

TP4 : analyse de trames DHCP avec Wireshark

Sommaire

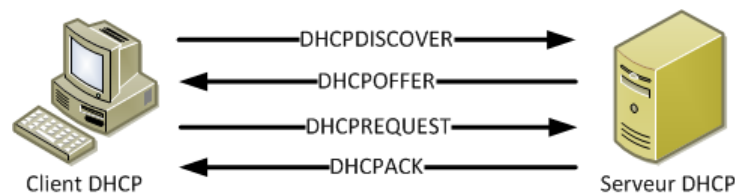
Objectifs :	1
1. Processus d'acquisition d'une adresse IPv4	1
2. Capture de trames DHCP avec Wireshark.	1
4. Etude de la trame DHCP DISCOVER.	5

Objectifs :

- Découvrir les **trames DHCP** ;
- Identifier les **champs** des différents **en-têtes** dans une **trame Ethernet** et mettre en évidence la **structure en couche** du **modèle TCP/IP** ainsi que le mécanisme de l'**encapsulation** ;
- Etude spécifique du **datagramme UDP**.

1. Processus d'acquisition d'une adresse IPv4

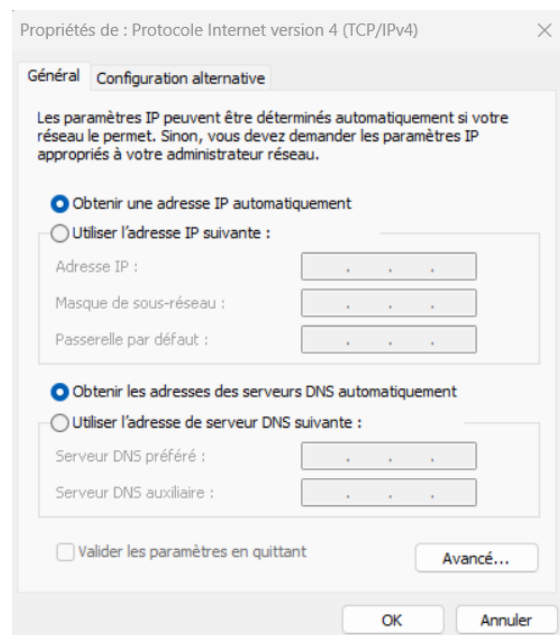
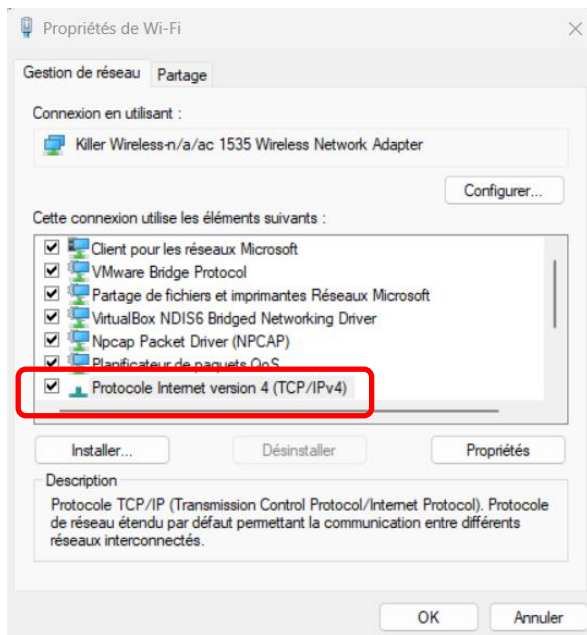
Ce processus comporte quatre phases comme montré dans la figure suivante :



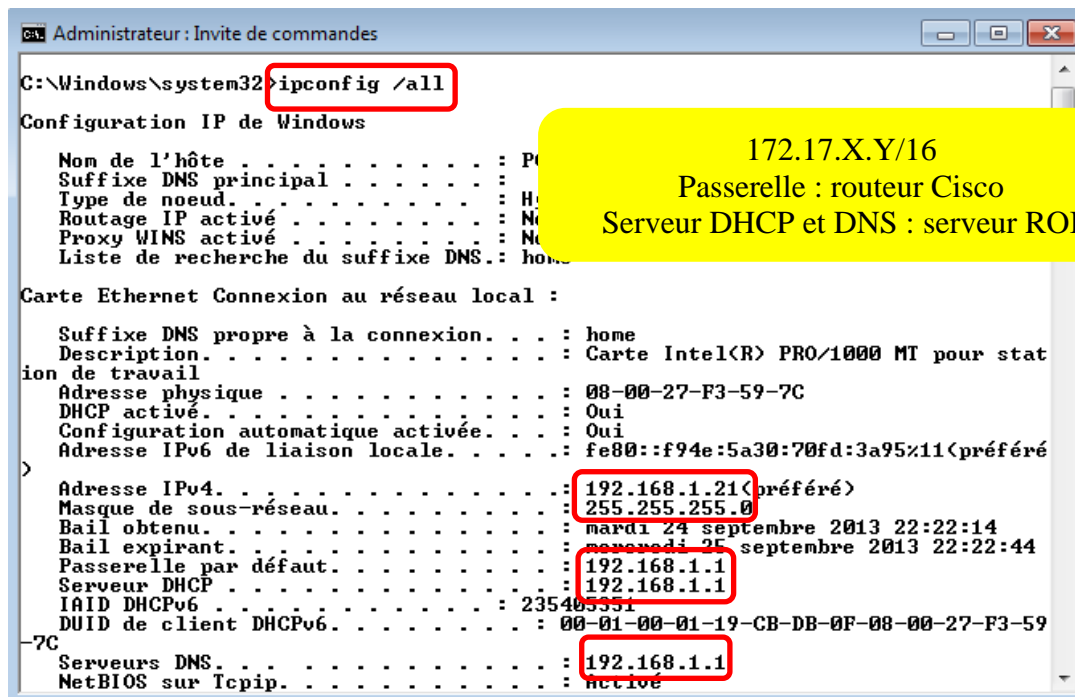
- Le **protocole DHCP** (**Dynamic Host Configuration Protocol**) permet à un hôte (client DHCP) de contacter un serveur DHCP afin d'obtenir une adresse IP dynamiquement. Le client DHCP envoie pour cela un **message DHCP DISCOVER** (**trame de broadcast**) du **port source UDP 68** (client DHCP) vers le **port destination UDP 67** (serveur DHCP). Tout serveur DHCP recevant le message DHCPDISCOVER doit traiter cette requête.
- Le serveur DHCP détermine dans quelle **étendue** se trouve le demandeur et lui assigne une adresse provenant des adresses libres de l'étendue. L'envoi de l'adresse du serveur au client se fait au moyen d'un **message DHCP OFFER** depuis le **port UDP 67** vers le **port UDP 68** contenant l'**adresse IP**, le **masque de sous-réseau**, la **durée du bail**, l'**adresse de la passerelle** ainsi que l'**adresse du serveur DNS**.
- Le client est tenu d'accepter la première adresse IP offerte provenant d'un DHCPOFFER quel que soit le serveur DHCP (si présence de plusieurs serveurs DHCP) et de retourner un **message DHCP REQUEST** (**trame de broadcast**) du **port UDP 68** vers le **port UDP 67** afin de signifier qu'il veut utiliser cette adresse IP.
- Le serveur DHCP concerné retourne auprès du client un **message DHCPACK** en utilisant le **port UDP 67** vers le **port UDP 68**, ce qui permet au client d'utiliser l'adresse IP pendant la durée du bail.

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** :

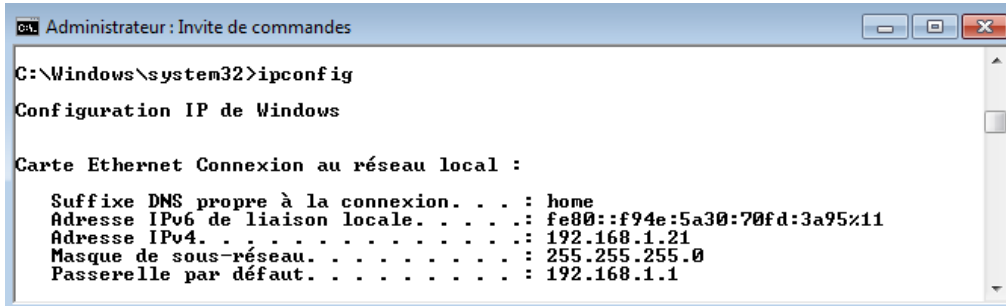


Quelle est l'adresse IP attribuée par le **serveur DHCP « ROI »** à votre poste de travail ?

- Renseignez les autres éléments ci-dessous :

DHCP activé _____
 Masque de sous-réseau _____
 Bail obtenu _____
 Bail expirant _____
 Passerelle par défaut _____
 Serveur DHCP _____
 Serveur DNS _____

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



```
Administrateur : Invite de commandes
C:\Windows\system32>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . : home
    Adresse IPv6 de liaison locale. . . . : fe80::f94e:5a30:70fd:3a95%11
    Adresse IPv4. . . . . : 192.168.1.21
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1
```

- 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**
- 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 nommez « TramesDHCP » :

La commande **ipconfig /release** permet de libérer l'adresse IP qui avait été obtenue (**trame DHCP RELEASE**). L'adresse devient alors **0.0.0.0** ce qui signifie en réalité que la carte réseau correspondante ne dispose plus d'une adresse IP.
La commande **ipconfig /renew** provoque l'envoi d'une requête à un serveur DHCP (**trame DHCPDISCOVER**) dont l'objet est d'obtenir ou de renouveler un bail, c'est-à-dire à la fois une adresse IP et le droit de l'utiliser pendant un certain temps.

- A partir des renseignements obtenus à l'aide de la commande **ipconfig /release**, renseignez les éléments ci-dessous :
 - Adresse IPv4 _____
 - Masque de sous-réseau _____
 - Passerelle par défaut _____
- A partir des renseignements obtenus à l'aide de la commande **ipconfig /renew**, renseignez les éléments ci-dessous :
 - Adresse IPv4 _____
 - Masque de sous-réseau _____
 - Passerelle par défaut _____
- 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) :

172.17.X.Y/16

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
76	79.1886730	192.168.1.10	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x39d2f089
506	191.528655	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xd16feba0
511	194.781582	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xd16feba0
512	194.799957	192.168.1.1	192.168.1.10	DHCP	342	DHCP Offer - Transaction ID 0xd16feba0
513	194.800823	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0xd16feba0
514	194.815509	192.168.1.1	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xd16feba0

Frame 506: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: HonHaiPr_3a:b9:15 (90:4c:e5:3a:b9:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: HonHaiPr_3a:b9:15 (90:4c:e5:3a:b9:15)

Type: IP (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

Bootstrap Protocol

```

0000 ff ff ff ff ff ff 90 4c e5 3a b9 15 08 00 45 00 .....L.....E.
0010 01 48 5d e5 00 00 80 11 db c0 00 00 00 00 ff ff .H].....
0020 ff ff 00 44 00 43 01 34 3c d6 01 01 06 00 d1 6f ...D.C.4 <.....o
0030 eb a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 00 00 90 4c e5 3a b9 15 00 00 00 00 .....L.....
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 .....

```

ET de trame :
14 octets
(6 pour MAC D + 6 pour MAC S + 2 pour Ethertype)

Cette fenêtre est scindée en 3 parties :

La **partie supérieure** est un résumé des échanges. Elle affiche la liste des trames. Chaque trame capturée par l'analyseur de protocole fait l'objet d'une ligne qui ne reprend que l'essentiel à savoir un numéro, le temps écoulé depuis le début de la capture, l'adresse IP source, l'adresse IP destination, le **protocole le plus élevé** décelé dans la trame (celui qui est encapsulé de la façon la plus profonde) et un commentaire succinct.

La première trame est un message **DHCP RELEASE**. Elle a été générée par la saisie de la commande **ipconfig /release** à partir du poste client DHCP.

La deuxième requête DHCP émise par le poste client est un message **DHCP DISCOVER**. Elle est la conséquence de la saisie de la commande **ipconfig /renew**. Le serveur répond par un message **DHCP OFFER**, en particulier pour soumettre une adresse IP au client. Le client répond par un message **DHCP REQUEST** pour faire valider son adresse IP. Le serveur répond par un **DHCP ACK** pour confirmation de l'attribution.

La **partie centrale** présente le détail de la trame sélectionnée dans la partie supérieure. On trouve, dans cette partie, les **en-têtes** des différents **protocoles** encapsulés dans la trame Ethernet ainsi que les **données** DHCP.

La **partie basse** affiche, au format hexadécimal, les données brutes de la trame sélectionnée, à raison de **16 octets** par ligne. Si la valeur d'un octet correspond à un caractère visualisable de la table ASCII, alors celui-ci est affiché dans la partie droite. Dans le cas contraire, le caractère est remplacé par un point. Ainsi, si une partie de trame comporte du texte brut, l'analyseur de protocole permet d'en prendre immédiatement connaissance.

4. 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 :

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

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

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

- Quels sont les protocoles inclus dans cette trame ?

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

En-tête IP

Version: 4
 Header Length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 328
 Identification: 0x5de5 (24037)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 128
 Protocol: UDP (17)
 Header checksum: 0xdb0c [correct]
 Source: 0.0.0.0 (0.0.0.0)
 Destination: 255.255.255.255 (255.255.255.255)
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

ET de paquet :
 20 octets
 (le 10^{ème} est le champ
 protocole et les 8
 derniers sont les IP
 Source et IP
 Destination)

- 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 = _____

IHL (val. déci. et hexa.) = _____

Protocole (val. déci. et hexa.) = _____

Source address (val. déci. et hexa.) = _____

Destination address (val. déci. et hexa.) = _____

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

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

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

En-tête de transport

ET de datagramme UDP :
8 octets
(les 4 1^{er} sont les ports Source et Destination)

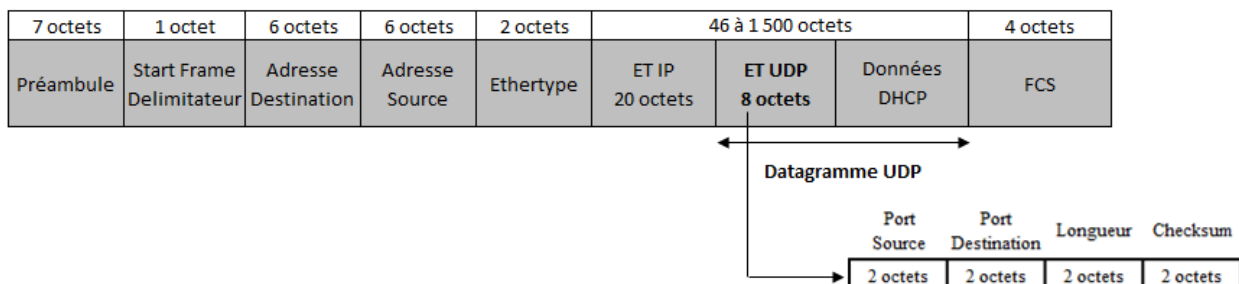
Rappel :

On distingue deux types d'**application** : celles qui nécessitent un transport **fiable** des données **sans nécessité de rapidité** (serveur web, de messagerie, SSH...) et celles qui nécessitent un transport **rapide** des informations **sans nécessité de fiabilité** (applications de streaming comme la radio et la télévision sur Internet, téléphonie sur Internet). Ces dernières peuvent se permettre de perdre des informations alors que les premières ont besoin que chaque paquet émis soit reçu coûte que coûte.

C'est la raison pour laquelle on trouve deux protocoles de transport qui répondent à deux types de besoin bien distincts : le protocole **TCP** (Transmission Control Protocol) et le protocole **UDP** (User Datagram Protocol).

UDP est un protocole **rapide** mais donc « **peu fiable** ». Contrairement à **TCP**, c'est un protocole dit « **non connecté** », c'est-à-dire **sans phase préalable d'ouverture de connexion** avant le transfert des données, sans acquittement par le receveur pour chaque paquet envoyé et sans fermeture de connexion. L'objectif est de transférer les données le plus rapidement possible et non pas de savoir si elles ont été bien reçues. En conséquence, **UDP** est un **protocole très simple** avec un **en-tête de transport** de seulement **8 octets** (contre 20 octets pour l'en-tête TCP).

Le format de la **trame DHCP** et du **datagramme UDP** est le suivant :



- 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) ;
- Quel est le protocole applicatif encapsulé dans le datagramme UDP ?
- 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.
- Sélectionnez la section **Bootstrap Protocol** contenu dans la trame **DHCP Discover** :

Protocole applicatif BOOTP

The screenshot displays a network capture in Wireshark. The top pane shows a list of packets, with packet 512 highlighted as a DHCP Discover message. The middle pane shows the details of this packet, including the Bootstrap Protocol section where the message type is identified as 'Boot Request (1)'. The bottom pane shows the raw packet bytes in hexadecimal and ASCII. A callout box points to the value '01' at offset 0x10 in the raw data, which corresponds to the DHCP message type field.

Données applicatives BOOTP à partir de l'octet de position 0x10 ligne 0020

Le format d'une trame DHCP est identique à celle d'une trame BOOTP. Le premier champ de la section **Bootstrap Protocol** comporte la valeur 1 si le message est un **Boot Request** (trame DHCP émise par le client à destination du serveur) et 2 s'il s'agit d'un **Boot Reply** (trame DHCP émise par le serveur à destination du client).

Dans les **options**, figure la valeur permettant d'identifier le **type de message DHCP** : DHCP DISCOVER (1), DHCP OFFER (2), DHCP REQUEST (3), DHCP ACK (5), DHCP RELEASE (7).