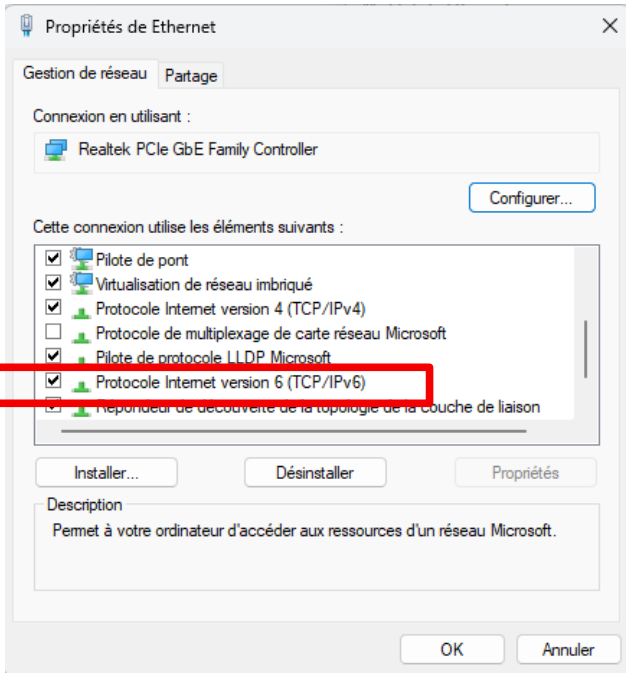
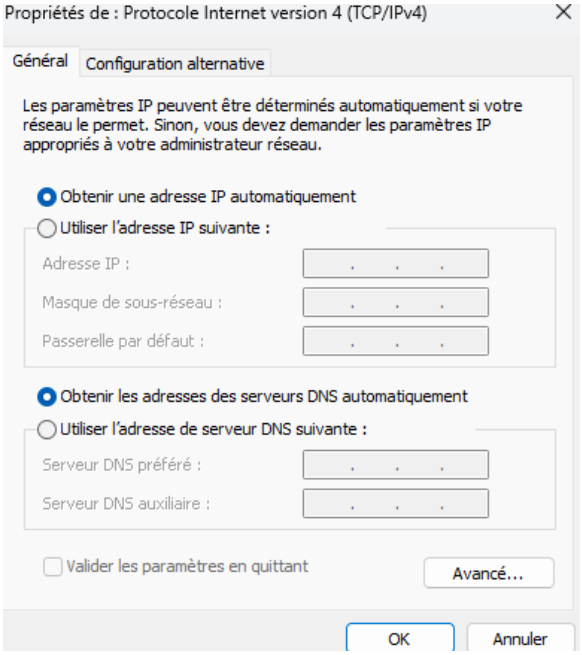
TP4-analyse de trames DHCP avec WS rafael correia marta

sommaire

2.capture de trames DHCP avec Wireshark.





ouvrez une invite de commandes et saisissez la commande ipconfig /all :

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

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . : G102-GB11
   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-82-CE
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . . :d519:3b2c%8(préféré)
   Adresse IPv4. . . . . . . . . . . . . . : 172.17.2.9(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : mercredi 1 octobre 2025 10:43:46
   Bail expirant. . . . . . . . . . . . . : mercredi 1 octobre 2025 11:13:33
   Passerelle par défaut. . . . . . . . . : 172.17.250.3
   Serveur DHCP . . . . . . . . . . . . . : 172.17.254.1
   IAID DHCPv6 . . . . . . . . . . . :
   DUID de client DHCPv6. . . . . . . . . -32-0E-74-56-3C-2F-82-CE
   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-00-27-00-00-0F
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::6d05:6f9:d34c:1d1c%15(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-CB-32-0E-74-56-3C-2F-82-CE
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

TP4-analyse de trames DHCP avec WS rafael correia marta

- Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?
  172.20.224.1
- Renseignez les autres éléments ci-dessous :
- DHCP activé :Non
- Masque de sous-réseau : 255.255.240.0
- Bail obtenu :jeudi 2 octobre 2025 17:02:36
- Bail expirant :jeudi 2 octobre 2025 17:22:41
- Passerelle par défaut :172.17.250.3
- Serveur DHCP : 172.17.254.1
- Serveur DNS :172.17.254.1

▪ Démarrez une capture de trames à l'aide de Wireshark
Vous allez générer un peu de trafic entre votre poste de travail et le serveur DHCP « Roi ». Ouvrez une invite de commandes et tapez successivement les commandes :

- ipconfig /release

```
C:\Users\rcorreia> ip config /release
'ip' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\rcorreia>ipconfig /release

Configuration IP de Windows


Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6588:a4e0:2430:5cb4%20
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.224.1
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dfdc:828c:360a:c04f%8
   Passerelle par défaut. . . . . . . . . :
```

- ipconfig /renew

```
arte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::408b:f1ad:c9d7:8
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.197.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

te Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::97c5:1ec5:8e8d:6
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.40.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Users\rcorreia>ipconfig /renew

figuration IP de Windows


te Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::ef29:b5d2:e9c0:e
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.224.1
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . :
```

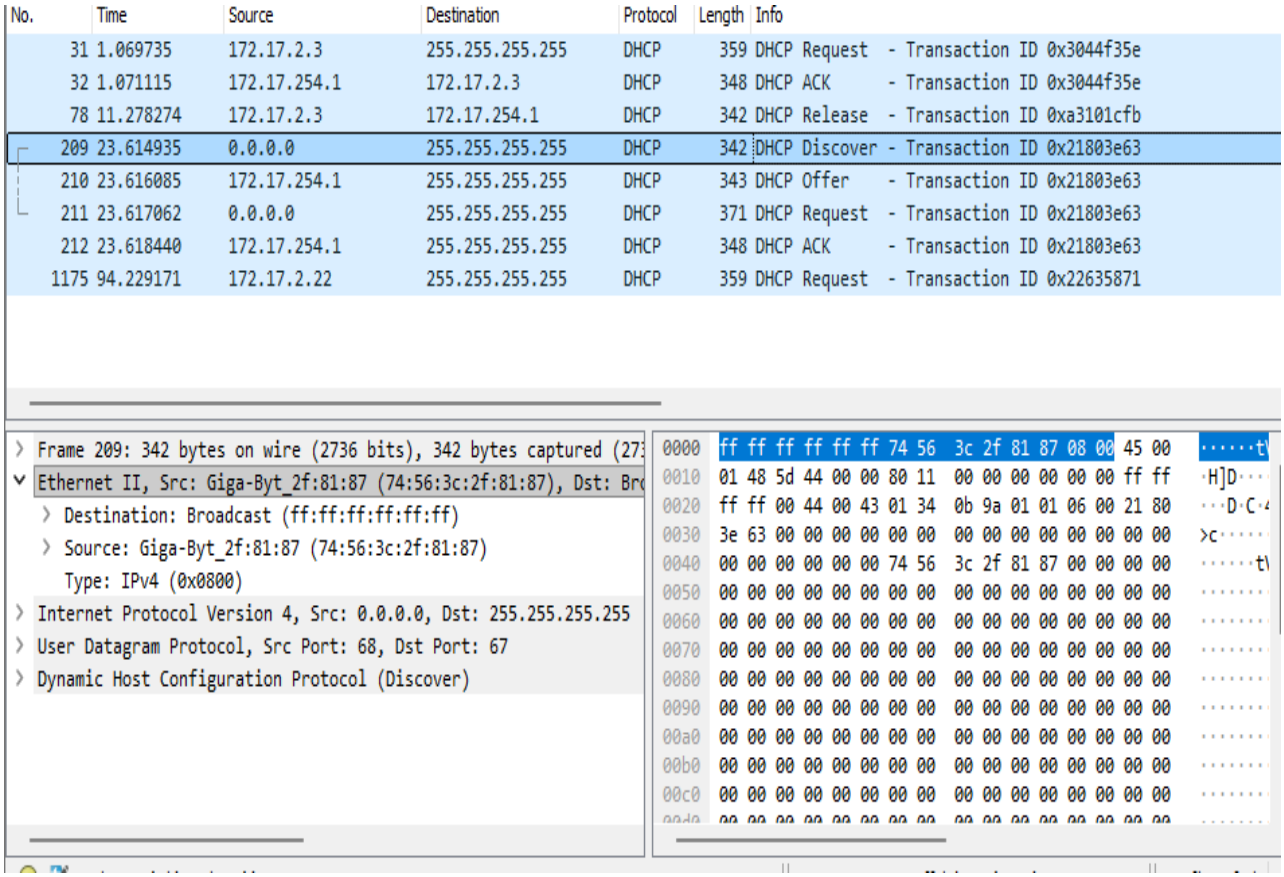
▪ A partir des renseignements obtenus à l'aide de la commande ipconfig /release, renseignez les éléments ci-dessous :
Adresse IPv4 :aprés le release ont a plus d'adresse IP v 4
Masque de sous-réseau :aprés le release ont a plus de masque
Passerelle par défaut :aprés le release ont a plus de passerelle

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dfdc:828c:360a:c04f%8
   Passerelle par défaut. . . . . . . . . :
```

A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :
Adresse IPv4 : 172.17.2.3
Masque de sous-réseau : 255.255.0.0
Passerelle par défaut :172.17.250.3

```
rte Ethernet Ethernet :

 Suffixe DNS propre à la connexion. . . : prince.local
 Adresse IPv6 de liaison locale. . . . .: fe80::dfdc:828c:360a:c04f%8
 Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.3
 Masque de sous-réseau. . . . . . . . . : 255.255.0.0
 Passerelle par défaut. . . . . . . . . : 172.17.250.3
```

ont limite l'affichage des trames à celles encapsulant les protocoles DHCP (zone Filter). En ecrivant « BOOTP » dans la zonne filter



4. 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 :

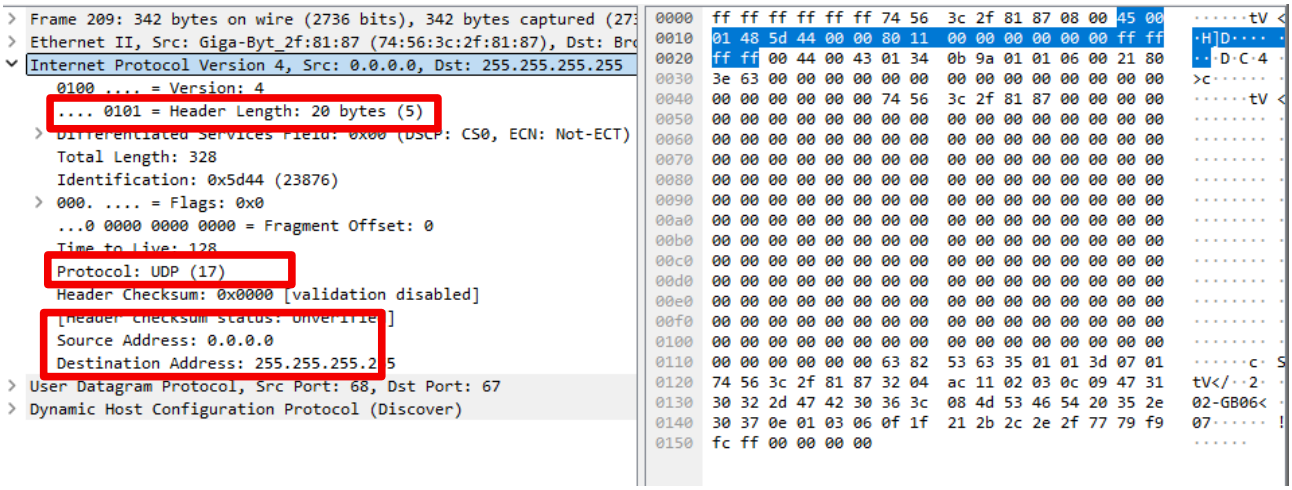
destination – ff .ff .ff.ff.ff.ff

source – 74:56:3c:2f:81:87

▪ Caractérisez l'adresse de couche 2 de destination de cette trame :
c'est une adresse de MAC broadcast

▪ Quel est le champ qui suit immédiatement les deux adresses MAC ?
Le champ ethertype
▪ Quelle valeur contient-il ? Que signifie t-elle ?
Il contient la valeur 0x0800 ce qui signifie que le protocole que ce trouve dans la couche suivante est de IPv4
Quels sont les protocoles inclus dans cette trame ?
Ehternet
IPv4
UDP
DHCP-BOOTP

▪ 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 ? Préciser la valeur de ce champ ainsi que le nom du protocole.
Le champ UDP et cest valeur sont 11(en hexa) et 17 (en decimale)
▪ Renseignez ci-dessous les champs d'en-tête IP suivants :
Version = v4
IHL (val. déci. et hexa.) = 20 bytes
Protocole (val. déci. et hexa.) = UDP(decimal 17)
Source address (val. déci. et hexa.) = 0.0.0.0

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

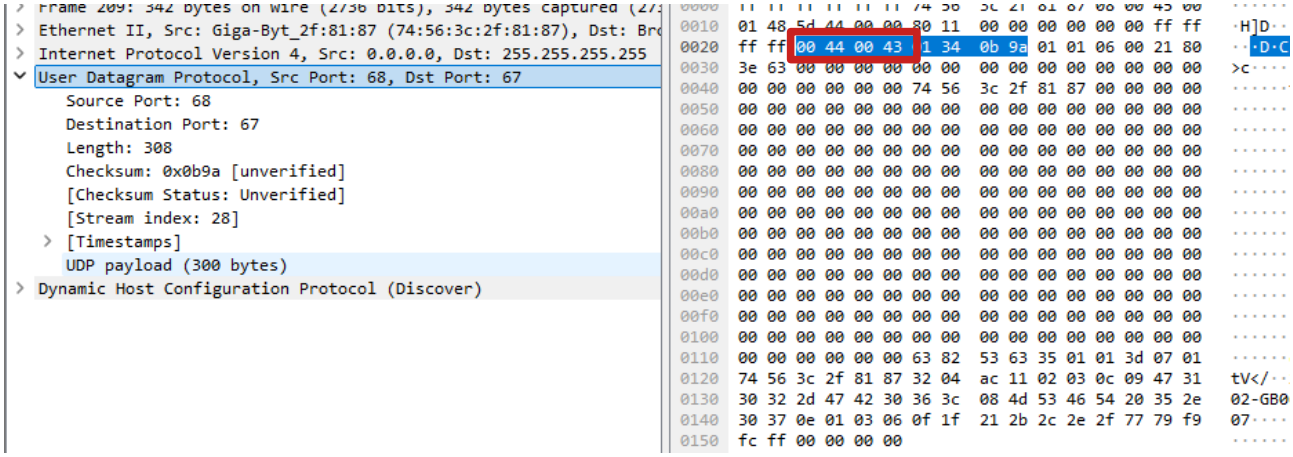
- Que signifie la valeur contenue dans le champ adresse IP source ?

Que la machine ne possede pas adresse IP

- Caractérisez l'adresse de couche 3 de destination de cette trame :

c'est le broadcast IPv4

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

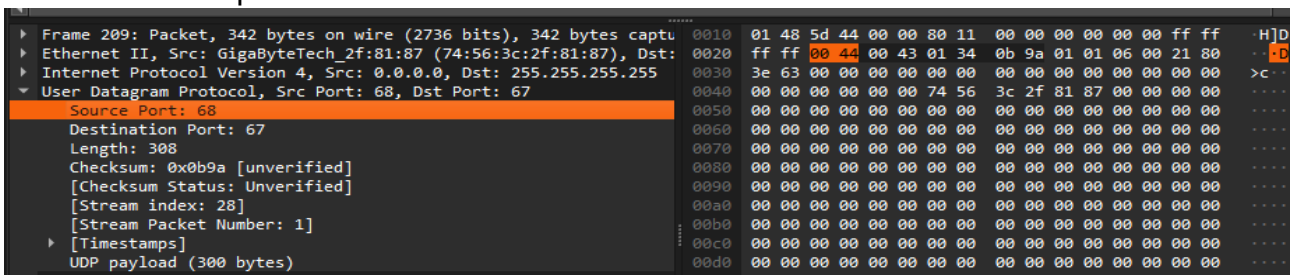


Quel est le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole ?

Le champ "Numéro de 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 `68 qui est utilisé le client DHCP.` la valeur hexadecimal est `0x0044`



Quel est le protocole applicatif encapsulé dans le datagramme UDP ?

Le protocol 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 :

Le serveur DHCP écoute sur le port UDP 67, représenté en hexadécimal par 0x0043.

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