

TP 5 – Trames ARP, ICMP et DNS

Table des matières :

4.1. Capture de trames ARP et ICMP.....	1
4.2 Capture de trames ARP, DNS et ICMP.....	6
4.3. Commande Tracert et capture de trames ICMP.....	11

4.1. Capture de trames ARP et ICMP.

J'ai ping le serveur aviateur (172.17.254.5) et pris une capture de trame en ayant entré la commande « arp or icmp »

The screenshot displays two windows side-by-side. The left window is Wireshark, showing a packet capture filter 'arp or icmp' and a list of captured packets. The right window is the Windows Command Prompt, showing the execution of a ping command to 172.17.254.5 and the resulting statistics.

No.	Time	Source	Destination	Protocol	Length	Info
13	2.535859	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request 1d-0x0001, seq=1/256, ttl=128 (reply
14	2.535571	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply 1d-0x0001, seq=1/256, ttl=64 (request
29	3.539235	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request 1d-0x0001, seq=2/512, ttl=128 (reply
30	3.539797	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply 1d-0x0001, seq=2/512, ttl=64 (request
32	4.542665	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request 1d-0x0001, seq=3/768, ttl=128 (reply
33	4.543228	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply 1d-0x0001, seq=3/768, ttl=64 (request
38	5.547070	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request 1d-0x0001, seq=4/1024, ttl=128 (reply
39	5.547886	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply 1d-0x0001, seq=4/1024, ttl=64 (request
42	7.134314	Giga-Byt_2f:9d:13	Synology_32:137:85	ARP	42	Who has 172.17.254.5? Tell 172.17.2.13
43	7.134976	Synology_32:137:85	Giga-Byt_2f:9d:13	ARP	60	172.17.254.5 is at 00:11:32:13:2:13:85

```
C:\Users\Mvovello>ping 172.17.254.5

Envoi d'une requête 'Ping' 172.17.254.5 avec 32 octets de données :
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.17.254.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Mvovello>
```


- Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ?

EtherType = 0x0806 (ARP)

- Quelle est la fonction de la trame ARP Request ?

Elle demande qui possède l'adresse IP 172.17.244.2 afin d'obtenir l'adresse MAC correspondante

- Quelle signification ont les octets de position 0x04 et 0x05 ligne 0010 ?

les octets de position 0x04 et 0x05 ligne 0010 correspondent aux octets 00 01 ce qui signifie que le hardware type est Ethernet 1

- Quelle est la longueur d'un message ARP contenu dans la trame ?

La longueur d'un message ARP est de 28 octets

- Quelle est la longueur de la trame ARP Request ?

La longueur de la trame ARP request est de 60 octets

- Quelle est la longueur de la trame ARP Reply ?

La longueur de la trame ARP Reply est de 60 octets

- Combien d'octets sont utilisés pour le padding ?

Il y a 18 octets qui sont utilisés pour le padding

- @MAC destination = ff:ff:ff:ff:ff:ff

- @MAC source = 00:0c:29:76:e3:f7

- Ethernet Type = 0806

- Opcode (valeurs hexa.) = 00 01

- @MAC de la cible = 00:00:00:00:00:00

- @IP de la cible = 172.17.244.2

▪ Quelle signification a l'octet de position 0x02 ligne 00020 ?

La signification est que l'octet correspond au champ code =0 (code du message) et type =8 (Protocole ICMP Echo request)

▪ A quoi correspondent les octets à partir de l'octet 0x0A, ligne 00020 ?

Ce sont les octets ASCII ou l'on trouve toutes les données du message ICMP

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0x02 ligne 00020 ?

Sa valeur est 0x00 ce qui signifie que le champ ICMP type = 0 et le champ code = 0

4.2 Capture de trames ARP, DNS et ICMP.

J'ai réalisé un ping vers le serveur www.ac-nice.fr

The screenshot shows a Windows command prompt window with the following text:

```
if_addr Spécifie l'adresse Internet de l'interface dont la table de traduction d'adresses doit être modifiée. Si ce paramètre n'est pas indiqué, la première interface applicable sera utilisée. Exemples : > arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Ajoute une entrée statique. > arp -a .... Affiche la table ARP. C:\Users\Mnovello>ping www.ac-nice.fr Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.105] avec 32 octets de données : Réponse de 141.101.90.105 : octets=32 temps=19 ms TTL=53 Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53 Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53 Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53 Statistiques Ping pour 141.101.90.105: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 16ms, Maximum = 19ms, Moyenne = 16ms C:\Users\Mnovello>
```

The screenshot also shows a Wireshark network traffic capture window. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
352	20.690190	Giga-Byt_2f9c:cd	Broadcast	ARP	60	Who has 172.17.5.6? Tell 172.17.2.5
359	21.691470	Giga-Byt_2f9c:cd	Broadcast	ARP	60	Who has 172.17.5.6? Tell 172.17.2.5
360	21.691470	Giga-Byt_2f9c:cd	Broadcast	ARP	60	Who has 172.17.5.6? Tell 172.17.2.5
368	23.079530	172.17.2.13	172.17.254.1	DNS	74	Standard query 0x7292 A www.ac-nice.fr
369	23.104153	172.17.2.13	172.17.254.1	DNS	74	Standard query 0x7292 A www.ac-nice.fr
370	23.124236	172.17.254.1	172.17.2.13	DNS	185	Standard query response 0x7292 A www.ac-nice.fr CNAME www.ac-nice.fr.cdn.cloudflare.net A 141.101.90.105 A 141.101.90.104 A 141.101.90.107 A 141.101.90.106
371	23.129648	172.17.2.13	141.101.90.105	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=53 (reply in 374)
374	23.149242	141.101.90.105	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=53 (request in 371)
379	24.148897	172.17.2.13	141.101.90.105	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 381)

The packet details pane for packet 368 shows the following information:

```
Frame 368: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C8760449-A077-4055-908B-1D545} Ethernet II, Src: Giga-Byt_2f9d:13 (74:56:3c:2f:9d:13), Dst: Dell_7d:8e:2b (d4:ae:52:7d:8e:2b) Internet Protocol Version 4, Src: 172.17.2.13, Dst: 172.17.254.1 User Datagram Protocol, Src Port: 50604, Dst Port: 53 Domain Name System (query)
```

▪ La liste des trames commence par une requête et une réponse ARP. Quelle est la machine dont l'adresse MAC est recherchée ?

La machine dont l'adresse MAC est recherché est la machine 172.17.5.65

▪ Complétez les rubriques ci-dessous : Trame ARP request

@MAC destination = ff:ff:ff:ff:ff:ff

@MAC source = 74 56 3c 2f 9c cd

Ethernet Type = 08 06

Opcode (valeurs hexa.) = 00 01

@MAC de la cible = 00:00:00:00:00:00

@IP de la cible = 172.17.5.65

- Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?

Parce que avant d'envoyer les trames ICMP pour ping la machine doit d'abord savoir vers quelle adresse IP l'envoyer et c'est le rôle du DNS

- Consultez le cache DNS à l'aide de la commande ipconfig /displaydns et vérifiez la présence de l'enregistrement DNS ac-nice.fr et de l'adresse IP associée :

```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 441011
Longueur de données . : 8
Section . . . . . : Réponse
Enregistrement CNAME : www.ac-nice.fr.cdn.cloudflare.net

Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie . . . . : 441011
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105
```

J'ai bien la présence de l'enregistrement DNS ac-nicfe.fr avec l'adresse IP associé qui est 141.101.90.105

J'ai effectué une deuxième capture de trame en ayant pin www.ac-nice.fr et je ne constate pas de trame DNS affiché :

The screenshot shows the Wireshark interface with a packet list table. The table contains the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
11	4.036196	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
12	4.564332	Whare_22:87:6d	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.243.11
17	4.847688	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
21	5.486178	Whare_22:87:6d	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.243.11
22	5.847790	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
23	6.486352	Whare_22:87:6d	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.243.11
24	7.058814	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
27	7.496797	172.17.2.13	141.181.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 28)
28	7.512714	141.181.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=53 (request in 27)
29	7.847404	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
32	8.507790	172.17.2.13	141.181.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=14/3384, ttl=128 (reply in 33)
33	8.524861	141.181.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3384, ttl=53 (request in 32)
35	8.847457	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
37	9.514719	172.17.2.13	141.181.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 38)
38	9.538398	141.181.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=53 (request in 37)
43	18.923838	172.17.2.13	141.181.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=16/4896, ttl=128 (reply in 44)
44	18.539385	141.181.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4896, ttl=53 (request in 43)
51	13.066826	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
53	13.047828	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
56	14.847627	Dell_7d70e2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1

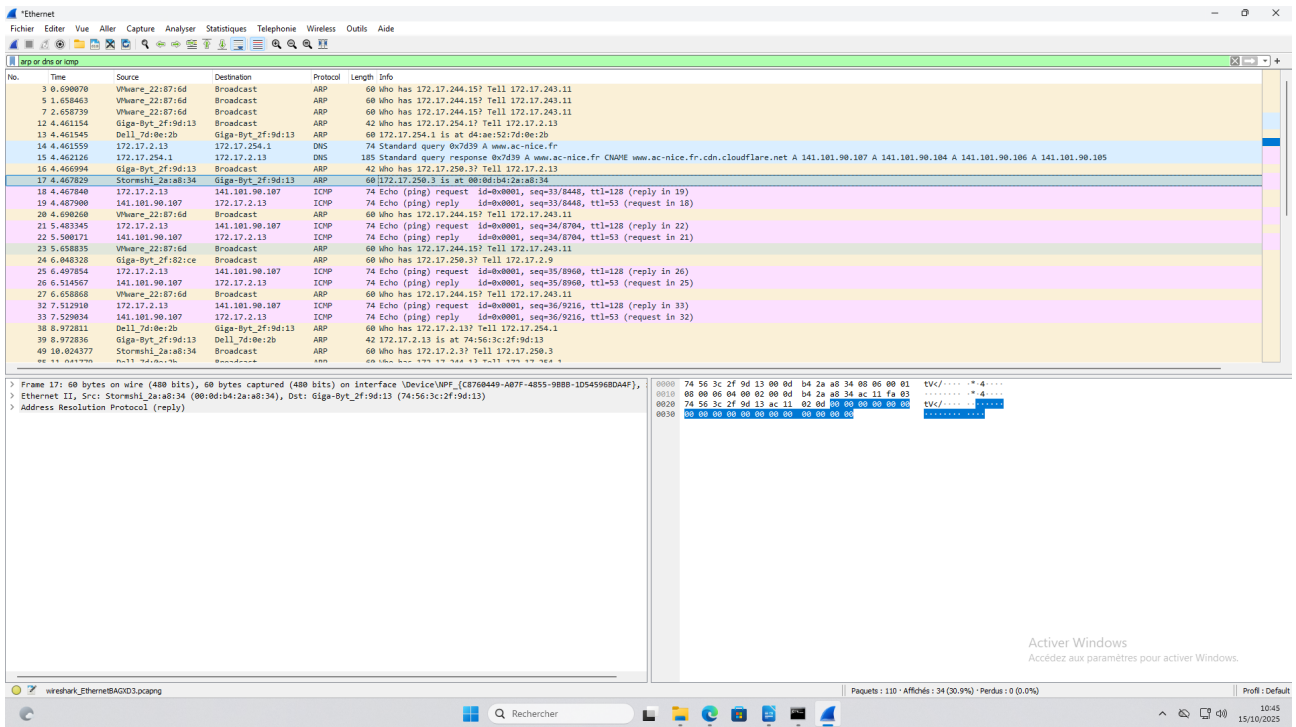
The packet details pane for frame 11 shows:

```
> Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on Interface \Device\NPF_{C870449-407F-4855-9088-1D54596804F},  
> Ethernet II, Src: Dell_7d70e2b (d8:ae:52:7d:0e:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)
```

The packet bytes pane shows the raw data of the ARP request:

```
0000 ff ff ff ff ff ff 84 ae 52 7d 0e 2b 08 06 00 01 ..... R] .....  
0010 08 00 06 04 00 01 04 ae 52 7d 0e 2b ac 11 fe 01 ..... R] .....  
0020 00 00 00 00 00 ac 11 fe 01 00 00 00 00 00 00 .....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

J'ai visualiser de nouveau une requête DNS :



▪ Quels sont les différents protocoles encapsulés dans une trame DNS ?

Liaison = Ethernet II

Réseau = IPv4

Transport = UDP

Application = DNS

▪ Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (cf. en-tête IP) ?

La machine destinataire dans la requête DNS est la mienne, son IP est donc : 172.17.254.1

▪ Quelle signification ont les octets de position 0x0C, 0x0D ligne 0000 et 0x07 ligne 0010 ?

EtherType = 0x0800 (08 00) ce qui signifie que la trame transporte un paquet IPv4

Champ TTL = 0x07 (40) signifie que le paquet peut traversé 64 routeurs avant d'être supprimé

▪ Quelle est l'EtherType = 0x0800 a longueur de l'en-tête IP ?

Longueur de l'en tête IP est de 20 octets

▪ Quelle est la longueur de l'en-tête de transport dans cette trame ?

La longueur de l'en tête de transport est de 8 octets

▪ Quelle signification ont les octets de position 0x04 et 0x05 ligne 0020 ?

Les octets de position 0x04 et 0x05 ligne 0020 signifie que le port de destination est DNS (53)

▪ Développez la section Domain Name System (query) et plus précisément la rubrique Queries. Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac nice.fr ?

61 63 2d 6e 69 63 65 = ac nice

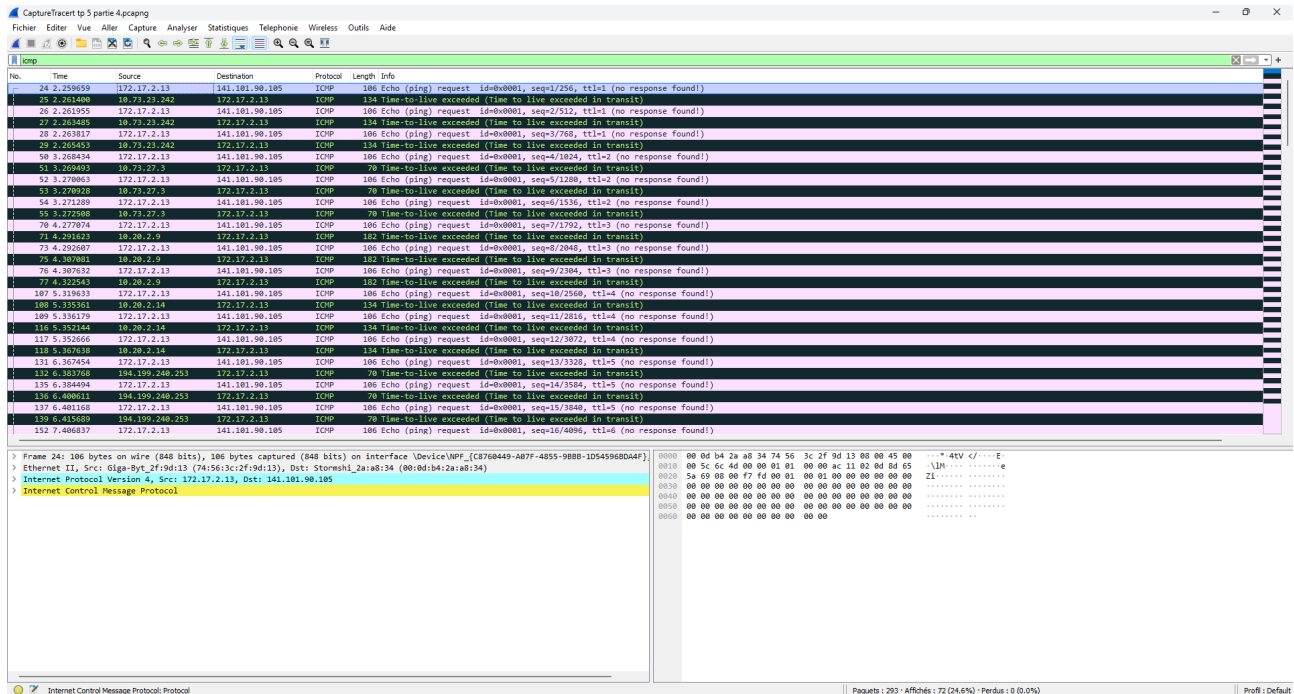
66 72 = fr

▪ Sélectionnez la trame comportant la réponse à la requête DNS et développez la section Domain Name System (response) et plus particulièrement la rubrique Answers. Recherchez les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice.

Adresse IP du serveur = 141.101.90.105 = 8D 65 5A 69

4.3. Commande Tracert et capture de trames ICMP.

J'ai effectué une capture de trame en saisissant la commande tracert www.ac-nice.fr. depuis l'invite de commande :



The screenshot shows a Wireshark capture of ICMP Echo (ping) requests. The packet list pane displays the following information for the selected packet (No. 24):

No.	Time	Source	Destination	Protocol	Length	Info
24	2.259659	172.17.2.13	141.101.90.105	ICMP	106	Echo (ping) request id=0x0001, seq=1/256, ttl=1 (no response found)

The packet details pane shows the following structure:

- Ethernet II, Src: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13), Dst: Storshl_2a:a8:34 (00:0d:b4:2a:a8:34)
- Internet Protocol Version 4, Src: 172.17.2.13, Dst: 141.101.90.105
- Internet Control Message Protocol

▪ Sélectionnez la première trame ICMP Echo request. Développez l'en-tête IP. Quelle est l'adresse IP Destination (valeurs déci. et hexa.) ?

L'adresse IP destination est 141.101.90.105 =

▪ Sélectionnez le champ TTL. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ?

La valeur portée par ce champ est 01 =

▪ Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

La valeur portée par le champ Type est 08 =

▪ Sélectionnez la trame, comportant un message d'erreur ICMP Time-to-live exceeded, envoyée par le premier routeur rencontré. Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

La valeur portée par le champ TTL dans la trame ICMP Time-to-live exceeded est de 11 = 0b en héra