

Compte-Rendu TP2Bloc1exSI2- TrameDHCP

2.Capture de trames DHCP avec Wireshark

```
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::1960:4a09:9423:9eae%16(préfééré)
  Adresse IPv4. . . . . : 172.17.1.203(préfééré)
  Masque de sous-réseau. . . . . : 255.255.0.0
  Bail obtenu. . . . . : mercredi 14 octobre 2020 09:15:34
  Bail expirant. . . . . : mercredi 14 octobre 2020 10:18:26
  Passerelle par défaut. . . . . : 172.17.250.2
  Serveur DHCP . . . . . : 172.17.254.1
  IAID DHCPv6 . . . . . : 416849651
  DUID de client DHCPv6. . . . . : 00-01-00-01-24-A8-00-97-D8-9E-F3-12-D2-D9
  Serveurs DNS. . . . . : 172.17.254.1
                          80.10.246.2
                          172.17.244.1
                          80.10.246.129
  NetBIOS sur Tcip. . . . . : Activé
```

L'adresse IP attribuée par le serveur est 172.17.1.203

Renseignez les autres éléments :

- Masque de sous-réseau : 255.255.0.0
- Bail obtenu : Mercredi 14 Octobre 2020 09 :15 :34
- Bal expirant : Mercredi 14 Octobre 2020 10 :18 :26
- Passerelle par défaut : 172.17.250.2
- Serveur DHCP : 172.17.254.1
- Serveur DNS : 172.17.254.1

```
C:\Windows\system32>ipconfig /release

Configuration IP de Windows

Carte Ethernet VirtualBox Host-Only Network :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::a836:54c6:fde4:5bce%9
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::1960:4a09:9423:9eae%16
    Passerelle par défaut. . . . . :
```

Adresse IPv4 : 0.0.0.0

Masque de sous-réseau : 0.0.0.0

Passerelle par défaut : 0.0.0.0

```
C:\Windows\system32>ipconfig /renew

Configuration IP de Windows

Carte Ethernet VirtualBox Host-Only Network :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::a836:54c6:fde4:5bce%9
    Adresse IPv4. . . . . : 192.168.56.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : prince.local
    Adresse IPv6 de liaison locale. . . . . : fe80::1960:4a09:9423:9eae%16
    Adresse IPv4. . . . . : 172.17.1.203
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.2
```

Adresse IPv4 : 172.17.1.203

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.2

4. Etude de la trame DHCP Discover

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|--------------|-----------------|----------|--------|-----------------------|
| 25 | 10.337391 | 172.17.1.203 | 172.17.254.1 | DHCP | 342 | DHCP Release - Trans |
| 101 | 11.400592 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Trans |
| 102 | 11.401201 | 172.17.254.1 | 255.255.255.255 | DHCP | 355 | DHCP Offer - Trans |
| 103 | 11.401637 | 0.0.0.0 | 255.255.255.255 | DHCP | 375 | DHCP Request - Trans |
| 104 | 11.402511 | 172.17.254.1 | 255.255.255.255 | DHCP | 360 | DHCP ACK - Trans |
| 286 | 16.557487 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Trans |
- Packet Details (Frame 101):**
 - Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7)
 - 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)
- Packet Bytes:**

```

0000  ff ff ff ff ff ff d8 9e f3 12 d6 a7 08 00 45 00  .....E.
0010  01 48 00 40 00 00 80 11 39 66 00 00 00 00 ff ff  .H@...9f....
0020  ff ff 00 44 00 43 01 34 f4 0e 01 01 06 00 e8 73  ...D.C.4.....s
0030  7e 91 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 a7 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  .....

```

L'adresse MAC Source de la trame DHCP Discover dans le volet des octets est :

d8 :9e :f3 :12 :d6 :a7 :08 :00

L'adresse MAC destination de la trame DHCP Discover dans le volet des octets est : ff :ff :ff :ff :ff :ff

L'adresse de couche 2 de destination de cette trame est une adresse de broadcast.

Le champ qui suit immédiatement les deux adresses MAC est le champ éthertype.

Le champ éthertype comporte la valeur : 08 00 , ce qui signifie que le protocole IPv4 sera transporté derrière l'en-tête de trame, soit un paquet IP.

Cette trame inclut les protocoles :

IPv4

UDP (valeur 11 dans l'en-tête IP)

DHCP (valeur 00 43 pour le port destination 67, dans l'en-tête de transport)

The screenshot shows the Wireshark interface for a PCAP file named 'Trames DHCP.pcapng'. The packet list pane displays two DHCP packets:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|--------------|-----------------|----------|--------|-----------------------|
| 25 | 10.337391 | 172.17.1.203 | 172.17.254.1 | DHCP | 342 | DHCP Release - Trans |
| 101 | 11.400592 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Trans |

The packet details pane for the selected packet (No. 101) shows the following structure:

- Type: IPv4 (0x0800)
- 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: 0x0040 (64)
 - > Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: UDP (17)
 - Header checksum: 0x3966 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 0.0.0.0
 - Destination: 255.255.255.255

The packet bytes pane shows the hex and ASCII representation of the packet. The destination port 43 is highlighted in red in the hex representation: 45 00.

Le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP est le champ sur la ligne 10 qui porte la valeur 11, soit le protocole UDP.

Version : 4

IHL (val. Déc. Et Hexa.) = 20 en décimale et 14 en hexadécimale

Protocole (val. Déc. et Hexa.) = 11 en hexadécimale et 17 en décimale

Source address (val. déci. et hexa.) = 00.00.00.00 en hexadécimale et 0.0.0.0 en décimale

Destination address (val. déci. et hexa) = ff ff ff ff en hexadécimale et 255.255.255.255 en décimale

La valeur contenue dans le champ adresse IP source signifie qu'il n'y a pas d'adresse IP attribué à la machine.

L'adresse de couche 3 de destination de cette trame est une adresse IP de broadcast.

The screenshot displays the Wireshark interface for a capture file named 'Trames DHCP.pcapng'. The main window shows a list of captured packets. Two DHCP packets are visible:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|--------------|-----------------|----------|--------|-----------------------|
| 25 | 10.337391 | 172.17.1.203 | 172.17.254.1 | DHCP | 342 | DHCP Release - Trans |
| 101 | 11.400592 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Trans |

The details pane for the selected packet (No. 101) shows the following structure:

- Ethernet II, Src: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: Dell_12:d6:a7 (d8:9e:f3:12:d6:a7)
 - 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
 - Source Port: 68
 - Destination Port: 67
 - Length: 308
 - Checksum: 0xf40e [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 13]
 - [Timestamps]
- Dynamic Host Configuration Protocol (Discover)

The packet bytes pane shows the raw data of the UDP header, with the source port field (00 44 00 43) highlighted in red:

```

0020 ff ff 00 44 00 43 01 34 f4 0e 01 01 06 00 e8 73 ..D.C.4...s
0030 7e 91 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 a7 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 .....
  
```

Le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole est le champ port.

Le port UDP utilisé par le client DHCP est le port correspondant à la valeur hexadécimale 00 44, soit le port 68.

Le protocole encapsulé dans le datagramme UDP est le protocole DHCP.

Le serveur DHCP utilise le port 67 pour recevoir et écouter la requête. Elle correspond à la valeur 00 43 en hexadécimale.