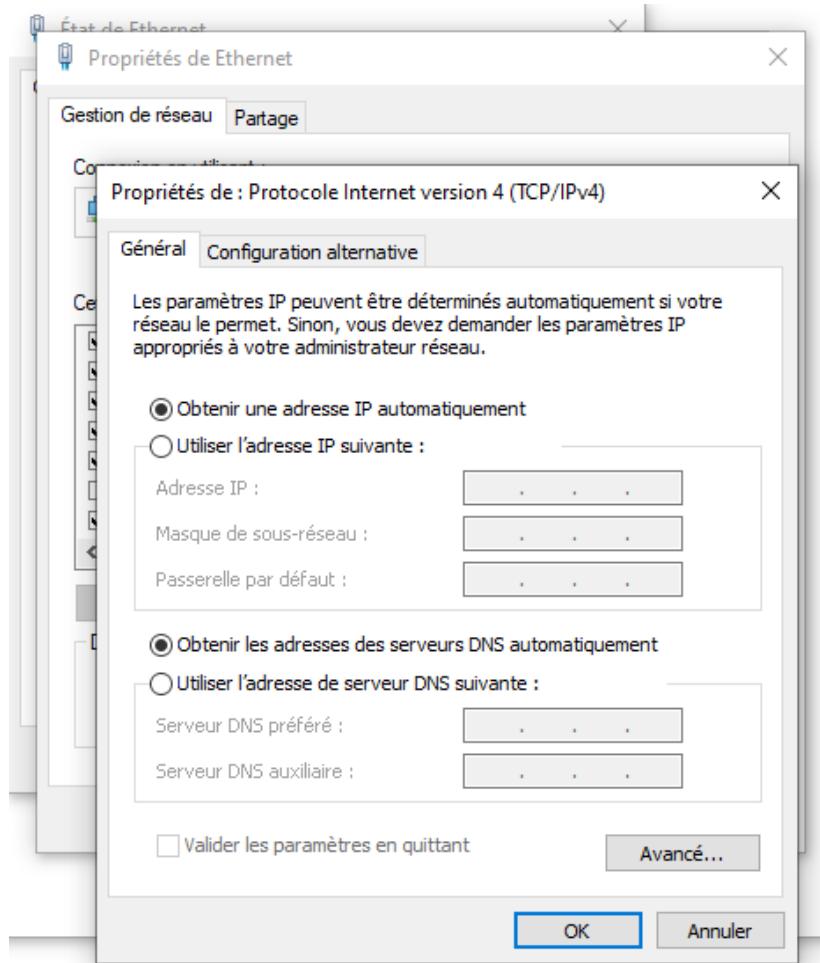


TP2: analyse de trames DHCP avec Wireshark

2) Capture de trames DHCP avec Wireshark



1ère étape: Vérifier les propriétés TCP/IPv4 de notre machine physique. Celle-ci doivent être définies de manière à obtenir automatiquement les paramètres IP.

2ème étape: Une invite de commande (cmd) est ouverte depuis notre machine physique, dans celle-ci la commande “**ipconfig /all**”.

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

Adresse IP : 172.17.2.140

Renseignez les autres éléments ci-dessous :

DHCP activé : Oui

Masque de sous-réseau : 255.255.0.0

Bail obtenu : mardi 5 octobre 2021 15:50:04

Bail expirant : jeudi 21 octobre 2021 12:10:28

Passerelle par défaut : 172.17.250.1

Serveur DHCP : 172.17.244.1

Serveur DNS : 172.17.254.1

3ème étape : Durant une capture de trame sur Wireshark, la commande “**ipconfig /release**” est effectuée, celle-ci permet de libérer l’adresse IP qui avait été obtenue.

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

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : Absence de passerelle par défaut

4ème étape: Ici nous saisissons la commande “ipconfig /renew”, celle-ci envoie une requête à un serveur DHCP dont l’objectif est d’obtenir ou de renouveler un bail pour une adresse IP.

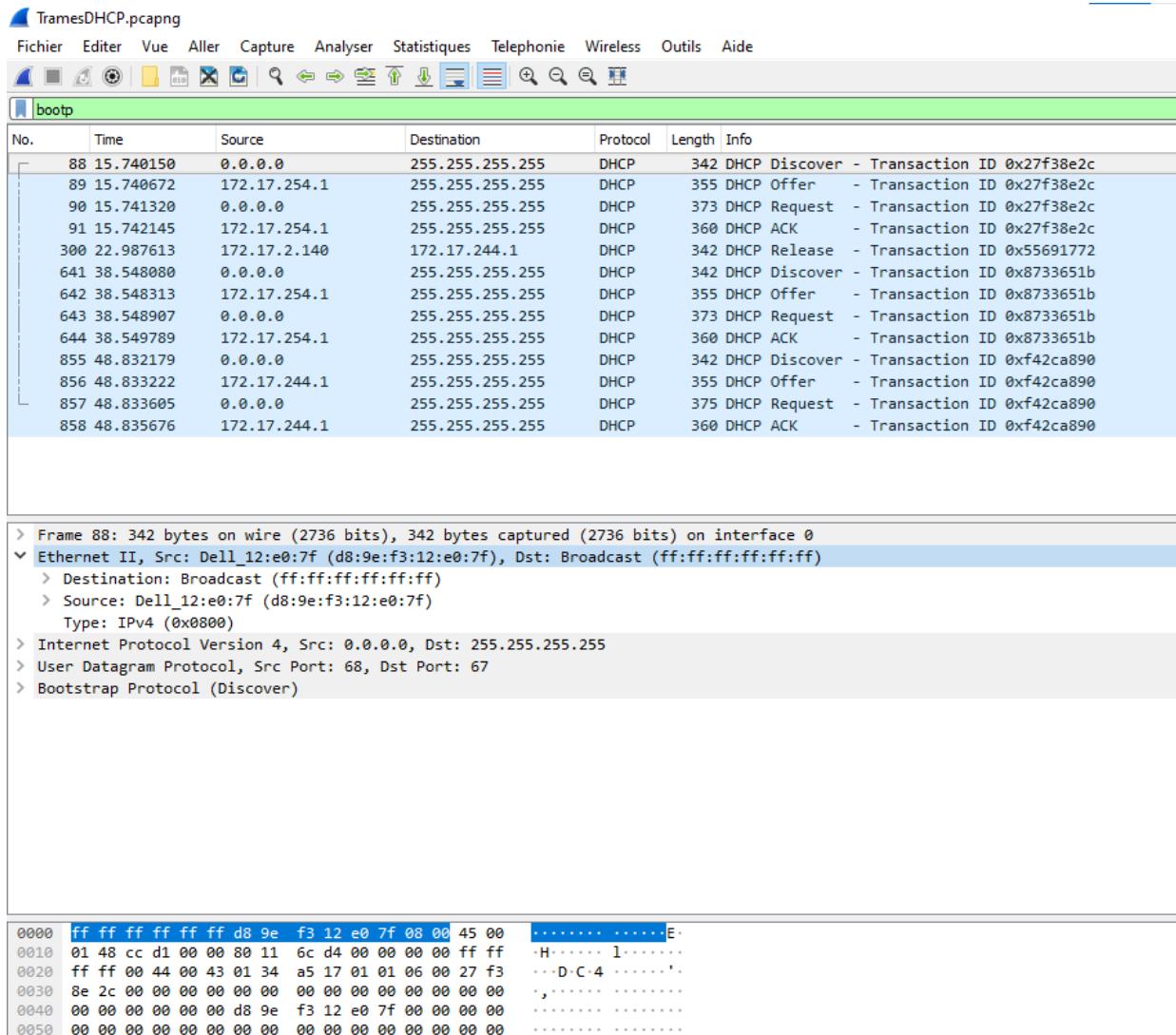
A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : Absence de passerelle par défaut

4) Etude de la trame DHCP Discover



Identifiez les adresses MAC source et destination dans le volet des octets :

Adresse MAC destination : ff ff ff ff ff ff

Adresse Mac source : d8 9e f3 12 e0 7f

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

L'adresse de couche 2 de destination de la trame est représenté par ff ff ff ff ff, celle-ci signifie donc que c'est une adresse de broadcast.

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

Le champ Ethertype.

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

Il contient la valeur 0800.

Elle signifie donc que suit l'en-tête IP après le champ Ethertype.

Quels sont les protocoles inclus dans cette trame ?

Dans cette trame on retrouve donc un protocole

- Datagramme UDP (11)
- IPv4 (0800)
- Port source : 68 (44)
- Port destination 67 (43)

TramesDHCP.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

bootp

No.	Time	Source	Destination	Protocol	Length	Info
88	15.740150	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x27f38e2c
89	15.740672	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x27f38e2c
90	15.741320	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x27f38e2c
91	15.742145	172.17.254.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x27f38e2c
300	22.987613	172.17.2.140	172.17.244.1	DHCP	342	DHCP Release - Transaction ID 0x55691772
641	38.548080	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8733651b
642	38.548313	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x8733651b
643	38.548907	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x8733651b
644	38.549789	172.17.254.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x8733651b
855	48.832179	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf42ca890
856	48.833222	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0xf42ca890
857	48.833605	0.0.0.0	255.255.255.255	DHCP	375	DHCP Request - Transaction ID 0xf42ca890
858	48.835676	172.17.244.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0xf42ca890

> Frame 88: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

> Ethernet II, Src: Dell_12:e0:7f (d8:9e:f3:12:e0:7f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> 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: 0xccd1 (52433)

> Flags: 0x0000

 Time to live: 128

 Protocol: UDP (17)

 Header checksum: 0x6cd4 [validation disabled]

 [Header checksum status: Unverified]

 Source: 0.0.0.0

 Destination: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

> Bootstrap Protocol (Discover)

0000 ff ff ff ff ff d8 9e f3 12 e0 7f 08 00 45 00 E.

0010 01 48 cc d1 00 00 80 11 6c d4 00 00 00 00 ff ff ..H..... 1.....

0020 ff ff 00 44 00 43 01 34 a5 17 01 01 06 00 27 f3 ..D C 4 ..'.

0030 8e 2c 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 e0 7f 00 00 00 00

0050 00 00 00 00 00 00 00 00 00 00 00 00 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.

Ce champ ce nomme le champ protocole, celui-ci est dans cette exemple de trame le protocole de transport Datagramme UDP (11)

Renseignez ci-dessous les champs d'en-tête IP suivants : Version = 4

IHL (val. déci. et hexa.) = Hexa : 45 00 01 48 cc d1 00 00 80 11 6c d4 00 00 00 00 ff ff ff ff
Déci : 69 0 1 72 204 209 0 0 128 17 108 212 0 0 0 255 255 255 255

Protocole (val. déci. et hexa.) = UDP, Hexa : 11, Déci : 17

Source address (val. déci. et hexa.) = Hexa : 00 00 00 00, Deci : 0 0 0 0

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

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

Cela signifie qu'il n'y a pas encore d'adresse ip connue dans ce champ.

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

L'adresse de chouche 3 est donc une adresse de broadcast(diffusion) en 255.255.255.255

TramesDHCP.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

bootp

No.	Time	Source	Destination	Protocol	Length	Info
88	15.740150	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x27f38e2c
89	15.740672	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x27f38e2c
90	15.741320	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x27f38e2c
91	15.742145	172.17.254.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x27f38e2c
300	22.987613	172.17.2.140	172.17.244.1	DHCP	342	DHCP Release - Transaction ID 0x55691772
641	38.548080	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8733651b
642	38.548313	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x8733651b
643	38.548907	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x8733651b
644	38.549789	172.17.254.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x8733651b
855	48.832179	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf42ca890
856	48.833222	172.17.244.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0xf42ca890
857	48.833605	0.0.0.0	255.255.255.255	DHCP	375	DHCP Request - Transaction ID 0xf42ca890

> Frame 89: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{A2E487D7-0741-460A-9C66-CD8B90433CD0}, id 0

> Ethernet II, Src: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 172.17.254.1, Dst: 255.255.255.255

>User Datagram Protocol, Src Port: 67, Dst Port: 68

Source Port: 67

Destination Port: 68

Length: 321

Checksum: 0xe6d0 [unverified]

[Checksum Status: Unverified]

[Stream index: 25]

[Timestamps]

UDP payload (313 bytes)

Dynamic Host Configuration Protocol (Offer)

0000 ff ff ff ff ff d4 ae 52 7d 0e 2b 08 00 45 00 R}+·E·

0010 01 55 3f 25 00 80 11 50 60 ac 11 fe 01 ff ff ·U?%..... P.....

0020 ff ff 00 43 00 44 01 41 e6 d0 02 01 06 00 27 f3 ..C-D-A'

0030 8e 2c 00 00 00 00 00 00 00 00 ac 11 02 14 ac 11 ..,.....

0040 fe 01 00 00 00 00 d8 9e f3 12 e0 7f 00 00 00 00

Quel est le nom du champ de l'en-tête de transport permettant 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) ; 0043 et 0044

Quel est le protocole encapsulé dans le datagramme UDP ?

Le protocole encapsulé dans le datagramme UDP est un 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 serveur DHCP écoute sur le port 0043 soit le port 67 tandis que le client écoute sur le port 00 44 soit 68

TramesDHCP.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

bootp

No.	Time	Source	Destination	Protocol	Length	Info
88	15.740150	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x27f38e2c
89	15.740672	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x27f38e2c
90	15.741320	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x27f38e2c
91	15.742145	172.17.254.1	255.255.255.255	DHCP	360	DHCP ACK - Transaction ID 0x27f38e2c
300	22.987613	172.17.2.140	172.17.244.1	DHCP	342	DHCP Release - Transaction ID 0x55691772
641	38.548080	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8733651b
642	38.548313	172.17.254.1	255.255.255.255	DHCP	355	DHCP Offer - Transaction ID 0x8733651b

▼ Bootstrap Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x27f38e2c
- 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:e0:7f (d8:9e:f3:12:e0:7f)
- Client hardware address padding: 000000000000000000000000
- 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
- Option: (12) Host Name
- Option: (60) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End
- Padding: 000000

0020	ff ff 00 44 00 43	01 34 a5 17 01 01 06 00 27 f3	... D C 4 ...
0030	8e 2c 00 00 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 e0 7f 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 01c Sc5 =
0120	d8 9e f3 12 e0 7f 32 04	ac 11 02 14 0c 0a 65 712.eq
0130	75 61 72 61 6e 74 61 39	3c 08 4d 53 46 54 20 35	uaranta9 <·MSFT 5
0140	2e 30 37 0e 01 03 06 0f	1f 21 2b 2c 2e 2f 77 79	.07. !+,./wy
0150	f9 fc ff 00 00 00	00

Option 53: DHCP option (bootp.option.dhcp), 1 byte

Ici la section Bootstrap Protocol à été développée pour observer le contenu dans la trame DHCP Discover.