

Compte-Rendu TP3Bloc1exSI2-tramesARP-ICMP-DNS

Fait à la maison

4.1 Capture de trames ARP et ICMP

172.17.254.1 d4-ae-52-7d-0e-2b dynamique

L'adresse IP et l'adresse MAC de roi sont bien présents dans le cache ARP.

Je n'ai pas réussi à obtenir d'échanges de trames ARP.

Trame ICMP Echo Request :

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F2902CCE-1279-4858-9099-F06CE85061FA}
  Ethernet II, Src: Dell_12:d2:d9 (d8:9e:f3:12:d2:d9), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
    > Destination: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
    > Source: Dell_12:d2:d9 (d8:9e:f3:12:d2:d9)
      Type: IPv4 (0x0800)
    > Internet Protocol Version 4, Src: 172.17.1.203, Dst: 172.17.254.1
    > Internet Control Message Protocol

<
0000  d4 ae 52 7d 0e 2b d8 9e f3 12 d2 d9 08 00 45 00  ..R}+... ..E.
0010  00 3c e0 ac 00 00 80 01 00 00 ac 11 01 cb ac 11  -<.....
0020  fe 01 08 00 4d 44 00 01 00 17 61 62 63 64 65 66  ....MD...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmnopqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
```

Les octets de position 0x0C et 0x0D de la ligne 0000, représentent le champ éthertype. Il possède la valeur 08 00, ce qui signifie que l'en-tête de trame transporte un protocole IPv4 et donc un paquet IP.

L'octet de position 0x07 de la ligne 0010 représente le champ protocole, il possède la valeur 01, ce qui signifie que l'en-tête de réseau transporte un message ICMP.

La longueur de la trame est de 74 octets.

La longueur du paquet IP est de 20 octets.

La longueur du message ICMP est de 40 octets.

Les octets de position 0x02 et 0x03 de la ligne 20 portent les valeurs 08 et 00. Le 08 signifie que le message ICMP est de type 8, donc que c'est un Echo Request, et le 00 signifie qu'il est de code 0.

Les octets à partir de l'octet 0x0A de la ligne 0020 correspondent aux données du messages ICMP.

Trame ICMP Echo Reply :

```

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F2902CCE-1279-4858-9099-F06CE85061FA}
> Ethernet II, Src: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b), Dst: Dell_12:d2:d9 (d8:9e:f3:12:d2:d9)
> Internet Protocol Version 4, Src: 172.17.254.1, Dst: 172.17.1.203
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x5544 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 23 (0x0017)
  Sequence number (LE): 5888 (0x1700)
  [Request frame: 3]
  [Response time: 0,271 ms]
> Data (32 bytes)

```

```

0000  d8 9e f3 12 d2 d9 d4 ae 52 7d 0e 2b 08 00 45 00  . . . . . R} . + . . E .
0010  00 3c 02 85 00 00 80 01 e0 4c ac 11 fe 01 ac 11  . < . . . . . L . . . . .
0020  01 cb 00 00 55 44 00 01 00 17 61 62 63 64 65 66  . . UD . . . abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi

```

Les octets de position 0x02 et 0x03 de la ligne 0020 possèdent les valeurs 00 et 00. L'octet de position 0x02 signifie que c'est un message ICMP de type 0 soit un Echo Reply, et celui de position 0x03 signifie qu'il est de code 0.

4.2 Capture de trames ARP, DNS et ICMP

No.	Time	Source	Destination	Protocol	Length	Info
1636	6.737248	ASUSTekC_60:e0:b9	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.31
1637	6.738521	Sagemcom_ad:78:40	ASUSTekC_60:e0:b9	ARP	42	192.168.1.1 is at a0:1b:29:ad:78:40
2033	8.360704	ASUSTekC_60:e0:b9	Broadcast	ARP	42	Who has 192.168.1.14? Tell 192.168.1.31
2055	8.418718	CloudNet_1d:9f:57	ASUSTekC_60:e0:b9	ARP	42	192.168.1.14 is at 0c:96:e6:1d:9f:57
2756	10.990464	fe80::2cb2:1550:ba7...	fe80::a21b:29ff:fea...	DNS	90	Standard query 0x59a9 AAAA ac-nice.fr
2760	11.014293	fe80::a21b:29ff:fea...	fe80::2cb2:1550:ba7...	DNS	142	Standard query response 0x59a9 AAAA ac-nice.fr SOA svrs.
2761	11.020354	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (re
2794	11.153082	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=52 (req
2926	12.023094	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (re
2943	12.165359	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=52 (req
3101	13.025383	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (re
3114	13.122437	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=52 (req
3273	14.028693	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (re
3289	14.190692	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=52 (req

L'adresse MAC recherchée est : a0:1b:29:ad:78:40

```

> Frame 1636: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{2F421340-3990-4674-BED8-5903DDC7429D}
▼ Ethernet II, Src: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9)
  Sender IP address: 192.168.1.31
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1

```

Trame ARP request :

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

@MAC source : 2c:fd:a1:60:e0:b9

Ethernet Type = ARP

Opcode (valeurs hexa.) = 01 (request)
 @MAC de la cible = 00:00:00:00:00:00
 @IP de la cible = 192.168.1.1

```
ac-nice.fr
-----
Nom d'enregistrement. : ac-nice.fr
Type d'enregistrement : 1
Durée de vie . . . . : 19131
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 194.167.84.108
```

No.	Time	Source	Destination	Protocol	Length	Info
1636	6.737248	ASUSTekC_60:e0:b9	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.31
1637	6.738521	Sagemcom_ad:78:40	ASUSTekC_60:e0:b9	ARP	42	192.168.1.1 is at a0:1b:29:ad:78:40
2033	8.360704	ASUSTekC_60:e0:b9	Broadcast	ARP	42	Who has 192.168.1.14? Tell 192.168.1.31
2055	8.418718	CloudNet_1d:9f:57	ASUSTekC_60:e0:b9	ARP	42	192.168.1.14 is at 0c:96:e6:1d:9f:57
2756	10.990464	fe80::2cb2:1550:ba7...	fe80::a21b:29ff:fea...	DNS	90	Standard query 0x59a9 AAAA ac-nice.fr
2760	11.014293	fe80::a21b:29ff:fea...	fe80::2cb2:1550:ba7...	DNS	142	Standard query response 0x59a9 AAAA ac-nice.fr SOA
2761	11.020354	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=1
2794	11.153082	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=5
2926	12.023094	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=1
2943	12.165359	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=5
3101	13.025383	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=1
3114	13.122437	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=5
3273	14.028693	192.168.1.31	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=1
3289	14.190692	194.167.84.108	192.168.1.31	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=5

```
> Frame 2756: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{2F421340-3990-4674-BEDB-5903DDC742}
> Ethernet II, Src: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9), Dst: Sagemcom_ad:78:40 (a0:1b:29:ad:78:40)
  > Destination: Sagemcom_ad:78:40 (a0:1b:29:ad:78:40)
  > Source: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9)
  Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::2cb2:1550:ba71:6ecf, Dst: fe80::a21b:29ff:fead:7840
> User Datagram Protocol, Src Port: 57617, Dst Port: 53
  Source Port: 57617
  Destination Port: 53
  Length: 36
  Checksum: 0x6786 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 12]
  > [Timestamps]
> Domain Name System (query)
  Transaction ID: 0x59a9
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
```

```
0000  a0 1b 29 ad 78 40 2c fd a1 60 e0 b9 86 dd 60 08  ..)x@.,. ....
0010  ab 9c 00 24 11 40 fe 80 00 00 00 00 00 2c b2  .4$.@. ....
0020  15 50 ba 71 6e cf fe 80 00 00 00 00 00 a2 1b  .Pqn.....
0030  29 ff fe ad 78 40 e1 11 00 35 00 24 67 86 59 a9  )...x@...5$.Y
0040  01 00 00 01 00 00 00 00 00 00 07 61 63 2d 6e 69  .....ac-ni
0050  63 65 02 66 72 00 00 1c 00 01  ce.fr.....
```

Il y a plusieurs protocoles encapsulés dans la trame DNS :
 Le protocole Ipv6 dans le champ éthertype qui a pour valeur 86 dd en hexa
 Le protocole UDP dans le champ protocole qui a pour valeur 11 en hexa
 Et le protocole DNS dans le champ port qui a pour valeur 00 35 en hexa
 La machine destinataire est le serveur de ac-nice.fr
 L'adresse IP de cette machine est 194.167.84.108

Les octets de position 0x0C et 0x0D de la ligne 0000 représentent le champ éthertype de l'en-tête de trame. L'octet de position 0x07 de la ligne 0010 devrait représenter le champ protocole de l'en-tête de réseau, mais ici il se situe à la position 0x05 de la ligne 10.
 Les octets de positions 0x04 et 0x05 de la ligne 0020 devrait représenter le champ port de l'en-tête de transport mais ici il se situe à la position 0x08 et 0x09 de la ligne 30.
 Les valeurs en hexadécimale correspondantes au nom du domaine sont :

07:61:63:2d:6e:69:63:65:02:66:72:00

4.3 Commande Tracert et capture de trames ICMP

No.	Time	Source	Destination	Protocol	Length	Info
600	2.779315	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=45/11520, ttl=1 (no respo...
601	2.780698	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
602	2.781002	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=46/11776, ttl=1 (no respo...
603	2.782100	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
604	2.782374	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=47/12032, ttl=1 (no respo...
605	2.783340	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1683	8.288288	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=48/12288, ttl=2 (no respo...
1685	8.293865	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1686	8.294268	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=49/12544, ttl=2 (no respo...
1689	8.299613	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1690	8.300481	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=2 (no respo...
1691	8.305993	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2941	13.844774	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=3 (no respo...
2943	13.852802	192.253.86.18	192.168.1.31	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2944	13.854425	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=3 (no respo...

> Frame 600: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{2F421340-3990-4674-BEDB-5903DDC7429D}, id 0
> Ethernet II, Src: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9), Dst: Sagemcom_ad:78:40 (a0:1b:29:ad:78:40)
v Internet Protocol Version 4, Src: 192.168.1.31, Dst: 194.167.84.155
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x9e2c (40492)
> Flags: 0x0000
Fragment offset: 0
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x426b [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.31
Destination: 194.167.84.155
> Internet Control Message Protocol

```
0000 a0 1b 29 ad 78 40 2c fd a1 60 e0 b9 08 00 45 00  ..).x@,.....E:
0010 00 5c 9e 2c 00 00 01 01 42 6b c0 a8 01 1f c2 a7  \.,.....Bk.....
0020 54 9b 08 00 f7 d1 00 01 00 2d 00 00 00 00 00 00  T.....
0030 00 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 00  .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

L'adresse IP destination en valeur décimale est : 194.167.84.155 , en valeur hexadécimale est : c2:a7:54:9b

Le champ TTL porte la valeur 1 en décimale et 01 en hexadécimale .

Le champ Type du message ICMP porte la valeur 8 en décimale et 08 en hexadécimale.

Trame comportant le message d'erreur :

No.	Time	Source	Destination	Protocol	Length	Info
600	2.779315	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=45/11520, ttl=1 (no respo...
601	2.780698	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
602	2.781092	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=46/11776, ttl=1 (no respo...
603	2.782100	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
604	2.782374	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=47/12032, ttl=1 (no respo...
605	2.783340	192.168.1.1	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1683	8.288288	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=48/12288, ttl=2 (no respo...
1685	8.293865	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1686	8.294268	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=49/12544, ttl=2 (no respo...
1689	8.299613	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
1690	8.300481	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=50/12800, ttl=2 (no respo...
1691	8.305993	80.10.236.5	192.168.1.31	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
2941	13.844774	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=51/13056, ttl=3 (no respo...
2943	13.852802	193.253.86.18	192.168.1.31	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2944	13.854425	192.168.1.31	194.167.84.155	ICMP	106	Echo (ping) request id=0x0001, seq=52/13312, ttl=3 (no respo...

> Frame 601: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{2F421340-3990-4674-BEDB-5903DDC7429D}, id 0
 > Ethernet II, Src: Sagencom_ad:78:40 (a0:1b:29:ad:78:40), Dst: ASUSTekC_60:e0:b9 (2c:fd:a1:60:e0:b9)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.31
 > Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0xf4ff [correct]
 [Checksum Status: Good]
 Unused: 00000000
 > Internet Protocol Version 4, Src: 192.168.1.31, Dst: 194.167.84.155
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xf7d1 [unverified] [in ICMP error packet]
 [Checksum Status: Unverified]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 45 (0x002d)
 Sequence number (LE): 11520 (0x2d00)
 > Data (64 bytes)

```

0010  00 78 ab 4f 00 00 40 01 4b 05 c0 a8 01 01 c0 a8  .x.O..@.K.....
0020  01 1f 08 00 f4 ff 00 00 00 00 45 00 00 5c 9e 2c  .[.....E...\,
0030  00 00 01 01 42 6b c0 a8 01 1f c2 a7 54 9b 08 00  ....Bk...T...
0040  f7 d1 00 01 00 2d 00 00 00 00 00 00 00 00 00 00  ....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Le champ Type du message ICMP est toujours le même, 8 en décimale et 08 en hexadécimale.