

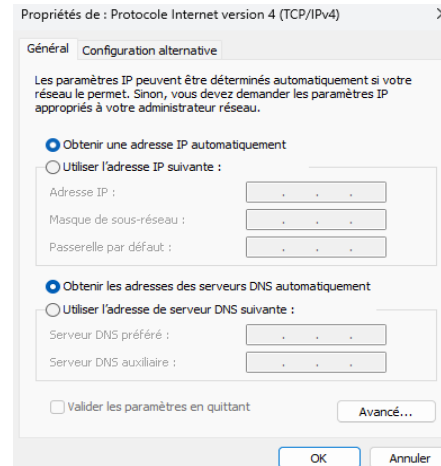
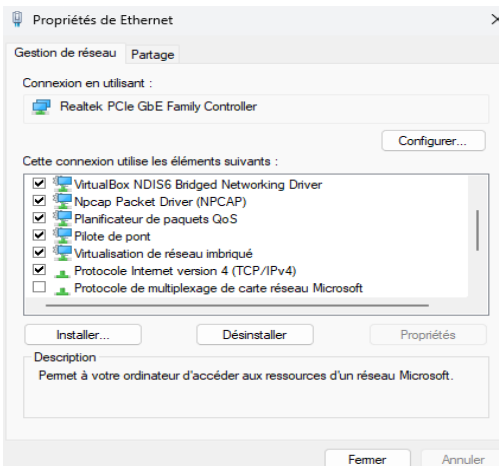
TP4 : analyse de trames DHCP avec Wireshark

Sommaire

- 1) Processus d'acquisition d'une adresse IPV4.....1
- 2) Capture de trames DHCP avec Wireshark.....1
- 3) Etude de la trame DHCP DISCOVER.....5

1) Processus d'acquisition d'une adresse IPV4

2) Capture de trames DHCP avec Wireshark



Saisie de ipconfig /all dans l'invite de commandes:

```
Invite de commandes
Description. . . . . : Hyper-V Virtual Ethernet Adapter
Adresse physique . . . . . : 00-15-5D-0A-A9-34
DHCP activé. . . . . : Non
Configuration automatique activée. . . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::2e35:c7bd:7baf:f0e%32(préféré)
Adresse IPv4. . . . . : 172.18.208.1(préféré)
Masque de sous-réseau. . . . . : 255.255.240.0
Passerelle par défaut. . . . . :
IAID DHCPv6 . . . . . : 536876381
DUID de cLient DHCPv6. . . . . : 00-01-00-01-2E-86-60-12-74-56-3C-2F-80-D8
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-80-D8
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::9072:83:49b8:adf%10(préféré)
Adresse IPv4. . . . . : 172.17.2.14(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mercredi 1 octobre 2025 09:56:15
Bail expirant. . . . . : mercredi 1 octobre 2025 10:46:56
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 326391356
DUID de cLient DHCPv6. . . . . : 00-01-00-01-2E-86-60-12-74-56-3C-2F-80-D8
Serveurs DNS. . . . . : 172.17.254.1
NetBIOS sur Tcpip. . . . . : Activé
```

l'adresse IP attribuée par le serveur DHCP « ROI » à mon poste de travail est 172.17.2.14

DHCP activé: Oui

Masque de sous-réseau: 255.255.0.0

Bail obtenu: mercredi 1 octobre 2025 09:56:15

Bail expirant: mercredi 1 octobre 2025 10:46:56

Passerelle par défaut: 172.17.250.3

Serveur DHCP: 172.17.254.1

Serveur DNS: 172.17.254.1

Démarrage d'une capture de trames sur Wireshark:

The screenshot shows the Wireshark interface with a network traffic capture in progress. The packet list pane displays several packets, including DHCP messages and ARP requests. The packet details pane shows the structure of a DHCPv4 packet, including the Ethernet II, Internet Protocol Version 4, and Internet Group Management Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
41	4.588953	::	::	IGMPv6	86	Multicast Listener Query
42	4.620251	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.168.100.1
43	4.628836	172.17.2.22	224.0.0.252	IGMPv2	60	Membership Report group 224.0.0.252
44	4.628836	172.17.2.22	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
45	4.635782	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.168.100.1
46	4.649683	Del11_7d19e:2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
47	4.655325	172.17.2.18	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
48	4.667551	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
49	4.682363	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
50	4.685143	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
51	4.678030	172.17.2.5	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.168.100.1 for any sources
52	5.649724	Del11_7d19e:2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
53	6.881344	172.17.2.6	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
54	6.898646	172.17.2.6	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
55	6.149756	172.17.254.1	239.255.255.254	IGMPv2	60	Membership Report group 239.255.255.254
56	6.418431	172.17.2.12	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
57	6.607933	172.17.2.12	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
58	7.149649	Del11_7d19e:2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1
59	7.475188	Synology_32:37:b5	Giga-Byt_2f:7f:ea	ARP	60	who has 172.17.2.18? Tell 172.17.254.5
60	7.689833	172.17.243.11	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
61	7.881837	172.17.2.22	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
62	7.956156	172.17.2.19	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
63	8.077455	172.17.2.19	224.168.100.1	IGMPv2	60	Membership Report group 224.168.100.1
64	8.186959	172.17.250.7	172.17.255.255	UDP	281	4554 → 4554 Len=239
65	8.149673	Del11_7d19e:2b	Broadcast	ARP	60	who has 172.17.244.1? Tell 172.17.254.1

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{90AD83AE-6A19-4C15-B3C8-SF1DF612DB83}.1
> Ethernet II, Src: Giga-Byt_2f:9c:fd (74:56:3c:2f:9c:fd), Dst: IPv4mcast_28:64:01 (01:00:5e:28:64:01)
> Internet Protocol Version 4, Src: 172.17.2.16, Dst: 224.168.100.1
> Internet Group Management Protocol
```

Utilisation des commandes:

- ipconfig /release (libérations de l'adresse IP)
- ipconfig /renew (renouvellement ou obtention d'un bail)

dans l'invite de commandes

ipconfig /release:

```
Invite de commandes
C:\Users\mballester>ipconfig /release

Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::2e35:c7bd:7baf:f0e%32
    Adresse IPv4. . . . . : 172.18.208.1
    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::9072:83:49b8:adf%10
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::16a0:d13f:db29:2fe8%17
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet VMware Network Adapter VMnet1 :

    Suffixe DNS propre à la connexion. . . . :
```

ipconfig /renew:

```
Invite de commandes
Passerelle par défaut. . . . . :

C:\Users\mballester>ipconfig /renew

Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::2e35:c7bd:7baf:f0e%32
    Adresse IPv4. . . . . : 172.18.208.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :

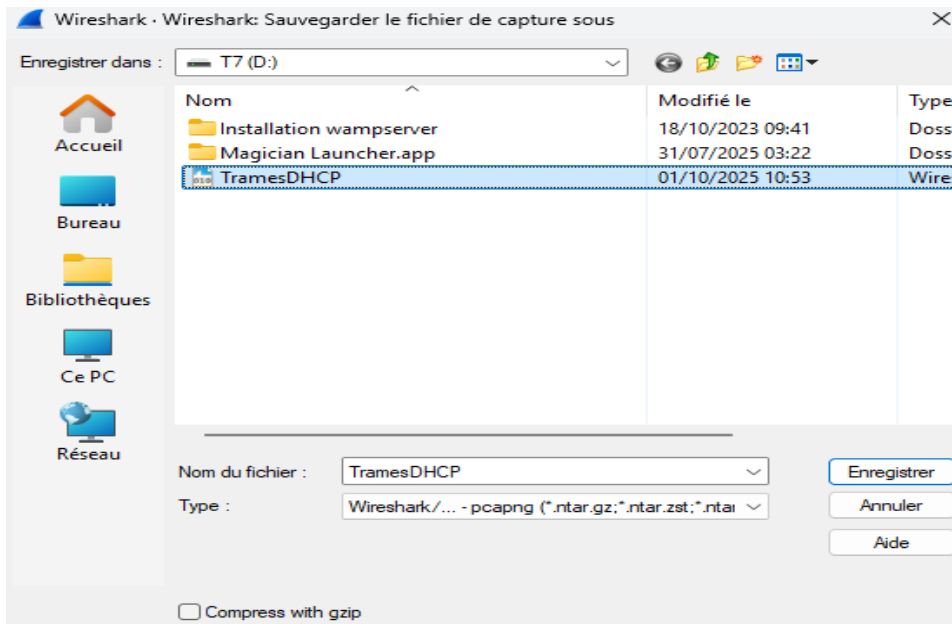
Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : prince.local
    Adresse IPv6 de liaison locale. . . . . : fe80::9072:83:49b8:adf%10
    Adresse IPv4. . . . . : 172.17.2.14
    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::16a0:d13f:db29:2fe8%17
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

Enregistrement de la capture de trames dans un fichiers:



Renseignement grâce a la commande ipconfig /release:

Adresse IPv4:

Masque de sous-réseau:

Passerelle par défaut:

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::9072:83:49b8:adf%10
Passerelle par défaut. . . . . :
  
```

Renseignement grâce a la commande ipconfig /renew:

Adresse IPv4: 172.17.2.14

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::9072:83:49b8:adf%10
Adresse IPv4. . . . . : 172.17.2.14
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 172.17.250.3
  
```

Limitations de l'affichage des Trames:

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets, with the following DHCP messages highlighted:

No.	Time	Source	Destination	Protocol	Length	Info
96795	11.805522	172.17.2.14	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xbfa2632a
97013	20.349759	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe56deaca
97014	20.350992	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xe56deaca
97015	20.351492	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0xe56deaca
97016	20.352817	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0xe56deaca
97017	20.354389	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xe56deaca

The bottom pane shows the details of frame 97013, a DHCP Discover message. The hex dump highlights the following bytes: ff ff ff ff ff 74 56 3c 2f 80 d8 08 00. The corresponding ASCII view shows:tV </.....E-.

3) Etude de la trame DHCP DISCOVER

Adresse MAC Source et Destinations de la Trame DHCP:

- MAC Source: 74-56-3c-2f-80-d8
- MAC Destination: FF-FF-FF-FF-FF-FF

Caractéristique de l'adresse de couche 2 de destination de cette trame :

- C'est une Adresse envoyer en Broadcast

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

- C'est le champ Ethertype qui suis immédiatement les deux adresses MAC

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

- Il contient la valeur 0800 ce qui signifie que derrière il va y avoir un paquet IP

Quels sont les protocoles inclus dans cette trame ?:

- Il y a le protocole IP
- le protocole UDP
- et le protocole DHCP

Sélection de l'en tête IP de la Trame DHCP:

The screenshot shows the Wireshark interface. On the left, the 'Packet Details' pane is expanded to show the 'Internet Protocol Version 4' section. The 'Protocol' field is highlighted in red and contains the value '17'. Below it, the 'Source Address' is '0.0.0.0' and the 'Destination Address' is '255.255.255.255'. On the right, the 'Packet Bytes' pane shows the hex data of the packet. The first few bytes are 'ff ff ff ff ff ff 74 56 3c 2f 80 d8 00 00 05 00', which correspond to the IP header fields: version (4), IHL (5), DSCP (0x00), total length (328), identification (0xa318), flags (0x00), fragment offset (0), and time to live (128).

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:

- Il s'agit du champ protocole, la valeur de ce champ ici est de 11(17 en hexa) il s'agit donc du protocole UDP

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

Version = 4

IHL (val. déci. et hexa.) = 20 octets (5 decimal, 0x05 hexadecimal)

Protocole (val. déci. et hexa.) = UDP (11 decimal, 17 hexadecimal)

Source adresses (val. déci. et hexa.) = 0.0.0.0 en décimal et 00.00.00.00 en hexadécimal

Destination adresses (val. déci. et hexa.) = 255.255.255.255 en décimal FF-FF-FF-FF en hexadécimal

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

- La valeur 0.0.0.0 qui est contenu dans le champ adresse IP source signifie que la machine qui envoie la Trame n'a pas encore d'adresse IP attribuer il cherche donc a en obtenir une via une trame DHCP

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

- Elle est en broadcast, elle envoie donc la trame a toute les machines du reseaux

Sélection de l'en tête du datagramme UDP de la Trame DHCP:

```
Frame 2503: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{90AD83AE-6A19-4C15-B3C0-5F1DF612D...
Ethernet II, Src: GigaByteTech_2f:80:d8 (74:56:3c:2f:80:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
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: 0x1c01 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 48]
  [Stream Packet Number: 2]
  [Timestamps]
  UDP payload (300 bytes)
  Dynamic Host Configuration Protocol (Discover)
0000 ff ff ff ff ff ff 74 56 3c 2f 80 d8 08 00 45 00 .....tV </... E
0010 01 48 f2 ab 00 00 00 11 00 00 00 00 00 00 ff ff H.....
0020 ff ff 00 44 00 43 01 34 1c 01 01 01 06 00 a5 7c ..D:C:4.....|
0030 ae 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Q.....
0040 00 00 00 00 00 00 74 56 3c 2f 80 d8 00 00 00 00 .....tV </...
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 63 82 53 63 35 01 01 3d 07 01 .....c Sc5 =...
0120 74 56 3c 2f 80 d8 32 04 ac 11 02 0e 0c 09 47 31 tv</...2.....G1
0130 30 32 2d 47 42 31 33 3c 08 4d 53 46 54 28 35 2e 02-G813< MSFT 5,
0140 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07.....1+,.../wy
0150 fc ff 00 00 00 00 .....
```

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

- C'est le champ Port qui permet le démultiplexage de protocole

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 utilisé par le client DHCP est le port 68

- La valeur en hexadécimal du port 68 est 00 44

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

- Le protocole applicatif encapsulé dans le datagramme UDP est 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 port UDP utilisé par le serveur DHCP est le port 67
- La valeur du port 67 en hexadécimal est 00 43

Sélection de la section Bootstrap Protocol ou Dynamic Host Configuration Protocol (Discover) de la trame DHCP Discover :

The screenshot displays a network traffic capture in Wireshark. The packet list pane shows a DHCP Discover packet (No. 2503) with the following details:

- No.: 2503
- Time: 102.748917
- Source: 172.17.2.14
- Destination: 255.255.255.255
- Protocol: DHCP
- Length: 342
- Transaction ID: 0xa57cae51

The packet details pane shows the following structure:

- Ethernet II, Src: GigaByteTech_Zf:80:d8 (74:58:3c:2f:80:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.17.2.14, 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 (0x08)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xa57cae51
 - 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_Zf:80:d8 (74:58:3c:2f:80:d8)
 - 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
 - Option (50) Requested IP Address (172.17.2.14)
 - Option (12) Host Name
 - Option (60) Vendor class Identifier
 - Option (55) Parameter Request List
 - Option (255) End

The packet bytes pane shows the hex and ASCII representation of the packet, with a red circle highlighting the port 67 (00 43) in the UDP header.