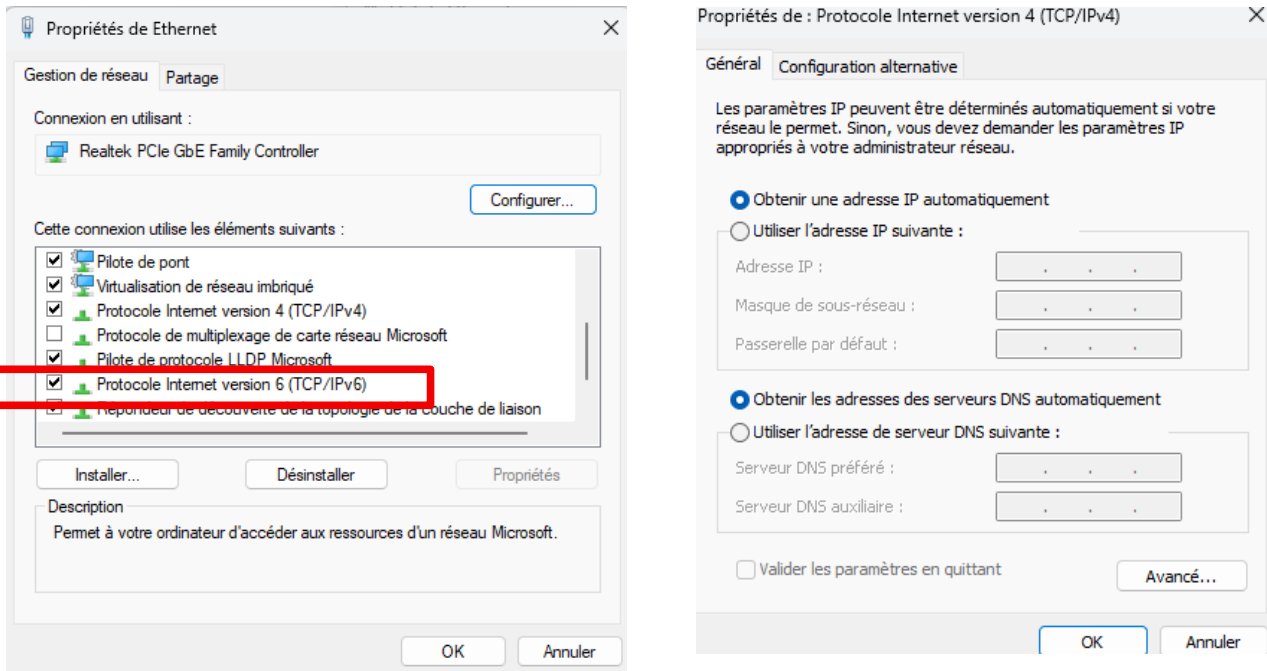


sommaire

- 2.capture de trames DHCP avec Wireshark.....1
- 4. Etude de la trame DHCP DISCOVER.....4

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. . . . . : fe80::42b7a7b1: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 . . . . . : 7453110
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. . . . . : Active

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. . . . . : Active
```

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

- ipconfig /renew

```
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. . . . . :

Carte Ethernet Ethernet 2 :

    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. . . . . :

Carte 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. . . . . :

Carte 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

Configuration IP de Windows

Carte 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 :après le release ont a plus d'adresse IP v 4

Masque de sous-réseau :après le release ont a plus de masque

Passerelle par défaut :après 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. . . . . :
```

TP4-analyse de trames DHCP avec WS rafael correia marta

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

```
Carte 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 écrivant « BOOTP » dans la zone filter

No.	Time	Source	Destination	Protocol	Length	Info
31	1.069735	172.17.2.3	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x3044f35e
32	1.071115	172.17.254.1	172.17.2.3	DHCP	348	DHCP ACK - Transaction ID 0x3044f35e
78	11.278274	172.17.2.3	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xa3101cfb
209	23.614935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x21803e63
210	23.616085	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0x21803e63
211	23.617062	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x21803e63
212	23.618440	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x21803e63
1175	94.229171	172.17.2.22	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x22635871

> Frame 209: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

▼ Ethernet II, Src: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87)
Type: IPv4 (0x0800)
- > 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 ff 74 56 3c 2f 81 87 08 00 45 00t
0010	01 48 5d 44 00 00 80 11 00 00 00 00 00 00 ff ff	..H]D...
0020	ff ff 00 44 00 43 01 34 0b 9a 01 01 06 00 21 80	...D.C...
0030	3e 63 00 00 00 00 00 00 00 00 00 00 00 00 00	>c.....
0040	00 00 00 00 00 00 74 56 3c 2f 81 87 00 00 00 00t)
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

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

source – 74:56:3c:2f:81:87

- Caractériser 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.

The screenshot shows the following details for the selected IP header:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 328
- Identification: 0x5d44 (23876)
- Flags: 0x0
- Fragment Offset: 0
- Time to Live: 128
- Protocol: UDP (17)
- Header Checksum: 0x0000 [validation disabled]
- Source Address: 0.0.0.0
- Destination Address: 255.255.255.255

The UDP section shows:

- Source Port: 68
- Destination Port: 67

- 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 possède pas adresse IP
- Caractériser 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.

```

> Frame 209: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Giga-Byt_2f:81:87 (74:56:3c:2f:81:87), 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: 0xb9a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 28]
    > [Timestamps]
    UDP payload (300 bytes)
  > Dynamic Host Configuration Protocol (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 0x02 et 0x03 ligne 0020)

Port 68 qui est utilisé le client DHCP. la valeur hexadécimale est 0x0044

```

> Frame 209: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: GigaByteTech_2f:81:87 (74:56:3c:2f:81:87), 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: 0xb9a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 28]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (300 bytes)

```

Quel est le protocole applicatif encapsulé dans le datagramme UDP ?

Le protocole 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 :

TP4-analyse de trames DHCP avec WS rafael correia marta

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** :

The image shows a Wireshark capture of a DHCP Discover packet. The packet list pane at the top shows a list of packets, with the 209th packet (DHCP Discover) selected and circled in blue. The packet details pane below shows the structure of the DHCP Discover message. The 'Dynamic Host Configuration Protocol (Discover)' section is expanded, and the 'DHCP: Discover (1)' option is highlighted in orange and circled in blue. The packet bytes pane on the right shows the raw data of the packet, with the '01' byte in the DHCP Discover option field circled in blue.

No.	Time	Source	Destination	Protocol	Length	Info
31	1.009733	172.17.2.3	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x3044f35e
32	1.071115	172.17.254.1	172.17.2.3	DHCP	348	DHCP Offer - Transaction ID 0x3044f35e
78	11.278274	172.17.2.3	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xa3101cfb
209	23.614935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x21803e63
210	23.616085	172.17.254.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x21803e63
211	23.617062	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x21803e63
212	23.618440	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0x21803e63
1175	94.229171	172.17.2.22	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x22635871

Dynamic Host Configuration Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x21803e63
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
 - 0... .. = Broadcast flag: Unicast
 - .000 0000 0000 0000 = Reserved flags: 0x0000
- 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:81:87 (74:56:3c:2f:81:87)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- DHCP: Discover (1)
 - Length: 1
- Option: (61) Client Identifier
- Option: (50) Requested IP Address (172.17.2.3)
- Option: (12) Host Name

0000 ff ff ff ff ff 74 56 3c 2f 81 87 08 00 45 00
0010 01 48 5d 44 00 00 80 11 00 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 0b 9a 01 01 06 00 21 80
0030 3e 63 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 74 56 3c 2f 81 87 00 00 00
0050 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
0070 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
0090 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
00b0 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
00d0 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
00f0 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
0110 00 00 00 00 00 00 63 82 53 63 35 01 31 07 01
0120 74 56 3c 2f 81 87 32 04 ac 11 02 63 0c 00 47 31
0130 30 32 2d 47 42 30 36 3c 00 40 53 46 00 00 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