

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..... 3
- 4.3. Commande Tracert et capture de trames ICMP..... 5

4.1. Capture de trames ARP et ICMP.

Vous allez capturer les trames **ICMP** générées par la saisie d'une commande **ping** depuis votre machine physique.

- Ouvrez Wireshark et démarrez une capture de trames.
- Ouvrez une invite de commandes et pinguez le serveur Aviateur (172.17.254.5). Effectuez une capture d'écran.
- L'échange démarre avec une requête et une réponse **ARP** pour obtenir l'adresse MAC du serveur Aviateur. Ensuite l'échange de trames **ICMP** a lieu. Arrêtez la capture une fois les 8 trames ICMP obtenues. Sauvegardez la sous le nom « CaptureICMP ».

No.	Time	Source	Destination	Protocol	Length	Info
474	7.782688	RivetNet_ee...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.11
475	7.786149	Sagemcom_1a...	RivetNet_ee...	ARP	60	192.168.1.1 is at 24:f7:20:1a:99:20
498	9.985382	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 499)
499	9.989772	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=64 (request in 498)
541	10.998...	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (reply in 542)
542	11.004...	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=64 (request in 541)
551	12.009...	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 552)
552	12.013...	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=64 (request in 551)
554	13.024...	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 555)
555	13.028...	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=64 (request in 554)

- ☞ Si vous ne visualisez pas d'échange ARP, videz le cache ARP (ouvrir une invite de commandes en tant qu'administrateur et saisir la commande **arp -d ***) puis, sans tarder, recommencez une nouvelle capture et ressaisissez la commande **ping** :

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.22631.4169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>arp -a

Interface : 192.168.1.10 --- 0x19
    Adresse Internet    Adresse physique    Type
    192.168.1.1         0c-73-29-35-27-6e   dynamique
    224.0.0.2           01-00-5e-00-00-02   statique
    224.0.0.22          01-00-5e-00-00-16   statique
    224.0.0.251         01-00-5e-00-00-fb   statique
    224.0.0.252         01-00-5e-00-00-fc   statique
    239.255.255.250     01-00-5e-7f-ff-fa   statique
    255.255.255.255     ff-ff-ff-ff-ff-ff   statique

C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

Interface : 192.168.1.10 --- 0x19
    Adresse Internet    Adresse physique    Type
    224.0.0.2           01-00-5e-00-00-02   statique
```

- Après la saisie de la commande ping et la capture des trames ARP/ICMP, arrêtez cette dernière et consultez le contenu du cache ARP : vérifiez la présence de l'association @IP-@MAC correspondant à Aviateur (capture d'écran à réaliser).
- A l'aide du **Chapitre 5 (page 2)**, analysez l'**échange de trames ARP** (Request et Reply) **précédant l'échange de trames ICMP** :

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

Quelle est la fonction de la trame ARP Request ?

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

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

Quelle est la longueur de la **trame** ARP Request ? _____

Quelle est la longueur de la **trame** ARP Reply ? _____

Combien d'octets sont utilisés pour le padding ? _____

- Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination =
@MAC source =
Ethernet Type =
Opcode (valeurs hexa.) =
@MAC de la cible =
@IP de la cible =

N'oubliez pas que la « **Target MAC address** » est la question associée à la trame ARP Request.

- Sélectionnez une trame **ICMP Echo Request**. A l'aide du **Chapitre 5 (pages 4 et 5)**, répondez aux questions suivantes :

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

Quelle signification a l'octet de position 0×07 ligne 0010 ?

Quelle est la longueur de la trame ? _____

Quelle est la longueur du paquet IP ? _____

Quelle est la longueur du message ICMP ? _____

Quelle signification a l'octet de position 0×02 ligne 00020 ?

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 ?
-

4.2. Capture de trames ARP, DNS et ICMP.

- Démarrez une capture de trames depuis votre machine physique.
- Ouvrez une invite de commandes, videz le cache ARP (commande **arp -d ***) puis effectuez une requête ping vers le serveur web **www.ac-nice.fr** (ping « nom » et non plus ping « @IP ») :

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.22631.4169]
(c) Microsoft Corporation. Tous droits réservés.

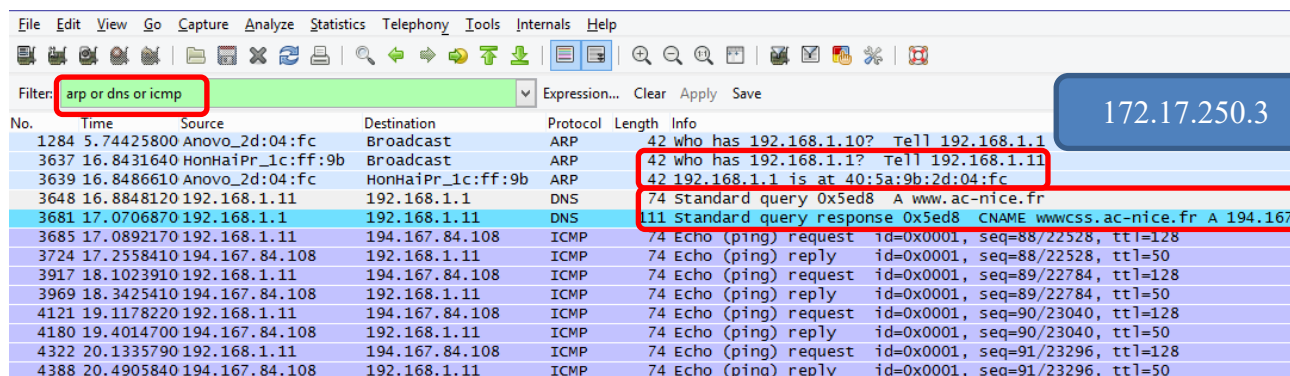
C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur cs234.wpc.alphacdn.net [93.184.221.161] avec 32 octets de données :
Réponse de 93.184.221.161 : octets=32 temps=17 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=20 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=22 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=20 ms TTL=55

Statistiques Ping pour 93.184.221.161:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 17ms, Maximum = 22ms, Moyenne = 19ms

C:\Windows\System32>
```

- Arrêtez la capture et sauvegardez la sous le nom « CaptureIcmpDns » :



- La liste des trames commence par une requête et une réponse ARP. Quelle est la machine dont l'adresse MAC est recherchée ? _____
- Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination =
@MAC source =
Ethernet Type =
Opcode (valeurs hexa.) =
@MAC de la cible =
@IP de la cible =

- 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 ? _____
- 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 :

```

Administrateur : Invite de commandes

C:\Windows\system32>ipconfig /displaydns

Configuration IP de Windows

pc-01
-----
Nom d'enregistrement. : PC-01.home
Type d'enregistrement : 1
Durée de vie          : 3132
Longueur de données  : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 192.168.1.18

1.0.0.127.in-addr.arpa
-----
Nom d'enregistrement. : 1.0.0.127.in-addr.arpa.
Type d'enregistrement : 12
Durée de vie          : 86400
Longueur de données  : 8
Section . . . . . : Réponse
Enregistrement PTR.  : localhost

ac-nice.fr
-----
Nom d'enregistrement. : ac-nice.fr
Type d'enregistrement : 1
Durée de vie          : 6976
Longueur de données  : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 194.167.84.108

localhost
-----
Nom d'enregistrement. : localhost
Type d'enregistrement : 1
Durée de vie          : 86400
Longueur de données  : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 127.0.0.1

```



- Démarrez une nouvelle capture et ressaisissez la commande **ping www.ac-nice.fr** dans l'invite de commandes. **Vous ne devriez pas constater de requête DNS** puisque l'enregistrement est présent dans le cache DNS.
- Videz le cache DNS à l'aide de la commande **ipconfig /flushdns** et redémarrez une nouvelle capture **afin de visualiser de nouveau une requête DNS** (capture d'écran à faire) :

Filter: **arp or dns or icmp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1284	5.74425800	Anovo_2d:04:fc	Broadcast	ARP	42	who has 192.168.1.10? Tell 192.168.1.1
3637	16.8431640	HonHaiPr_1c:ff:9b	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.11
3639	16.8486610	Anovo_2d:04:fc	HonHaiPr_1c:ff:9b	ARP	42	192.168.1.1 is at 40:5a:9b:2d:04:fc
3648	16.8848120	192.168.1.11	192.168.1.1	DNS	74	Standard query 0x5ed8 A www.ac-nice.fr
3681	17.0706870	192.168.1.1	192.168.1.11	DNS	111	Standard query response 0x5ed8 CNAME wwwcss.ac-nice.fr A 194.167.84.108
3685	17.0892170	192.168.1.11	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=88/22528, ttl=128
3724	17.2558410	194.167.84.108	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=88/22528, ttl=50
3917	18.1023910	192.168.1.11	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=89/22784, ttl=128
3969	18.3425410	194.167.84.108	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=89/22784, ttl=50
4121	19.1178220	192.168.1.11	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=90/23040, ttl=128
4180	19.4014700	194.167.84.108	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=90/23040, ttl=50
4322	20.1335790	192.168.1.11	194.167.84.108	ICMP	74	Echo (ping) request id=0x0001, seq=91/23296, ttl=128
4388	20.4905840	194.167.84.108	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=91/23296, ttl=50

Frame 3648 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: HonHaiPr_1c:ff:9b (b8:76:3f:1c:ff:9b), Dst: Anovo_2d:04:fc (40:5a:9b:2d:04:fc)

Destination: Anovo_2d:04:fc (40:5a:9b:2d:04:fc)

Source: HonHaiPr_1c:ff:9b (b8:76:3f:1c:ff:9b)

Type: IP (0x0800)

Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1)

User Datagram Protocol, Src Port: 65024 (65024), Dst Port: domain (53)

Source port: 65024 (65024)

Destination port: domain (53)

Length: 46

Checksum: 0xf27d [validation disabled]

Domain Name System (query)

Response in: 3681

Transaction ID: 0x5ed8

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

Type: A (Host address)

Class: IN (0x0001)

0000 40 5a 9b 2d 04 fc b8 76 3f 1c ff 9b 08 00 45 00 @Z...v?...E.

0010 00 3c 5a 16 00 00 80 11 5d 3e c0 a8 01 0b c0 a8 .<Z....]>....

0020 01 01 fe 00 00 35 00 48 f3 7a 5e d8 01 00 00 015(C)A.....

0030 00 00 00 00 00 00 03 77 77 77 07 61 63 2d 6e 69www.ac-ni

0040 63 65 02 66 72 00 00 01 00 01 ce.fr....

- Quels sont les différents protocoles encapsulés dans une trame DNS ?
- Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (cf. en-tête IP) ?

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

- Quelle est la longueur de l'en-tête IP ? _____
- Quelle est la longueur de l'en-tête de transport dans cette trame ? _____
- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

- 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 ? _____
- 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. _____

4.3. Commande Tracert et capture de trames ICMP.

- On a vu que la commande **ping** génère deux types de message ICMP : une machine émet une trame **Echo request (type 8)** à laquelle répond la machine destinataire avec un message **Echo reply (type 0)**. Lorsque l'on arrive à pinger une autre machine, on en déduit que les couches 1, 2 et 3 sont opérationnelles sur toutes les machines participant à l'échange de trames (**ICMP est un protocole de la couche 3**) et que, en conséquence, **le routage** est fonctionnel dans les deux sens.
- La commande **tracert** permet de connaître tous les **routeurs** entre la machine locale et une destination donnée, par exemple le site web de l'Académie de Nice (**tracert www.ac-nice.fr**) :

```

C:\Windows\system32>tracert www.ac-nice.fr

Détermination de l'itinéraire vers wwwcss.ac-nice.fr [194.167.84.108]
avec un maximum de 30 sauts :

  0  0 ms  0 ms  0 ms  livebox.hone [192.168.1.1]
  1  2 ms  *  *  *  Délai d'attente de la demande dépassé.
  2  21 ms  23 ms  20 ms  10.125.4.70
  3  26 ms  21 ms  19 ms  ge-2-0-0-0.nctln102.Toulon.francetelecom.net [19
3.253.84.37]
  4  30 ms  30 ms  29 ms  ae47-0.nilyo102.Lyon.francetelecom.net [193.252.
101.210]
  5  36 ms  37 ms  196 ms  81.253.184.54
  6  38 ms  41 ms  38 ms  tengige0-13-0-7.auvtr1.Aubervilliers.opentransit
.net [193.251.129.177]
  7  39 ms  40 ms  38 ms  tengige0-7-0-8.auvtr4.Aubervilliers.opentransit.
net [193.251.132.161]
  8  35 ms  36 ms  38 ms  tiscali-1.GW.opentransit.net [193.251.254.70]
  9  50 ms  49 ms  49 ms  xe-7-0-0.mrs10.ip4.tinet.net [141.136.109.42]
 10  48 ms  50 ms  47 ms  renater-gw.ip4.tinet.net [77.67.90.122]
 11  50 ms  56 ms  50 ms  193.51.179.185
 12  55 ms  55 ms  55 ms  tel-2-sophia-rtr-021.noc.renater.fr [193.51.189.
261]
 13  64 ms  64 ms  62 ms  rectorat-nice-admin-gi9-8-sophia-rtr-021.noc.ren
ater.fr [193.51.187.1]
 14  58 ms  58 ms  59 ms  194.167.90.1
 15  60 ms  58 ms  58 ms  wwwcss.ac-nice.fr [194.167.84.108]

Itinéraire déterminé.
C:\Windows\system32>

```

Elle génère l'envoi de messages **ICMP Echo request** dans le but de recevoir en retour un **message automatique ICMP TTL exceeded** de la part des différents routeurs rencontrés **permettant ainsi d'obtenir leur adresse IP**.

Comment faire pour provoquer l'envoi de ce message d'erreur par le **premier routeur** ? Il suffit de mettre le **TTL à 1** dans la trame **Echo request** adressée au serveur web de l'Académie de Nice. Le premier routeur rencontré (le routeur Stormshield 172.17.250.3 ou la box chez vous) décrémente le TTL de 1 et le met donc à 0. Il supprime en conséquence le paquet reçu et renvoie un message d'erreur **TTL exceeded**. Ainsi, obtenons-nous son adresse IP.

Pour connaître l'adresse du **second routeur**, il suffit de mettre le **TTL à 2** dans le message **Echo request à destination du serveur web**. Le TTL sera décrémenté de 1 lors du passage du premier routeur qui routera le paquet reçu vers le second routeur. Celui-ci décrémenté à son tour le TTL de 1 et le met donc à 0. Il supprime en conséquence le paquet reçu et renvoie un message d'erreur **TTL exceeded**. Ainsi, obtenons-nous également son adresse IP.

Et ainsi de suite jusqu'à la destination finale.

- Démarrez une capture de trames **depuis votre machine physique**.
- Ouvrez une invite de commandes et saisissez la commande **tracert www.ac-nice.fr**.
- Une fois l'itinéraire déterminé, arrêtez la capture et sauvegardez la sous le nom « CaptureTracert ».
- Limitez l'affichage des trames à celles encapsulant le protocole ICMP (zone **Filter**) :

No.	Time	Source	Destination	Protocol	Length	Info
9	0.56201500	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=2/512, ttl=1
10	0.56446100	192.168.1.21	192.168.1.21	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
11	0.56534500	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=3/768, ttl=1
12	0.57001000	192.168.1.21	192.168.1.21	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	0.57068000	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=4/1024, ttl=1
14	0.57405700	192.168.1.21	192.168.1.21	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
17	1.62531100	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=5/1280, ttl=2
18	5.57947000	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=6/1536, ttl=2
21	9.57831200	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=7/1792, ttl=2
31	13.57993800	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=8/2048, ttl=3
32	13.60134300	10.125.4.78	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
33	13.60207700	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=9/2304, ttl=3
34	13.62515400	10.125.4.78	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
35	13.62583000	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=10/2560, ttl=3
37	13.64605200	10.125.4.78	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
73	29.18627900	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=4
74	29.21225100	193.253.84.37	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
75	29.21311000	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=4
76	29.23482400	193.253.84.37	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
77	29.23564700	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=4
78	29.25532400	193.253.84.37	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
82	30.32690900	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=5
83	30.35767800	193.252.101.210	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
84	30.37418200	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=5
85	30.40448200	193.252.101.210	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	30.40502800	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=5
87	30.43492000	193.252.101.210	192.168.1.21	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
90	31.49909200	192.168.1.21	194.167.84.108	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=6
91	31.53581900	81.253.184.54	192.168.1.21	ICMP	70	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.) ? _____
- Sélectionnez le champ **TTL**. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ? _____
- Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ **Type** (valeurs déci. et hexa.) ? _____
- 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.) ? _____