

TP 4- Analyse des trames DHCP avec Wireshark

Nesrine EL AHMADI

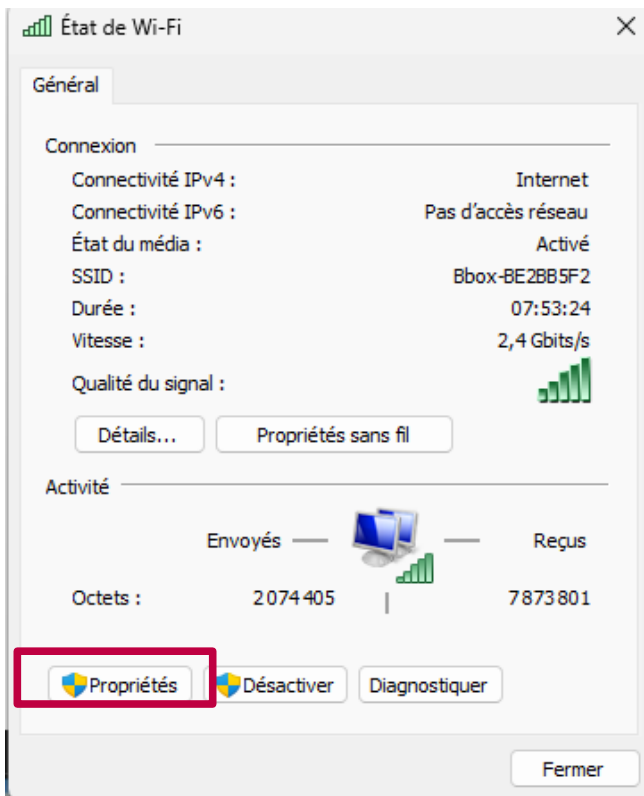
BTS SIO

Table des matières

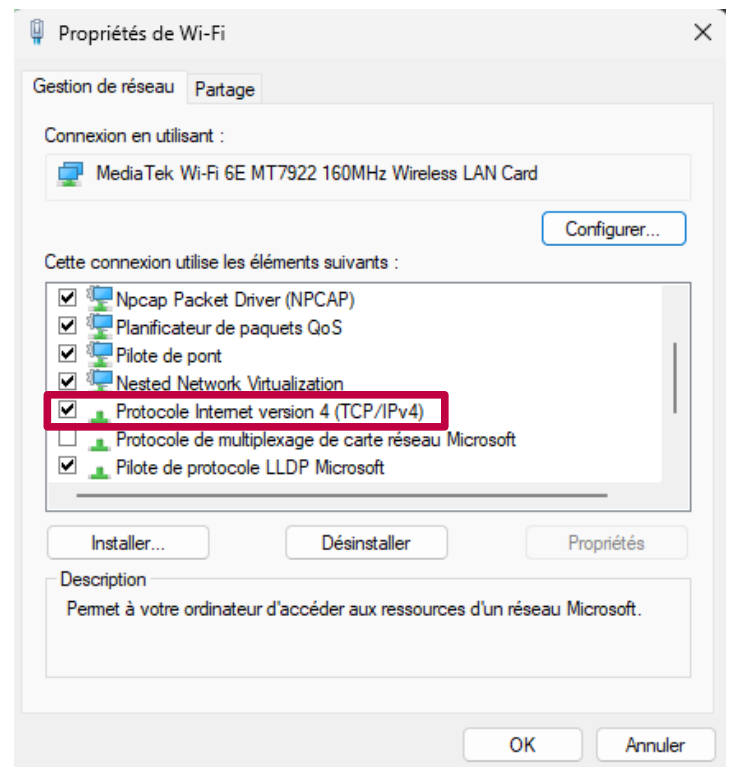
1. Capture de trames DHCP avec Wireshark.....	2
2. Étude de trame DHCP DISCOVER.....	11

1. Capture de trames DHCP avec Wireshark

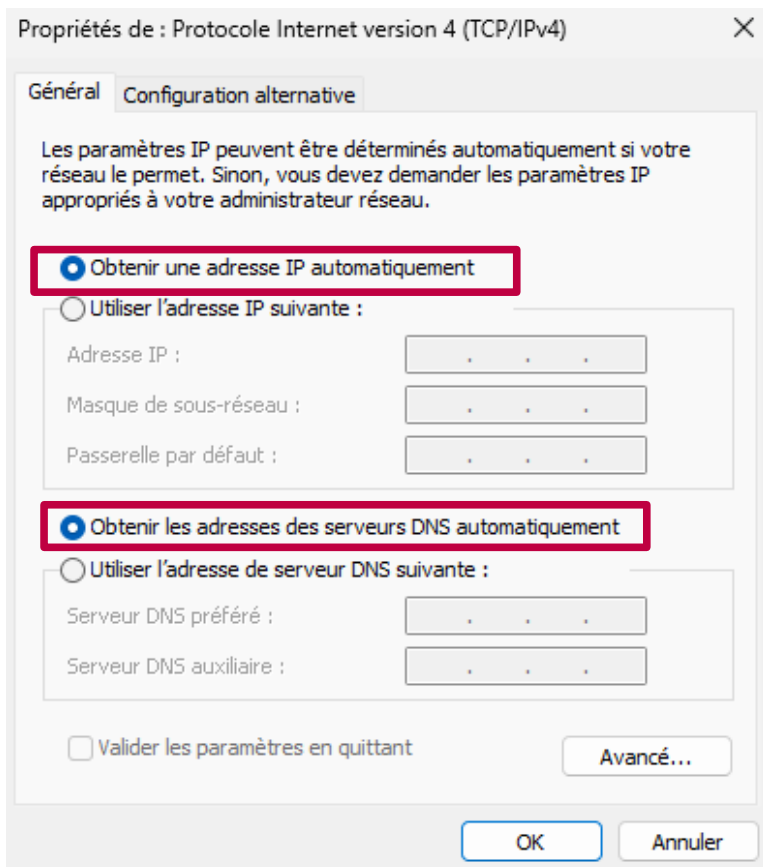
On modifie les propriétés TCP/IPv4 de manière à obtenir automatiquement les paramètre IP du serveur DHCP (Capture 1, 2 et 3) .



Capture 1



Capture 2



Capture 3

→ On exécute la commande **ipconfig /all** dans l'invite de commande(capture 4).

```
C:\Windows\System32>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 2 :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : VirtualBox Host-Only Ethernet Adapter
Adresse physique . . . . . : 0A-00-27-00-00-10
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::b74c:e62:bed4:2fbb%16(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-CB-32-0E-74-56-3C-2F-82-CE
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-82-CE
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::425f:a7ba:d519:3b2c%10(préfééré)
Adresse IPv4. . . . . : 172.17.2.9(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : lundi 13 octobre 2025 16:49:41
Bail expirant. . . . . : mardi 14 octobre 2025 16:49:32
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 74733116
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-CB-32-0E-74-56-3C-2F-82-CE
Serveurs DNS. . . . . : 172.17.254.1
NetBIOS sur Tcpip. . . . . : Activé
```

Capture 4

Carte Ethernet VMware Network Adapter VMnet1 :

```
Suffixe DNS propre à la connexion. . . :  
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet1  
Adresse physique . . . . . : 00-50-56-C0-00-01  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::d135:51a0:1091:9393%9(préfééré)  
Adresse IPv4. . . . . : 192.168.121.1(préfééré)  
Masque de sous-réseau. . . . . : 255.255.255.0  
Bail obtenu. . . . . : lundi 13 octobre 2025 16:49:17  
Bail expirant. . . . . : lundi 13 octobre 2025 17:49:15  
Passerelle par défaut. . . . . :  
Serveur DHCP . . . . . : 192.168.121.254  
IAID DHCPv6 . . . . . : 704663638  
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-CB-32-0E-74-56-3C-2F-82-CE  
NetBIOS sur Tcpip. . . . . : Activé
```

Carte Ethernet VMware Network Adapter VMnet8 :

```
Suffixe DNS propre à la connexion. . . :  
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet8  
Adresse physique . . . . . : 00-50-56-C0-00-08  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::a098:71fd:b4ae:dc49%15(préfééré)  
Adresse IPv4. . . . . : 192.168.17.1(préfééré)  
Masque de sous-réseau. . . . . : 255.255.255.0  
Bail obtenu. . . . . : lundi 13 octobre 2025 16:49:27  
Bail expirant. . . . . : lundi 13 octobre 2025 17:49:15  
Passerelle par défaut. . . . . :  
Serveur DHCP . . . . . : 192.168.17.254  
IAID DHCPv6 . . . . . : 738218070  
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-CB-32-0E-74-56-3C-2F-82-CE  
Serveur WINS principal . . . . . : 192.168.17.2  
NetBIOS sur Tcpip. . . . . : Activé
```

Carte Ethernet vEthernet (Default Switch) :

```
Suffixe DNS propre à la connexion. . . :  
Description. . . . . : Hyper-V Virtual Ethernet Adapter  
Adresse physique . . . . . : 00-15-5D-20-01-00  
DHCP activé. . . . . : Non  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::d1ee:d393:194e:ad24%20(préfééré)  
Adresse IPv4. . . . . : 172.28.240.1(préfééré)  
Masque de sous-réseau. . . . . : 255.255.240.0  
Passerelle par défaut. . . . . :  
IAID DHCPv6 . . . . . : 335549789  
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-CB-32-0E-74-56-3C-2F-82-CE  
NetBIOS sur Tcpip. . . . . : Activé
```

C:\Windows\System32>

Capture 4

---Quelle est l'adresse IP attribuée par le serveur DHCP a votre poste de travail ?

- Adresse IP : 172.17.2.9

---D'autres éléments sont inscrits :

- DHCP activé : OUI
- Masque de sous- réseau : 255.255.0.0

- Bail obtenu : lundi 13 octobre 2025 16:49:41
- Bail expirant : mardi 14 octobre 2025 16:49:32
- Passerelle par défaut : 172.17.250.3
- Serveur DHCP : 172.17.254.1
- Serveur DNS : 172.17.254.1

→ On exécute la commande **ipconfig** a titre de comparaison (capture 5).

```
C:\Windows\System32>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::b74c:e62:bed4:2fbb%16
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : prince.local
    Adresse IPv6 de liaison locale. . . . : fe80::425f:a7ba:d519:3b2c%10
    Adresse IPv4. . . . . : 172.17.2.9
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.3

Carte Ethernet VMware Network Adapter VMnet1 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::d135:51a0:1091:9393%9
    Adresse IPv4. . . . . : 192.168.121.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet VMware Network Adapter VMnet8 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::a098:71fd:b4ae:dc49%15
    Adresse IPv4. . . . . : 192.168.17.1
    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::d1ee:d393:194e:ad24%20
    Adresse IPv4. . . . . : 172.28.240.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :
```

→ Après avoir exécuté la commande **ipconfig /release** dans l'invite de commande on obtiens certaines informations (capture 6) :

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

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::b74c:e62:bed4:2fbb%16
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::425f:a7ba:d519:3b2c%10
    Passerelle par défaut. . . . . :

Carte Ethernet VMware Network Adapter VMnet1 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::d135:51a0:1091:9393%9
    Passerelle par défaut. . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::a098:71fd:b4ae:dc49%15
    Passerelle par défaut. . . . . :

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::d1ee:d393:194e:ad24%20
    Adresse IPv4. . . . . : 172.28.240.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :
```

Capture 6

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : ?

→ On exécute ensuite la commande **ipconfig /renew** (capture 7) et obtiens :

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

Configuration IP de Windows

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::b74c:e62:bed4:2fbb%16
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : prince.local
    Adresse IPv6 de liaison locale. . . . : fe80::425f:a7ba:d519:3b2c%10
    Adresse IPv4. . . . . : 172.17.2.9
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.3

Carte Ethernet VMware Network Adapter VMnet1 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::d135:51a0:1091:9393%9
    Adresse IPv4. . . . . : 192.168.121.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 

Carte Ethernet VMware Network Adapter VMnet8 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::a098:71fd:b4ae:dc49%15
    Adresse IPv4. . . . . : 192.168.17.1
    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. . . :
```

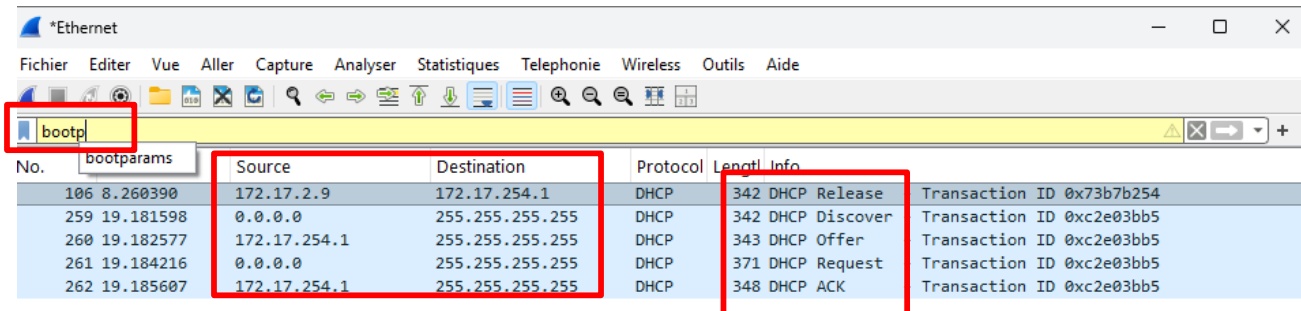
Capture 7

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : ?

→ On a fait une **capture de trames a l'aide de Wireshark** tout en générer un peu de trafic entre le poste de travail et le serveur DHCP. On a ensuite limité l'affichage des trames a celle encapsulant les protocoles DHCP (Capture 8) .

A screenshot of the Wireshark network protocol analyzer interface. The title bar reads '*Ethernet'. The menu bar includes 'Fichier', 'Editer', 'Vue', 'Aller', 'Capture', 'Analyser', 'Statistiques', 'Telephonie', 'Wireless', 'Outils', and 'Aide'. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows a list of captured packets, with the first packet (No. 106) selected. The packet details pane on the right shows the structure of the selected packet, with the 'DHCP Release' message highlighted. The packet bytes pane at the bottom is empty. The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
106	8.260390	172.17.2.9	172.17.254.1	DHCP	342	DHCP Release Transaction ID 0x73b7b254
259	19.181598	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover Transaction ID 0xc2e03bb5
260	19.182577	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer Transaction ID 0xc2e03bb5
261	19.184216	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request Transaction ID 0xc2e03bb5
262	19.185607	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK Transaction ID 0xc2e03bb5

Capture 8

On obtient plusieurs trames comme **DHCP RELEASE** (généré par la commande ipconfig /release), **DHCP DISCOVER** (conséquence de la commande ipconfig /renew), **DHCP OFFER** (réponse du serveur), **DHCP REQUEST** (réponse du client pour faire valider son adresse IP) et la trame **DHCP ACK** (pour confirmer l'attribution)

2. Étude de trame DHCP DISCOVER

→ On s'intéresse à la trame **DHCP DISCOVER** et on développe l'en-tête Ethernet (capture 9)

The image shows a Wireshark capture of network traffic. The packet list at the top shows several DHCP packets. The packet at frame 259, time 19.181598, is a DHCP Discover packet from source 0.0.0.0 to destination 255.255.255.255, with a length of 342 bytes. This packet is highlighted with a red box. The packet details pane below shows the structure of the packet, including the Ethernet II header and the DHCP Discover message.

No.	Time	Source	Destination	Protocol	Length	Info
106	8.260390	172.17.2.9	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0x73b7b254
259	19.181598	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2e03bb5
260	19.182577	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xc2e03bb5
261	19.184216	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0xc2e03bb5
262	19.185607	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xc2e03bb5

Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce)

Type: IPv4 (0x0800)

[Stream index: 4]

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 82 ce 08 00 45 00tv <

0010 01 48 11 40 00 00 00 00 00 00 00 00 00 00 ff ff ..H.@....

0020 ff ff 00 44 00 43 01 34 6f 52 01 01 06 00 c2 e0 ...D.C.4 o

0030 3b b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;.....

0040 00 00 00 00 00 00 74 56 3c 2f 82 ce 00 00 00 00tv <

0050 00 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 00<

0070 00 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 00<

0090 00 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 00<

00b0 00 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 00<

00d0 00 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 00<

00f0 00 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 00<

0110 00 00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01c. S

0120 74 56 3c 2f 82 ce 32 04 ac 11 02 09 0c 09 47 31 tv</...2. <

0130 30 32 2d 47 42 31 31 3c 08 4d 53 46 54 20 35 2e 02-GB11<

0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07.....!

0150 fc ff 00 00 00 00

Capture 9

---A l'aide de la l'en-tête de trame DHCP DISCOVER on identifie l'adresse MAC source et destination.

- MAC source : 74:56:3c:2f:82:ce
- MAC destination: ff:ff:ff:ff:ff:ff

--- Caractérisiez l'adresse de couche 2 de destination de cette trame :

C'est une adresse en broadcast c'est dire qu'elle est diffusé a tout le monde afin de savoir a qui est ce que l'adresse MAC appartient appartient.

--- Quel est le champ qui suit immédiatement les deux adresses MAC ? Quelle valeur contient-il ? Que signifie t-elle ?

Ce qui se trouve juste après les deux adresse MAC est le champ Ethertype (de 2 octets) permettant le démultiplexage. Celui nous indique le protocole supérieur encapsulé dans la trame. Dans ce cas sa valeur est de 0x0800 donc IPv4.

---Quels sont les protocoles inclus dans cette trames ?

Dans une trame DHCP, plusieurs protocoles sont encapsules. Tout commence par Ethernet qui transporte les adresses MAC et le champs Ethertype qui nous informe que le protocole supérieur encapsulé dans la trame est le protocole IPv4. Ensuite le datagramme UDP qui assure le transport entre les ports 67 et 68. Enfin, le protocole DHCP est encapsulé au niveau applicatif.

→ On sélectionne **l'en-tête IP** contenu dans la trame DHCP Discover (Capture 10)

The image shows a Wireshark capture of a DHCP Discover packet. The packet list at the top shows frame 259 as a DHCP Discover packet from 0.0.0.0 to 255.255.255.255. The packet details pane shows the Internet Protocol Version 4 header with Source Address 0.0.0.0 and Destination Address 255.255.255.255. The packet bytes pane shows the raw data with the IP header fields highlighted by red boxes.

No.	Time	Source	Destination	Protocol	Length	Info
106	8.260390	172.17.2.9	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0x73b7b254
259	19.181598	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2e03bb5
260	19.182577	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xc2e03bb5
261	19.184216	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0xc2e03bb5
262	19.185607	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xc2e03bb5

Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736) on interface 0, from 0.0.0.0 to 255.255.255.255 on interface 0

Ethernet II, Src: GigaByteTech_2f:83:ce (74:56:3c:2f:83:ce), Dst: 01:00:5e:00:00:00 (01:00:5e:00:00:00)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 328
 Identification: 0x1140 (4416)
 > 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
 [Stream index: 32]
 > User Datagram Protocol, Src Port: 68, Dst Port: 67
 > Dynamic Host Configuration Protocol (Discover)

Capture 10

---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 .

▪C'est le champ protocole qui nous indique le protocole de couche 4 qui est encapsulé dans le paquet IP.

Champ d'en-tête IP :

- Version : 4 (IPv4)
- IHL (val.déci) : 20 octets (en hexadécimal) : 0x14
- Protocole (val.déci) : 17 (en hexadécimal) : 0x11
- Source adresse (val. Déci.) : 0.0.0.0 (client sans IP) (en hexadécimal) : 00 00 00 00
- Destination adresse (val déci) : 255.255.255.255 (en hexadécimal) : FF FF FF FF

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

- Elle indique que le client ne possède pas encore d'adresse IP. Il envoie une requête DHCP pour obtenir dynamiquement une configuration réseau l'adresse 0.0.0.0 est utilisé temporairement pour la communication avec le serveur DHCP.

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

- L'adresse de couche 3 destination une adresse de broadcast . Elle permet d'envoyer sa requête a tous les hôtes du réseau, notamment le serveur DHCP sans connaître leur adresse IP .

→ On sélectionne l'en-tête du datagramme UDP contenue dans la trame DHCP DISCOVER (capture 11)

> Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736	0000 ff ff ff ff ff 74 56 3c 2f 82 ce 08 00 45 00tv </
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst:	0010 01 48 11 40 00 00 80 11 00 00 00 00 00 ff ff ..H.@.....
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255	0020 ff ff 00 44 00 43 01 34 6f 52 01 01 06 00 c2 e0 ..D.C.4. OR
> User Datagram Protocol, Src Port: 68, Dst Port: 67	0030 3b b5 00 00 00 00 00 00 00 00 00 00 00 00 00 ;.....
Source Port: 68	0040 00 00 00 00 00 00 74 56 3c 2f 82 ce 00 00 00tv </
Destination Port: 67	0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
Length: 308	0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
Checksum: 0x6f52 [unverified]	0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
[Checksum Status: Unverified]	0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
[Stream index: 33]	0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
[Stream Packet Number: 1]	00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
> [Timestamps]	00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
UDP payload (300 bytes)	00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<..
> Dynamic Host Configuration Protocol (Discover)	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 01c. Sc5
	0120 74 56 3c 2f 82 ce 32 04 ac 11 02 09 0c 09 47 31 tv</...2. ...
	0130 30 32 2d 47 42 31 31 3c 08 4d 53 46 54 20 35 2e 02-GB11< .MS
	0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07..... !+,
	0150 fc ff 00 00 00 00<..

Capture 11

---Quel est le nom de l'en-tête de transport permettant le démultiplexage de protocoles ?

▪C'est l'en-tête de segment ou ici datagramme car le protocole après le démultiplexage est UDP et on parle de datagramme UDP.

--- Quel est le port UDP utilisé par le client DHCP ?

▪C'est le port 68 qui est utilisé par le client DHCP pour envoyer sa requête DHCP.
(La requête vient du client)

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

→ 00 44

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

▪Le protocole applicatif encapsulé dans le datagramme UDP est le protocole DHCP.

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

C'est le port 67 (utilisé par le serveur)

---Identifier la valeur hexadécimale correspondante figurant dans le volet des octets.

→ 0x0043

→ On sélectionne la section Bootstrap Protocole contenu dans la trame
DHCP DISCOVER (Capture 12)

The image shows a Wireshark packet capture of a DHCP Discover message. The left pane displays the packet details, and the right pane displays the packet bytes. A red line connects the 'Message type: Boot Request (1)' field in the details pane to the value '01' in the packet bytes pane.

Packet Details:

- Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
- Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), 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
- Dynamic Host Configuration Protocol (Discover)
 - Message type: Boot Request (1)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xc2e03bb5
 - Seconds elapsed: 0
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0
 - Your (client) IP address: 0.0.0.0
 - Next server IP address: 0.0.0.0
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (Discover)
 - Length: 1
 - DHCP: Discover (1)
 - Option: (61) Client identifier

Packet Bytes:

Offset	Hex	ASCII
0000	ff ff ff ff ff 74 56 3c 2f 82 ce 00 00 45 00tv </...E
0010	01 48 11 40 00 00 80 11 00 00 00 00 00 00 ff ff	..H@.....
0020	ff ff 00 44 00 43 01 34 6f 52 01 01 06 00 c2 e0	...D.C.4 oR.....
0030	3b b5 00 00 00 00 00 00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 74 56 3c 2f 82 ce 00 00 00 00tv </...E
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 b5 01 3d 07 01c Sc5.....
0120	74 56 3c 2f 82 ce 32 04 11 02 09 0c 09 47 31	tv</...2.....G1
0130	30 32 2d 47 43 31 31 3c 08 4d 53 46 54 20 35 2e	02-G011< MSFT 5.
0140	80 3f 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9	07.....!+.,/wy.
0150	fc ff 00 00 00 00

Capture 12

La valeur 1 montre que le message est un Boot Request. Si elle avait été de 2 ca signifiait qu'il s'agit d'un boot Reply.