DUPUIS Laurent

TP4 : Analyse de trames DHCP avec Wireshark

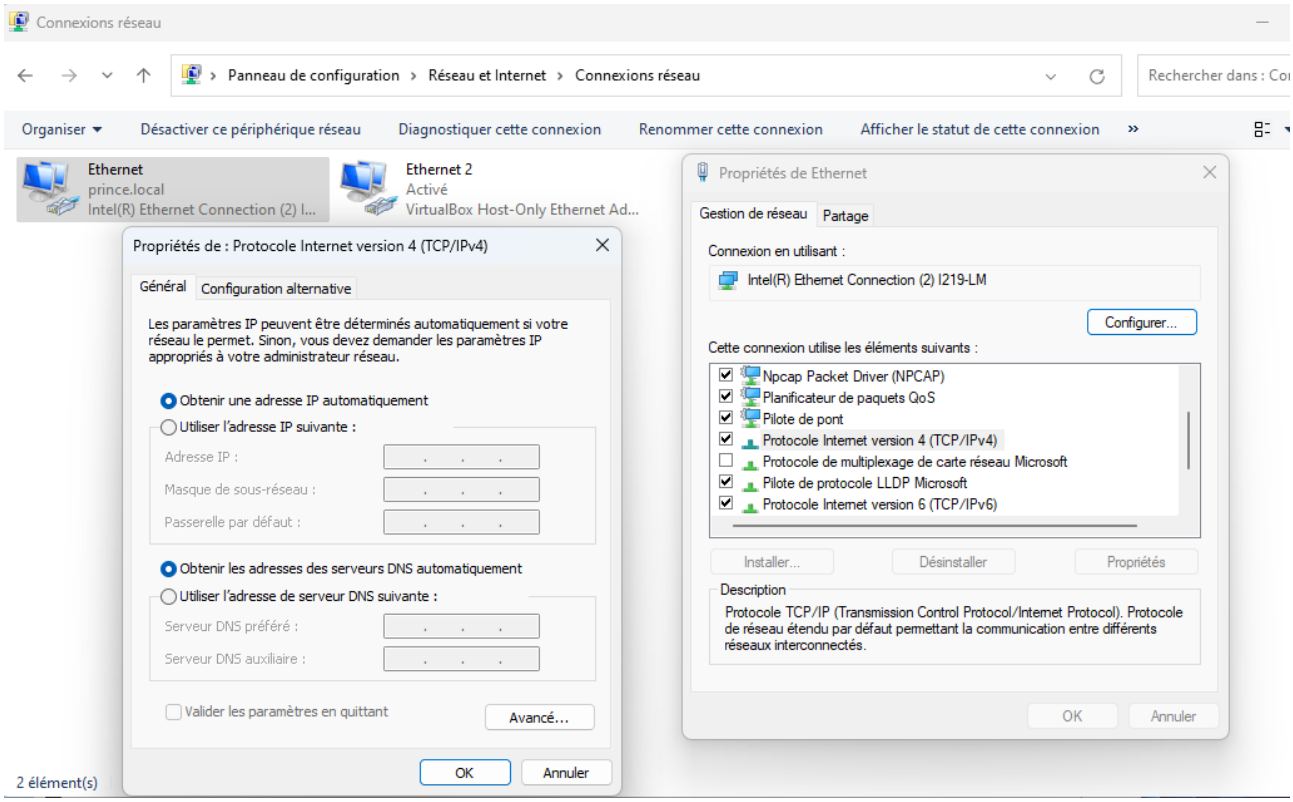
Sommaire

1. Processus d'acquisition d'une adresse IPv4

- *Cours sur le protocole DHCP.*

2. Capture de trames DHCP avec Wireshark

- Affichage des connexions réseaux ainsi que des paramètres de la carte réseau physique : On remarque que l'adresse IP est décernée automatiquement



- Ouverture d'une invite de commande et on saisit **ipconfig /all** afin de regarder quelle ip on a actuellement

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Adresse physique . . . . . . . . . . . : D8-9E-F3-12-D2-D9
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::efb:a7c:ea13:271a%3(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.1.203(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 12 octobre 2023 10:07:49
   Bail expirant. . . . . . . . . . . . . : dimanche 22 octobre 2023 11:08:32
   Passerelle par défaut. . . . . . . . . : 172.17.250.2
   Serveur DHCP . . . . . . . . . . . . . : 172.17.254.1
   IAID DHCPv6 . . . . . . . . . . . : 332963571
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2C-30-EA-95-D8-9E-F3-12-D2-D9
   Serveurs DNS. . . . . . . . . . . . . : 172.17.254.1
                                   172.17.244.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

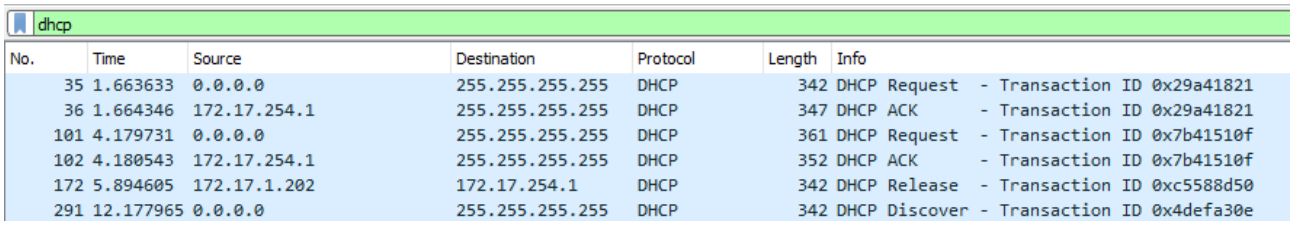
1. Questions :

- DHCP Activé : Oui
- Masque de sous-réseau : 255.255.0.0
- Bail obtenu : Jeudi 12 octobre 2023 10:07:49
- Bail expirant : Dimanche 22 octobre 2023 11:08:32
- Passerelle par défaut : 172.17.250.2
- Serveur DHCP : 172.17.254.1
- Serveur DNS : 172.17.254.1

- Capture de trame suite aux commandes :

  - ipconfig /release

  - ipconfig /renew



dhcp

No.	Time	Source	Destination	Protocol	Length	Info
35	1.663633	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x29a41821
36	1.664346	172.17.254.1	255.255.255.255	DHCP	347	DHCP ACK - Transaction ID 0x29a41821
101	4.179731	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x7b41510f
102	4.180543	172.17.254.1	255.255.255.255	DHCP	352	DHCP ACK - Transaction ID 0x7b41510f
172	5.894605	172.17.1.202	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xc5588d50
291	12.177965	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4defa30e

- Commande ipconfig /release :

  Adresse IPv4 : 0.0.0.0

  Masque de sous-réseau : 0.0.0.0

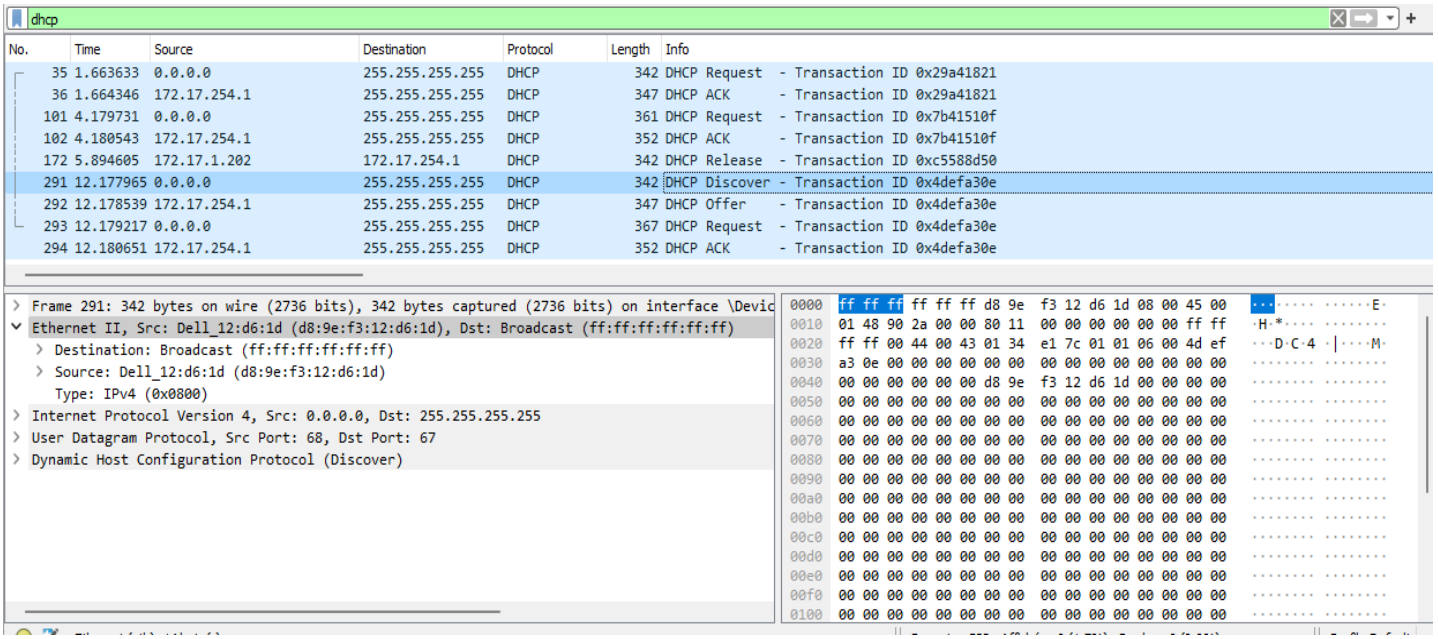
  Passerelle par défaut : Aucune

- Commande ipconfig /renew :

  Adresse IPv4 : 172.17.1.202

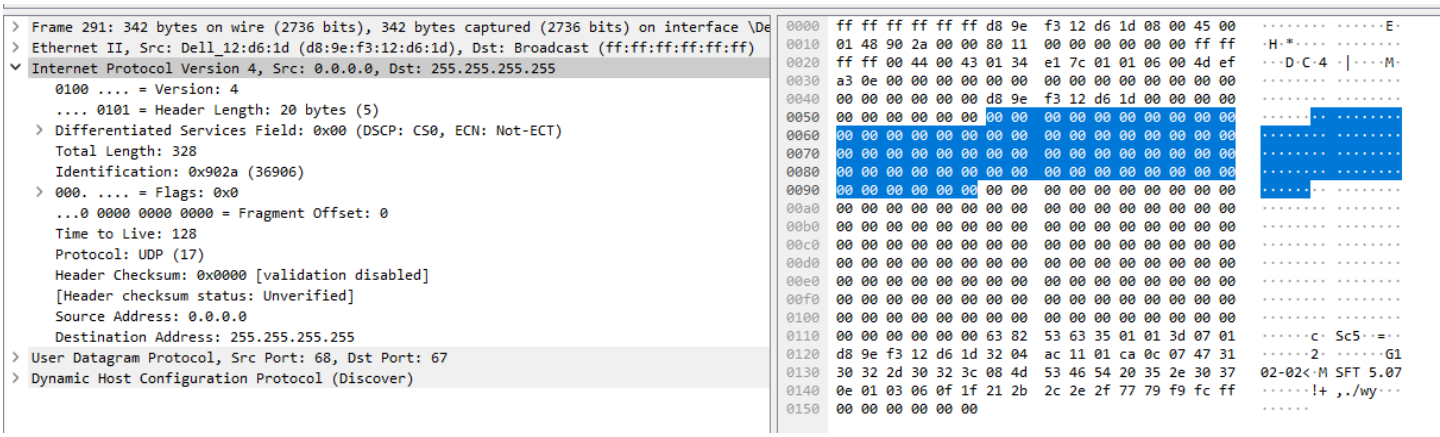
  Masque de sous-réseau : 255.255.0.0

  Passerelle : 172.17.250.2

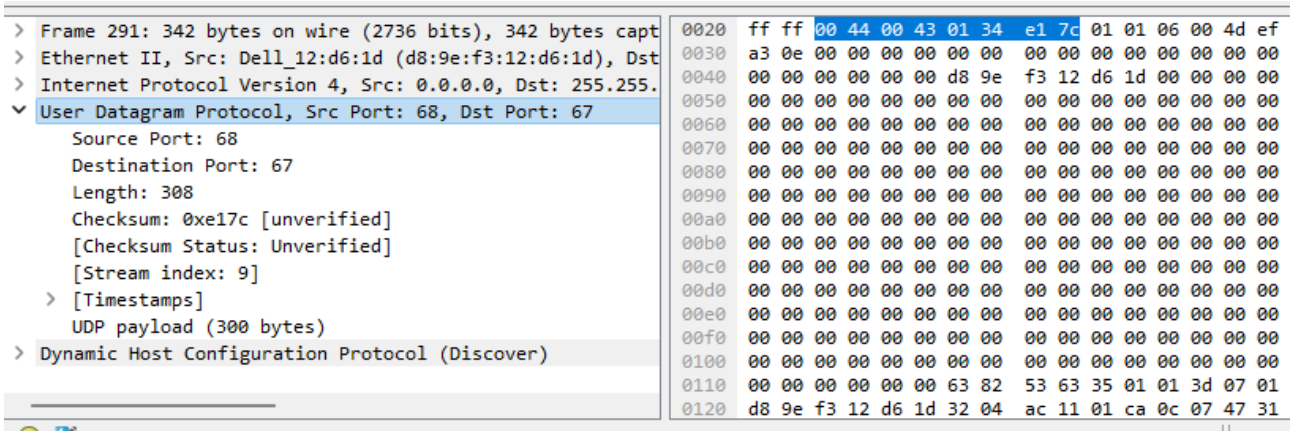


4. Etude de la trame DHCP Discover

- Adresse MAC destination : FF.FF.FF.FF.FF.FF
- Adresse MAC source : d8.9e.f3.12.d6.1d
- L'adresse de couche 2 de destination est une adresse de broadcast limité
- Le champ qui suit les deux adresses MAC est le champ Ethertype
- La valeur comprise dans le champ Ethertype est 08 00 soit IPv4 (80 en décimal)
- Les différents protocoles sont : Ethernet, IPv4, UDP, DHCP

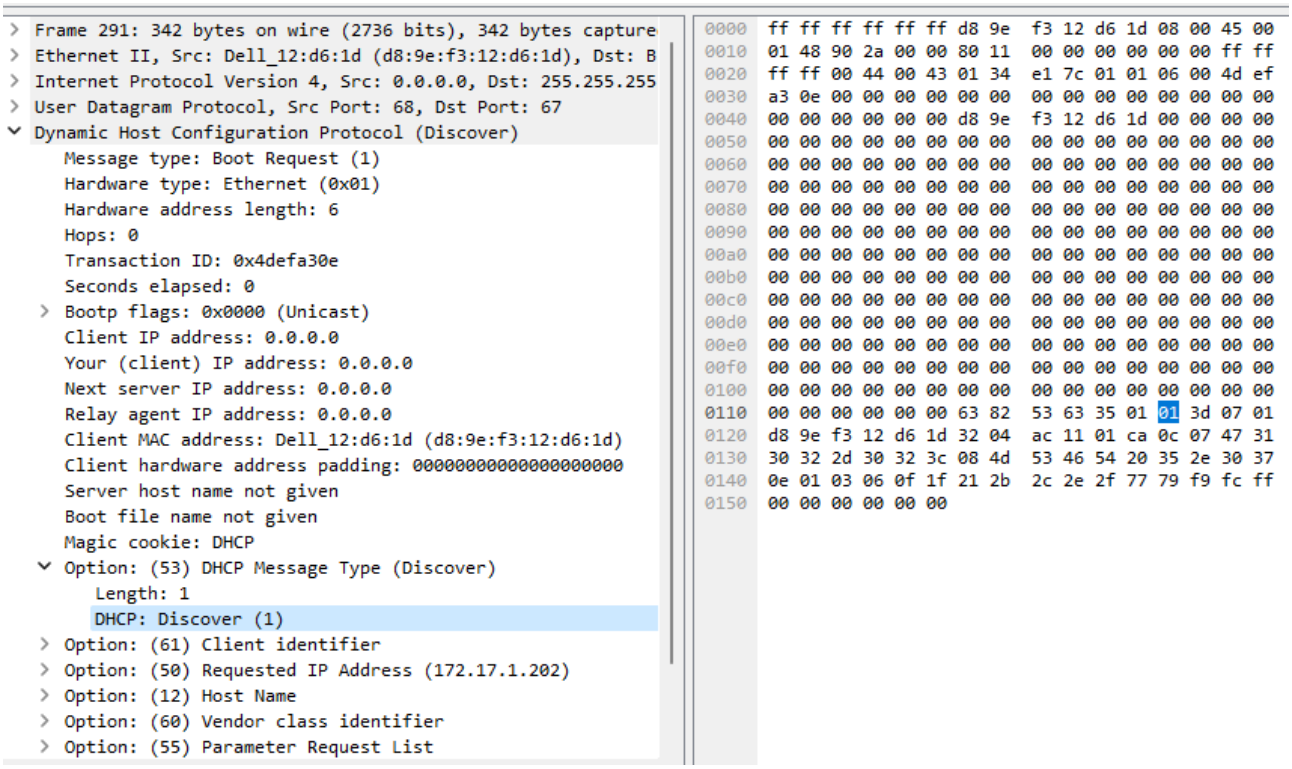


- C’est le champ protocole, il contient en valeur 11 (17 en décimal), il s’agit du protocole UDP.
- Version : 4
- IHL : 5_{16} soit 5_{10}
- Protocole : 11_{16} soit 17_{10}
- Source address : 00 00 00 00 soit 0.0.0.0
- Destination address : 255.255.255.255 soit FF FF FF FF
- L’adresse de couche 3 de destination est une adresse de Broadcast limité



- Le champ de l’en-tête de transport permettant le démultiplexage de protocole est le champ port
- Le port UDP utilisé par le Client est le port 68 (00 44)
- Le protocole applicatif encapsulé dans UDP est DHCP (67/68)
- Le port UDP utilisé par le Serveur DHCP est 67 (00 43)

Contenu de la couche Protocole Applicative


Frame 291: 342 bytes on wire (2736 bits), 342 bytes capture
Ethernet II, Src: Dell_12:d6:1d (d8:9e:f3:12:d6:1d), Dst: B
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 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: 0x4defa30e
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: Dell_12:d6:1d (d8:9e:f3:12:d6:1d)
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 (172.17.1.202)
Option: (12) Host Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
0000 ff ff ff ff ff ff d8 9e f3 12 d6 1d 08 00 45 00
0010 01 48 90 2a 00 00 80 11 00 00 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 e1 7c 01 01 06 00 4d ef
0030 a3 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 d8 9e f3 12 d6 1d 00 00 00 00
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
0120 d8 9e f3 12 d6 1d 32 04 ac 11 01 ca 0c 07 47 31
0130 30 32 2d 30 32 3c 08 4d 53 46 54 20 35 2e 30 37
0140 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 fc ff
0150 00 00 00 00 00 00