protocole en cliquant sur les quatre signes "+".

Nous allons consacrer un peu de temps à l'étude de ces informations.

Dans le PDU Ethernet :

Question 3. *Retrouvez les adresses MAC "Source" et "Destination" qui ont été utilisées ?*

Question 4. *L'adresse MAC de destination correspond-elle à l'adresse MAC de la passerelle ?*

```

Frame 3 (74 bytes on wire (74 bytes captured)
Arrival Time: Sep 20, 2009 23:15:36.069395000
[Time delta from previous captured frame: 0.004696000 seconds]
[Time delta from previous displayed frame: 0.004696000 seconds]
[Time since reference or first frame: 0.039862000 seconds]
Frame Number: 3
Frame Length: 74 bytes
Capture Length: 74 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: Dell_bd:b6:75 (00:21:70:bd:b6:75), Dst: FreeboxS_b6:b9:75 (00:07:cb:b6:b9:75)
  Destination: FreeboxS_b6:b9:75 (00:07:cb:b6:b9:75)
  Source: Dell_bd:b6:75 (00:21:70:bd:b6:75)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.0.13 (192.168.0.13), Dst: 209.85.229.103 (209.85.229.103)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 60
  Identification: 0xf021 (61473)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (0x01)
  Header checksum: 0x0000 [incorrect, should be 0xd32c]
  Source: 192.168.0.13 (192.168.0.13)
  Destination: 209.85.229.103 (209.85.229.103)
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0 ()
  Checksum: 0x245c [correct]

```

FIGURE 3 – Développement d'une trame

Question 5. *Rechercher sur internet le rôle du champ **Type**.*

Question 6. *Quelle est la valeur du champ **Type** ?*

Dans le PDU Internet Protocol :

Question 7. *Retrouvez les adresses IP "Source" et "Destination" qui ont été utilisées ?*

Question 8. *L'adresse IP de destination correspond-t-elle à l'adresse IP de la passerelle ?*

Question 9. *Rechercher sur internet le rôle du champ **Protocol**.*

Question 10. *Quelle est la valeur du champ **Protocol** ?*

2.2 Analyse ARP

Effacez toutes les entrées présentes dans la table ARP à l'aide de la commande `ip n`. Et relancer une capture avec Wireshark.

Remarque : la commande ping utilise le protocole ICMP pour contacter la machine distante et le protocole ARP pour obtenir l'adresse ethernet de la machine distante.

Relancez la commande `ping -c 1 hostname` (l'option `-c 1` sert à envoyer un seul message ping, sinon par default la commande ne s'arrête pas), ou `hostname` est l'adresse IP du PC de votre voisin. Revenez sur Wireshark et stopper la capture de la trame.

Question 11. *Donnez un chronogramme montrant la sequence des messages ARP et ICMP échangés lors de l'exécution entre votre machine et celle de votre voisin et expliquez.*

Question 12. *Dans un terminal, entrez la commande `arp -a`. Qu'affiche t-elle ?*

3 Analyse du protocole DHCP

Lancez une capture de trames et depuis le terminal, taper dans un terminal la commande :

```
dhclient -r  
dhclient -d
```

Une fois la réponse obtenue, arrêtez la capture de la trame et filtrez par le protocole bootp.

Question 13. *A quoi correspond l'acronyme DHCP ?*

Question 14. *Quelle est l'adresse IP du serveur DHCP ?*

Question 15. *Donnez un chronogramme montrant la sequence des messages DHCP échangés lors de l'exécution entre votre machine et le serveur. Sachant que la première trame ne doit pas être prises en compte (le `dhclient -r` permet de liberer l'IP de la machine)*

4 Analyse du protocoles DNS

Lancez une capture de trames et depuis le terminal, taper la commande :
`nslookup www.uca.fr`

Une fois la réponse obtenue, arrêtez la capture de la trame et filtrez par le protocole dns.

Question 16. *A quoi correspond l'acronyme DNS ?*

Question 17. *Quelle est l'adresse IP du serveur DNS ?*

Question 18. *Dans la réponse DNS, retrouvez le nom du site dont l'adresse IP est 193.49.117.66 ?*

Question 19. *Quelle type de trame est échangée pour le protocole DNS ?*

5 Analyse du protocoles HTTP

Lancez une capture de trames. Ouvrez un navigateur et connectez vous sur votre ENT. Une fois que vous êtes connecté, arrêtez la capture de trame et répondez aux questions suivantes :

Question 20. *Quelle est le port du protocole https ?*

Question 21. *Existe t-il une trame dont le protocole est TLSv2 ?*

Question 22. *Donnez le sens aux acronymes SSL et TLS ?*

Question 23. *Que fait TLS ?*