

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 4

4.1. Capture de trames ARP et ICMP.

ping d'aviateur

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindow
s

PS C:\Users\mhidaoui> 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=1 ms 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
PS C:\Users\mhidaoui>
```

Démarrage d'une trame WireShark

540	26.288757	Giga-Byt 2f:81:87	Vmware 76:e3:f7	ARP	42 172.17.2.3 is at 74:56:3c:2f:81:87
541	26.532695	Vmware 22:87:6d	Broadcast	ARP	60 who has 172.17.244.15? Tell 172.17.243.11
542	26.595421	172.17.2.3	172.17.254.5	ICMP	74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 543)
543	26.595947	172.17.254.5	172.17.2.3	ICMP	74 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 542)
545	26.600392	172.17.254.5	172.17.2.3	ICMP	450 Destination unreachable (Port unreachable)
547	26.601053	172.17.254.5	172.17.2.3	ICMP	406 Destination unreachable (Port unreachable)
548	27.603672	172.17.2.3	172.17.254.5	ICMP	74 Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 550)
550	27.604174	172.17.254.5	172.17.2.3	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 548)
551	27.604174	172.17.254.5	172.17.2.3	ICMP	450 Destination unreachable (Port unreachable)
555	28.608961	172.17.2.3	172.17.254.5	ICMP	74 Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 556)

exécution de la commande "arp -a"

```
C:\Users\mhidaoui>arp -a

Interface : 192.168.48.1 --- 0x4
    Adresse Internet      Adresse physique      Type
    192.168.48.255        ff-ff-ff-ff-ff-ff    statique
    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
    224.168.100.1         01-00-5e-28-64-01    statique
    239.192.0.0           01-00-5e-40-00-00    statique
    239.255.255.250      01-00-5e-7f-ff-fa    statique
    239.255.255.254      01-00-5e-7f-ff-fe    statique

Interface : 172.17.2.3 --- 0x7
    Adresse Internet      Adresse physique      Type
    172.17.1.14           88-ce-62-2b-49-0f    dynamique
    172.17.1.15           68-f6-77-22-76-58    dynamique
    172.17.5.2            5c-5f-67-eb-4c-f4    dynamique
    172.17.244.1          00-0c-29-76-e3-f7    dynamique
    172.17.250.3          00-0d-b4-2a-a8-34    dynamique
    172.17.250.6          00-a5-bf-e9-d6-00    dynamique
    172.17.250.7          00-a5-bf-e9-e8-00    dynamique
    172.17.254.1          d4-ae-52-7d-8e-2b    dynamique
    172.17.254.5          00-11-37-37-37-b5    dynamique
```

Partie ARP question

Signification : Type Ethernet = 0x0806 = protocole ARP

Fonction ARP Request : Recherche l'adresse MAC à l'aide d'une adresse IP donnée

Position 0x04 et 0x05 ligne 0010 : Protocol size = 0x04 = longueur de l'adresse IP en octets

message ARP : 28 octets

trame ARP Request : 42 octets = 14 octets Ethernet + 28 octets ARP

trame ARP Reply : 42 octets

padding : 18 octets

Rubriques

Trame ARP Request :

- @MAC destination = ff:ff:ff:ff:ff:ff = broadcast
- @MAC source = 00:0c:29:22:87:6d
- Ethernet Type = 0x0806
- Opcode = 0x0001 = request
- @MAC de la cible = 00:00:00:00:00:00
- @IP de la cible = 172.17.244.15

Partie Questions ICMP Echo Request

Signification : Type Ethernet = 0x0800 = protocole IPv4

Signification : TTL (Time To Live) = 128

Longueur de la trame : 74 octets

Longueur paquet IP : 60 octets

Longueur du message ICMP : 40 octets = 60 octets IP - 20 octets en-tête IP

Signification : Message type ICMP Echo Request

Octets à partir de 0x0A ligne 0020 :

- Octets 0x0A-0x0B : Sequence Number (LE) = 256 (0x0100)
- Octets suivants : Données (payload) du message ICMP = 32 octets

Trame ICMP Echo Reply

Nom et valeur position 0x02 ligne 0020 : Type ICMP = 0 = Echo Reply

4.2. Capture de trames ARP, DNS et ICMP

ping de "www.ac-nice.fr"

```
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.
PS C:\Users\mhidaoui> ping www.ac-nice.fr
La requête Ping n'a pas pu trouver l'hôte www.ac-nice.fr. Vérifiez le nom et essayez à nouveau.
PS C:\Users\mhidaoui> ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53

Statistiques Ping pour 141.101.90.107:
Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
Durée approximative des boucles en millisecondes :
Minimum = 16ms, Maximum = 16ms, Moyenne = 16ms
PS C:\Users\mhidaoui> |
```

Trame qui à démarrer avant la commande ping

Time	Source	Destination	Protocol	Length	Info
582 28.033037	172.17.254.1	172.17.2.3	DNS	185	Standard query response 0xd741 A ww.ac-nice.fr CNAME ww.ac-nice.fr.cdn.cloudflare.net A ...
583 28.039042	172.17.2.3	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 586)
586 28.068553	141.101.90.106	172.17.2.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=53 (request in 583)
587 28.304180	Arkinohi_02:30:96	Broadcast	ARP	60	Who has 172.17.200.100? Tell 172.17.250.2
588 29.051084	172.17.2.3	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 589)
589 29.077009	141.101.90.106	172.17.2.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=53 (request in 588)
590 29.423707	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.87? Tell 172.17.2.5
592 30.064611	172.17.2.3	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 593)
593 30.090289	141.101.90.106	172.17.2.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=53 (request in 592)
594 30.319227	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.87? Tell 172.17.2.5
603 31.049354	172.17.2.3	172.17.254.1	DNS	101	Standard query 0xcb41 A addons-pa.clients6.google.com
605 31.049409	172.17.2.3	172.17.254.1	DNS	101	Standard query 0xc97 HTTPS addons-pa.clients6.google.com
608 31.068008	172.17.2.3	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 609)
609 31.093720	141.101.90.106	172.17.2.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=53 (request in 608)
610 31.097506	172.17.254.1	172.17.2.3	DNS	119	Standard query response 0xcb41 A addons-pa.clients6.google.com A 142.250.201.42
612 31.097885	172.17.254.1	172.17.2.3	DNS	153	Standard query response 0xc97 HTTPS addons-pa.clients6.google.com SOA ns1.google.com
639 31.318650	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.87? Tell 172.17.2.5
647 31.552193	Arkinohi_02:30:96	Broadcast	ARP	60	Who has 172.17.200.100? Tell 172.17.250.2
650 32.443136	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
651 32.552198	Arkinohi_02:30:96	Broadcast	ARP	60	Who has 172.17.200.100? Tell 172.17.250.2
654 32.598625	Giga-Byt_2f:81:87	Broadcast	ARP	42	Who has 172.17.2.14? Tell 172.17.2.3
660 33.429334	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
662 33.552163	Arkinohi_02:30:96	Broadcast	ARP	60	Who has 172.17.200.100? Tell 172.17.250.2
663 33.561698	Giga-Byt_2f:81:87	Broadcast	ARP	42	Who has 172.17.2.14? Tell 172.17.2.3

vide du cash ARP

```
C:\Windows\System32>arp -d
C:\Windows\System32>
```

Partie Question ARP, ICMP et DNS

Analyse de la capture réseau (trames ARP, DNS, ICMP) :

Identification de la machine recherchée

Machine dont l'adresse MAC est recherchée : 172.17.2.8

Rubriques

Trame ARP Request (Frame 594) :

- @MAC destination = ff:ff:ff:ff:ff:ff = broadcast
- @MAC source = 74:56:3c:2f:9c:cd
- Ethernet Type = 0x0806
- Opcode = 0x0001 = request
- @MAC de la cible = 00:00:00:00:00:00
- @IP de la cible = 172.17.2.8

Raison de la requête DNS avant ICMP

Execution de ping”www.ac-nice.fr au lieu d'une adresse IP, le système doit d'abord résoudre le nom en IP à l'aide de la requête DNS. La séquence est :

Exécution de ipconfig /displaydns

```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 8714
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 . . . . : 8714
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.106
```

Exécution de “ipconfig /flushdns”

```
Configuration IP de Windows
Cache de résolution DNS vidé.
```

Les Trames après le vide du cash DNS

Time	Source	Destination	Protocol	Length	Info
79 12.862392	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.8? Tell 172.17.2.5
81 13.480377	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.8? Tell 172.17.2.5
82 14.479831	Giga-Byt_2f:9c:cd	Broadcast	ARP	60	Who has 172.17.2.8? Tell 172.17.2.5
87 18.104952	172.17.2.3	172.17.254.1	DNS	74	Standard query 0xb7ac A www.ac-nice.fr
88 18.157647	172.17.254.1	172.17.2.3	DNS	185	Standard query response 0xb7ac A www.ac-
89 18.162961	172.17.2.3	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=17/4
99 22.738682	172.17.2.3	141.101.90.107	ICMP	74	Echo (ping) request id=0x0001, seq=18/4
103 22.765182	141.101.90.107	172.17.2.3	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4
106 23.345171	Dell_7d:0e:2b	Broadcast	ARP	60	Who has 172.17.253.2? Tell 172.17.254.1

Frame 88: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface \Device\NPF_{405F72F5-58ED...}

Ethernet II, Src: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b), Dst: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87)

Internet Protocol Version 4, Src: 172.17.254.1, Dst: 172.17.2.3

User Datagram Protocol, Src Port: 53, Dst Port: 61914

- Source Port: 53
- Destination Port: 61914
- Length: 151
- Checksum: 0x3204 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 7]
- [Timestamps]
 - [Time since first frame: 0.052695000 seconds]
 - [Time since previous frame: 0.052695000 seconds]
- UDP payload (143 bytes)
- Domain Name System (response)

Partie Questions analyse de la trame DNS

Protocoles encapsulés : Ethernet II → IPv4 → UDP → DNS

Destinataire : 172.17.254.1 (serveur DNS)

Signification des octets

Signification : Type Ethernet = 0x0800 IPv4

Signification : TTL (Time To Live) du paquet IP

En-tête IP : 20 octets

En-tête UDP : 8 octets

Signification : Port source UDP = 53 = 0x0035

"www.ac-nice.fr", les valeurs hexa. = 03 77 77 77 02 61 63 04 6e 69 63 65 02 66 72 00

Answers, l'adresse IP du serveur web hébergeant www.ac-nice.fr :

Valeurs hexadécimales : AC 11 02 03

Valeurs décimales : 172.17.2.3

4.3. Commande Tracert et capture de trames ICMP

Oublie de faire un capture mais je l'ai fait pour la commande tracert www.ac-nice.fr

```
Administrateur : Invite de commandes
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

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 :

  1    2 ms    4 ms    3 ms    livebox.hone [192.168.1.1]
  2    *        *        *        Délai d'attente de la demande dépassé.
  3   21 ms   23 ms   20 ms   10.125.4.70
  4   26 ms   21 ms   19 ms   ge-2-0-0-0.nctln102.Toulon.francetelecom.net [19
3.253.84.37]
  5   30 ms   30 ms   29 ms   ae47-0.nilyo102.Lyon.francetelecom.net [193.252.
101.210]
  6   36 ms   37 ms   196 ms  81.253.184.54
  7   38 ms   41 ms   38 ms   tengige0-13-0-7.auvtr1.Aubervilliers.opentransit
.net [193.251.129.177]
  8   39 ms   40 ms   38 ms   tengige0-7-0-8.auvtr4.Aubervilliers.opentransit.
net [193.251.132.16]
  9   35 ms   36 ms   38 ms   tiscali-1.GW.opentransit.net [193.251.254.70]
 10  50 ms   49 ms   49 ms   xe-7-0-0.mrs10.ip4.tinet.net [141.136.109.42]
 11  48 ms   50 ms   47 ms   renater-gu.ip4.tinet.net [77.67.90.122]
 12  50 ms   56 ms   50 ms   193.51.179.185
 13  55 ms   55 ms   55 ms   tel-2-sophia-rtr-021.noc.renater.fr [193.51.189.
26]
 14  64 ms   64 ms   62 ms   rectorat-nice-admin-gi9-8-sophia-rtr-021.noc.ren
ater.fr [193.51.187.1]
 15  58 ms   58 ms   59 ms   194.167.90.1
 16  60 ms   58 ms   58 ms   wwwcss.ac-nice.fr [194.167.84.108]

Itinéraire déterminé.
C:\Windows\system32>
```

Trame apres la commande tracert www.ac-nice.fr

No.	Time	Source	Destination	Protocol	Length	Info
28	3.297595	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=1 (no response found!)
29	3.299247	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
31	3.300013	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=1 (no response found!)
33	3.301729	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
34	3.302131	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=1 (no response found!)
35	3.303695	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
46	4.305300	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=2 (no response found!)
47	4.306291	10.73.27.3	172.17.2.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
48	4.306779	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=2 (no response found!)
49	4.307221	10.73.27.3	172.17.2.3	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

ICMP Echo Request et TTL

Frame 28: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{405F72F5-58ED-41...} Ethernet II, Src: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87), Dst: Stormsh1_2a:a8:34 (00:0d:b4:2a:a8:34)

Internet Protocol Version 4, Src: 172.17.2.3, Dst: 141.101.90.104

- 0100 = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0xd1cc (53708)
- 0000 = Flags: 0x0
- ... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 1

- [Expert Info (Note/Sequence): "Time To Live" only 1]
- Protocol: ICMP (1)
- Header Checksum: 0x51f3 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 172.17.2.3
- Destination Address: 141.101.90.104

Internet Control Message Protocol

Message ICMP de la Trame "Time-to-live exceeded"

No.	Time	Source	Destination	Protocol	Length	Info
28	3.297595	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=5
29	3.299247	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live e
31	3.300013	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=5
33	3.301729	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live e
34	3.302131	172.17.2.3	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=5
35	3.303695	10.73.23.242	172.17.2.3	ICMP	134	Time-to-live exceeded (Time to live e

Internet Protocol Version 4, Src: 10.73.23.242, Dst: 172.17.2.3

Internet Control Message Protocol

- Type: 11 (Time-to-live exceeded)
- Code: 0 (Time to live exceeded in transit)
- Checksum: 0x6277 [correct]
- [Checksum Status: Good]
- Unused: 00000000

Internet Protocol Version 4, Src: 172.17.2.3, Dst: 141.101.90.104

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 92
- Identification: 0xd1cc (53708)
- 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 1
- [Expert Info (Note/Sequence): "Time To Live" only 1]
- Protocol: ICMP (1)

Partie Question Trame ICMP et Exceeded

Adresse IP Destination :

- Valeur décimale : 141.101.90.104
- Valeur hexadécimale : 8D 65 5A 68

Champ TTL (Time To Live) :

- Valeur décimale : 1
- Valeur hexadécimale : 0x01

Champ Type ICMP (Echo Request) :

- Valeur décimale : 8
- Valeur hexadécimale : 0x08

Champ Type ICMP (Time-to-live exceeded) :

- Valeur décimale : 11
- Valeur hexadécimale : 0x0B

Code ICMP :

- Valeur décimale : 0 (Time to live exceeded in transit)
- Valeur hexadécimale : 0x00