

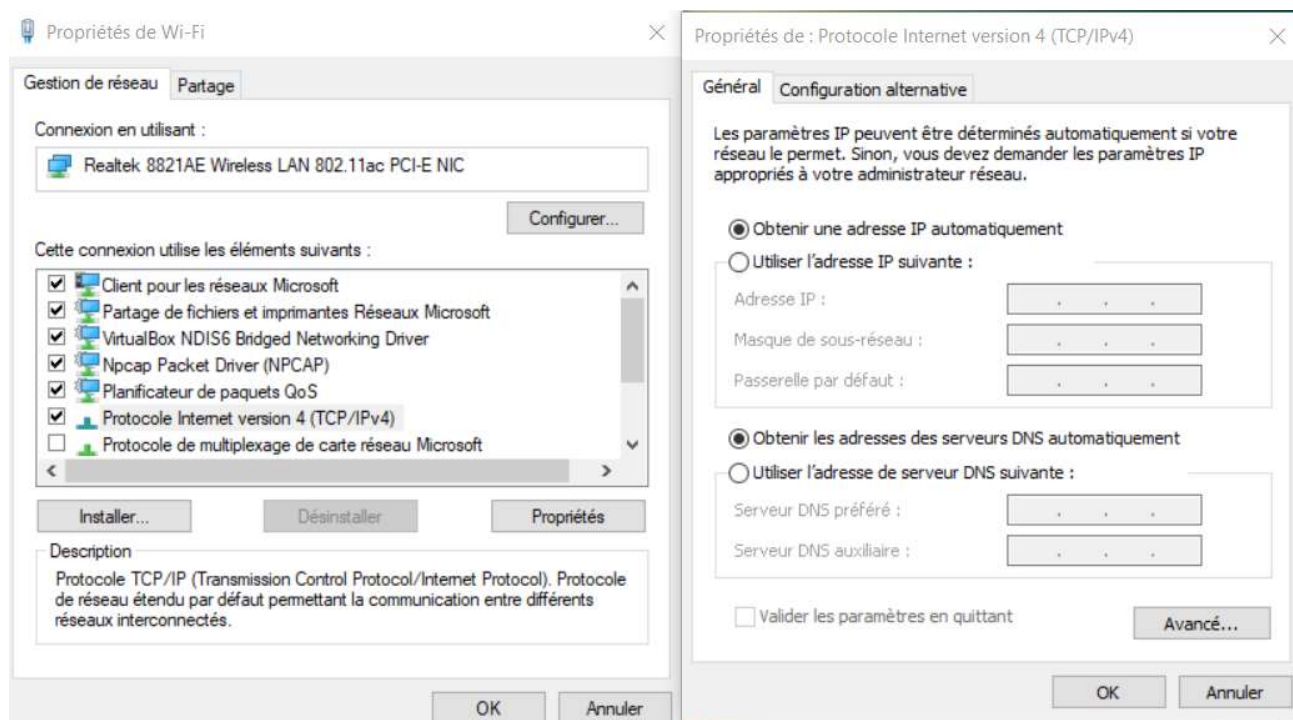
TD4 : analyse de trames DHCP avec Wireshark

Sommaire

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

1. Capture de trames DHCP avec Wireshark

On doit afficher les connexions réseau et on fait clic droit sur la carte réseau puis sélectionner Propriétés



Sur l'invite de commande, on saisit la commande « ipconfig /all » :

```
CA Invite de commandes X + v
C:\Users\llopez>ipconfig /all

Configuration IP de Windows :

Nom de l'hôte . . . . . : G102-01
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 . . . . . : Intel(R) Ethernet Connection (2) I219-LM
Adresse physique . . . . . : D8-9E-F3-12-DA-64
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::749:59c:556e:4737%17(préfééré)
Adresse IPv4 . . . . . : 172.17.1.201(préfééré)
Masque de sous-réseau . . . . . : 255.255.0.0
Bail obtenu . . . . . : mercredi 18 octobre 2023 09:31:14
Bail expirant . . . . . : mercredi 25 octobre 2023 12:02:13
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-35-BA-86-D8-9E-F3-12-DA-64
Serveurs DNS . . . . . : 172.17.254.1
                        172.17.244.1
NetBIOS sur Tcpip . . . . . : Activé
```

Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?

C'est 172.17.1.201

▪ Renseignez les autres éléments ci-dessous :

DHCP activé : Oui

Masque de sous-réseau:255.255.0.0

Bail obtenu : Mercredi 18 octobre 2023 à 9h31min et 14 secondes

Bail expirant : Mercredi 25 octobre 2023 à 12h02min et 13 secondes

Passerelle par défaut : 172.17.250.2

Serveur DHCP : 172.17.254.1

Serveur DNS : 172.17.254.1

Alors que la commande ipconfig ne renvoie que les informations suivantes :

```

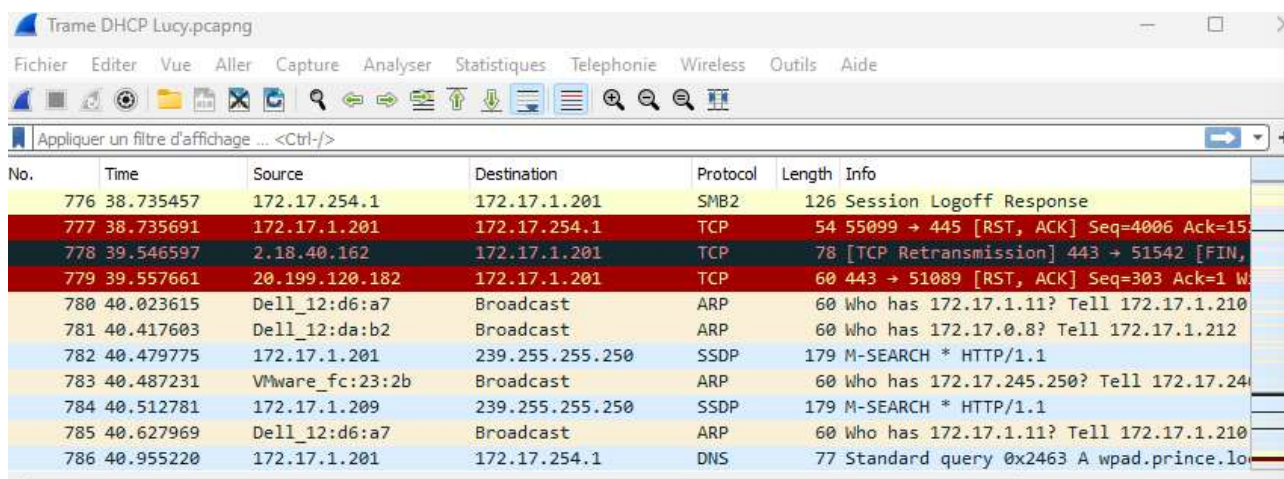
Carte Ethernet Ethernet :

  Suffixe DNS propre à la connexion. . . . : prince.local
  Adresse IPv6 de liaison locale. . . . . : fe80::749:59c:556e:4737%17
  Adresse IPv4. . . . . : 172.17.1.201
  Masque de sous-réseau. . . . . : 255.255.0.0
  Passerelle par défaut. . . . . : 172.17.250.2

Carte Ethernet Ethernet 2 :

```

Ensuite, on démarre une capture de trame avec Wireshark sur l'invite de commande avec les commandes :**ipconfig /release** et **ipconfig /renew**



No.	Time	Source	Destination	Protocol	Length	Info
776	38.735457	172.17.254.1	172.17.1.201	SMB2	126	Session Logoff Response
777	38.735691	172.17.1.201	172.17.254.1	TCP	54	55099 → 445 [RST, ACK] Seq=4006 Ack=15
778	39.546597	2.18.40.162	172.17.1.201	TCP	78	[TCP Retransmission] 443 → 51542 [FIN,
779	39.557661	20.199.120.182	172.17.1.201	TCP	60	443 → 51089 [RST, ACK] Seq=303 Ack=1 W
780	40.023615	Dell_12:d6:a7	Broadcast	ARP	60	Who has 172.17.1.11? Tell 172.17.1.210
781	40.417603	Dell_12:da:b2	Broadcast	ARP	60	Who has 172.17.0.8? Tell 172.17.1.212
782	40.479775	172.17.1.201	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
783	40.487231	VMware_fc:23:2b	Broadcast	ARP	60	Who has 172.17.245.250? Tell 172.17.24
784	40.512781	172.17.1.209	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
785	40.627969	Dell_12:d6:a7	Broadcast	ARP	60	Who has 172.17.1.11? Tell 172.17.1.210
786	40.955220	172.17.1.201	172.17.254.1	DNS	77	Standard query 0x2463 A wpad.prince.lo

- A partir des renseignements obtenus à l'aide de la commande **ipconfig /release**, renseignez les éléments ci-dessous :

Adresse IPv4 : 0.0.0.0

Masque de sous-réseau : 0.0.0.0

Passerelle par défaut :Aucune passerelle

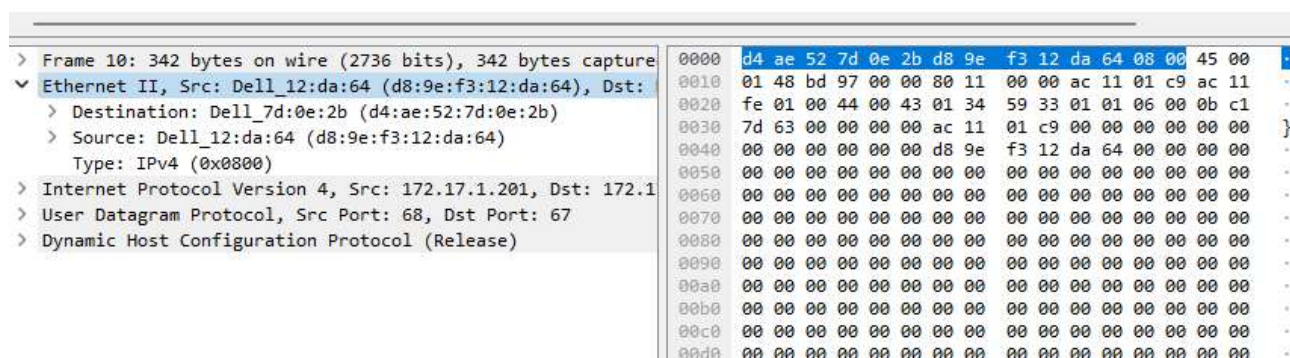
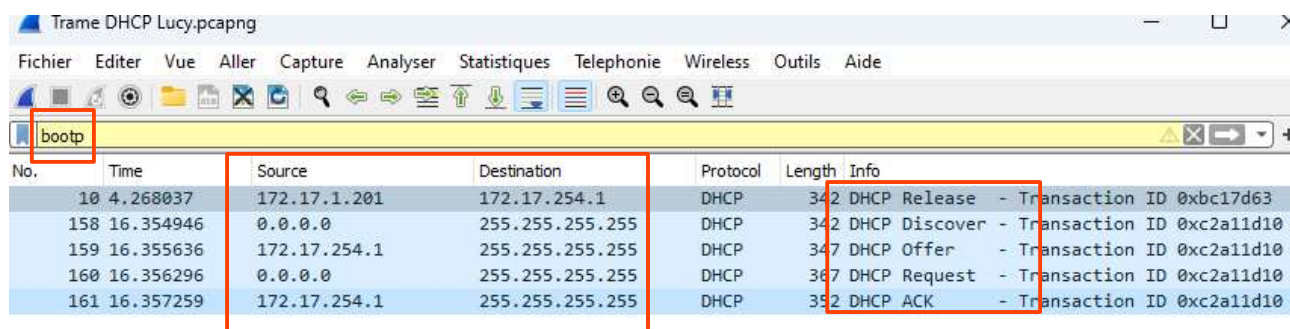
- A partir des renseignements obtenus à l'aide de la commande **ipconfig /renew**, renseignez les éléments ci-dessous :

Adresse IPv4 : 172.17.1.201

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.2

Sur Wireshark, on limite l'affichage des trames à celles encapsulant les protocoles DHCP (zone Filter), comme DHCP est une extension du protocole BOOTP, dans la zone filtrer, on tape BOOTP :



2. 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 :

NO.	Time	Source	Destination	Protocol	Length	Info
10	4.268037	172.17.1.201	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xbc17d63
158	16.354946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2a11d10
159	16.355636	172.17.254.1	255.255.255.255	DHCP	347	DHCP Offer - Transaction ID 0xc2a11d10
160	16.356296	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request - Transaction ID 0xc2a11d10
161	16.357259	172.17.254.1	255.255.255.255	DHCP	352	DHCP ACK - Transaction ID 0xc2a11d10

> Frame 158: 342 bytes on wire (2736 bits), 342 bytes captured	0000	ff ff ff ff ff ff	d8 9e f3 12 da 64	08 00	45 00
> Ethernet II, Src: Dell 12:da:64 (d8:9e:f3:12:da:64), Dst:	0010	01 40 c7 a0 00 00	80 11	00 00 00 00	00 00 ff ff
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.25	0020	ff ff 00 44 00 43 01 34	eb 3b 01 01 06 00 c2 a1		
> User Datagram Protocol, Src Port: 68, Dst Port: 67	0030	1d 10 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
> Dynamic Host Configuration Protocol (Discover)	0040	00 00 00 00 00 00 d8 9e	f3 12 da 64 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		

L'adresse mac destination est FF:FF:FF:FF:FF:FF et l'adresse source est d8 9e f3 12 da 64

▪ **Caractérisiez l'adresse de couche 2 de destination de cette trame :**

L'adresse de destination de couche 2 est une adresse de Broadcast (en couche 2 = FF:FF:FF:FF:FF:FF)

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

Le champs qui suis les deux adresses mac est le Champ Ethertype

▪ **Quelle valeur contient-il ? Que signifie t-elle ?**

La valeur est 0800 cela signifie que le protocole de la couche 3 est le protocole IPv4

▪ **Quels sont les protocoles inclus dans cette trame ?**

Les protocoles sont :

- Dans la couche réseau (couche 2) c'est le protocole Ethernet
- Dans la couche internet (couche 3) c'est le protocole IPv4
- Dans la couche transport (couche 4) C'est le protocole UDP
- Dans la couche application (couche 5,6,7), c'est le protocole DHCP .

Puis on sélectionne, l'en-tête **IP** contenu dans la trame DHCP Discover :

10	4.268037	172.17.1.201	172.17.254.1	DHCP	342	DHCP Release	- Transaction ID 0xbc17d63
158	16.354946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0xc2a11d10
159	16.355636	172.17.254.1	255.255.255.255	DHCP	347	DHCP Offer	- Transaction ID 0xc2a11d10
160	16.356296	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request	- Transaction ID 0xc2a11d10
161	16.357259	172.17.254.1	255.255.255.255	DHCP	352	DHCP ACK	- Transaction ID 0xc2a11d10

> Frame 158: 342 bytes on wire (2736 bits), 342 bytes captured

> Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst: Bro

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.2

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E

Total Length: 328

Identification: 0xe7a9 (59305)

> 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

```

0000 ff ff ff ff ff ff d8 9e f3 12 da 64 08 00 45 00
0010 01 48 e7 a9 00 00 00 11 00 00 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 eb 3b 01 01 06 00 c2 a1
0030 1d 10 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 d8 9e f3 12 da 64 00 00 00 00
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 35 01 01 3d 07 01
0120 d8 9e f3 12 da 64 32 04 ac 11 01 c9 0c 07 47 31

```

▪ 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.

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

Version = IPv4 donc c'est version 4

IHL (val. déci. et hexa.) = 20 bytes (en hexadécimal 5) et 5 en décimal

Protocole (val. déci. et hexa.) = 17 (en hexadécimal 11)

Source address (val. déci. et hexa.) = 0.0.0.0 (en hexadécimal 0.0.0.0)

Destination address (val. déci. et hexa.) = 255.255.255.255 (en hexadécimal FF:FF:FF:FF)

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

Cela veut dire que la machine source n'a pas adresse IP

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

L'adresse de destination est 255.255.255.255 donc c'est une adresse de broadcast (en hexadécimal FF:FF:FF:FF)

Troisièmement, on sélectionne, l'en-tête du **datagramme UDP** contenu dans la trame DHCP Discover.

10	4.268037	172.17.1.201	172.17.254.1	DHCP	342 DHCP Release	- Transaction ID 0xbc17d63
158	16.354946	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0xc2a11d10
159	16.355636	172.17.254.1	255.255.255.255	DHCP	347 DHCP Offer	- Transaction ID 0xc2a11d10
160	16.356296	0.0.0.0	255.255.255.255	DHCP	367 DHCP Request	- Transaction ID 0xc2a11d10
161	16.357259	172.17.254.1	255.255.255.255	DHCP	352 DHCP ACK	- Transaction ID 0xc2a11d10

Frame 158: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), 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: 0xeb3b [unverified]

[Checksum Status: Unverified]

[Stream index: 19]

[Timestamps]

UDP payload (300 bytes)

Dynamic Host Configuration Protocol (Discover)

0020 ff ff 00 44 00 43 01 34 eb 3b 01 01 06 00 c2 a1

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

Le champ port est le nom du champ permettant le démultiplexage de protocole (ici c'est les 4 1^{er} octets (port source et port destination))

▪ 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) ;

Le port UDP utilisé par le client est le 00 44 = 68 donc DHCP

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

C'est en hexadécimal 00 44 et 00 43 ce qui correspond en décimal 67/68 qui est le protocole applicatif 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 est 00 43 = 67

Pour finir, on sélectionne la section **Bootstrap Protocol** contenu dans la trame DHCP Discover :

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
10	4.268037	172.17.1.201	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xbc17d63
158	16.354946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2a11d10
159	16.355636	172.17.254.1	255.255.255.255	DHCP	347	DHCP Offer - Transaction ID 0xc2a11d10
160	16.356296	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request - Transaction ID 0xc2a11d10
161	16.357259	172.17.254.1	255.255.255.255	DHCP	352	DHCP ACK - Transaction ID 0xc2a11d10

> Frame 158: 342 bytes on wire (2736 bits), 342 bytes captured
> Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst: Bro
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.2
> 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: 0xc2a11d10
 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:da:64 (d8:9e:f3:12:da:64)
 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 (172.17.1.201)

0000 ff ff ff ff ff ff d8 9e f3 12 da 64 08 00 45 00
0010 01 48 e7 a9 00 00 80 11 00 00 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 eb 3b 01 01 06 00 c2 a1
0030 1d 10 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 d8 9e f3 12 da 64 00 00 00 00
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 35 01 3d 07 01
0120 d8 9e f3 12 da 64 32 04 ac 11 01 c9 0c 07 47 31
0130 30 32 2d 30 31 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