



ANALYSE DE FLUX TCP/IP

TP N° 3– RESEAUX ET PROTOCOLES

LAHLOU BELABBAS
KAREN HAYOUN
FATIMA-ZAHRA LAGROU

TABLE DES MATIERES

Aucune entrée de table des matières n'a été trouvée.

1. ANALYSE DE TRAMES

PRELIMINAIRES

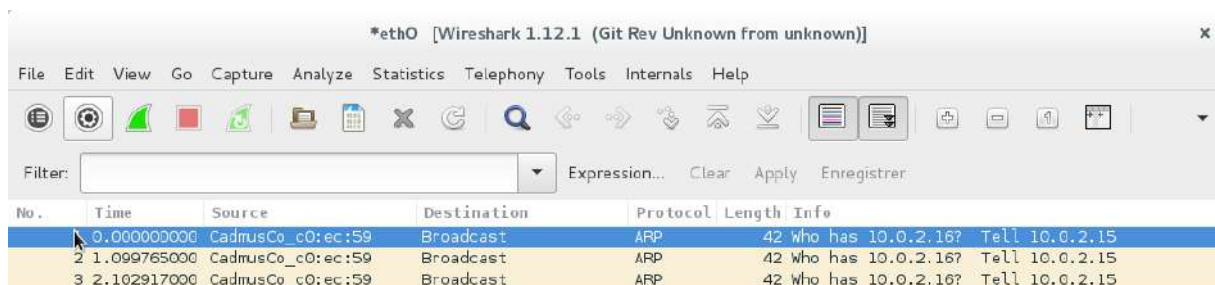
```
eth0      Link encap:Ethernet  HWaddr 08:00:27:c0:ec:59
          inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fec0:ec59/64 Scope:Lien
          I  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:2847 (2.7 KiB)  TX bytes:10272 (10.0 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:2784 (2.7 KiB)  TX bytes:2784 (2.7 KiB)

root@debian1:~#
```

CAPTURE DE TRAMES

Ping 10.0.2.16



No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000000	CadmusCo_c0:ec:59	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15
2	1.099765000	CadmusCo_c0:ec:59	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15
3	2.102917000	CadmusCo_c0:ec:59	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15

Traceroute www.cisco.com

Capturing from eth0 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
17	5.013656000	10.0.2.15	23.40.0.8	UDP	74	Source port: 46013 Destination port: 33438
18	5.013743000	10.0.2.15	23.40.0.8	UDP	74	Source port: 40691 Destination port: 33438
19	5.013880000	10.0.2.15	23.40.0.8	UDP	74	Source port: 50690 Destination port: 33440
20	5.014035000	10.0.2.15	23.40.0.8	UDP	74	Source port: 42890 Destination port: 33441
21	5.014190000	10.0.2.15	23.40.0.8	UDP	74	Source port: 54157 Destination port: 33442
22	5.014220000	10.0.2.15	23.40.0.8	UDP	74	Source port: 36866 Destination port: 33443
23	5.014309000	10.0.2.15	23.40.0.8	UDP	74	Source port: 52101 Destination port: 33444
24	5.014456000	10.0.2.15	23.40.0.8	UDP	74	Source port: 58808 Destination port: 33445
25	5.014563000	10.0.2.15	23.40.0.8	UDP	74	Source port: 56286 Destination port: 33446
26	5.014645000	10.0.2.15	23.40.0.8	UDP	74	Source port: 47902 Destination port: 33447
27	5.014734000	10.0.2.15	23.40.0.8	UDP	74	Source port: 53834 Destination port: 33448
28	5.014969000	10.0.2.15	23.40.0.8	UDP	74	Source port: 57498 Destination port: 33449
29	5.015105000	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
30	5.015111000	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
31	5.015114000	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
32	5.015477000	10.0.2.15	10.0.1.1	DNS	81	Standard query 0xa797 PTR 2.2.0.10.in-addr.
33	5.016086000	10.0.1.1	10.0.2.15	DNS	175	Standard query response 0xa797 No such name
34	5.016525000	10.0.2.15	10.0.1.1	DNS	81	Standard query 0x666f PTR 2.2.0.10.in-addr.
35	5.017085000	10.0.1.1	10.0.2.15	DNS	175	Standard query response 0x666f No such name

ANALYSE FLUX ARP ET ICMP

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames Capturées ? ARP

Quelles sont les longueurs des messages échangés par les différents protocoles ? 42

❖ Caractéristiques Ethernet :

- Que transporte la trame Ethernet ? Un message, @destination , @emeteur
- Quelle est l'adresse MAC source de la trame Ethernet ? Emetteur du message

Source: CadmusCo_3d:c9:84 (08:00:27:3d:c9:84)

- Quelle est l'adresse MAC destination trame Ethernet ? Destinataire du message

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

- Quelle est la signification de cette valeur ? Le type de message

❖ Caractéristiques ARP :

- Quelle est la taille l'en-tête ? 28 bytes

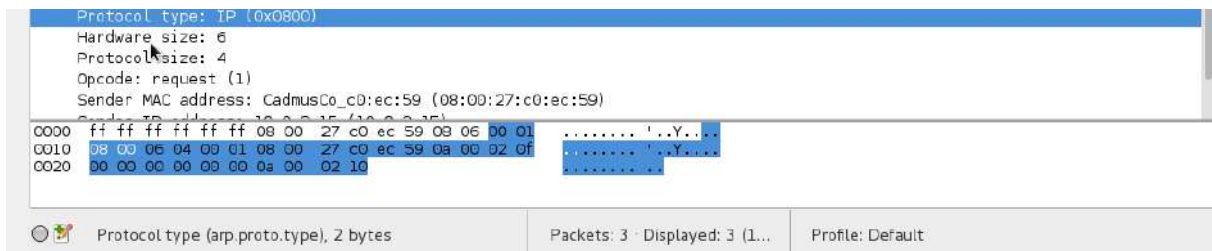
0000	ff ff ff ff ff 08 00 27 c0 ec 59 08 06 00 01	 !..Y...
0010	08 00 06 04 00 01 08 00 27 c0 ec 59 0a 00 02 0f	 !..Y...
0020	00 00 00 00 00 00 0a 00 02 10	

Address Resolution Protocol (arp), 28 bytes Packets: 3 · Displayed: 3 (1...

- Quelle la taille des données transportées ? 0 bytes

Commandes de base - Linux & Windows

- Quelle est la valeur du champ Protocol Type contenu dans le message ARP? 08 00



- Quelle est l'adresse IP Source du paquet ARP? Notre ip

Sender IP address: 10.0.3.15 (10.0.3.15)

- Quelle est l'adresse IP destination du paquet ? L'ip de destination

Target IP address: 10.0.3.2 (10.0.3.2)

- Quelle est l'adresse MAC Source incluse dans le message ARP ?

Sender MAC address: CadmusCo_3d:c9:84 (08:00:27:3d:c9:84)

- Quelle est l'adresse MAC destination incluse dans le message ARP ?

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

ÉTUDE DU PAQUET IP CORRESPONDANT au SECOND MESSAGE ARP REPLY

❖ Caractéristiques Ethernet :

- Quelle est l'adresse MAC source de la trame Ethernet ?

Source: RealtekU_12:35:02 (52:54:00:12:35:02)

- Quelle est l'adresse MAC destination trame Ethernet ?

Destination: CadmusCo_3d:c9:84 (08:00:27:3d:c9:84)

❖ Caractéristiques ARP :

- Quelle est la taille l'en-tete ? 28 bytes (en bleu)

```
08 00 27 3d c9 84 52 54 00 12 35 02 08 06 00 01
08 00 06 04 00 02 52 54 00 12 35 02 0a 00 03 02
08 00 27 3d c9 84 0a 00 03 0f 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- Quelle la taille des données transportées ? 0

```
0000 08 00 27 3d c9 84 52 54 00 12 35 02 08 06 00 01
0010 08 00 06 04 00 02 52 54 00 12 35 02 0a 00 03 02
0020 08 00 27 3d c9 84 0a 00 03 0f 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- Quelle est la valeur du champ Protocol Type contenu dans le message ARP? 08 00

Protocol type: IP (0x0800)

- Quelle est l'adresse IP Source du paquet ARP?

Sender IP address: 10.0.3.2 (10.0.3.2)

- Quelle est l'adresse IP destination du paquet ?

Target IP address: 10.0.3.15 (10.0.3.15)

- Quelle est l'adresse MAC Source incluse dans le message ARP ?

Sender MAC address: RealtekU_12:35:02 (52:54:00:12:35:02)

- Quelle est l'adresse MAC destination incluse dans le message ARP ?

Target MAC address: CadmusCo_3d:c9:84 (08:00:27:3d:c9:84)

- Quelle action effectue la station émettrice après réception du message ARP reply ?

Elle remplit la table ARP en transmettant l'adresse IP source et l'adresse MAC

ANALYSE DU MESSAGE ICMP

MESSAGE ICMP «ECHO REQUEST»

Les données en bleu

0000	52	54	00	12	35	02	08	00	27	3d	c9	84	08	00	45	00	RT..5... '=...E.
0010	00	54	5b	dd	40	00	40	01	cb	d3	0a	00	03	0f	bc	7d	.T[.@.@.}
0020	49	6c	08	00	de	9c	07	41	00	01	cf	f6	8a	56	c0	d0	I\.....A V..
0030	0c	00	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	 !"# \$%
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	&'()*+,-./012345
0060	36	37															67

- Quelle est la taille l'en-tete ? 64 bytes

49 6c 08 00 de 9c 07 41 00 01 cf f6 8a 56 c0 d0
 0c 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
 36 37

- Quelle la taille des données transportées ? 0

- Quel est le type de message ICMP ?

Internet Control Message Protocol
 Type: 8 (Echo (ping) request)

Commandes de base - Linux & Windows

Le type de données est 8 : echo request

- Quel est son identificateur ? 1857

Identifier (BE): 1857 (0x0741)

BE : big endian representation

- Quel est le numéro de séquence ? 1

Sequence number (BE): 1 (0x0001)

BE : big endian representation

- Quelle est l'adresse IP destination du paquet ?

Destination: 188.125.73.108 (188.125.73.108)

- Quelle est la valeur du champ Protocol Type ?

Protocol: ICMP (1)

- Quelle est la valeur du champ Time to Live ?

Time to live: 64

MESSAGE ICMP «ECHO REPLY»

- Quel est le type de message ICMP ?

Internet Control Message Protocol
Type: 0 (Echo (ping) reply)

Le type de données est 8 : 0 reply

- Quel est son identificateur ? 1857

Identifier (BE): 1857 (0x0741)

On constate que c'est le même identificateur.

- Quel est le numéro de séquence ? 1

Sequence number (BE): 1 (0x0001)

- Quelle est l'adresse IP destination du paquet ?

Destination: 10.0.3.15 (10.0.3.15)

- Quelle est la valeur du champ Protocol Type ?

Protocol: ICMP (1)

- Quelle est la valeur du champ Time to Live ?

Time to live: 54

Commandes de base - Linux & Windows

ÉTUDE DU MESSAGE ICMP – COMPLEMENTS

FZL

- Comparer ces données avec celles affichées dans le message de requête avec celles affichées dans le message de réponse.
- Comment les champs d'identification et numéro de séquence évoluent dans le temps ?

Les champs d'identification et les numéros de séquence n'évoluent pas dans le temps. (Cf screenshots)

Internet Control Message Protocol	Internet Control Message Protocol
Type: 8 (Echo (ping) request)	Type: 0 (Echo (ping) reply)
Code: 0	Code: 0
Checksum: 0xda9c [correct]	Checksum: 0xe69c [correct]
Identifier (BE): 1857 (0x0741)	Identifier (BE): 1857 (0x0741)
Identifier (LE): 16647 (0x4107)	Identifier (LE): 16647 (0x4107)
Sequence number (BE): 1 (0x0001)	Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)	Sequence number (LE): 256 (0x0100)
[Response frame: 6]	[Request frame: 5]
Timestamp from icmp data: Jan 4, 2016 23:48:47.839872000 CET	[Response time: 60,424 ms]
[Timestamp from icmp data (relative): 0.000025000 seconds]	Timestamp from icmp data: Jan 4, 2016 23:48:47.839872000 CET
	[Timestamp from icmp data (relative): 0.060449000 seconds]

- Est-ce que les séquences de données des requêtes et des réponses changent ?
- Calculer l'écart de temps entre l'émission de chaque message Echo Request et la réception de chaque message Echo Reply.

[Response time: 60,424 ms]	[Response frame: 6]
Timestamp from icmp data: Jan 4, 2016 23:48:47.839872000 CET	Timestamp from icmp data: Jan 4, 2016 23:48:47.839872000 CET
[Timestamp from icmp data (relative): 0.060449000 seconds]	[Timestamp from icmp data (relative): 0.000025000 seconds]

L'écart de temps entre l'émission de chaque message Echo Request et la réception du message Echo Reply est indiquée par le logiciel et indiquée en jaune sur la capture d'écran ci-dessus.

- Comparer les résultats avec les valeurs maximum, moyenne et minimum fournies par la commande ping.

ANALYSE AVEC (TCP) TRACEROUTE