

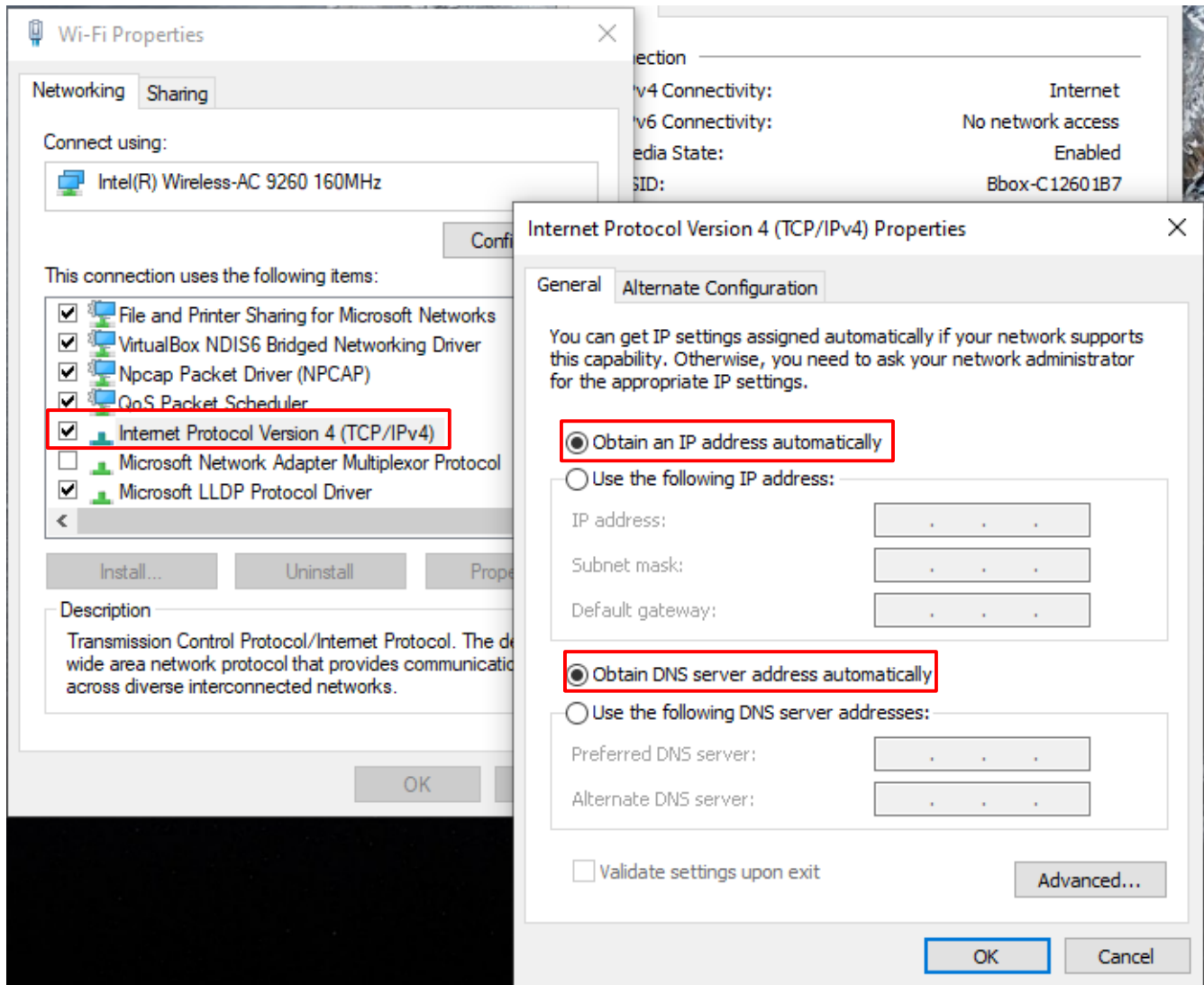
# TP4 : analyse de trames DHCP avec Wireshark

## Sommaire

<i>1. Capture de trames DHCP avec Wireshark.....</i>	<i>2</i>
<i>2. Etude de la trame DHCP DISCOVER.....</i>	<i>6</i>

# 1. Capture de trames DHCP avec Wireshark

→ On modifie les propriétés de **TCP/IPv4** de manière à obtenir les paramètres IP automatiquement :



→ On saisit la commande **ipconfig /all** dans l'invite de commande :

```
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . : lan
    Description . . . . . : Intel(R) Wireless-AC 9260 160MHz
    Physical Address . . . . . : D8-3B-BF-B7-EB-84
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.16(Preferring)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, October 17, 2024 6:05:54 PM
    Lease Expires . . . . . : Friday, October 18, 2024 6:59:39 PM
    Default Gateway . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.254
    DNS Servers . . . . . : 192.168.1.254
    NetBIOS over Tcpi. . . . . : Enabled
```

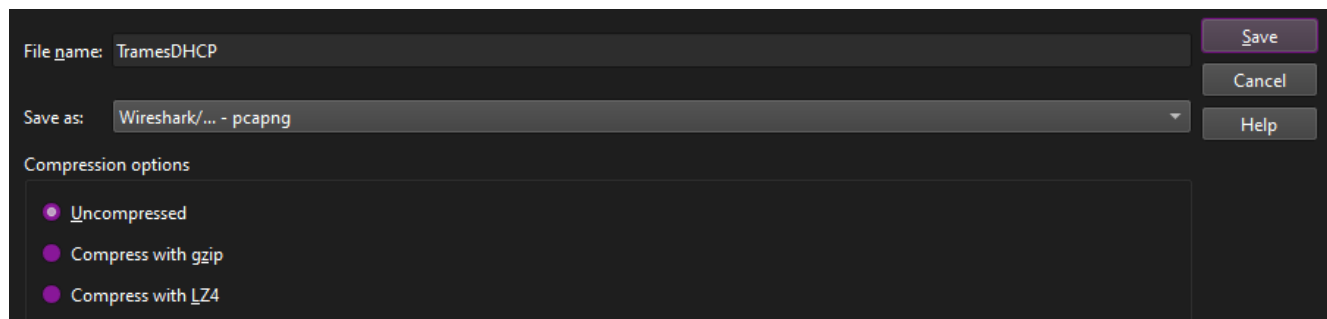
- \* L'adresse IP attribuée par la box est l'adresse **192.168.1.16**
- \* DHCP activé : **Oui**
- \* Masque de sous-réseau : **255.255.255.0**
- \* Bail obtenu : **Jeudi 17 Octobre 2024 18:05:54**
- \* Bail expirant : **Vendredi 18 Octobre 2024 18:59:39**
- \* Passerelle par défaut : **192.168.1.254**
- \* Serveur DHCP : **192.168.1.254**
- \* Serveur DNS : **192.168.1.254**

→ On démarre une **capture de trame** sur WireShark et on tape les commandes **ipconfig /release** puis **ipconfig /renew** pour créer du **trafic** :

No.	Time	Source	Destination	Protocol	Length	Info
71	16.188950	192.168.1.16	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x105d485e
93	23.850377	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x5f910a75
94	23.854397	192.168.1.254	192.168.1.16	DHCP	342	DHCP Offer - Transaction ID 0x5f910a75
95	23.854735	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5f910a75
96	23.857441	192.168.1.254	192.168.1.16	DHCP	363	DHCP ACK - Transaction ID 0x5f910a75

# 4

→ On arrête la capture de trames et on **enregistre** les informations capturées dans un fichier TramesDHCP :



→ Renseignements obtenus à l'aide de la commande **ipconfig /release** :

```
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Default Gateway . . . . . : 
```

- \* Adresse IPv4 : **0.0.0.0 (aucune)**
- \* Masque de sous réseau : **0.0.0.0 (aucun)**
- \* Passerelle par défaut : **255.255.255.255 (broadcast)**

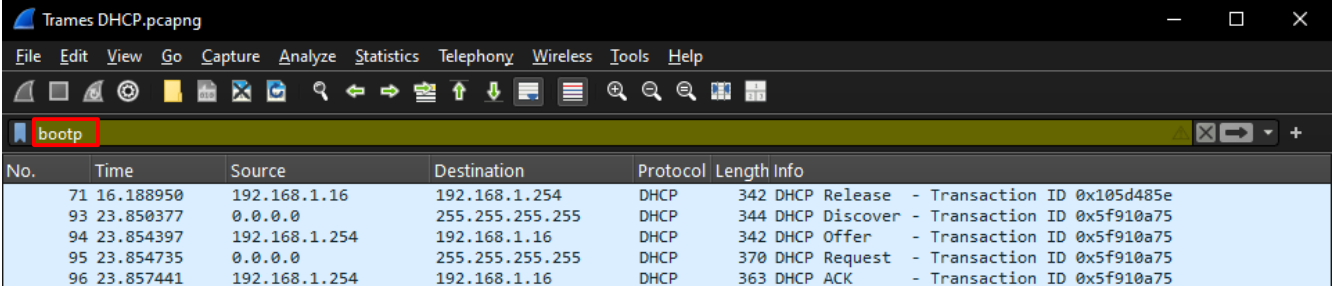
→ Renseignements obtenus à l'aide de la commande **ipconfig /renew** :

```
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : lan
    IPv4 Address. . . . . : 192.168.1.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

- \* Adresse IPv4 : **192.168.1.16**
- \* Masque de sous réseau : **255.255.255.0**
- \* Passerelle par défaut : **192.168.1.254**

→ On ouvre le fichier **TramesDHCP** enregistré juste avant et on applique un filtre **bootp** :



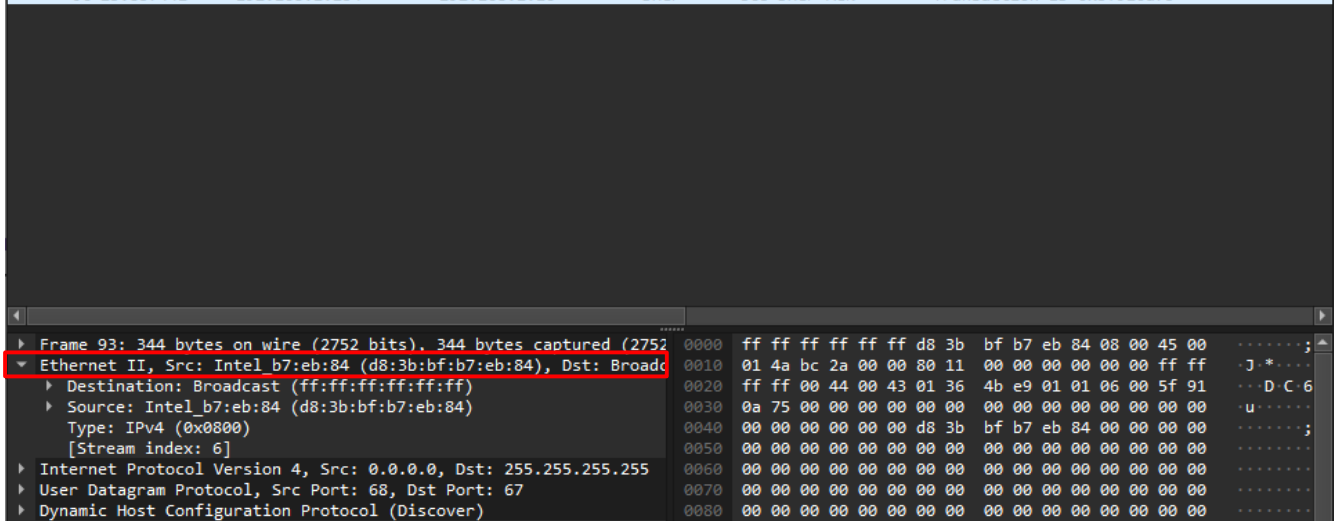
The screenshot shows the Wireshark interface with the file 'Trames DHCP.pcapng' open. A filter 'bootp' is applied to the packet list. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
71	16.188950	192.168.1.16	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x105d485e
93	23.850377	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x5f910a75
94	23.854397	192.168.1.254	192.168.1.16	DHCP	342	DHCP Offer - Transaction ID 0x5f910a75
95	23.854735	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5f910a75
96	23.857441	192.168.1.254	192.168.1.16	DHCP	363	DHCP ACK - Transaction ID 0x5f910a75

## 2. Etude de la trame DHCP DISCOVER

→ On développe l'en-tête Ethernet de la trame DHCP Discover :

71	16.188950	192.168.1.16	192.168.1.254	DHCP	342	DHCP Release	- Transaction ID 0x105d485e
93	23.850377	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0x5f910a75
94	23.854397	192.168.1.254	192.168.1.16	DHCP	342	DHCP Offer	- Transaction ID 0x5f910a75
95	23.854735	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request	- Transaction ID 0x5f910a75
96	23.857441	192.168.1.254	192.168.1.16	DHCP	363	DHCP ACK	- Transaction ID 0x5f910a75

```

Frame 93: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bytes) on interface 0
    Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
      Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Source: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84)
      Type: IPv4 (0x0800)
      [Stream index: 6]
    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)
  
```

\* Adresse MAC source : **FF:FF:FF:FF:FF:FF (broadcast)**

\* Adresse MAC destination : **D8:3B:BF:B7:EB:84**

\* L'adresse de couche 2 de destination de cette trame est une adresse de **broadcast**.

\* Le champ qui suit immédiatement les deux adresses MAC est le champ **Ethertype**.

\* Il contient la valeur **08 00** qui signifie que l'en-tête Ethernet transporte un **paquet IPv4**.

\* Les protocoles inclus dans cette trame sont :

- Le protocole **Ethernet**
- Le protocole **IP**
- Le protocole **UDP**
- Le protocole **DHCP**

→ On développe l'en-tête réseau de la trame **DHCP Discover** :

No.	Time	Source	Destination	Protocol	Length	Info
71	16.188950	192.168.1.16	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x105d485e
93	23.850377	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x5f910a75
94	23.854397	192.168.1.254	192.168.1.16	DHCP	342	DHCP Offer - Transaction ID 0x5f910a75
95	23.854735	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5f910a75
96	23.857441	192.168.1.254	192.168.1.16	DHCP	363	DHCP ACK - Transaction ID 0x5f910a75

Offset	Hex	ASCII
0000	ff ff ff ff ff ff d8 3b bf b7 eb 84 08 00 45 00	.....;.....
0010	01 4a bc 2a 00 00 80 11 00 00 00 00 00 00 ff ff	..J.*....
0020	ff ff 00 44 00 43 01 36 4b e9 01 01 06 00 5f 91	...DC6
0030	0a 75 00 00 00 00 00 00 00 00 00 00 00 00 00	u.....
0040	00 00 00 00 00 00 d8 3b bf b7 eb 84 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	.....
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 01	.....c
0120	d8 3b bf b7 eb 84 32 04 c0 a8 01 10 0c 0f 44 45	.....2
0130	53 4b 54 4f 50 2d 32 43 42 4d 33 46 38 3c 08 4d	.....SKTOP-2C
0140	53 46 54 20 35 2e 30 37 0e 01 03 06 0f 1f 21 2b	.....SFT 5.07

\* Le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP est le champ **Protocole (10ème octet de l'en-tête)**. Ce champ vaut **11** ce qui correspond au protocole **UDP**.

\* Champs de l'en-tête IP :

- Version : **4**

- IHL : **5 / 45**

- Protocole : **17 / 11**

- Adresse source : **0.0.0.0 / 00:00:00:00**

- Adresse destination : **255.255.255.255 / FF:FF:FF:FF**

\* La valeur contenue dans le champ adresse IP source signifie que le client **n'a pas d'adresse IP assignée** et en demande une au serveur DHCP.

\* L'adresse de couche 3 de destination de cette trame est le port DHCP / BOOTP.

→ On développe l'en-tête de transport de la trame DHCP Discover :

```

▶ Frame 93: 344 bytes on wire (2752 bits), 344 bytes captured (2752) on interface 0:00:00:00:00:00
▶ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▼ User Datagram Protocol, Src Port: 68, Dst Port: 67
  Source Port: 68
  Destination Port: 67
  Length: 310
  Checksum: 0x4be9 [Unverified]
  [Checksum Status: Unverified]
  [Stream index: 9]
  [Stream Packet Number: 1]
  ▶ [Timestamps]
    UDP payload (302 bytes)
▶ Dynamic Host Configuration Protocol (Discover)
  0010  01 4a bc 2a 00 00 80 11 00 00 00 00 00 00 ff ff  .J*...
  0020  ff ff 00 44 00 43 01 36 4b e9 01 01 06 00 5f 91  .D.C.6
  0030  0a 75 00 00 00 00 00 00 00 00 00 00 00 00 00  .u.....
  0040  00 00 00 00 00 00 d8 3b bf b7 eb 84 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  .....
  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  .....

```

\* Le nom du champ de l'en-tête de transport permettant le **démultiplexage de protocole** est le champ **port**.

\* Le **port UDP** utilisé par le **client** DHCP est le port **68 (00 44)**.

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

\* Le **port UDP** utilisé par le **serveur** DHCP pour écouter et recevoir la requête du client est le port **67 (00 43)**.

→ On développe la section **Bootstrap Protocol** contenu dans la trame DHCP Discover :

```

▼ Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x5f910a75
  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: Intel_b7:eb:84 (d8:3b:bf:b7:eb:84)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (61) Client identifier
  ▶ Option: (50) Requested IP Address (192.168.1.16)
  ▶ Option: (12) Host Name
  ▶ Option: (60) Vendor class identifier
  ▶ Option: (55) Parameter Request List
  ▶ Option: (255) End

```