

TP 4 : ANALYSE DE TRAMES DHCP AVEC WIRESHARK

Sommaire : COMPTE RENDU

Objectifs :

1. Processus d'acquisition d'une adresse IPv4
2. Capture de trames DHCP avec Wireshark
3. Étude de la trame DHCP DISCOVER

1. Processus d'acquisition d'une adresse IPv4.

2. Capture de trames DHCP avec Wireshark

Dans cette partie je vais effectuer des captures de trames DHCP avec Wireshark.

- J'ai constaté en regardant dans mes paramètres de mon ordinateur que l'adresse IP est attribuer automatiquement par le serveur DHCP.

➔ J'ai ouvert une invite de commandes et j'ai saisi la commande ipconfig/all :

```
Invite de commandes
C:\Users\bigbo> ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : BigBob
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: home

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : VirtualBox Host-Only Ethernet Adapter
Adresse physique . . . . . : 0A-00-27-00-00-02
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::a287:600c:8740:947a%2(préféré)
Adresse IPv4. . . . . : 192.168.56.1(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
IAID DHCPv6 . . . . . : 638189607
DUID de client DHCPv6. . . . . : 00-01-00-01-2A-CB-4B-F9-10-6F-D9-4E-23-4F
NetBIOS sur Tcip. . . . . : Activé

Suffixe DNS propre à la connexion. . . : home
Description. . . . . : Realtek 8821CE Wireless LAN 802.11ac P
Adresse physique . . . . . : 10-6F-D9-4E-23-4F
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6. . . . . : 2a01:cb1d:7:8d00:937f:1af2:1a79:ee0(pre
Adresse IPv6 temporaire . . . . . : 2a01:cb1d:7:8d00:5ca5:ef1d:6f8e:71ab(pi
Adresse IPv6 de liaison locale. . . . . : fe80::2509:8a79:9950:6c2e%19(préféré)
Adresse IPv4. . . . . : 192.168.1.20(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 20 octobre 2023 14:35:18
Bail expirant. . . . . : samedi 21 octobre 2023 14:37:54
Passerelle par défaut. . . . . : fe80::4e22:f3ff:fe45:de86%19
192.168.1.1
```

- Quelle est l'adresse IP attribuée par mon serveur DHCP ?

L'adresse IP attribuer par mon routeur est 192.168.1.1

L'état DHCP est activé : oui

Masque de sous réseau est : 255.255.255.0

Le Bail obtenu est : vendredi 20 octobre 2023

Le Bail expirant est : samedi 21 octobre 2023

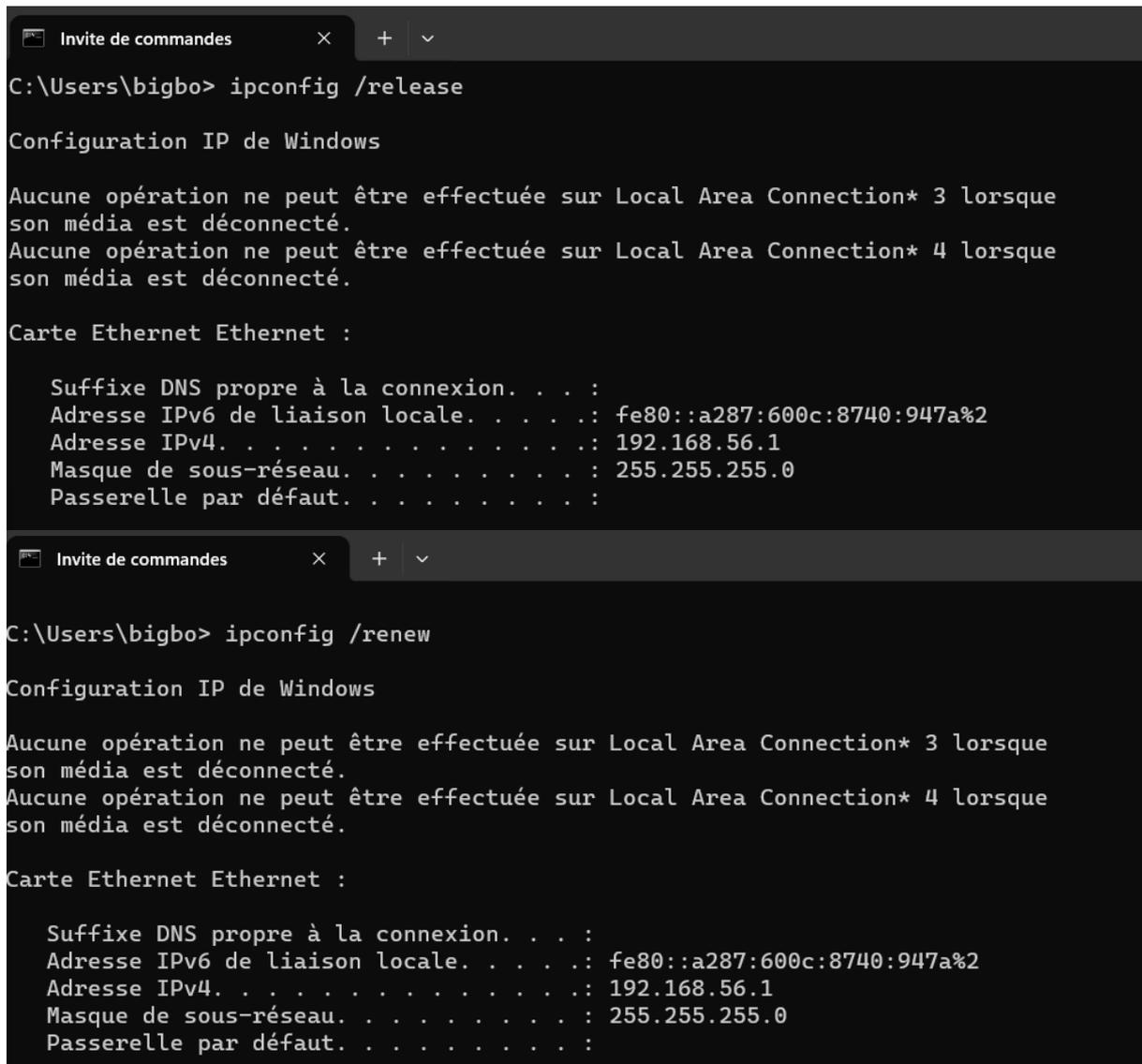
La passerelle par défaut est : 192.168.1.1

Serveur DHCP est : 192.168.1.1

Serveur DNS est : 192.168.1.1

- ➔ J'ai démarré une capture de trames sur Wireshark.
- ➔ J'ai ouvert l'invite de commandes et j'ai tapé successivement les commandes :

- **ipconfig /release**
- **ipconfig /renew**



```
C:\Users\bigbo> ipconfig /release

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Local Area Connection* 3 lorsque
son média est déconnecté.
Aucune opération ne peut être effectuée sur Local Area Connection* 4 lorsque
son média est déconnecté.

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::a287:600c:8740:947a%2
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

C:\Users\bigbo> ipconfig /renew

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Local Area Connection* 3 lorsque
son média est déconnecté.
Aucune opération ne peut être effectuée sur Local Area Connection* 4 lorsque
son média est déconnecté.

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::a287:600c:8740:947a%2
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

- A partir des renseignements obtenus à l'aide de la commande **ipconfig /release**, renseignez les éléments ci-dessous :

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : (censé être 192.168.1.1)

- A partir des renseignements obtenus à l'aide de la commande `ipconfig /renew`, renseignez les éléments ci-dessous :

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : (censé être 192.168.1.1)

➔ Zone Filter : bootp. La capture obtenue :

(Trame 342 DHCP Discover est sélectionnée et la section qui correspond à l'en-tête Ethernet a été développé)

No.	Time	Source	Destination	Protocol	Length	Info
101	62.966532	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release Transaction ID 0xa0c98c3f
287	74.566758	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover Transaction ID 0x71623a1b
288	74.611705	192.168.1.1	192.168.1.20	DHCP	381	DHCP Offer Transaction ID 0x71623a1b
289	74.613024	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request Transaction ID 0x71623a1b
290	74.633347	192.168.1.1	192.168.1.20	DHCP	381	DHCP ACK Transaction ID 0x71623a1b

```
> Frame 287: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF...
Ethernet II, Src: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
  Dynamic Host Configuration Protocol (Discover)
```

4. Étude de la trame DHCP DISCOVER.

Dans cette partie de vais étudier la trame DHCP Discover

- J'ai sélectionné la section Ethernet (en-tête de trame) de la trame DHCP DISCOVER et j'ai identifié les adresses MAC source et destination dans le volet des octets :

L'adresse MAC de source est = 10 : 6f : d9 : 4e : 23 : 4f

L'adresse MAC de destination est = ff : ff : ff : ff : ff : ff

- Caractérissez l'adresse de couche 2 de destination de cette trame :

La couche 2 de destination (ff : ff : ff : ff : ff : ff) est une adresse MAC spéciale qui correspond à une diffusion nommée broadcast à toutes les machines locales. Donc la trame est destinée à être reçue par toutes les machines connectées au même réseau.

- Quel est le champ qui suit immédiatement les deux adresses MAC :

Le champ qui suit immédiatement les deux adresses MAC est le champ Type dans une trame Ethernet. Elle indique le type de protocole encapsulé dans la trame.

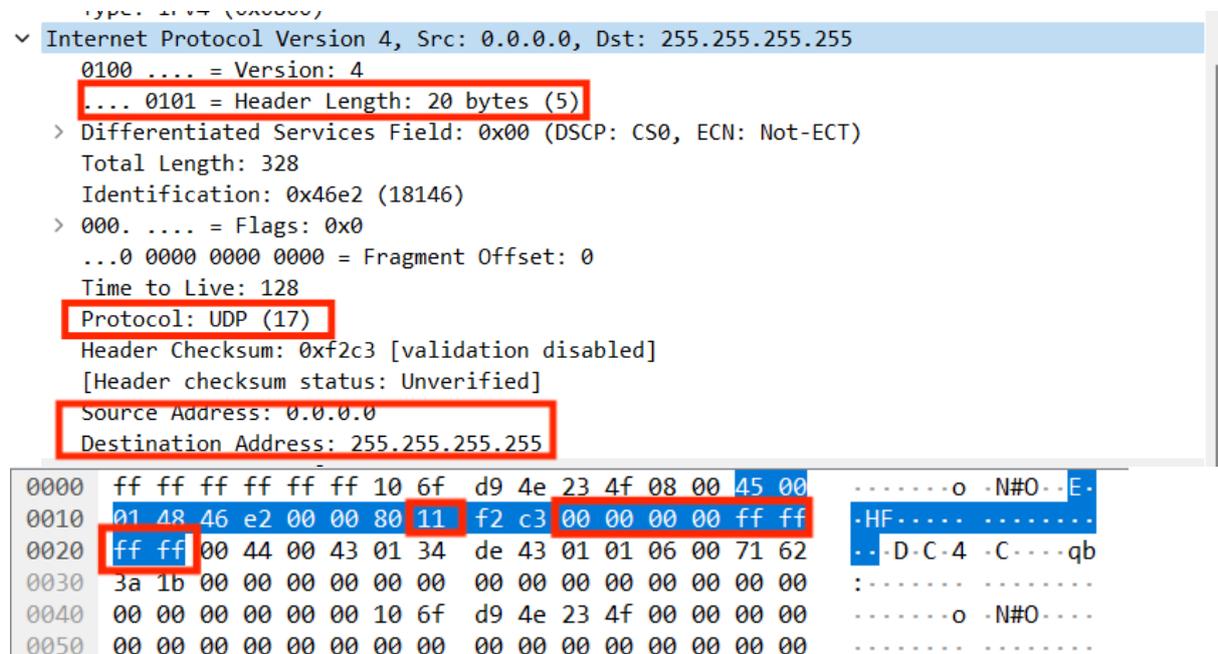
- Quelle valeur contient-il ? Que signifie-t-elle ?

Elle contient la valeur "08 00" qui correspond au champ "Type" de l'en-tête Ethernet. Elle signifie que le protocole de couche supérieure utilisé après l'en-tête Ethernet est IPv4. -> Encapsulée dans un paquet IPv4.

- Quels sont les protocoles inclus dans cette trame ?

Le protocole UDP est inclus dans cette trame.

➔ Sélectionnez comme dans la figure ci-dessous, l'en-tête IP contenu dans la trame DHCP DISCOVER.



```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x46e2 (18146)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xf2c3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
0000  ff ff ff ff ff ff 10 6f  d9 4e 23 4f 08 00 45 00  .....o -N#O--E-
0010  01 48 46 e2 00 00 80 11  f2 c3 00 00 00 00 ff ff  ..HF.....
0020  ff ff 00 44 00 43 01 34  de 43 01 01 06 00 71 62  ..-D-C-4 -C---qb
0030  3a 1b 00 00 00 00 00 00  00 00 00 00 00 00 00 00  :-----
0040  00 00 00 00 00 00 10 6f  d9 4e 23 4f 00 00 00 00  .....o -N#O---
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
```

(Et de paquet : 20 octets (le 10ème est le champ protocole et les 8 derniers sont les IP Source et IP Destination))

- Quel est le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP ? Préciser la valeur de ce champ ainsi que le nom du protocole.

- Renseignez ci-dessous les champs d'en tête IP suivants :

Version = valeur décimale 4 et valeur hexa 45

IHL = valeur décimale 5 et valeur hexa 45

Protocole = valeur décimale 17 et valeur hexa 11

Source address = valeur décimale 0.0.0.0 et valeur hexa 00.00.00.00

Destination address = valeur décimale 255.255.255.255 et valeur hexa ff ff ff ff

- Que signifie la valeur contenue dans le champ adresse IP source ?

L'adresse IP source 00 00 00 00 est utilisé par un client DHCP pour demander une adresse IP au serveur DHCP. Elle indique donc l'absence d'une adresse IP attribuée au client.

- Caractérissez l'adresse de couche 3 de destination de cette trame :

L'adresse de couche 3 destination sert à l'envoi en diffusion elle envoie à toute les machines d'un réseau local.

- ➔ Sélectionnez, comme dans la figure ci-dessous, l'en-tête du datagramme UDP contenu dans la trame DHCP Discover.

User Datagram Protocol, Src Port: 68, Dst Port: 67												
Source Port: 68												
Destination Port: 67												
Length: 308												
Checksum: 0xde43 [unverified]												
0020	ff	ff	00	44	00	43	01	34	de	43	01 01 06 00 71 62	-- .D.C.4 .C qb
0030	3a	1b	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00	:
0040	00	00	00	00	00	00	10	6f	d9	4e	23 4f 00 00 00 00 o N#O
0050	00	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 00
0070	00	00	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00

(Et de datagramme UDP : 8 octets (les 4 1^{er} sont les ports Source et Destination))

- Quel est le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole :

Le champ permettant le démultiplexage des protocoles est le port destination en l'occurrence le port 67 ou 0043 correspondant à DHCP.

- Quel est le port UDP utilisé par le client DHCP ? identifier la valeur hexadécimale correspondante figurant dans le volet des octets :

Le port utilisé par le serveur DHCP est le port source 68 ou 0044

- Quel est le protocole applicatif encapsulé dans le datagramme UDP ?

Le protocole applicatif encapsulé dans le datagramme UDP est le protocole DHCP.

- Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client ?

Le port utilisé par le serveur DHCP pour écouter et recevoir la requête client est le port 68 ou 0044.

➔ Sélectionnez la section Bootstrap Protocol contenu dans la trame DHCP Discover :

No.	Time	Source	Destination	Protocol	Length	Info
101	62.966532	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xa0c98c3f
287	74.566758	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x71623a1b
288	74.611705	192.168.1.1	192.168.1.20	DHCP	381	DHCP Offer - Transaction ID 0x71623a1b
289	74.613024	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x71623a1b
290	74.633347	192.168.1.1	192.168.1.20	DHCP	381	DHCP ACK - Transaction ID 0x71623a1b

```

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x71623a1b
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: CloudNet_4e:23:4f (10:6f:d9:4e:23:4f)
Client hardware address padding: 0000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
v Option: (53) DHCP Message Type (Discover)
  Length: 1
  DHCP: Discover (1)
  
```

0010	01 48 46 e2 00 00 80 11 f2 c3 00 00 00 00 ff ff	-HF.....
0020	ff ff 00 44 00 43 01 34 de 43 01 01 06 00 71 62	...D-C-4 -C....qb
0030	3a 1b 00 00 00 00 00 00 00 00 00 00 00 00 00	:.....
0040	00 00 00 00 00 00 10 6f d9 4e 23 4f 00 00 00 00o -N#0....
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
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110	00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01c- Sc5- =..
0120	10 6f d9 4e 23 4f 32 04 c0 a8 01 14 0c 06 42 69	-o-N#02-Bi
0130	67 42 6f 62 3c 08 4d 53 46 54 20 35 2e 30 37 0e	gBob<-MS FT 5.07-

(Données applicatives BOOTP à partir de l'octet de position 0x10 ligne 0020)