Dersim Besiktas
TP 5 – Trames ARP, ICMP et DNS

SOMMAIRE :

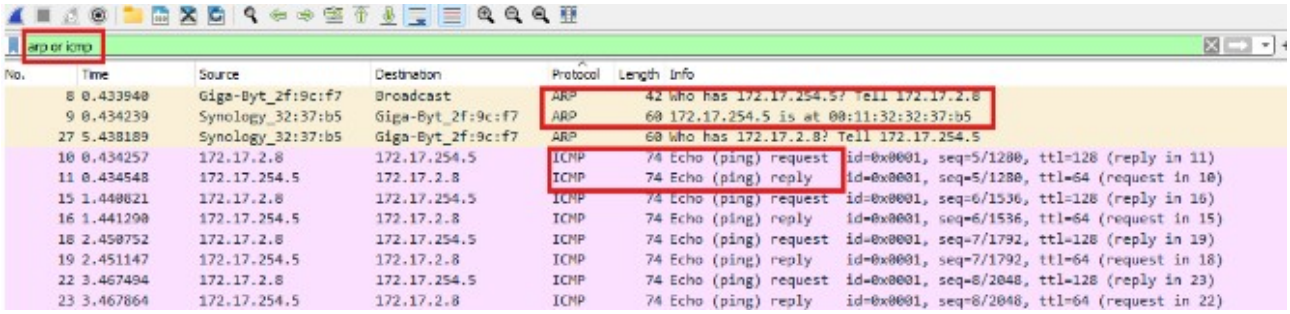
4.1. Capture de trames ARP et ICMP

Je saisie la commande ping sur le cmd et en même temps je lance une capture de trame depuis WireShark

```
C:\Windows\System32>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 = 0ms, Moyenne = 0ms
```



Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

→ Ces octets correspondent au champ **EtherType**, ici la valeur **0x0806**, qui indique qu'il s'agit d'une **trame ARP** (Address Resolution Protocol).

Quelle est la fonction de la trame ARP Request ?

→ La trame **ARP Request** sert à **demander l'adresse MAC associée à une adresse IP**.

Elle est diffusée en **broadcast** (destination FF:FF:FF:FF:FF:FF) à tous les équipements du réseau local.

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?
→ Ces octets contiennent le **champ Opcode**.

- Valeur **0x0001 → ARP Request**
- Valeur **0x0002 → ARP Reply**

Quelle est la longueur d'un message ARP contenu dans la trame ?
→ 28 octets

Quelle est la longueur de la trame ARP Request ?
→ 42 octets

Quelle est la longueur de la trame ARP Reply ?
→ 60 octets

Combien d'octets sont utilisés pour le padding ?
→ 18 octets (le padding complète la trame Ethernet jusqu'à la taille minimale de 60 octets).

Champ	Valeur typique	Signification
@MAC destination	FF:FF:FF:FF:FF:FF	Diffusion sur le réseau local (broadcast)
@MAC source	ex. 08:00:27:AB:CD:EF	Adresse MAC de la machine émettrice
Ethernet Type	0x0806	Indique le protocole ARP
Opcode (val. hexa)	0x0001	Requête ARP
@MAC de la cible	00:00:00:00:00:00	Inconnue au moment de la requête
@IP de la cible	172.17.2.14	Adresse IP du voisin à découvrir

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

→ Ce champ correspond à **EtherType = 0x0800**, indiquant que la trame transporte un **paquet IPv4**.

Quelle signification a l'octet de position 0×07 ligne 0010 ?
→ C'est le **champ TTL** du paquet IP, qui définit le **nombre maximal de sauts** autorisés avant que le paquet soit détruit (valeur typique : 128).

Quelle est la longueur de la trame ?
→ 74 **octets**

Quelle est la longueur du paquet IP ?
→ 60 octets

Quelle est la longueur du message ICMP ?
→ 40 octets

Quelle signification a l'octet de position 0×02 ligne 00020 ?
→ Cet octet correspond au **type de message ICMP** :

- **8** → ICMP Echo Request (demande)

À quoi correspondent les octets à partir de l'octet 0×0A ligne 00020 ?
→ Ce sont les **données du message ICMP**, souvent un **texte ou motif répétitif** utilisé pour tester la communication.

Quel est le nom et la valeur de l'octet de position 0×02 ligne 0020 ?
→ **Champ Type = 0x00 (décimal 0)** → correspond à une **réponse ICMP Echo Re**, indiquant que la machine distante a bien reçu et répondu au ping

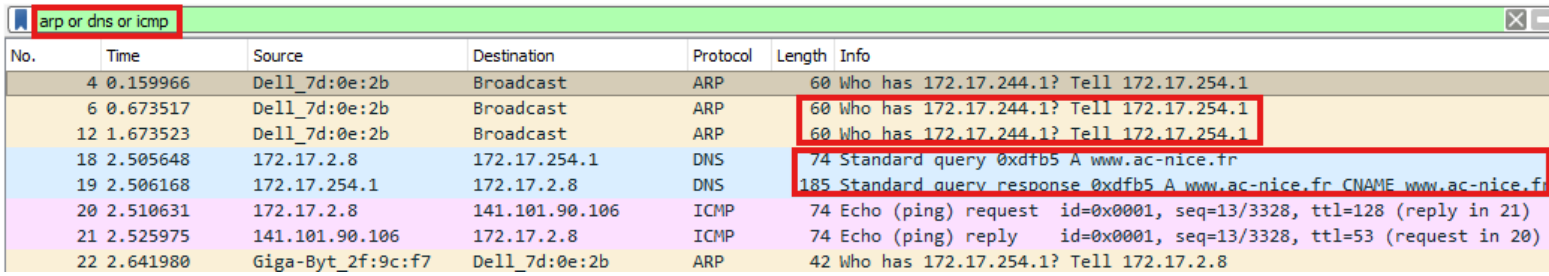
4.2. Capture de trames ARP, DNS et ICMP

Je ping le site www.ac-nice.fr et en même temps je lance une capture de trame

```
C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.104] avec 32 octets de données :
Réponse de 141.101.90.104 : octets=32 temps=14 ms TTL=55
Réponse de 141.101.90.104 : octets=32 temps=9 ms TTL=55
Réponse de 141.101.90.104 : octets=32 temps=12 ms TTL=55
Réponse de 141.101.90.104 : octets=32 temps=14 ms TTL=55

Statistiques Ping pour 141.101.90.104:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 14ms, Moyenne = 12ms
```



arp or dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.159966	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
6	0.673517	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
12	1.673523	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
18	2.505648	172.17.2.8	172.17.254.1	DNS	74	Standard query 0xdfb5 A www.ac-nice.fr
19	2.506168	172.17.254.1	172.17.2.8	DNS	185	Standard query response 0xdfb5 A www.ac-nice.fr CNAME www.ac-nice.fr
20	2.510631	172.17.2.8	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 21)
21	2.525975	141.101.90.106	172.17.2.8	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=53 (request in 20)
22	2.641980	Giga-Byt_2f:9c:f7	Dell_7d:0e:2b	ARP	42	Who has 172.17.254.1? Tell 172.17.2.8

Champ	Valeur typique	Signification
@MAC destination	FF:FF:FF:FF:FF:FF	Diffusion sur tout le réseau local (broadcast)
@MAC source	74:d0:2b:de:2b:ec	Adresse MAC de la machine émettrice (le client)
Ethernet Type	0x0806	Indique une trame de type ARP
Opcode (valeurs hexa.)	0x0001	Requête ARP (ARP Request)
@MAC de la cible	00:00:00:00:00:00	Inconnue
@IP de la cible	172.17.254.1	Adresse IP recherchée

Pourquoi trouve-t-on ensuite une requête DNS avant l'échange ICMP ?

→ Avant de pouvoir envoyer les trames ICMP (ping), le poste doit d'abord traduire le nom de domaine saisi (`ac-nice.fr`) en adresse IP.

Cette traduction est réalisée par une requête DNS (Domain Name System).
Le client interroge donc son serveur DNS pour obtenir l’adresse IP du domaine avant de pouvoir lancer la commande ping

Consultation du cache DNS

La commande :

`ipconfig /displaydns`

Elle permet d’afficher le cache DNS local, c’est-à-dire la liste des noms de domaines récemment résolus.

On y retrouve un enregistrement pour :

- **Nom : `ac-nice.fr`**
- **Adresse IP associée : 141.101.90.104**

➡ Cela confirme que la résolution DNS a bien eu lieu avant le ping, et que la correspondance nom ↔ adresse IP est mémorisée dans le cache DNS.

Quels sont les différents protocoles encapsulés dans une trame DNS ?

→ Une trame DNS contient plusieurs niveaux d’encapsulation :
Ethernet → IPv4 → UDP → DNS
Chaque couche ajoute son propre en-tête pour assurer la transmission des données jusqu’à l’application DNS.

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

→ La machine destinataire est le serveur web
C’est ce serveur qui reçoit et traite la requête DNS du client.

Son adresse IP est 172.17.254..1

Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?

→ Les octets 0x0C et 0x0D correspondent au champ EtherType = 0x0800, indiquant un paquet IPv4.
→ L’octet 0x07 à la ligne 0010 correspond au champ TTL (Time To Live) du paquet IP, qui définit le nombre maximal de routeurs que le paquet peut traverser avant de s’arrêter

Quelle est la longueur de l’en-tête IP ?

→ La longueur de l’en-tête IP est de 20 octets (IHL = 5, donc 5 × 4 = 20).

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

→ La longueur de l’en-tête UDP est de 8 octets.

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

→ Ces octets correspondent au champ “Length” de l’en-tête UDP.

Ils indiquent la taille totale du segment UDP, en incluant l’en-tête (8 octets) et les données DNS.

Quelles sont les valeurs hexadécimales des octets **correspondant au nom de domaine internet ac-nice.fr ?**

→ Les octets correspondant au nom de domaine sont :

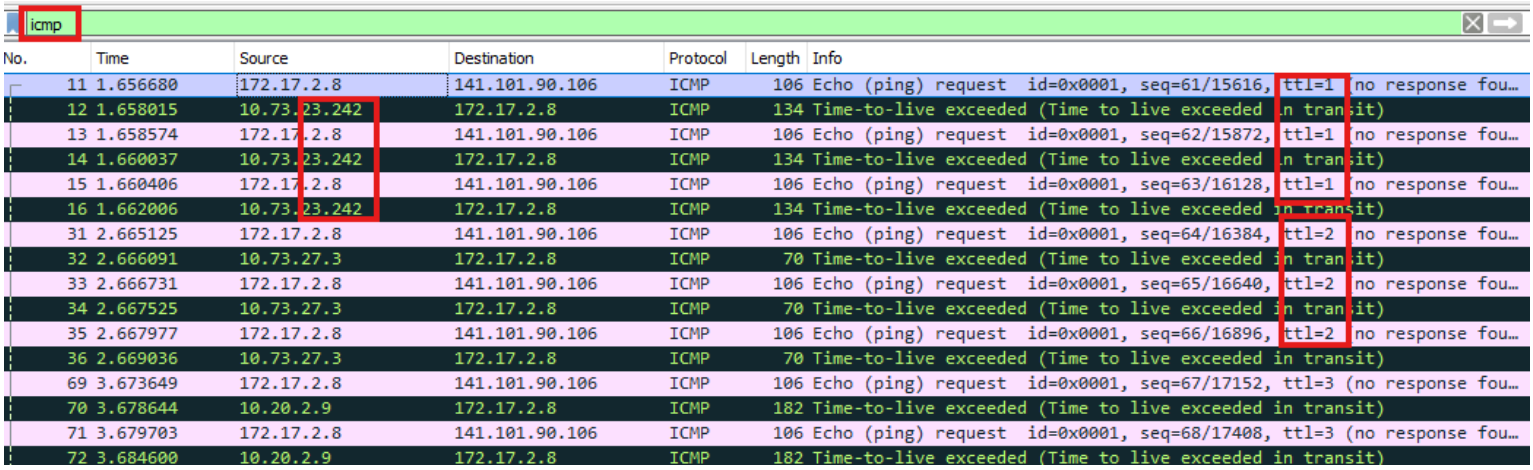
```
61 63 05 6E 69 63 65 02 66 72
```

Recherchez les valeurs hexadécimales et décimales de l’adresse IP du serveur web hébergeant le site de l’académie de Nice.

- Hexadécimal : `C2 C7 14 0A`
- Décimal : `194.199.20.10`

4.3. Commande Tracert et capture de trames ICMP

Depuis l'invite de commande j'éxecute la commande **tracert www.ac-nice.fr** et en même temps je lance une capture depuis WireShark



No.	Time	Source	Destination	Protocol	Length	Info
11	1.656680	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=1 (no response fou…
12	1.658015	10.73.23.242	172.17.2.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	1.658574	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=1 (no response fou…
14	1.660037	10.73.23.242	172.17.2.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
15	1.660406	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=1 (no response fou…
16	1.662006	10.73.23.242	172.17.2.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
31	2.665125	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=2 (no response fou…
32	2.666091	10.73.27.3	172.17.2.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
33	2.666731	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=2 (no response fou…
34	2.667525	10.73.27.3	172.17.2.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
35	2.667977	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=2 (no response fou…
36	2.669036	10.73.27.3	172.17.2.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69	3.673649	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=3 (no response fou…
70	3.678644	10.20.2.9	172.17.2.8	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
71	3.679703	172.17.2.8	141.101.90.106	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=3 (no response fou…
72	3.684600	10.20.2.9	172.17.2.8	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

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 est 141.101.90.106

Valeur hexadécimale 8D 65 5A 6A

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

Valeur décimale: 1

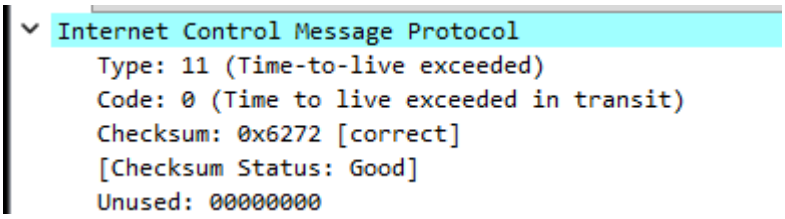
Valeur hexadécimale: 0x01

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

Valeur décimale: 8

Valeur hexadécimale: 0x08

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.) ?



Le message ICMP est 11 ce qui indique le message d'erreur Time to live exceeded

La valeur hexadécimale est 0x0B