

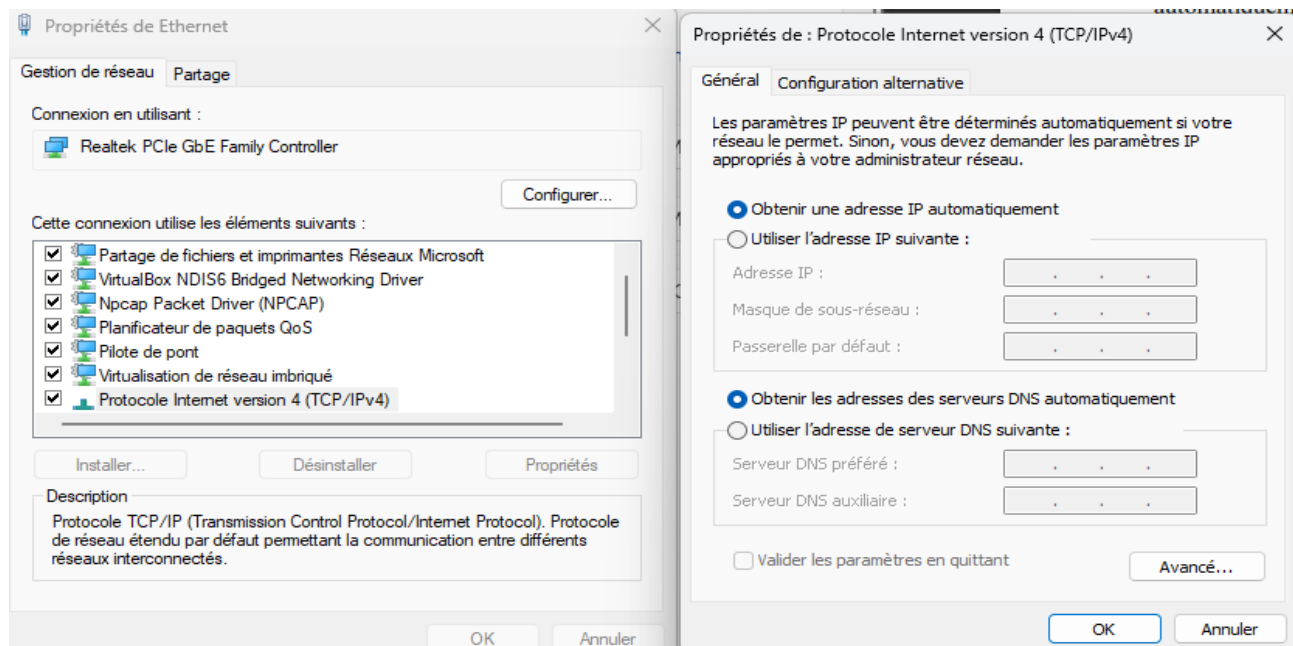
# TP4 : analyse de trames DHCP avec Wireshark

## SOMMAIRE :

2. Capture de trames DHCP avec Wireshark.....	2
4. Etude de la trame DHCP DISCOVER.....	5

## 2. Capture de trames DHCP avec Wireshark

J'ai affiché les connexion réseau dans les paramètres



J'ai effectué la commande : ipconfig /all

```
C:\Users\Mnovello>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : G102-GB18
    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 Ethernet :

    Suffixe DNS propre à la connexion. . . : prince.local
    Description. . . . . : Realtek PCIe GbE Family Controller
    Adresse physique . . . . . : 74-56-3C-2F-9D-13
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::35af:39f7:fd41:8705%15(préfééré)
    Adresse IPv4. . . . . : 172.17.2.13(préfééré)
    Masque de sous-réseau. . . . . : 255.255.0.0
    Bail obtenu. . . . . : mercredi 1 octobre 2025 08:08:58
    Bail expirant. . . . . : mercredi 1 octobre 2025 11:11:59
    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-DD-CE-E0-74-56-3C-2F-9D-13
    Serveurs DNS. . . . . : 172.17.254.1
    NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Description. . . . . : VirtualBox Host-Only Ethernet Adapter
    Adresse physique . . . . . : 0A-00-27-00-00-11
    DHCP activé. . . . . : Non
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::3600:e406:54dd:5d8a%17(préfééré)
    Adresse IPv4. . . . . : 192.168.56.1(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
    IAID DHCPv6 . . . . . : 302645287
    DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DD-CE-E0-74-56-3C-2F-9D-13
    NetBIOS sur Tcpip. . . . . : Activé
```

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

L'adresse IP attribué par le serveur DHCP ROI est 172.17.2.13

- DHCP activé : oui
- Masque de sous-réseau : 255.255.0.0
- Bail obtenu : mercredi 1 octobre 2025 08:08:58
- Bail expirant : mercredi 1 octobre 2025 11:11:59
- Passerelle par défaut : 172.17.250.3
- Serveur DHCP : 172.17.254.1
- Serveur DNS : 172.17.254.1

J'ai effectué la commande ipconfig /release

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

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::35af:39f7:fd1:8705%15
    Passerelle par défaut. . . . . : 

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::3600:e406:54dd:5d8a%17
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::6c81:bedd:e515:9075%20
    Adresse IPv4. . . . . : 172.26.224.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :
```

J'ai effectué la commande ipconfig /renew

```
C:\Users\Mnovello>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : prince.local
    Adresse IPv6 de liaison locale. . . . : fe80::35af:39f7:fd1:8705%15
    Adresse IPv4. . . . . : 172.17.2.13
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.3

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::3600:e406:54dd:5d8a%17
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet vEthernet (Default Switch) :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
```

## En amont j'ai effectué une capture de trames

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.244.14	224.0.0.252	IGMPv2	60	Membership Report group 224.0.0.252
2	0.147721	172.17.2.12	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
3	0.235735	172.17.2.12	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
4	0.255880	172.17.243.11	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
5	0.808581	01:00:00:00:00:00	Broadcast	ARP	60	Iho has 172.17.244.17 Tell 172.17.254.1
6	1.698862	01:00:00:00:00:00	Broadcast	ARP	60	Iho has 172.17.244.17 Tell 172.17.254.1
7	2.231777	172.17.2.19	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
8	2.611438	172.17.2.19	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
9	2.699868	01:00:00:00:00:00	Broadcast	ARP	60	Iho has 172.17.244.17 Tell 172.17.254.1
10	2.791268	172.17.2.22	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
11	3.152632	172.17.2.22	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
12	3.395141	172.17.2.6	224.0.0.2	IGMPv2	60	Leave Group 224.168.100.1
13	3.312411	172.17.2.6	224.0.0.2	IGMPv2	60	Leave Group 224.168.100.1
14	3.414331	172.17.2.6	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
15	3.608093	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.168.100.1
16	3.615463	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.168.100.1
17	3.615669	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
18	3.616193	172.17.2.6	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
19	3.633181	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
20	3.883434	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
21	3.898810	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
22	3.998232	172.17.250.7	172.17.255.255	UDP	201	4554 → 4554 Len=239
23	4.966923	172.17.2.12	224.0.0.251	PDNS	85	Standard query 0x0000 PTR microsoft_mcc_top.local, "QI" question
24	4.966923	fe80::931a:159f:52a:f821:f8	224.168.100.1	PDNS	105	Standard query 0x0000 PTR microsoft_mcc_top.local, "QI" question
25	5.535546	172.17.2.16	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
26	5.982357	172.17.2.12	224.0.0.251	PDNS	85	Standard query 0x0000 PTR microsoft_mcc_top.local, "QI" question
27	5.982357	fe80::931a:159f:52a:f821:f8	224.168.100.1	PDNS	105	Standard query 0x0000 PTR microsoft_mcc_top.local, "QI" question
28	6.000000	172.17.2.16	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1

## La trame DHCP release est la suivante :

No.	Time	Source	Destination	Protocol	Length	Info
36	12.563917	172.17.2.5	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x53136ac7
54	12.701829	172.17.2.13	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0x81dc9c9f
128	18.823256	172.17.5.31	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x393978a8
201	23.823970	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6f56559f
202	23.825058	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0x6f56559f
203	23.826533	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x6f56559f
204	23.827933	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x6f56559f

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

Adresse IPv4 : 0.0.0.0

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.3

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

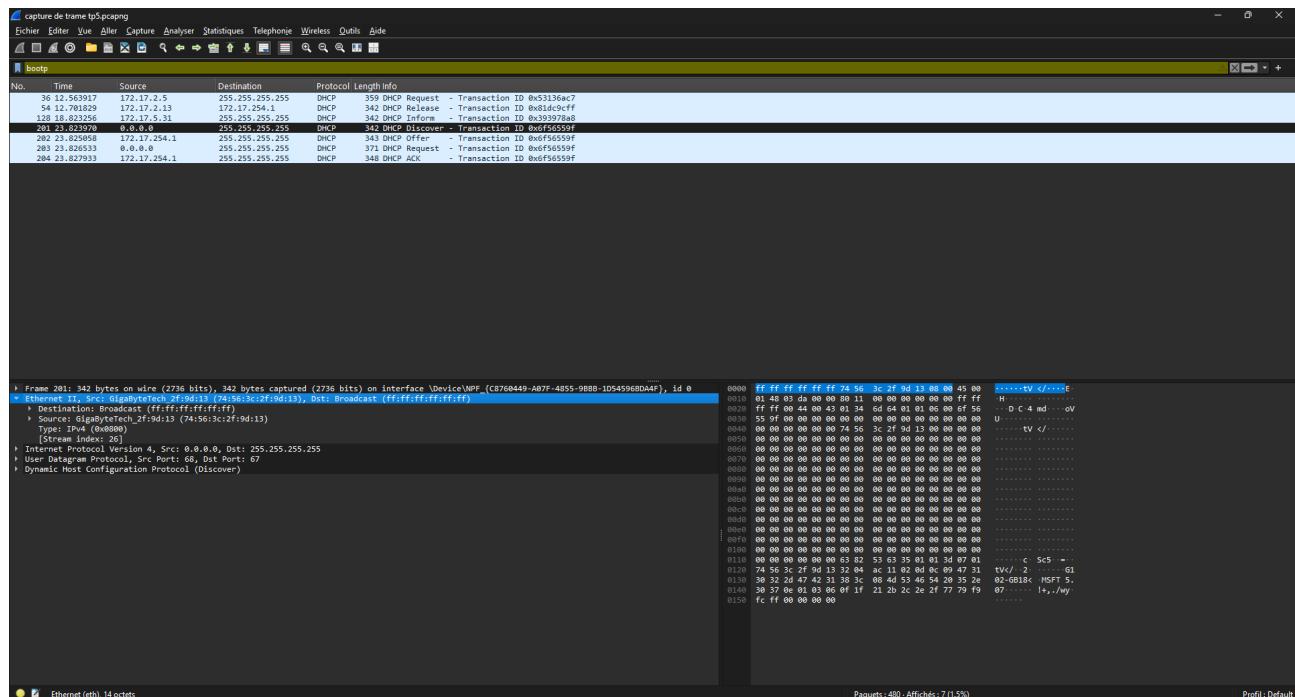
Adresse IPv4 : 172.17.254.1

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.3

## 4. Etude de la trame DHCP DISCOVER.

J'ai sélectionné la section Ethernet de la trame DHCPDISCOVER



■ 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 :

Mac S : 0.0.0.0 = ff ff ff ff ff ff

Mac D : 255.255.255.255 = 74 56 3c 2f 9d 13

■ Caractérisez l'adresse de couche 2 de destination de cette trame :

C'est une trame Broadcast diffusion elle permet d'envoyer la trame à toute les machines du réseau local

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

Le champ qui suit immédiatement les 2 adresses mac est le champ Ethertype (0800)

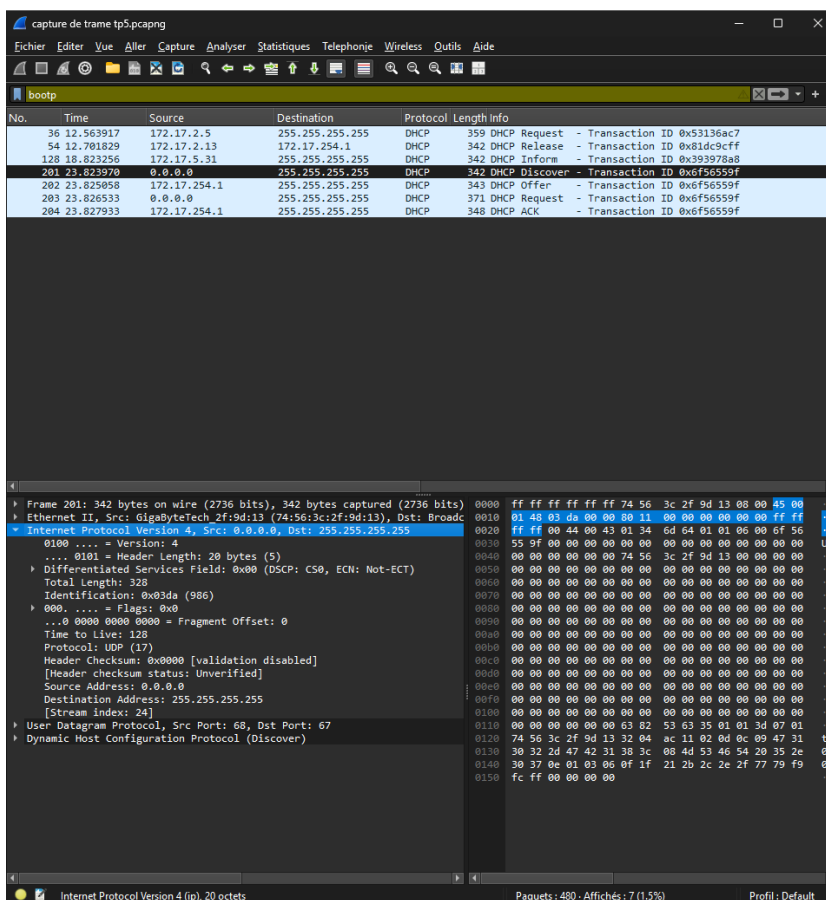
■ Quelle valeur contient-il ? Que signifie t-elle ?

La valeur est 0800 cela signifie que la trame transporte un paquet IPv4

■ Quels sont les protocoles inclus dans cette trame ?

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

J'ai sélectionné l'en tête IP contenue dans la trame DHCP Discover



▪ 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.

Le champ qui permet de connaître le protocole de transport est Protocole la valeur est 17

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

Version = 4

IHL (val. déci. et hexa.) = 20 = 45

Protocole (val. déci. et hexa.) = 17 = 11

Source address (val. déci. et hexa.) = 0.0.0.0 = 00 00 00 00

Destination address (val. déci. et hexa.) = 255.255.255.255 = ff ff ff ff

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

Cela signifie que le client DHCP ne possède pas encore d'adresse IP

▪ Caractériser l'adresse de couche 3 de destination de cette trame :

c'est une adresse de diffusion Broadcast car l'adresse 255.255.255.255 indique que le message est reçu par tout les hôtes du serveur local

```

> Frame 201: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: GigaByteTech_2f:9d:13 (74:56:3c:2f:9d:13), Dst: Broadcast
> 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: 0x6d64 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 22]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (300 bytes)
> Dynamic Host Configuration Protocol (Discover)
  0000 ff ff ff ff ff ff 74 56 3c 2f 9d 13 08 00 45 00 ...
  0010 01 48 03 da 00 00 80 11 00 00 00 00 00 00 ff ff ...
  0020 ff ff 00 44 00 43 01 34 6d 64 01 01 06 00 6f 56 ...
  0030 55 9f 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
  0040 00 00 00 00 00 00 74 56 3c 2f 9d 13 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 ...
  0120 74 56 3c 2f 9d 13 32 04 ac 11 02 0d 0c 09 47 31 ...
  0130 30 32 2d 47 42 31 38 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

```

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

Le nom du champ permettant le démultiplexage sont Source port et Destination 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 0x02 et 0x03 ligne 0020) ;

Le port UDP utilisé par le client DHCP est UDP 68

-ligne = 0020

-position = 00 44

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

Le protocole applicatif encapsulé est DHCP (Dynamic Host Configuration Protocol)

▪ 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.

Le serveur DHCP utilise le port UDP 67 (Destination port) pour écouter et recevoir la requête du client