

TP 5 – Trames ARP, ICMP et DNS

Sommaire

4.1. Capture de trames ARP et ICMP.....	1
4.2. Capture de trames ARP, DNS et ICMP.....	4
4.3. Commande Tracert et capture de trames ICMP.....	10

4.1. Capture de trames ARP et ICMP.

The image shows a Windows command prompt window and a Wireshark network traffic capture window. The command prompt shows the execution of a ping command to 172.17.254.5, which fails initially but succeeds on the second attempt. The Wireshark window shows the captured traffic, including ARP requests and ICMP Echo (ping) requests and replies.

Command Prompt Output:

```
Microsoft Windows [version 10.0.22631.5039]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\hsouri>ping (172.17.254.5)
La requête Ping n'a pas pu trouver l'hôte (172.17.254.5. Vérifiez le nom et essayez à nouveau.

C:\Users\hsouri>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=1 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=1 ms 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\hsouri>
```

Wireshark Capture:

No.	Time	Source	Destination	Protocol	Length	Info
3	0.153217	VMware_76:e3:f7	Broadcast	ARP	60	Who has 172.17.250.2? Tell 172.17.244.1
27	1.689447	GigaByteTech_2f:9c:...	Broadcast	ARP	42	Who has 172.17.254.5? Tell 172.17.2.12
28	1.689856	Synology_32:37:b5	GigaByteTech_2f:9c:...	ARP	60	172.17.254.5 is at 00:11:32:32:37:b5
29	1.689867	172.17.2.12	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128
30	1.690384	172.17.254.5	172.17.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64
31	2.694613	172.17.2.12	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
32	2.695067	172.17.254.5	172.17.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64
46	3.044283	VMware_76:e3:f7	Broadcast	ARP	60	Who has 172.17.250.2? Tell 172.17.244.1
53	3.653758	VMware_76:e3:f7	Broadcast	ARP	60	Who has 172.17.250.2? Tell 172.17.244.1

Packet 28 Details:

- Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
- Ethernet II, Src: Synology_32:37:b5 (00:11:32:32:37:b5), Dst: GigabitEthernet 0 (00:00:00:00:00:00)
- Address Resolution Protocol (reply)

Packet 28 Hex:

```
0000 74 56 3c 2f 9c c6 00 11 32 32 37 b5 08 06 00 01  tv</...
0010 08 00 06 04 00 02 00 11 32 32 37 b5 ac 11 fe 05  .....
0020 74 56 3c 2f 9c c6 ac 11 02 0c 00 00 00 00 00 00  tv</...
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```


TP 5 – Trames ARP, ICMP et DNS

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

C'est le champ EtherType = 0x0806, ce qui signifie ARP.

Quelle est la fonction de la trame ARP Request ?

C'est une requête pour trouver l'adresse client elle demande :(who has «IP cible»?) et(tell «IP source») pour découvrir l'adresse MAC associée a l'adresse IP

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

Ces les octets 0x 00 01 c'est l'Opcode=0x00 01 donc une ARP Request

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

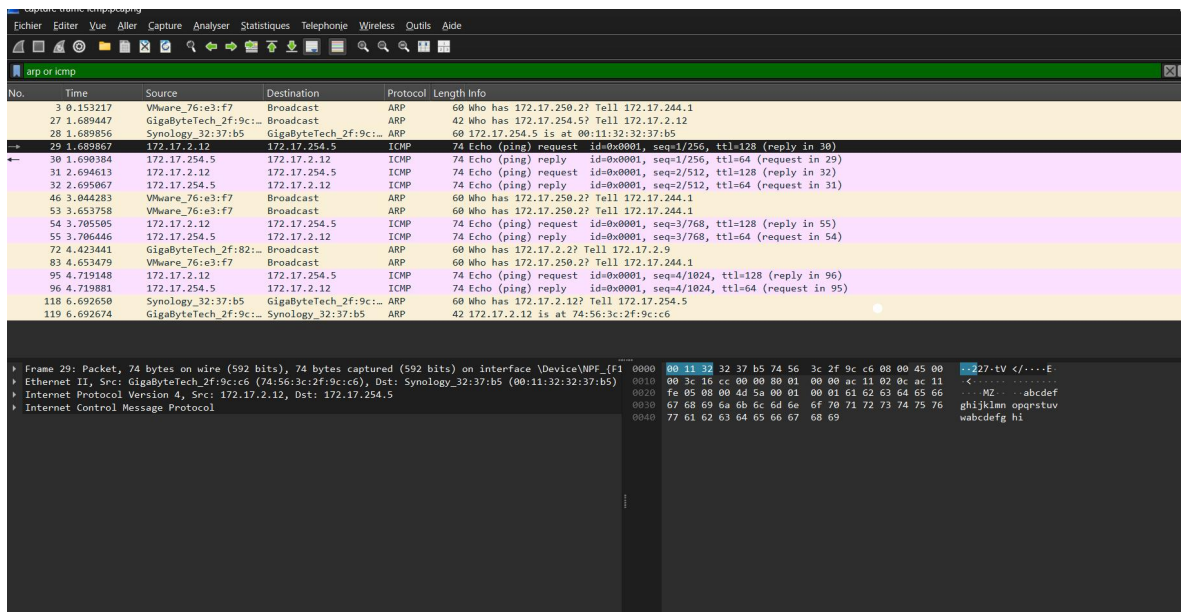
Quelle est la longueur de la trame ARP Request ? 60 octets

Quelle est la longueur de la trame ARP Reply ? 42 octets

Combien d'octets sont utilisés pour le padding ? 18 octets

Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = ff:ff:ff:ff:ff:ff @MAC source = 00:0c:29:76:e3:f7 Ethernet Type = 0x0806
Opcode (valeurs hexa.) =0x0001 @MAC de la cible = 00:00:00:00:00:00 @IP de la cible = 172.17.250.2



TP 5 – Trames ARP, ICMP et DNS

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?
C'est le champ Ethertype =0x0800 ce qui signifie IPv4

Quelle signification a l'octet de position 0×07 ligne 0010 ?
C'est le 2eme octet de l'adresse MAC source ,
0x56 (6 octets source = 74:56:3c:2f:9c:c6).

Quelle est la longueur de la trame ? 74 octets (74 bytes on wire)

Quelle est la longueur du paquet IP ? 60 octets

Quelle est la longueur du message ICMP ? 40 octets (60 – 20 octets d'en-tête IP = 40).

Quelle signification a l'octet de position 0×02 ligne 00020 ?
C'est une trame de type ICMP echo request

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

Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0×02 ligne 00020 ?

C'est un octet de position de type (ICMP) et l'octet 0x03 signifie que c'est une trame ICMP type 0 = echo reply

4.2. Capture de trames ARP, DNS et ICMP

TP 5 – Trames ARP, ICMP et DNS

The screenshot shows two windows. On the left is Wireshark, displaying a packet capture of network traffic. The top pane shows a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of a selected packet (No. 37), including Ethernet II, Internet Control Message Protocol (request), and Address Resolution Protocol (request). A callout box points to the ARP request packet with the text "Capture de trame réaliser en cour".

On the right is a Windows Command Prompt window. It shows the execution of the following commands and their outputs:

```
C:\Users\haike>arp -d *
La suppression de l'entrée ARP a échoué : L'opération demandée nécessite une élévation.

C:\Users\haike>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [2a06:98c1:3200::90:82] avec 32 octets de données :
Réponse de 2a06:98c1:3200::90:82 : temps=12 ms
Réponse de 2a06:98c1:3200::90:82 : temps=12 ms
Réponse de 2a06:98c1:3200::90:82 : temps=11 ms
Réponse de 2a06:98c1:3200::90:82 : temps=10 ms

Statistiques Ping pour 2a06:98c1:3200::90:82 :
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 10ms, Maximum = 12ms, Moyenne = 11ms

C:\Users\haike>
```

A callout box points to the Command Prompt with the text "Commande réaliser chez moi".

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 rechercher est 172.17.254.1

Trame ARP request
@MAC destination = ff:ff:ff:ff:ff:ff @MAC source = 74:56:3c:2f:7f:bf Ethernet Type =0x0806 (arp)
Opcode (valeurs hexa.) = 0000 (request) @MAC de la cible = 00:00:00:00:00:00 @IP de la cible = 172.17.254.1

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 ?

TP 5 – Trames ARP, ICMP et DNS

Avant d'envoyer les trames ICMP la machine doit savoir vers quel adresse IP l'envoyer, c'est le DNS qui s'en occupe

- 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 :

J'ai effectué la commande :

```
C:\Users\haike>ipconfig /displaydns
```

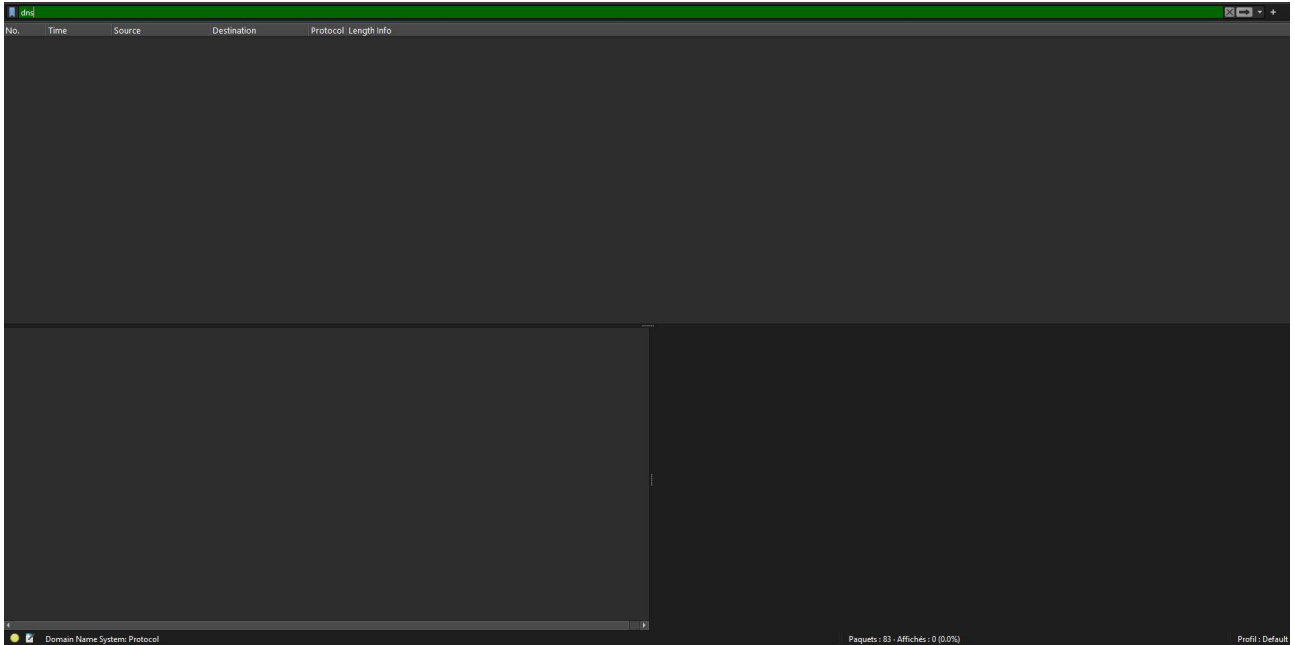
Et je cherche la présence de l'enregistrement DNS

```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 87273
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 . . . . : 87273
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.107
```

Je démarre une nouvelle capture et je ressaisie la commande ping www.ac-nice.fr

TP 5 – Trames ARP, ICMP et DNS



Je constate qu'il n'y a pas de DNS

Je vide donc le cache DNS et je recommence

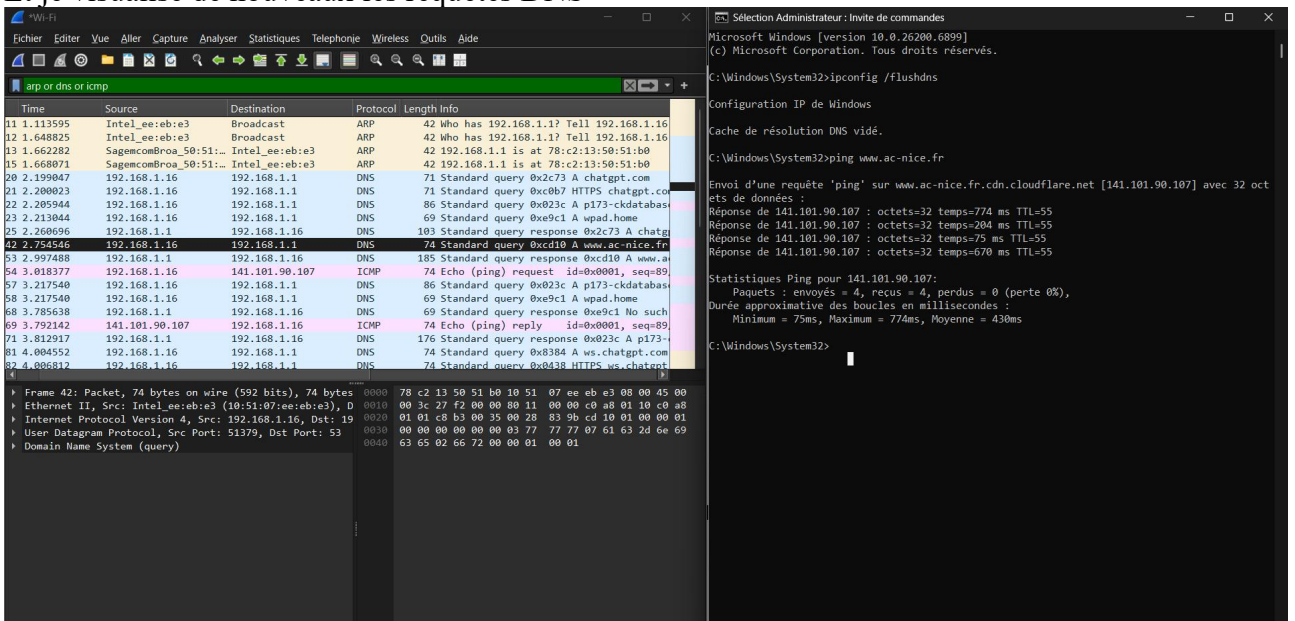
```
C:\Windows\System32>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Windows\System32>
```

Et je visualise de nouveaux les requêtes DNS



TP 5 – Trames ARP, ICMP et DNS

Time	Source	Destination	Protocol	Length	Info
11	1.113595	Intel_ee:eb:e3	Broadcast	ARP	42 Who has 192.168.1.1? Tell 19
12	1.648825	Intel_ee:eb:e3	Broadcast	ARP	42 Who has 192.168.1.1? Tell 19
13	1.662282	SagemcomBroa_50:51:...	Intel_ee:eb:e3	ARP	42 192.168.1.1 is at 78:c2:13:5
15	1.668071	SagemcomBroa_50:51:...	Intel_ee:eb:e3	ARP	42 192.168.1.1 is at 78:c2:13:5
20	2.199047	192.168.1.16	192.168.1.1	DNS	71 Standard query 0x2c73 A chat
21	2.200023	192.168.1.16	192.168.1.1	DNS	71 Standard query 0xc0b7 HTTPS
22	2.205944	192.168.1.16	192.168.1.1	DNS	86 Standard query 0x023c A p173
23	2.213044	192.168.1.16	192.168.1.1	DNS	69 Standard query 0xe9c1 A wpad
25	2.260696	192.168.1.1	192.168.1.16	DNS	103 Standard query response 0x2c
42	2.754546	192.168.1.16	192.168.1.1	DNS	74 Standard query 0xcd10 A www.
53	2.997488	192.168.1.1	192.168.1.16	DNS	185 Standard query response 0xcd
54	3.018377	192.168.1.16	141.101.90.107	ICMP	74 Echo (ping) request id=0x00
57	3.217540	192.168.1.16	192.168.1.1	DNS	86 Standard query 0x023c A p173
58	3.217540	192.168.1.16	192.168.1.1	DNS	69 Standard query 0xe9c1 A wpad
68	3.785638	192.168.1.1	192.168.1.16	DNS	69 Standard query response 0xe9
69	3.792142	141.101.90.107	192.168.1.16	ICMP	74 Echo (ping) reply id=0x00
71	3.812917	192.168.1.1	192.168.1.16	DNS	176 Standard query response 0x02
81	4.004552	192.168.1.16	192.168.1.1	DNS	74 Standard query 0x8384 A ws.c
82	4.006812	192.168.1.16	192.168.1.1	DNS	74 Standard query 0x0438 HTTPS

```

▶ Frame 42: Packet, 74 bytes on wire (592 bits), 74
▶ Ethernet II, Src: Intel_ee:eb:e3 (10:51:07:ee:eb:e3), Dst: Intel_ee:eb:e3 (10:51:07:ee:eb:e3)
▶ Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
▶ User Datagram Protocol, Src Port: 51379, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0xcd10
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ www.ac-nice.fr: type A, class IN
      Name: www.ac-nice.fr
      [Name Length: 14]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 53]
  
```

Quels sont les différents protocoles encapsulés dans une trame DNS ?

Ethernet ,IP, UDP, DNS

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

Destination IP : 192.168.1.1

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

C'est l'EtherType = 0x0800 → protocole IPv4 et le datagram UDP

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

20 octets

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

UDP=8octets

TP 5 – Trames ARP, ICMP et DNS

- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?
0x0035 = 53 → Port DNS standard (UDP/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 ?

La valeur en Hexa du nom de domaine est 07 61 63 2d 6e 69 63 65 02 66 72 00 = ac nice.fr et 03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 = www.ac-nice.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.

Je sélectionne la trame comportant la trame DNS et plus précisément la réponse a la requete DNS

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of packets, with packet 53 selected, which is a DNS Standard query response. The middle pane shows the details of this packet, including the Domain Name System (response) section. The 'Answers' section lists five CNAME records for the domain www.ac-nice.fr, each pointing to a different IP address from Cloudflare. The bottom pane shows the raw hex and ASCII data of the packet, with the ASCII column displaying the domain name and IP addresses in a readable format.

Je constate plusieurs adresse IP :

- Décimal : 141.101.90.104 → 141.101.90.107
- Hexadécimal : 8D.65.5A.68 → 8D.65.5A.6B

4.3. Commande Tracert et capture de trames ICMP.

Je saisis la commande tracert et obtiens cette trame

The screenshot shows two windows from Wireshark. The left window displays a list of captured packets, with packet 6 selected. The right window shows the command prompt output of a Windows tracert command.

Packet 6 Details:

- Frame 6: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF... [Ethernet II]
- Ethernet II, Src: Intel_ee:eb:e3 (10:51:07:ee:eb:e3), Destination: SagecomRoa_50:51:b0 (78:c2:13:50:51:b0)
- Internet Protocol Version 4, Src: 192.168.1.16, Destination: 141.101.90.107
- Internet Control Message Protocol

Tracert Command Output:

```

C:\Users\haike>tracert www.ac-nice.fr

Détermination de l'itinéraire vers www.ac-nice.fr.cdn.cloudflare.net [141.101.90.106]
avec un maximum de 30 sauts :

  0  *  *  *  Délai d'attente de la demande dépassé.
  1  2 ms  3 ms  2 ms livebox.home [2a01:cb1d:51a:ec00:7ac2:13ff:f
e50:51b0]
  2  5 ms  3 ms  3 ms 2a01:cb08a00402110193025300750151.ipv6.abo.wa
nadoo.fr [2a01:cb08:a004:211:193:253:75:151]
  3  11 ms  9 ms  7 ms 2a01:cfc0:200:8000:193:252:102:82
  4  9 ms  9 ms  9 ms 2a01:cfc0:200:8000:193:252:102:81
  5  *  *  *  Délai d'attente de la demande dépassé.
  6  9 ms  12 ms  10 ms 2a06:98c1:3200::90:82

Itinéraire déterminé.

C:\Users\haike>tracert www.ac-nice.fr

Détermination de l'itinéraire vers www.ac-nice.fr.cdn.cloudflare.net [141.101.90.106]
avec un maximum de 30 sauts :

  1  5 ms  3 ms  3 ms livebox.home [192.168.1.1]
  2  3 ms  4 ms  3 ms 80.10.239.133
  3  3 ms  3 ms  4 ms lag-11.nespr00z.rbc1.orange.net [193.249.215
.126]
  4  6 ms  4 ms  5 ms ae103-0.ncnic202.rbc1.orange.net [193.253.84
.241]
  5  8 ms  8 ms  8 ms ae43-0.nimar202.rbc1.orange.net [193.252.103
.241]
  6  9 ms  10 ms  7 ms ae40-0.nimar201.rbc1.orange.net [193.252.161
.41]
  7  *  *  *  Délai d'attente de la demande dépassé.
  8  8 ms  9 ms  10 ms 193.251.131.2
  9  10 ms  9 ms  24 ms comserver.opentransit.net [193.251.150.110]
 10  9 ms  9 ms  24 ms 162.158.20.242
 11  10 ms  11 ms  7 ms 141.101.90.106

Itinéraire déterminé.
    
```

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

The screenshot shows a packet capture in Wireshark with packet 376 selected. The details pane shows the IP and ICMP headers.

Packet 376 Details:

- Frame 376: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF... [Ethernet II]
- Ethernet II, Src: Intel_ee:eb:e3 (10:51:07:ee:eb:e3), Dst: SagecomRoa_50:51:b0 (78:c2:13:50:51:b0)
- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 141.101.90.107
- Internet Control Message Protocol

- Decimale: 141.101.90.107

- Hexadecimale: 0x 8d 65 5a 6b

TP 5 – Trames ARP, ICMP et DNS

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

```

Frame 376: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{...}
Ethernet II, Src: Intel_ee:eb:e3 (10:51:07:ee:eb:e3), Dst: SagemcomBroa_50:51:b0 (78:c2:13:50:51:b0)
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 141.101.90.107
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0xd373 (54131)
000. .... = Flags: 0x0
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.16
Destination Address: 141.101.90.107
[Stream index: 5]
Internet Control Message Protocol
  
```

- Decimale: 1
- Hexadecimale: 0x 01

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

```

Frame 376: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{...}
Ethernet II, Src: Intel_ee:eb:e3 (10:51:07:ee:eb:e3), Dst: SagemcomBroa_50:51:b0 (78:c2:13:50:51:b0)
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 141.101.90.107
Internet Control Message Protocol
Type: Echo (ping) request (8)
Code: 0
Checksum: 0xf79f [connect]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 95 (0x005f)
Sequence Number (LE): 24320 (0x5f00)
[No response seen]
[Expert Info (Warning/Sequence): No response seen to ICMP request]
Data (64 bytes)
  
```

- Decimale: 8
- Hexadecimales: 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.) ?

No.	Time	Source	Destination	Protocol	Length	Info
376	2.408703	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl=1 (no response found)
384	2.411319	192.168.1.16	141.101.90.107	ICMP	138	Time-to-live exceeded (Time to live exceeded in transit)
385	2.413374	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl=1 (no response found)
391	2.421310	192.168.1.16	141.101.90.107	ICMP	138	Time-to-live exceeded (Time to live exceeded in transit)
392	2.424156	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl=1 (no response found)
411	2.457954	192.168.1.16	141.101.90.107	ICMP	138	Time-to-live exceeded (Time to live exceeded in transit)
506	3.480326	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl=2 (no response found)
507	3.483408	80.10.239.133	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
508	3.486024	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl=2 (no response found)
509	3.489523	80.10.239.133	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
510	3.492168	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=100/25600, ttl=2 (no response found)
512	3.495469	80.10.239.133	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
738	9.087318	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=101/25856, ttl=3 (no response found)
739	9.090354	193.249.215.126	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
740	9.092950	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=102/26112, ttl=3 (no response found)
741	9.104795	193.249.215.126	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
742	9.106421	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=103/26368, ttl=3 (no response found)
743	9.111262	193.249.215.126	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
757	10.160115	192.168.1.16	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=104/26624, ttl=4 (no response found)

```

Frame 384: Packet, 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{...}
Ethernet II, Src: SagemcomBroa_50:51:b0 (78:c2:13:50:51:b0), Dst: Intel_ee:eb:e3 (10:51:07:ee:eb:e3)
802.1Q Virtual LAN, Prio: 0, DEI: 0, ID: 0
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.16
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 120
Identification: 0x4377 (17271)
000. .... = Flags: 0x0
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xb2ec [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.16
Destination Address: 192.168.1.16
[Stream index: 4]
Internet Control Message Protocol
  
```

- Decimale: 64

TP 5 – Trames ARP, ICMP et DNS

-Hexadecimale:0x40