

TP 4 : Analyse de Trames DHCP avec Wireshark

SOMMAIRE :

1. Processus d'acquisition d'une adresse IPv4.....	2
2. Capture de trames avec WireShark.....	3
3. Analyse des trames DHCP.....	5
4. Etude du message DHCP.....	6

Objectifs :

L'objectif de ce TP est de **comprendre et analyser le fonctionnement du protocole DHCP (Dynamic Host Configuration Protocol)** à travers la capture et l'étude des trames réseau échangées entre un **client** et un **serveur DHCP**.

À l'aide de **Wireshark**, nous observons les différentes étapes du processus d'attribution d'adresse IP (Discover, Offer, Request, Ack) et identifions les **champs importants** des en-têtes **Ethernet, IP et UDP**.

1. Processus d'acquisition d'une adresse IPv4

La commande **ipconfig /all** permet d'afficher **toutes les informations de configuration réseau** d'un ordinateur sous Windows.

```
C:\Windows\System32> ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : G102-GB03
Suffixe DNS principal . . . . . : prince.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: prince.local

Carte Ethernet vEthernet (Default Switch) :

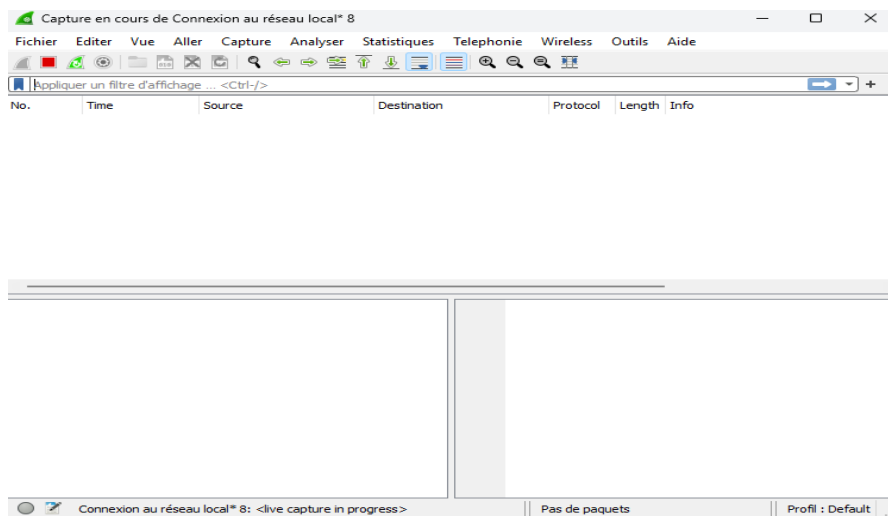
Suffixe DNS propre à la connexion. . . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Adresse physique . . . . . : 00-15-5D-0A-A9-34
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::3d30:e745:d20f:b8a8%27(préféré)
Adresse IPv4. . . . . : 172.21.128.1(préféré)
Masque de sous-réseau. . . . . : 255.255.240.0
Passerelle par défaut. . . . . :
IAID DHCPv6 . . . . . : 452990301
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-C9-F4-B9-74-56-3C-2F-9C-F7
NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . : prince.local
Description . . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 74-56-3C-2F-9C-F7
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . : 172.17.2.8(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mercredi 1 octobre 2025 09:55:18
Bail expirant. . . . . : mercredi 1 octobre 2025 10:45:22
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
Serveurs DNS. . . . . : 172.17.254.1
```

2. Capture de trames DHCP avec Wireshark

J'initie une capture de trames réseau à l'aide de **Wireshark**. Depuis l'**invite de commandes Windows**, j'exécute ensuite les commandes successives permettant de libérer et de renouveler l'adresse IP attribuée par le serveur DHCP.



ipconfig /release libère l'adresse IP actuelle du poste. L'ordinateur se déconnecte temporairement du réseau, car il n'a plus d'adresse IP.

```
C:\Windows\System32> ipconfig /release
Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::3d30:e745:d20f:b8a8%27
    Adresse IPv4. . . . . : 172.21.128.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::e973:6dc5:ff6f:f6e%13
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

ipconfig /renew demande ensuite une **nouvelle adresse IP** au serveur DHCP

```
C:\Windows\System32 ipconfig /renew
Configuration IP de Windows

Carte Ethernet Ethernet :

  Suffixe DNS propre à la connexion. . . : prince.local
  Adresse IPv4. . . . . : 172.17.2.8
  Masque de sous-réseau. . . . . : 255.255.0.0
  Passerelle par défaut. . . . . : 172.17.250.3
```

Paramètre	Valeur
Adresse IP attribuée	172.17.2.8
DHCP activé	Oui
Masque de sous-réseau	255.255.0.0
Bail obtenu	01/10/2025 – 09:55:18
Bail expirant	01/10/2025 – 10:45:22
Passerelle	172.17.2.8
Serveur DHCP	172.17.254.1 (<i>serveur « ROI »</i>)
Serveur DNS	172.17.254.1

3. Analyse des trames DHCP

No.	Time	Source	Destination	Protocol	Length	Info
5	0.598240	172.17.2.8	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0x339a1af
48	5.223772	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3dbcd009
49	5.224791	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0x3dbcd009
50	5.225173	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x3dbcd009
51	5.226234	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x3dbcd009
52	5.227470	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x3dbcd009

Frame 48: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF...
Ethernet II, Src: Giga-Byt_2f:9c:f7 (74:56:3c:2f:9c:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: Giga-Byt_2f:9c:f7 (74:56:3c:2f:9c:f7)
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)

```
0000 ff ff ff ff ff 74 56 3c 2f 9c f7 08 00 45 00 .....tV c/...E-
0010 01 48 63 43 00 00 00 11 00 00 00 00 00 ff ff ...HcC... ).....
0020 ff ff 00 44 00 43 01 34 29 d2 01 01 06 00 3d bc ...D C 4 ).....
0030 d0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0040 00 00 00 00 00 00 74 56 3c 2f 9c f7 00 00 00 ...tV c/.....
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 63 b2 53 63 35 01 01 3d 07 01 ...c Sc5...
0120 74 56 3c 2f 9c f7 32 04 ac 11 02 08 0c 09 47 31 tV c/ - 2 .....G1
0130 30 32 2d 47 42 30 33 3c 08 4d 53 46 54 20 35 2e 02-GB03< MSFT 5.
0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07..... +,./wy
0150 fc ff 00 00 00 00
```

Interprétation de la capture DHCP dans Wireshark

- La **partie supérieure** de la fenêtre montre la **liste des trames capturées**, avec pour chaque paquet : le **numéro**, le **temps**, la **source**, la **destination**, le **protocole** et une **description** du message DHCP (Discover, Offer, Request, Ack).
→ Elle permet de suivre le **dialogue complet** entre le client et le serveur DHCP.
- La **partie centrale** affiche le **détail du paquet sélectionné**, c'est-à-dire les informations des **différentes couches du modèle TCP/IP : Ethernet, IP, UDP et DHCP**.
→ Elle sert à analyser les champs des en-têtes et à comprendre comment les données sont encapsulées.
- La **partie inférieure** montre la **trame en hexadécimal**, c'est-à-dire les **données brutes** telles qu'elles ont circulé sur le réseau.
→ Elle permet de vérifier les valeurs exactes des champs (adresses, ports, identifiants...).

Pourquoi avoir filtré bootp ?

Le protocole **DHCP** est en réalité une **extension du protocole BOOTP**.
En filtrant bootp dans Wireshark, on affiche donc **uniquement les trames DHCP/BOOTP**, ce qui permet :

- De se concentrer sur les échanges **DHCP** (Discover, Offer, Request, Ack),

4. Étude du message DHCP

- **Caractérisez l'adresse de couche 2 de destination de cette trame :**

L'adresse MAC de destination est **inconnue** et contient la **valeur maximale en hexadécimal : ff:ff:ff:ff:ff:ff**

Cette valeur correspond à une **adresse de broadcast**, utilisée pour diffuser la trame à **tous les hôtes du réseau local**.

Elle est employée ici car le client ne connaît pas encore l'adresse du serveur DHCP.

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

Le champ situé juste après les adresses MAC est le **champ EtherType**, qui indique le **protocole de couche supérieure** encapsulé dans la trame Ethernet.

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

Le champ EtherType contient la valeur **0x0800**, ce qui signifie que la trame transporte un **paquet IPv4**.

Cela indique donc que la couche supérieure utilisée est le **protocole Internet (IP)**.

- **Quels sont les protocoles inclus dans cette trame ?**

Les protocoles encapsulés dans cette trame, du plus bas au plus haut niveau, sont :

- **Ethernet II** → couche liaison (couche 2)

- **IPv4** → couche réseau (couche 3)
- **UDP** → couche transport (couche 4)
- **DHCP** → couche application (couche 7)

```

> Frame 48: 342 bytes on wire (2736 bits), 342 bytes cap
> Ethernet II, Src: Giga-Byt_2f:9c:f7 (74:56:3c:2f:9c:f7
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.25
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN
    Total Length: 328
    Identification: 0x6343 (25411)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 0.0.0.0
  Destination Address: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
0000 ff ff ff ff ff 74 56 3c 2f 9c f7 08 00 45 00 .....tV </.....E.
0010 01 48 63 43 00 00 80 11 00 00 00 00 00 00 ff ff ..HcC.....
0020 fff ffi 00 44 00 43 01 34 29 d2 01 01 06 00 3d bc ..D.C.4 ).....=
0030 d0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 .....tV </.....
0040 00 00 00 00 00 00 74 56 3c 2f 9c f7 00 00 00 .....
0050 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 .....
0070 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 .....
0090 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 .....
00b0 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 .....
00d0 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 .....
00f0 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 .....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01 .....c. Sc5...=
0120 74 56 3c 2f 9c f7 32 04 ac 11 02 08 0c 09 47 31 tV</..2.....G1
0130 30 32 2d 47 42 30 33 3c 08 4d 53 46 54 20 35 2e 02-GB03<MSFT 5.
0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07.....!+.,/wy.

```

▪ **Champ qui indique le protocole de transport :**

Le protocole de transport est indiqué dans le **champ “Protocole”** de l’en-tête IP

Sa **valeur est 17 en décimal (soit 0x11 en hexadécimal)**, ce qui correspond au **protocole UDP**.

Les messages **DHCP** transitent donc via **UDP**

• **Champs d’en-tête IP :**

Champ	Valeur décimale	Valeur hexadécimale	Interprétation
Version	4	—	IPv4
IHL	5	0x05	Longueur d’en-tête = 5 × 4 = 20 octets
Protocole	17	0x11	UDP
Adresse source	0.0.0.0	00 00 00 00	Le client n’a pas encore d’adresse IP
Adresse destination	255.255.255.255	FF FF FF FF	Adresse de broadcast (diffusion)

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

L'adresse IP source est **0.0.0.0**.

Cette valeur indique que le client **n'a pas encore d'adresse IP** attribuée (il n'a pas encore reçu de configuration du serveur DHCP).

Il utilise donc **0.0.0.0** comme adresse temporaire pour se présenter sur le réseau.

Caractérisiez l'adresse de couche 3 de destination de cette trame :

L'adresse IP de destination est **255.255.255.255**, c'est-à-dire **l'adresse de broadcast IPv4**.

Elle permet d'envoyer le message à **tous les hôtes du réseau local**, afin que le serveur DHCP puisse recevoir la requête du client même sans connaître encore son adresse IP.

```
Frame 48: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF...
Ethernet II, Src: GigaByteTech 2f:9c:f7 (74:56:3c:2f:9c:f7), 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: 300
  Checksum: 0x29d2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (300 bytes)
Dynamic Host Configuration Protocol (Discover)
0000 ff ff ff ff ff 74 56 3c 2f 9c f7 08 00 45 00
0010 01 48 63 43 00 00 80 11 00 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 31 34 29 d7 01 01 06 00 3d bc
0030 d0 09 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 74 56 3c 2f 9c f7 08 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 63 42 53 63 35 01 01 3d 07 01
0120 74 56 3c 2f 9c f7 32 04 ac 11 02 08 0c 09 47 31
0130 30 32 2d 47 42 30 33 3c 08 4d 53 46 54 20 35 2e
0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9
0150 fc ff 00 00 00 00
```

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

▪ **Quel est le port UDP utilisé par le client DHCP ?**

Identifier la valeur hexadécimale correspondante figurant dans le volet des octets (octets de position 0×02 et 0×03 ligne 0020) :

- **Port UDP client DHCP : 68**
- **Valeur hexadécimale : 0x0044**
- **Explication : Ce port (68) est réservé au client DHCP (BOOTP client) pour l'envoi des requêtes vers le serveur.**

▪ **Quel est le protocole applicatif encapsulé dans le datagramme UDP ?**

- **Protocole applicatif : DHCP**
- **Nom complet : *Dynamic Host Configuration Protocol***
- **Rôle : Permet au client d'obtenir automatiquement une adresse IP et les paramètres réseau depuis un serveur DHCP.**

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

Identifier la valeur hexadécimale correspondante figurant dans le volet des octets :

- **Port UDP serveur DHCP : 67**
- **Valeur hexadécimale : 0x0043**
- **Explication : Le port 67 est utilisé par le serveur DHCP (BOOTP server) pour recevoir les requêtes envoyées par les clients.**

▪ **Que contient le premier champ de la section Bootstrap Protocol pour cette trame DHCP ?**

- **Valeur : 1**

- **Signification : Boot Request**

- **Explication :**

Le champ “op” (operation code) du protocole BOOTP vaut :

- **1 → Boot Request** : message émis par le **client** vers le serveur
- **2 → Boot Reply** : message émis par le **serveur** vers le client

Dans le cas d'un **DHCP Discover**, le client cherche un serveur DHCP, donc c'est bien un **Boot Request**.

▪ **Quelle est la valeur de l'option DHCP indiquant le type de message DHCP ?**

- **Valeur : 1**

- **Signification : DHCP DISCOVER**

- **Explication :**

Cette option indique le type précis du message DHCP :

- **1 → DHCP Discover** (recherche d'un serveur)