TP4 : analyse de trames DHCP avec Wireshark

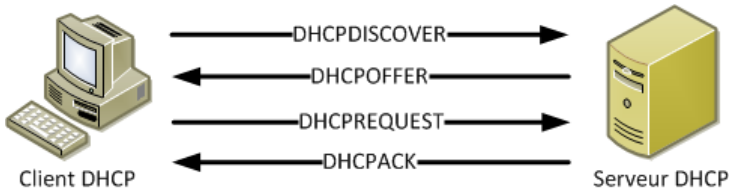
Sommaire

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

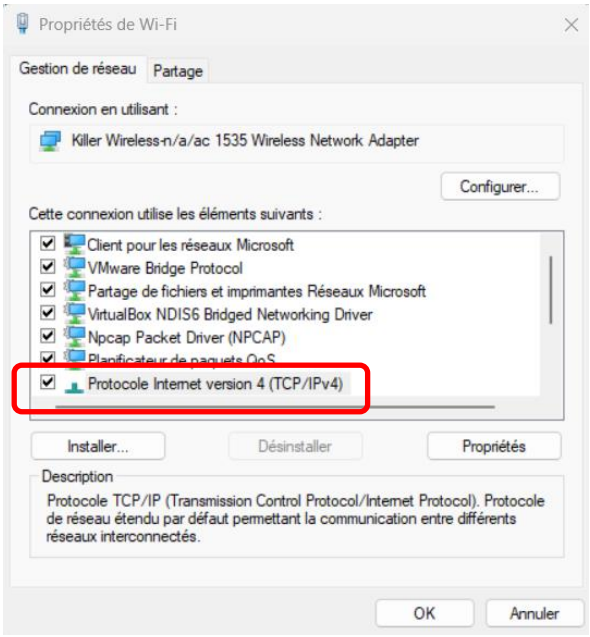
Ce processus comporte quatre phases comme montré dans la figure suivante :

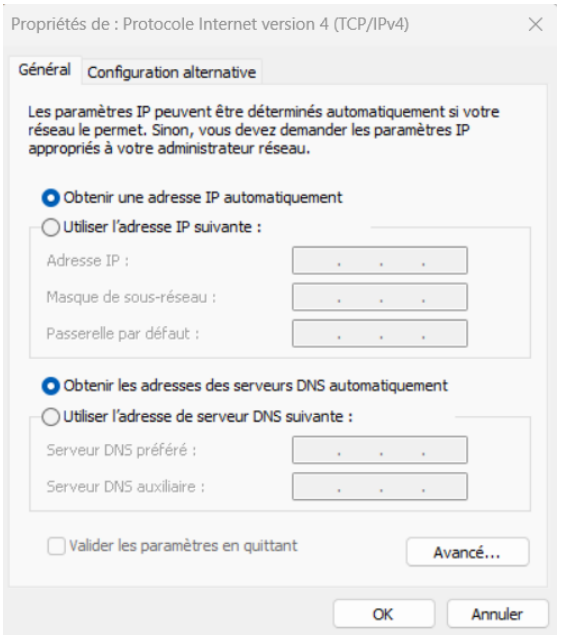


- Le **protocole DHCP** (**Dynamic Host Configuration Protocol**) permet à un hôte (client DHCP) de contacter un serveur DHCP afin d'obtenir une adresse IP dynamiquement. Le client DHCP envoie pour cela un **message DHCP DISCOVER** (trame de **broadcast**) du port source **UDP 68** (client DHCP) vers 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.

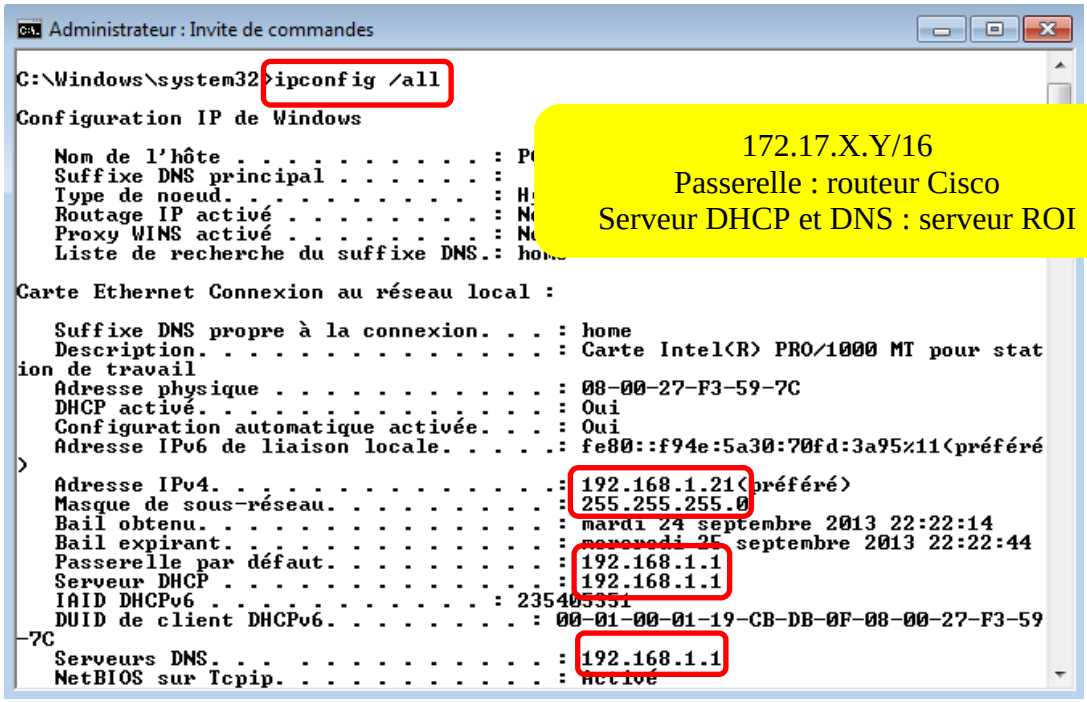
2. Capture de trames DHCP avec Wireshark.

- 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 :**



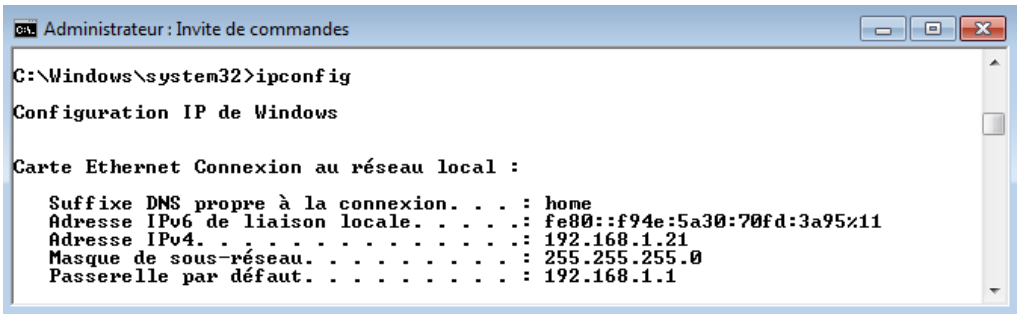
172.17.X.Y/16
Passerelle : routeur Cisco
Serveur DHCP et DNS : serveur ROI

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 :



- 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 _____

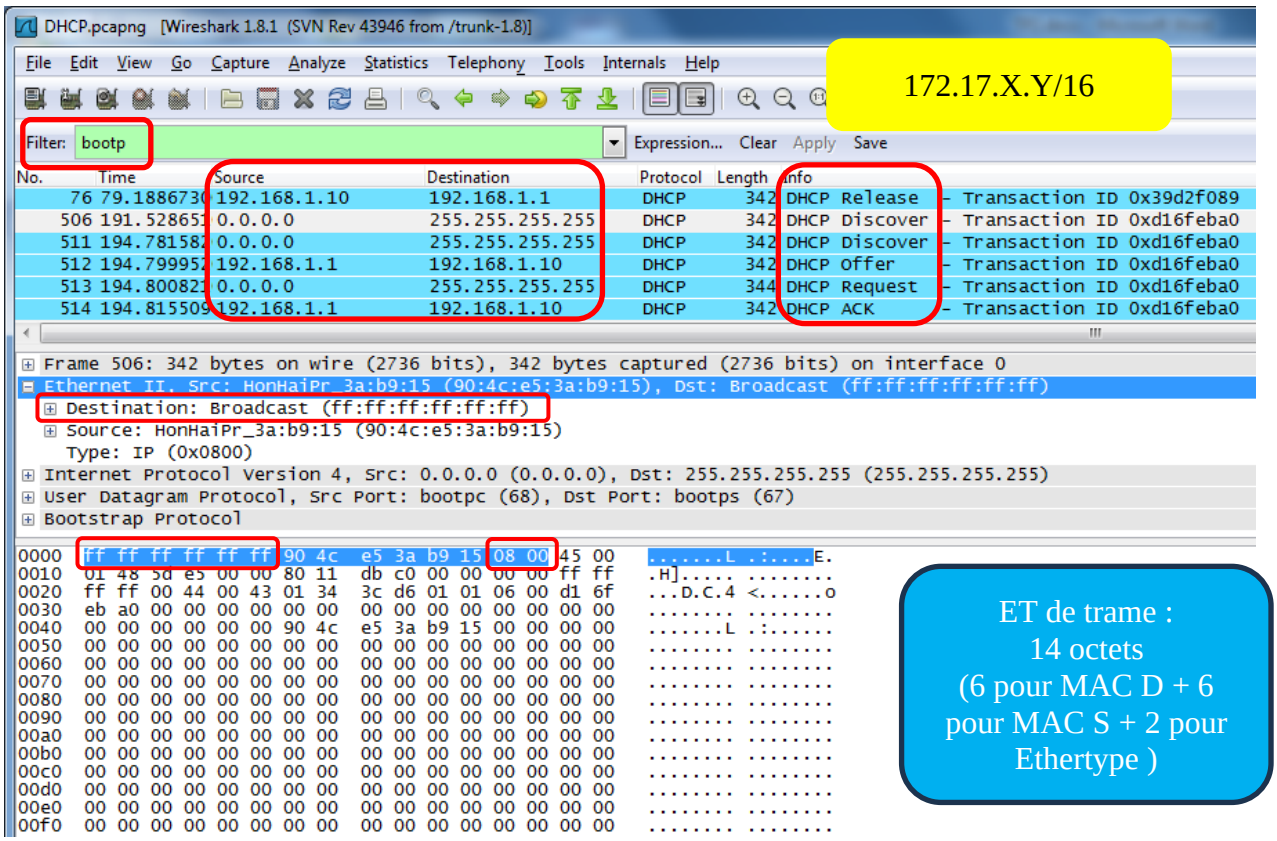
- A partir des renseignements obtenus à l'aide de la commande **ipconfig /renew**, renseignez les éléments ci-dessous :

  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) :



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 :

  _____

  _____

- Caractérisez 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 ?

  _____

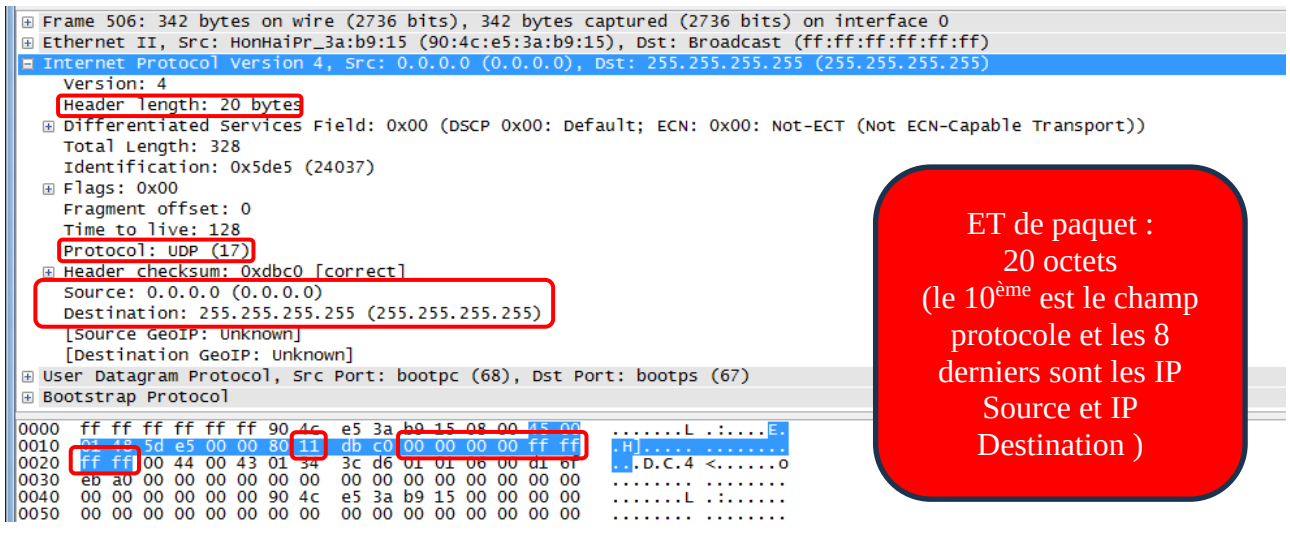
  _____

  _____

  _____

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

En-tête IP



- 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** ?

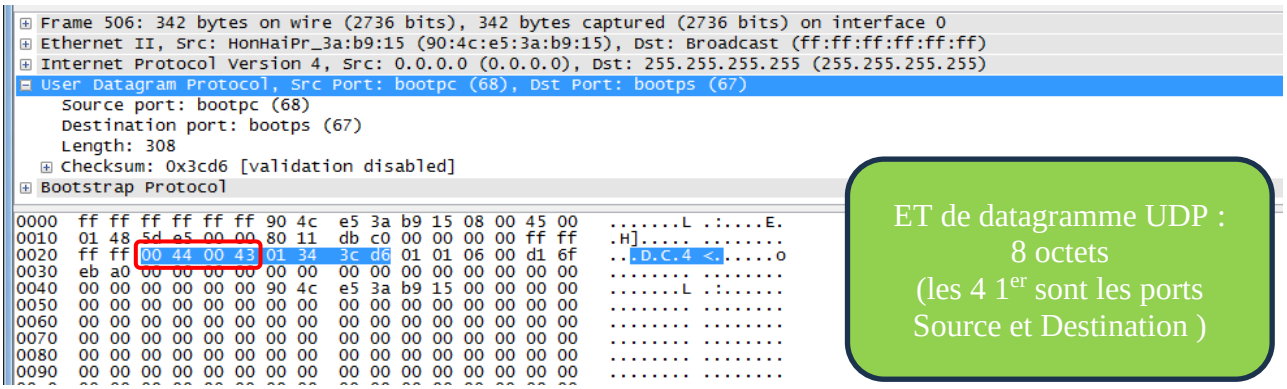
  _____

- Caractérisez 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 1er sont les ports Source et Destination)

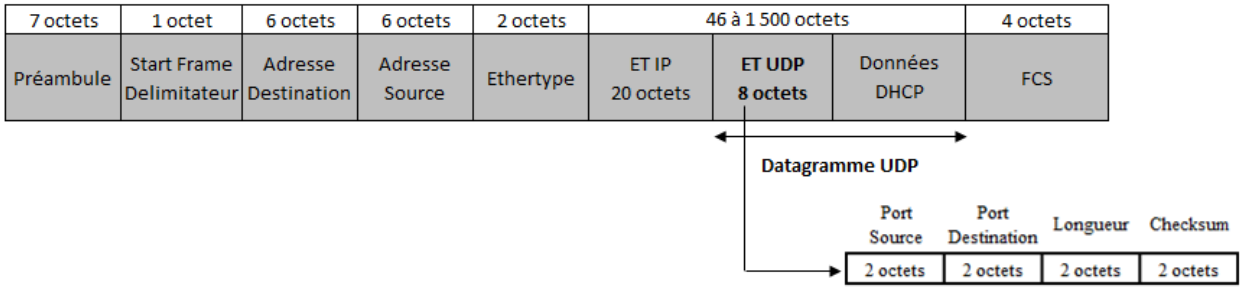
Rappel :

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** 0×02 et 0×03 ligne 0020) ;

  _____

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

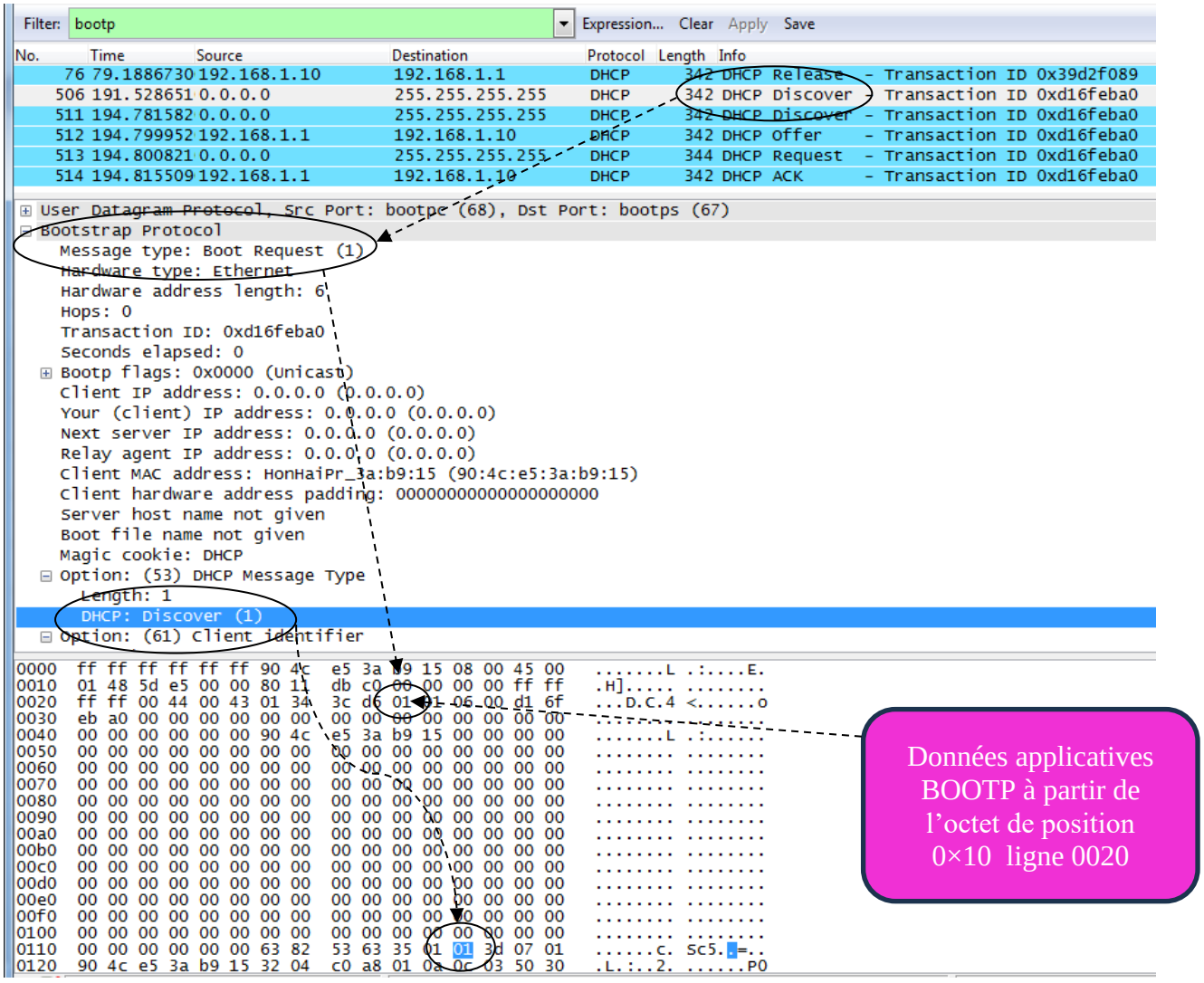
  _____

- 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



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).