

TP4 : analyse de trames DHCP avec Wireshark

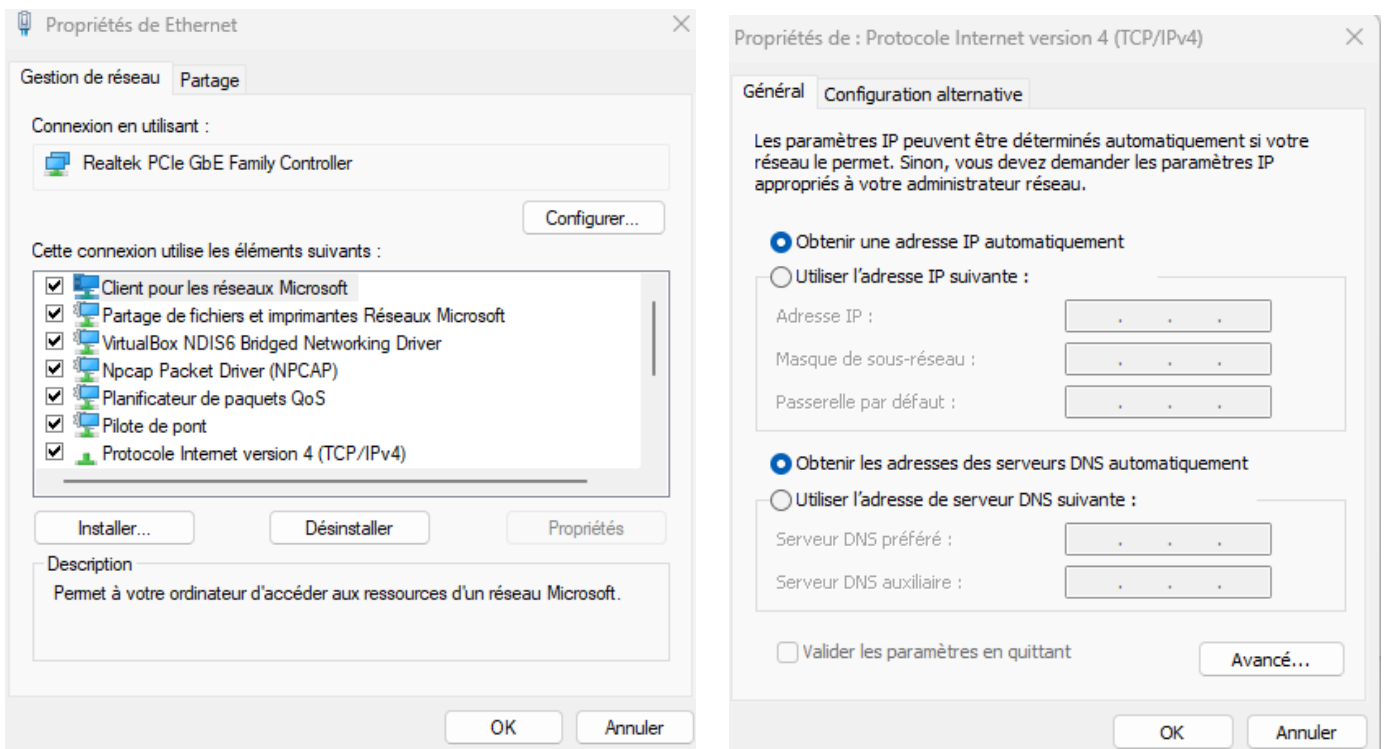
- 1. Processus d'acquisition d'une adresse IPv4 1
- 2. Capture de trames DHCP avec Wireshark..... 1
- 3. Etude de la trame DHCP DISCOVER 6

1. Processus d'acquisition d'une adresse IPv4

2. Capture de trames DHCP avec Wireshark.

- Les propriétés TCP/IPv4 de votre machine physique doivent être définies de manière à obtenir automatiquement les paramètres IP (adresse IP, masque de sous-réseau, passerelle ainsi que l'adresse du serveur DNS) auprès du serveur DHCP ROI :

Afficher les connexions réseau et cliquer droit sur la carte réseau puis sélectionner Propriétés :



- Ouvrez une invite de commandes et saisissez la commande ipconfig /all :

```
C:\Users\racroquelois>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : G102-GB05
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-9B-EC
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::9141:52fb:a4e9:45a7%14(préfééré)
Adresse IPv4. . . . . : 172.17.2.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : vendredi 18 octobre 2024 10:56:30
Bail expirant. . . . . : samedi 19 octobre 2024 15:10:07
Passerelle par défaut. . . . . : 172.17.250.2
Serveur DHCP . . . . . : 172.17.244.1
IAID DHCPv6 . . . . . : 326391356
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-8C-79-2A-74-56-3C-2F-9B-EC
Serveurs DNS. . . . . : 172.17.254.1
                        172.17.244.1
                        80.10.246.2
                        8.8.8.8

NetBIOS sur Tcpip. . . . . : Activé
```

Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?
172.17.2.2

- Renseignez les autres éléments ci-dessous :

DHCP activé : oui

Masque de sous-réseau : 255.255.0.0

Bail obtenu : vendredi 18 octobre 2024 10 :56 :30

Bail expirant : samedi 19 octobre 2024 15 :10 :07

Passerelle par défaut : 172.17.250.2

Serveur DHCP : 172.17.244.1

Serveur DNS : 172.17.254.1 / 172.17.244.1 / 80.10.246.2 / 8.8.8.8

A titre de comparaison, la commande ipconfig ne renvoie que les informations suivantes :

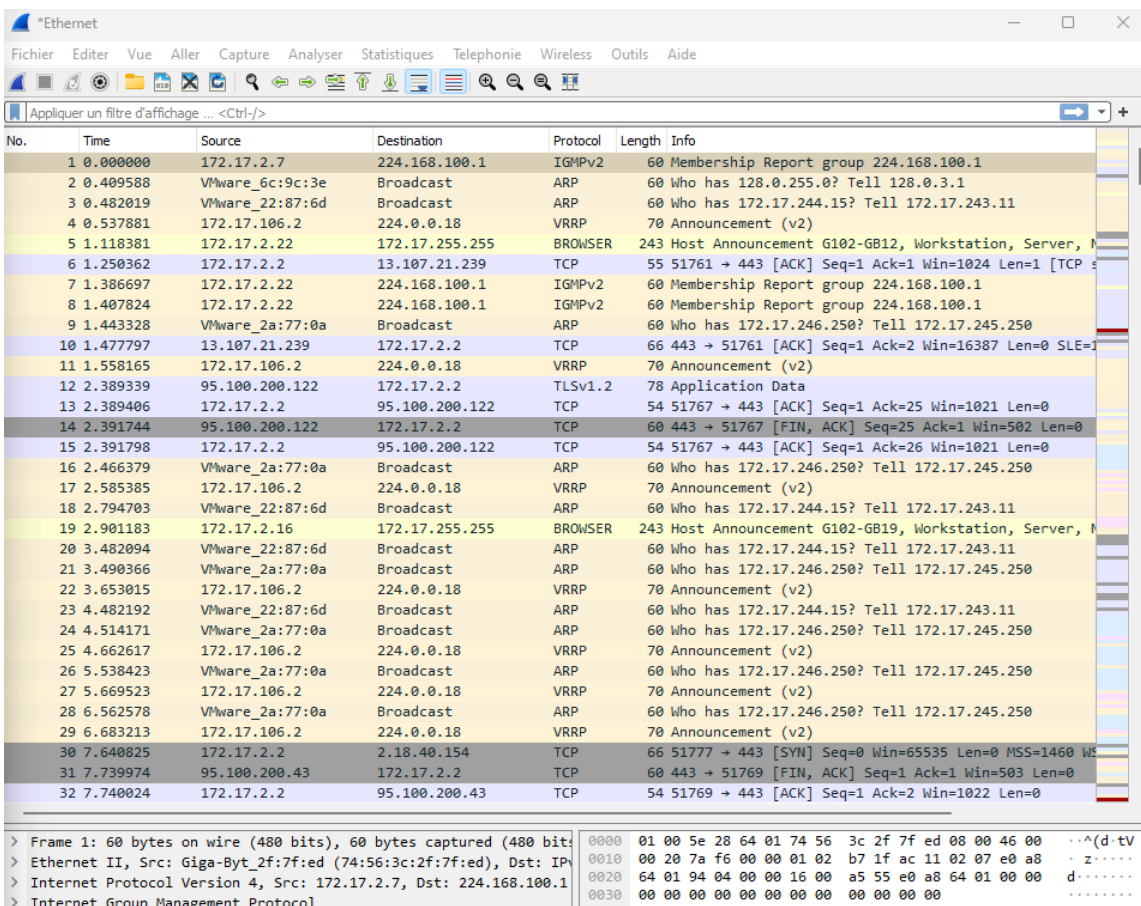
```
C:\Users\rcroquelois>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : prince.local
    Adresse IPv6 de liaison locale. . . . . : fe80::9141:52fb:a4e9:45a7%14
    Adresse IPv4. . . . . : 172.17.2.2
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.2
```

- 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 « Roi ». Ouvrez une invite de commandes et tapez successivement les commandes : - ipconfig /release - ipconfig /renew

```
C:\Users\rcroquelois>ipconfig /release

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::9141:52fb:a4e9:45a7%14
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::507e:75c4:c3b6:eea9%16
    Adresse IPv4. . . . . : 192.168.56.1
    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::f17d:fb8f:bdf3:628f%18
    Adresse IPv4. . . . . : 172.23.48.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :

C:\Users\rcroquelois>
```

```
C:\Users\rcroquelois>ipconfig /renew

Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::f17d:fb8f:bdf3:628f%18
    Adresse IPv4. . . . . : 172.23.48.1
    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::9141:52fb:a4e9:45a7%14
    Adresse IPv4. . . . . : 172.17.2.2
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.2

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::507e:75c4:c3b6:eea9%16
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

- Ne fermez pas l'invite de commandes, revenez à la fenêtre de Wireshark et cliquez sur le bouton Arrêt de la capture et enregistrez les informations capturées dans un fichier nommé « TramesDHCP » :

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

Adresse IPv4 : 172.23.48.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : vide

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

Adresse IPv4 : 172.17.2.2

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.2

- Limitez l'affichage des trames à celles encapsulant les protocoles DHCP (zone Filter). Rappelez-vous que le protocole DHCP est une extension du protocole BOOTP (Bootstrap protocole). A l'exception des adresses physiques et logiques, la fenêtre de capture obtenue devrait ressembler à celle figurant ci-après (la trame 506 DHCP DISCOVER a ici été sélectionnée et la section correspondant à l'en-tête Ethernet a été développée) :

The screenshot shows the Wireshark interface with a DHCP capture. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
45	4.055914	172.17.2.2	172.17.244.1	DHCP	342	DHCP Release - Transaction ID 0xbaa8eeb5
111	10.543978	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2e88a59b
112	10.544751	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x2e88a59b
113	10.545235	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x2e88a59b
114	10.547192	172.17.244.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x2e88a59b
506	15.323001	0.0.0.0	255.255.255.255	DHCP	365	DHCP Request - Transaction ID 0xc9216e05
507	15.325090	172.17.244.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0xc9216e05

The details pane for the selected packet (Frame 111) shows the following structure:

- Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), 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
- Dynamic Host Configuration Protocol (Discover)

The hexadecimal dump shows the raw bytes of the packet, with the destination MAC address (ff:ff:ff:ff:ff:ff) highlighted in red.

3. 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 :

Adresse MAC source : 74 : 56 : 3c : 2f : 9b : ec

Adresse MAC destination : ff : ff : ff : ff : ff : ff

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

L'adresse de la couche 2 est une adresse broadcast, elle est donc inconnue.

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

On peut voir que c'est le champ IPv4 (0800).

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

Ceci est la valeur 0800 ce qui signifie que nous sommes sous IPv4

- Quels sont les protocoles inclus dans cette trame ?

Nous avons les protocoles :

-Ethernet

-Réseau IP

-Transport UDP

-BOOTP

-Et DHCP

- Sélectionnez, comme dans la figure ci-dessous, l'en-tête IP contenu dans la trame DHCP Discover.

```

> Frame 111: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Broadcast
  > 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: 0x7f6a (32618)
    > 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
  > User Datagram Protocol, Src Port: 68, Dst Port: 67
  > Dynamic Host Configuration Protocol (Discover)
  
```

```

0000 ff ff ff ff ff 74 56 3c 2f 9b ec 00 00 45 00 .....tV<
0010 01 48 7f 6a 00 00 80 11 00 00 00 00 00 ff ff ..H.j....
0020 ff ff 00 44 00 43 01 34 63 90 01 01 06 00 2e 88 ...D.C.4 d
0030 a5 9b 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 00 00 74 56 3c 2f 9b ec 00 00 00 00 .....tV<
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 .....c.S
0120 74 56 3c 2f 9b ec 32 04 ac 11 02 02 0c 09 47 31 tv</-2:
0130 30 32 2d 47 42 30 35 3c 08 4d 53 46 54 20 35 2e 02-GB05<
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
  
```

- 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 11, qui est donc le protocole UDP

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

Version = 4

IHL (val. déci. et hexa.) = déci : 20 hexa : 45

Protocole (val. déci. et hexa.) = déci : 11 hexa : 17

Source address (val. déci. et hexa.) = déci : 0.0.0.0 hexa : 00 00 00 00

Destination address (val. déci. et hexa.) = déci : 255.255.255.255 hexa : ff : ff : ff : ff : ff : ff

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

C'est l'adresse IP de la machine qui a effectuée la requête.

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

L'adresse de la couche 3 est une broadcast, elle est donc inconnue.

- Sélectionnez, comme dans la figure ci-dessous, l'en-tête du datagramme UDP contenu dans la trame DHCP Discover.

```

> Frame 111: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: Brocade-CE_08:00:27:00:00:00
> 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: 0x6398 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
    > [Timestamps]
    UDP payload (300 bytes)
  > Dynamic Host Configuration Protocol (Discover)

```

0000	ff	ff	ff	ff	ff	74	56	3c	2f	9b	ec	08	00	45	00tv<
0010	01	48	7f	6a	00	00	00	00	00	00	00	00	00	ff	ff	..H.j....
0020	ff	ff	00	44	00	43	01	34	63	90	01	01	06	00	2e	...D.C.4<
0030	a5	9b	00	00	00	00	00	00	00	00	00	00	00	00	00<
0040	00	00	00	00	00	00	74	56	3c	2f	9b	ec	00	00	00tv<
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	07c.S
0120	74	56	3c	2f	9b	ec	32	04	ac	11	02	02	0c	09	47	..tv</-2-
0130	30	32	2d	47	42	30	35	3c	08	4d	53	46	54	20	35	..02-GB05<
0140	30	37	0e	01	03	06	0f	1f	21	2b	2c	2e	2f	77	79	..07.....!
0150	fc	ff	00	00	00	00	00	00	00	00	00	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 UDP

▪ 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 UDP utilisé par le client est le port 68 et sa valeur hexadécimale est 00 44.

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

Le protocole applicatif encapsulé dans UDP est 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.

Le port UDP utilisé par le serveur est le port 67 et sa valeur hexadécimale est 00 43.

- Sélectionnez la section Bootstrap Protocol contenu dans la trame DHCP Discover :

The screenshot shows the Wireshark interface with the following details:

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
45	4.055914	172.17.2.2	172.17.244.1	DHCP	342	DHCP Release - Transaction ID 0xbaa0eeb5
111	10.543978	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2e88a59b
112	10.544751	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x2e88a59b
113	10.545235	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0x2e88a59b
114	10.547192	172.17.244.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x2e88a59b
566	15.323001	0.0.0.0	255.255.255.255	DHCP	365	DHCP Request - Transaction ID 0xc9216e05
567	15.325090	172.17.244.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0xc9216e05

Packet Details (Frame 111):

- Ethernet II, Src: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec), Dst: ...
- 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: 0x2e88a59b
 - 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: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec)
 - 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
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: Giga-Byt_2f:9b:ec (74:56:3c:2f:9b:ec)
 - Option: (50) Requested IP Address (172.17.2.2)
 - Length: 4

Packet Bytes:

```

0000 ff ff ff ff ff ff 74 56 3c 2f 9b ec 08 00 45 00 .....tv <
0010 01 48 7f 6a 00 00 80 11 00 00 00 00 00 00 ff ff ..H.j....
0020 ff ff 00 44 00 43 01 34 63 90 01 01 06 00 2e 88 ...D.C.4 c
0030 a5 9b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....tv <
0040 00 00 00 00 00 00 74 56 3c 2f 9b ec 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 .....c.S
0120 74 56 3c 2f 9b ec 32 04 ac 11 02 02 0c 09 47 31 tv/<...2..
0130 30 32 2d 47 42 30 35 3c 08 4d 53 46 54 20 35 2e 02-G805<
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 .....
  
```