

Suiveng
Matéo

TP4 Boucly

Table des matières

- 1. Capture de trames DHCP avec Wireshark.2
- 2. Etude de la trame DHCP DISCOVER.3

1. Capture de trames DHCP avec Wireshark.

Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?

```
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 326391356
```

L'adresse IP attribuée par le serveur DHCP est 172.17.254.1

Renseignez les autres éléments ci-dessous :

DHCP activé: oui

Masque de sous-réseau: 255.255.0.0

Bail obtenu: mercredi 1 octobre 2025 09:56:12

Bail expirant: mercredi 1 octobre 2025 10:41:50

Passerelle par défaut: 172.17.250.3

Serveur DHCP: 172.17.254.1

Serveur DNS: 172.17.254.1

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . : prince.local
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 74-56-3C-2F-9C-CD
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::799d:d2f6:3731:5c6b%3(préfééré)
Adresse IPv4. . . . . : 172.17.2.5(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mercredi 1 octobre 2025 09:56:12
Bail expirant. . . . . : mercredi 1 octobre 2025 10:41:50
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 326391356
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-CA-1B-A7-74-56-3C-2F-9C-CD
Serveurs DNS. . . . . : 172.17.254.1
NetBIOS sur TcPIP. . . . . : Activé
```

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

Adresse IPv4: Il n'y a pas d'adresse IPv4 car elle est libérée

Masque de sous-réseau:il n'y a pas de masque de sous-réseau
Passerelle par défaut: il n'y a pas de passerelle par défaut

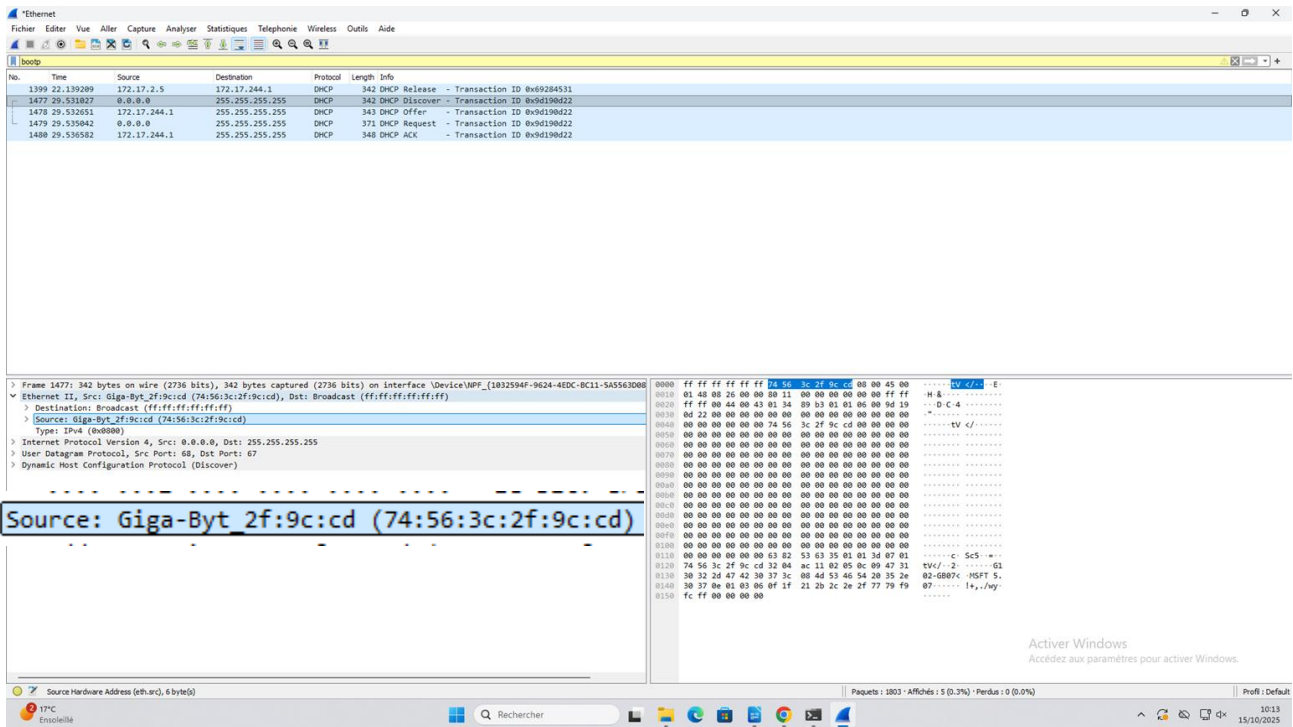
```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . . :  
Adresse IPv6 de liaison locale. . . . . : fe80::799d:d2f6:3731:5c6b%3  
Passerelle par défaut. . . . . :
```

A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :
Adresse IPv4:172.17.2.5
Masque de sous-réseau:255.255.0.0
Passerelle par défaut: 172.17.250.3

2. Etude de la trame DHCP DISCOVER.

- Sélectionnez, comme dans la figure ci-dessus, la section Ethernet (en-tête de trame) de la trame DHCPDISCOVER et identifiez les adresses MAC source et destination dans le volet des octets :

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several DHCP-related packets. Packet 1477 is a DHCP Discover packet from source 172.17.2.5 to destination 255.255.255.255. The packet details pane is expanded to show the Ethernet II header, where the destination MAC address is highlighted as ff:ff:ff:ff:ff:ff. The packet bytes pane shows the raw data of the frame, with the destination MAC address also highlighted in blue.



- Caractérissez l'adresse de couche 2 de destination de cette trame :
 C'est une adresse de broadcast (diffusion), c'est-à-dire que la trame est envoyée à toutes les machines du réseau local. (Tous les bits sont à 1 : ff:ff:ff:ff:ff:ff),

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

Le champ suivant est le champ "Type" (EtherType).

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

Valeur : 0x0800

Signification : Ce champ indique que la trame transporte un paquet IPv4.

- Quels sont les protocoles inclus dans cette trame ?

- Ethernet II
- IPv4
- UDP
- DHCP (Discover)

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

- Quel est le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP ?

Le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP est le champ protocol

Préciser la valeur de ce champ ainsi que le nom du protocole.

La valeur de ce champ est «11», et le nom du protocole est UDP

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

Version = IPv4

IHL (val. déci. et hexa.) = 20 bytes (val. décimale : 20, hexa : 0x14)

Protocole (val. déci. et hexa.) = 17 (0x11)

Source address (val. déci. et hexa.) = 0.0.0.0 (0x00000000)

Destination address (val. déci. et hexa.) =
255.255.255.255(0xFFFFFFFF)

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

La valeur 0.0.0.0 signifie que l'émetteur ne possède pas encore d'adresse IP attribuée.

C'est le cas lors d'un DHCP Discover, envoyé avant l'obtention d'une adresse.

- Caractérisiez l'adresse de couche 3 de destination de cette trame :
L'adresse 255.255.255.255 est une adresse de broadcast IPv4. Cela signifie que le message est envoyé à tous les hôtes du réseau local (diffusion).

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

The screenshot shows a Wireshark capture of a DHCP Discover packet. The left pane displays the packet tree with the following structure:

- > Frame 100: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on Interface \Device\NPF_{1032594F-9624-4EDC-BC11-5A5563D088}
- > Ethernet II, Src: Giga-Byt_2f:9c:cd (74:56:3c:2f:9c:cd), 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: 308
 - Checksum: 0x1a37 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 10]
 - > [Timestamps]
 - UDP payload (300 bytes)
- > Dynamic Host Configuration Protocol (Discover)

The right pane shows the packet bytes in hexadecimal and ASCII. The UDP header is highlighted in blue, showing the source port 68 and destination port 67.

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

Le nom du champ de l'ent-tête de transport permettant le démultiplexage de protocole est UDP au port destination

Quel est le port UDP utilisé par le client DHCP ? Identifier la valeur hexadécimale correspondante figurant dans le volet des octets (octets de position 0x02 et 0x03 ligne 0020) ;

Les valeurs hexadécimale sont :

00 44 en hexa qui est 68 en décimale
Ce qui correspond à DHCP client request

Quel est le protocole applicatif encapsulé dans le datagramme UDP ?

Le protocole applicatif est 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.

00 43 en hexa qui est de 67 en décimale
Correspond à DHCP serveur reply

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

The screenshot displays a network packet capture analysis tool. On the left, the 'Dynamic Host Configuration Protocol (Discover)' section is expanded, showing the 'Message type: Boot Request (1)'. Below this, various fields are listed, including 'Hardware type: Ethernet (0x01)', 'Transaction ID: 0x5e5a5ef1', and 'Option: (53) DHCP Message Type (Discover)'. On the right, the hex data is shown in a table format, with the first few lines corresponding to the DHCP Discover message structure.

0000	ff	ff	ff	ff	ff	74	56	3c	2f	9c	cd	08	00	45	00EV </.....E
0010	01	48	08	24	00	00	80	11	00	00	00	00	00	ff	ff	..H.S.....<.....Z
0020	ff	ff	00	44	00	43	01	34	76	a3	01	06	00	5e	5a	...D.C.4 v.....Z
0030	5e	f1	00	00	00	00	00	00	00	00	00	00	00	00	00	^.....<.....>
0040	00	00	00	00	00	74	56	3c	2f	9c	cd	00	00	00	00EV </.....
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	82	53	63	35	01	01	34	87	01c.SCS.....
0120	74	56	3c	2f	9c	cd	32	04	ac	11	02	05	0c	09	47	31tV</.....G1
0130	30	32	2d	47	42	30	37	3c	08	4d	53	46	54	20	35	2e02-GB07<..MSFT.5.
0140	30	37	0e	01	03	06	0f	1f	21	2b	2c	2e	2f	77	79	f907.....t+.,/ny?
0150	fc	ff	00	00	00	00	00	00	00	00	00	00	00	00	00<.....>