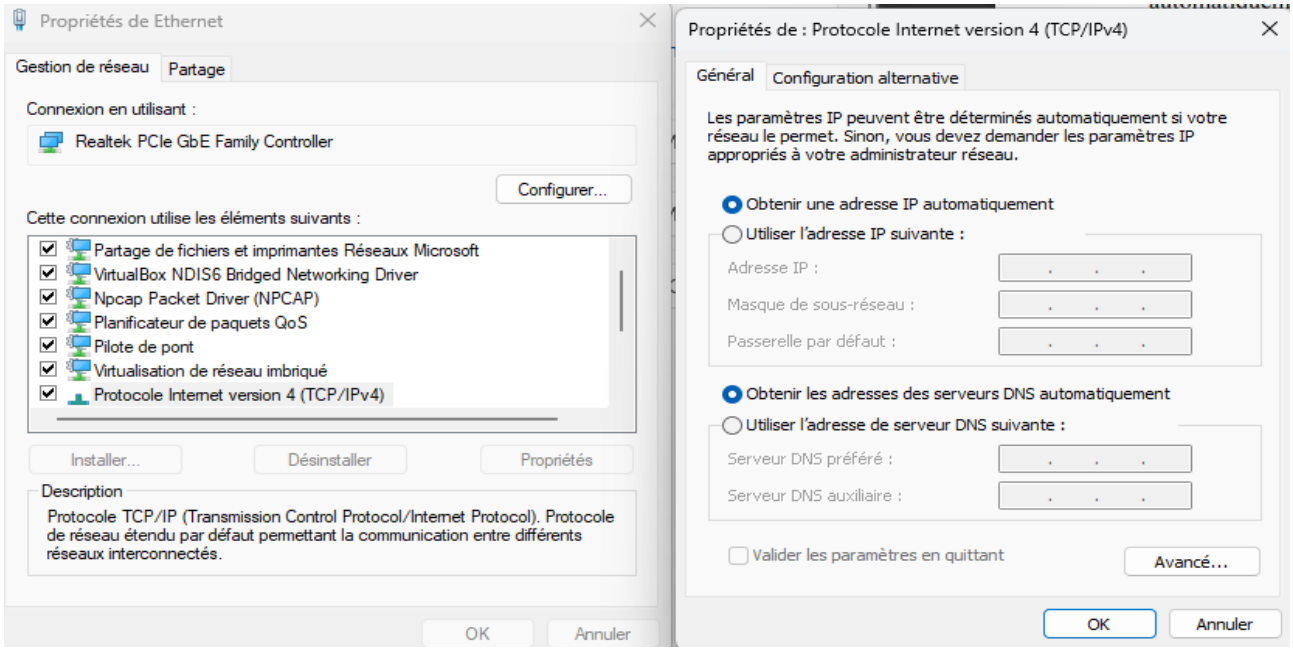
TP4 : analyse de trames DHCP avec Wireshark

SOMMAIRE :

2. Capture de trames DHCP avec Wireshark

J’ai afficher 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:fda1:8705%15(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.13(préféré)
   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(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1(préféré)
   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

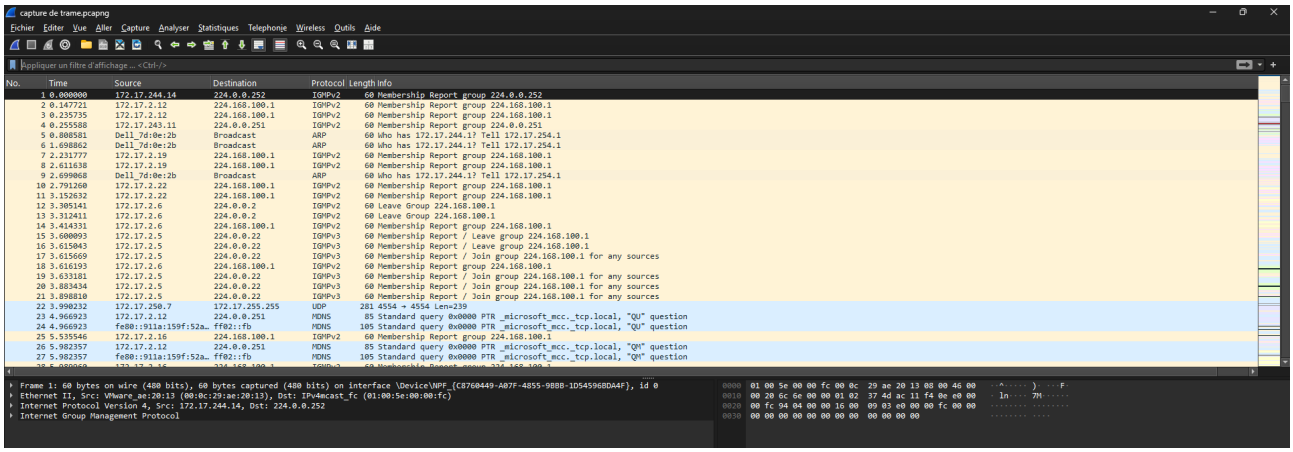
J’ai effectué la commande ipconfig /release

```
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:fda1:8705%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. . . . . :
```

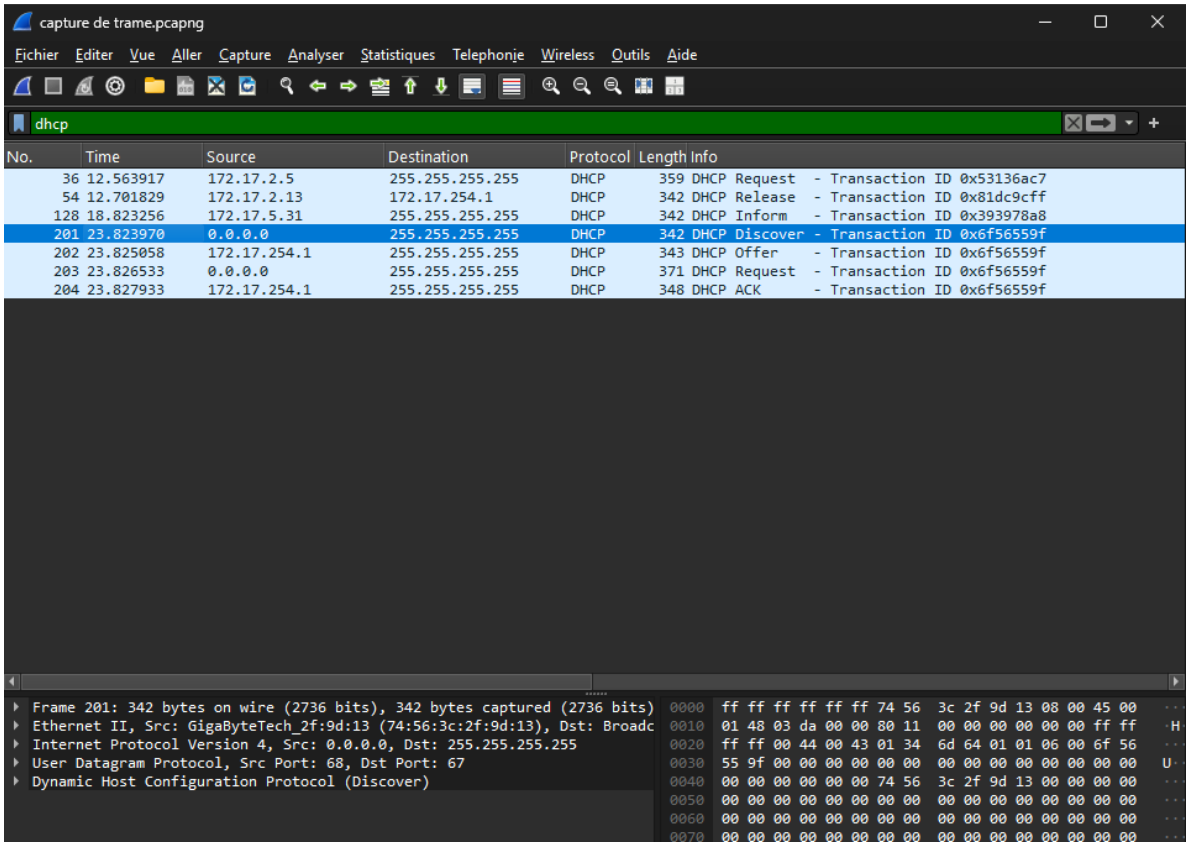
J’ai effectué la commande ipconfig /renew

```
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:fda1:8705%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



La trame DHCP release est la suivante :

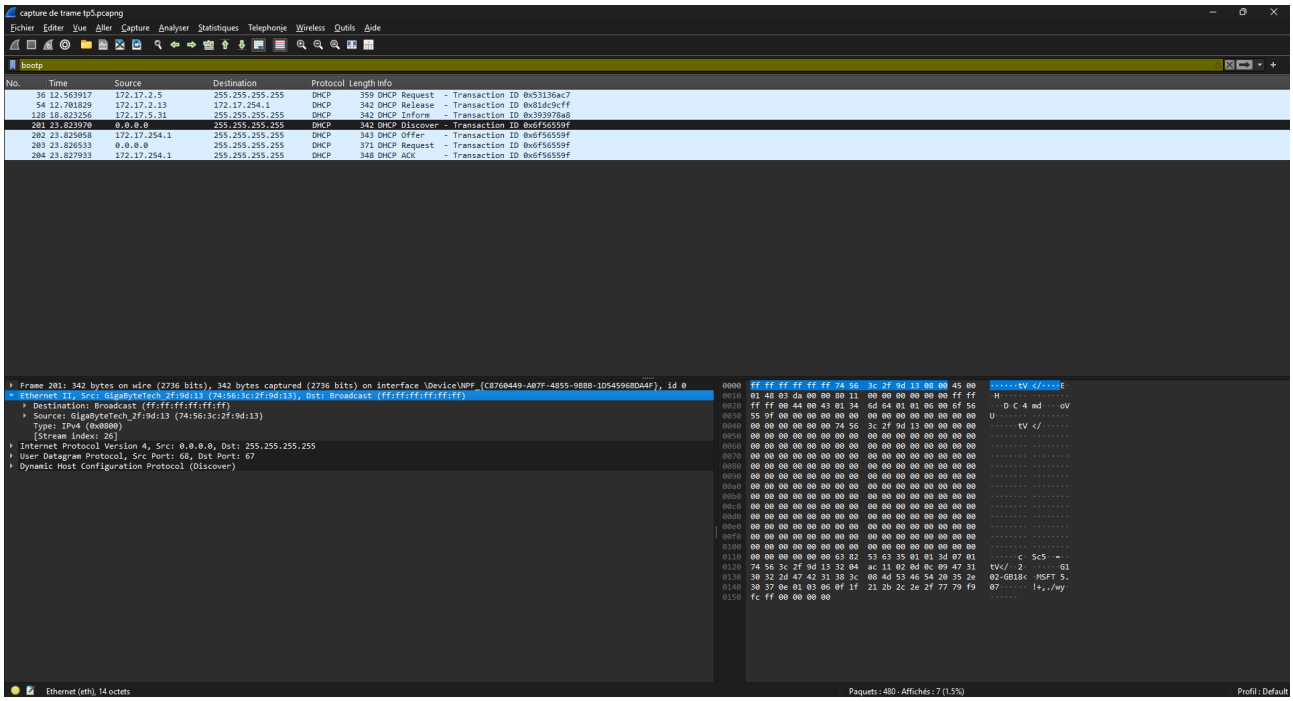


▪<u>A partir des renseignements obtenus à l’aide de la commande ipconfig /release, renseignez les éléments ci-dessous :</u>
Adresse IPv4 : 0.0.0.0
Masque de sous-réseau : 255.255.0.0
Passerelle par défaut : 172.17.250.3

▪<u>A partir des renseignements obtenus à l’aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :</u>
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

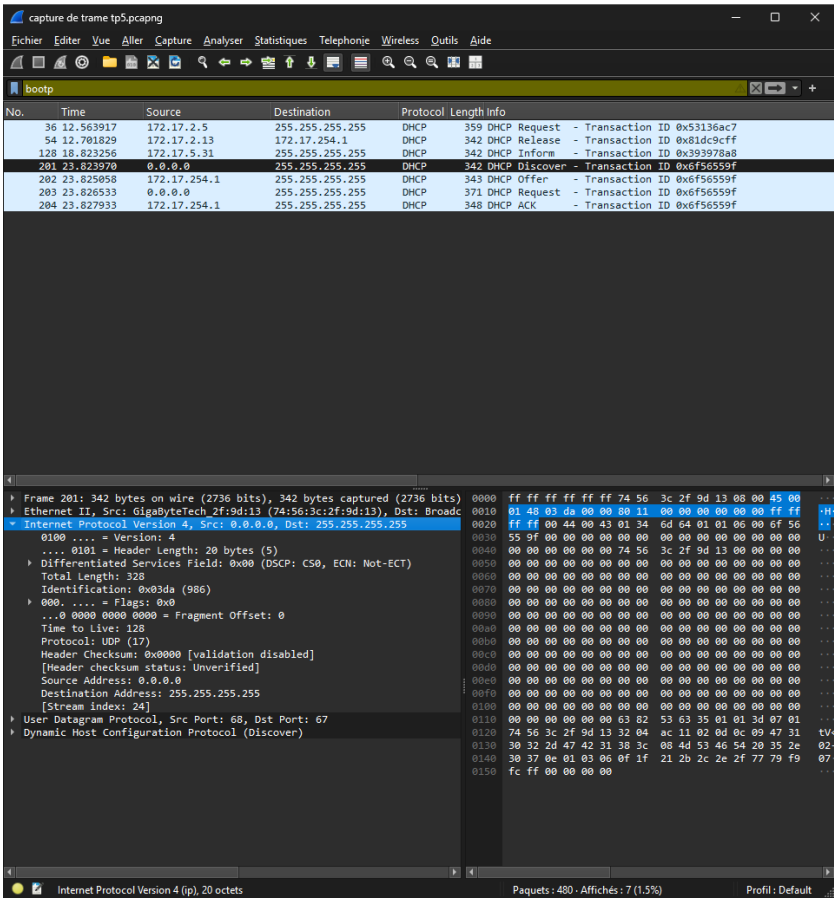
▪ Quel est le champ qui suit immédiatement les deux adresses MAC ?
Le champ qui suit immédiatement les 2 adresses mac est le champ Ethertype (0800)

▪ 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.

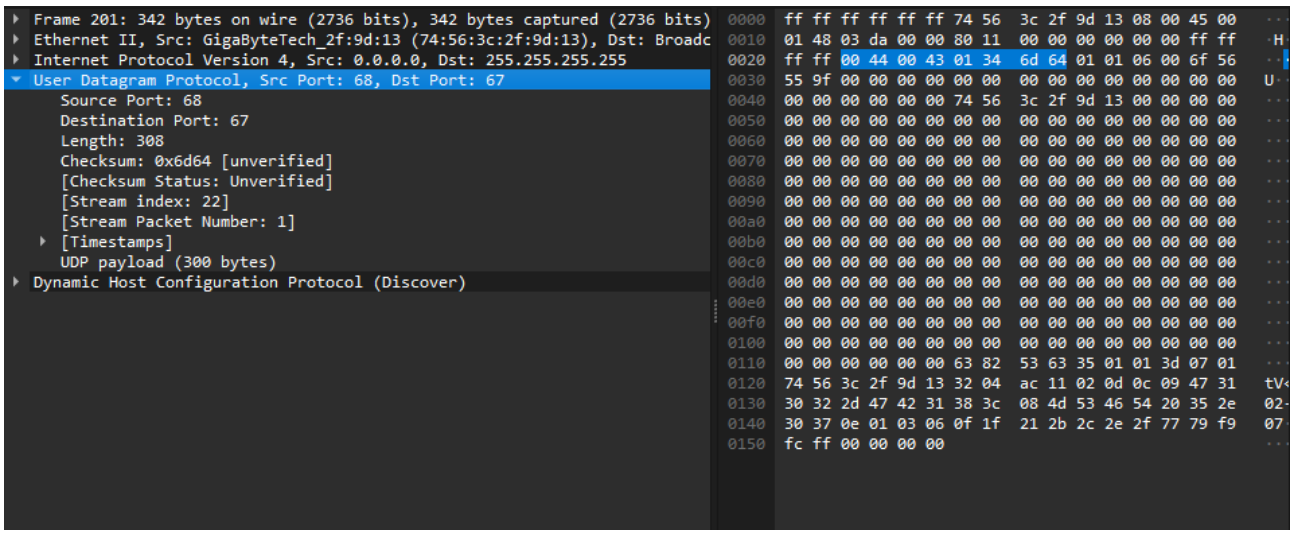
Le champ qui permet de connaître le protocole de transport est Protocole la valeur est 17

▪ 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

▪ Caractérisez 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



▪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 0×02 et 0×03 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