Exercices dirigés

Unité d'Enseignement RSX101

Réseaux et protocoles pour l'Internet : Services IPv4

E. Gressier-Soudan, S. Rovedakis, P.Sweid

2021-2022

Ce polycopié a été élaboré par l'équipe enseignante "Réseaux et protocoles" à partir d'exercices rédigés par MM. Florin, Gressier-Soudan qu'ils en soient ici remerciés.

ED Couche Réseau : Services associés à IPv4

Exercice 1 : Distribution d'adresses avec DHCP pour IPv4 (cours déguisé en exercice qui introduit DHCP)

DHCP ('Dynamic Host Configuration Protocol' RFC 2131 et 2132) est un protocole client serveur qui permet à un client hôte d'un réseau local (Ethernet ou Wifi) d'obtenir d'un serveur DHCP différents paramètres de configuration réseau. En utilisant DHCP on souhaite surtout fournir à un hôte, mais surtout à son interface, une adresse IP mais aussi le masque du sous-réseau auquel appartient cette interface, l'adresse IP du routeur par défaut ou encore l'adresse IP d'un serveur DNS. Pour affecter des adresses IP, un serveur DHCP reçoit un ensemble d'adresses IP qu'il attribue ensuite sur demande à des clients pour une période de temps donnée. En DHCP on appelle bail (lease en anglais) le fait pour un hôte d'obtenir une adresse IP pour une période de temps définie par le serveur. Le protocole d'acquisition d'un bail comporte quatre messages principaux :

A - Le client DHCP émet en diffusion un premier message de demande de bail. Le type de ce message est baptisé DHCPDISCOVER.

B – S'il existe plusieurs serveurs DHCP atteints par la diffusion et si ces serveurs disposent d'une adresse IP libre, ces serveurs DHCP[1] proposent au client cette adresse IP associée à une durée d'utilisation possible de l'adresse (une durée de bail). Ce message contient aussi l'adresse IP du serveur proposant l'offre. Le type de ce message de réponse est DHCPOFFER.

C - S'il a reçu plusieurs propositions, le client en choisit une et retourne une demande d'utilisation de cette adresse. Le type de ce troisième message est DHCPREQUEST. Ce message est également diffusé pour que les autres serveurs DHCP apprennent qu'ils n'ont pas été sélectionnés.

D - Le protocole se termine par la transmission d'un message DHCPACK par lequel le serveur DHCP sélectionné accuse réception de la demande et accorde l'adresse selon la durée de bail prévue. Les autres serveurs retirent définitivement leur offre.

https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp, (consulté le 13/11/2019 à 17h11) donne une bonne description du protocole dans le détail tout en restant assez visuel.

A la moitié de la période d'utilisation d'une adresse (moitié du bail) le client demande le renouvellement de l'allocation de cette adresse par un message DHCPREQUEST. Le bail est généralement renouvelé par un DHCPACK. Si la demande n'aboutit pas (cas d'une réponse DHCPNACK ou perte de contact avec le serveur DHCP), le client tente de contacter les autres

[1] Les serveurs peuvent être organisés de différentes façons. Si plusieurs serveurs sont actifs, le client prend le premier qui lui répond. On imagine donc que ces serveurs DHCP doivent se répartir la plage d'adresses IP allouables pour éviter les conflits.

Certaines configurations utilisent un serveur DHCP primaire, et un autre secondaire pour le reprendre en cas de panne. Pour plus de détails, des informations peuvent être trouvées au lien https://kb.isc.org/docs/aa-00502 "A Basic Guide to Configuring DHCP Failover " (consulté le 05/10/2020, 23h15).

serveurs DHCP pour obtenir une autre adresse. En l'absence de réponse positive, le client utilise l'adresse dont il disposait jusqu'à la fin du bail puis cesse de communiquer en IP.

Un analyseur de messages échangés sur un réseau local Ethernet/IP donne le résultat suivant. Il est constitué d'une suite de lignes correspondant à un message observé sur le réseau local. On trouve :

- un numéro d'ordre du message observé,
- la date de l'observation en seconde,
- les adresses IP source et destination,
- le nom du protocole pour lequel le message a circulé
- et le type du message

```
No  Time   Source        Destination     Protocol Info
1 0.000000 0.0.0.0       255.255.255.255 DHCP   DHCP Discover
2 0.001182 192.168.0.247 192.168.0.5     ICMP   Echo request
3 0.342454 192.168.0.247 192.168.0.5     DHCP   DHCP Offer
4 0.344405 0.0.0.0       255.255.255.255 DHCP   DHCP Request
5 0.348264 192.168.0.247 192.168.0.5     DHCP   DHCP ACK
6 0.353014 CIS_a8:52:24  Broadcast       ARP    Who has 192.168.0.5? Tell 192.168.0.5
```

Question 1

Pour le message numéro 1 de la trace expliquez la signification des adresses IP source et destination (pourquoi selon vous utilise-t-on ces adresses dans cet échange) ?

Question 2

La trace ne donne pas l'adresse MAC destination figurant dans le message numéro 1 (l'adresse MAC source correspond à l'adresse unique de l'émetteur). Même si elle ne figure pas dans le texte pouvez vous donner l'adresse destination ?

Question 3

Pour le message numéro 3 de la trace expliquez la signification des adresses source et destination (à quoi correspondent ces adresses) ? Comment est il possible que ce message parvienne correctement à son destinataire ?

Question 4

Pour le message numéro 4, expliquez la signification des adresses IP source et destination (pourquoi avoir choisi les adresses IP qui apparaissent dans le message 4)?

Question 5

Dans cette trace, le message numéro 2 semble ne pas être relié à une attribution d'adresse DHCP. Cependant ce message a circulé aussi dans le cadre de l'attribution d'adresse. Pourquoi le message numéro 2 a-t-il circulé (quel est le but poursuivi dans la circulation de ce message) ?

Question 6

Expliquez pourquoi le temps qui s'écoule entre les messages 2 et 3 est assez long ?

Question 7

De la même façon, décrivez pourquoi le message 6, rappelé ci-dessous, a circulé dans cette trace?

6 0.353014 CIS_a8:52:24 Broadcast ARP Who has 192.168.0.5? Tell 192.168.0.5

Un administrateur réseau installe un serveur DHCP sur une machine UNIX. Il doit configurer le serveur par un ensemble de directives contenues dans un fichier baptisé `dhcpd.conf`. La liste des directives préparées pour une configuration est la suivante :

```
default-lease-time 600;

max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1,192.168.1.2;
option domain-name "mondomaine.org";

subnet 192.168.1.0 netmask 255.255.255.0
// les 24 bits en partant de la gauche sont tous à 1 => 8 derniers bits sont à 0
// donne la notation compacte /24
{
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}

host ulysse
{
hardware ethernet 00:19:18:A6:47:36 ;
fixed-adress 192.168.0.10;
}
```

Question 8

Les adresses IP attribuées par ce serveur DHCP correspondent à un choix particulier. A quelle catégorie appartiennent ces adresses ?

Question 9

On constate dans le fichier de configuration `dhcpd.conf` deux types de directives d'allocation d'adresses IP. Dans le cas de la machine ulysse, celle-ci reçoit toujours la même adresse IP fixe (voir la ligne 'fixed-adress 192.168.0.10'). Citez les avantages que vous voyez à l'utilisation de DHCP dans ce cas ?

Question 10

Dans le cas du sous réseau 192.168.1.0 l'administrateur définit des plages d'adresses attribuables dynamiquement (dans les directives range comme range 192.168.1.10 192.168.1.100). Pourquoi préciser de telles plages d'adresses et quels avantages en tire-t-on ?

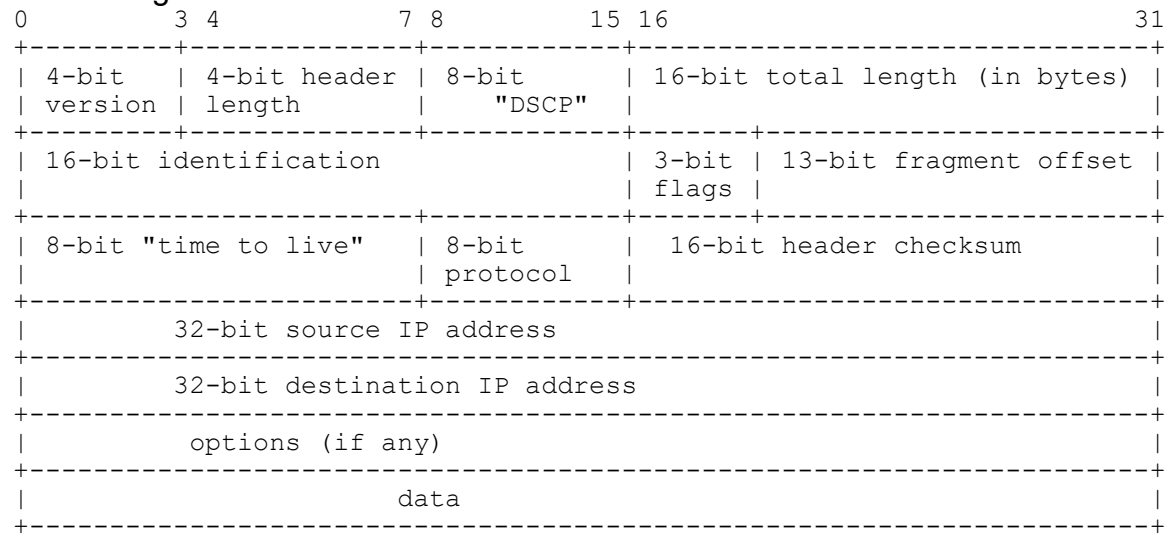
Exercice 2

On fournit les spécifications des différentes structures d'entête ou de message nécessaires pour analyser une trace en hexadécimal : Trame Ehernet, Entête d'un datagramme IP, entête d'un datagramme UDP respectivement. Ces entêtes ont déjà été données en cours et en exercices dirigés, elles sont justes rappelées pour que vous ne perdiez pas de temps. Elles seront utiles pendant tout l'examen. Vous vous servirez de ces entêtes en fonction des questions posées dans les deux problèmes.

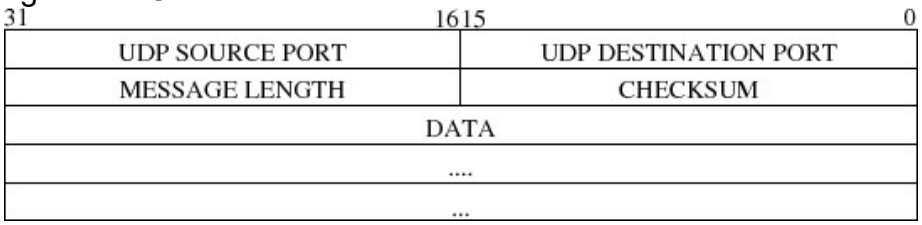
Structure d'une trame Ethernet II :

Adresse MAC destination	Adresse MAC source	Type	Charge utile-Données	FCS-contrôle d'erreur
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

Entête d'un datagramme IP :



Entête d'un datagramme UDP :

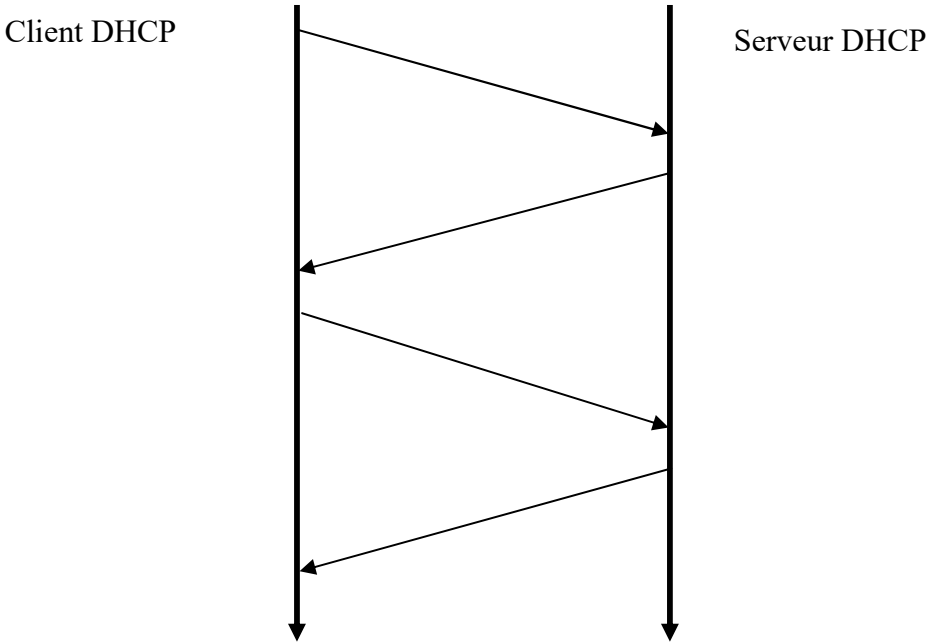


Le problème qui suit concerne une session DHCP (Dynamic Host Configuration Protocol) en IPv4. La capture Wireshark de cette communication est donnée ci-après :

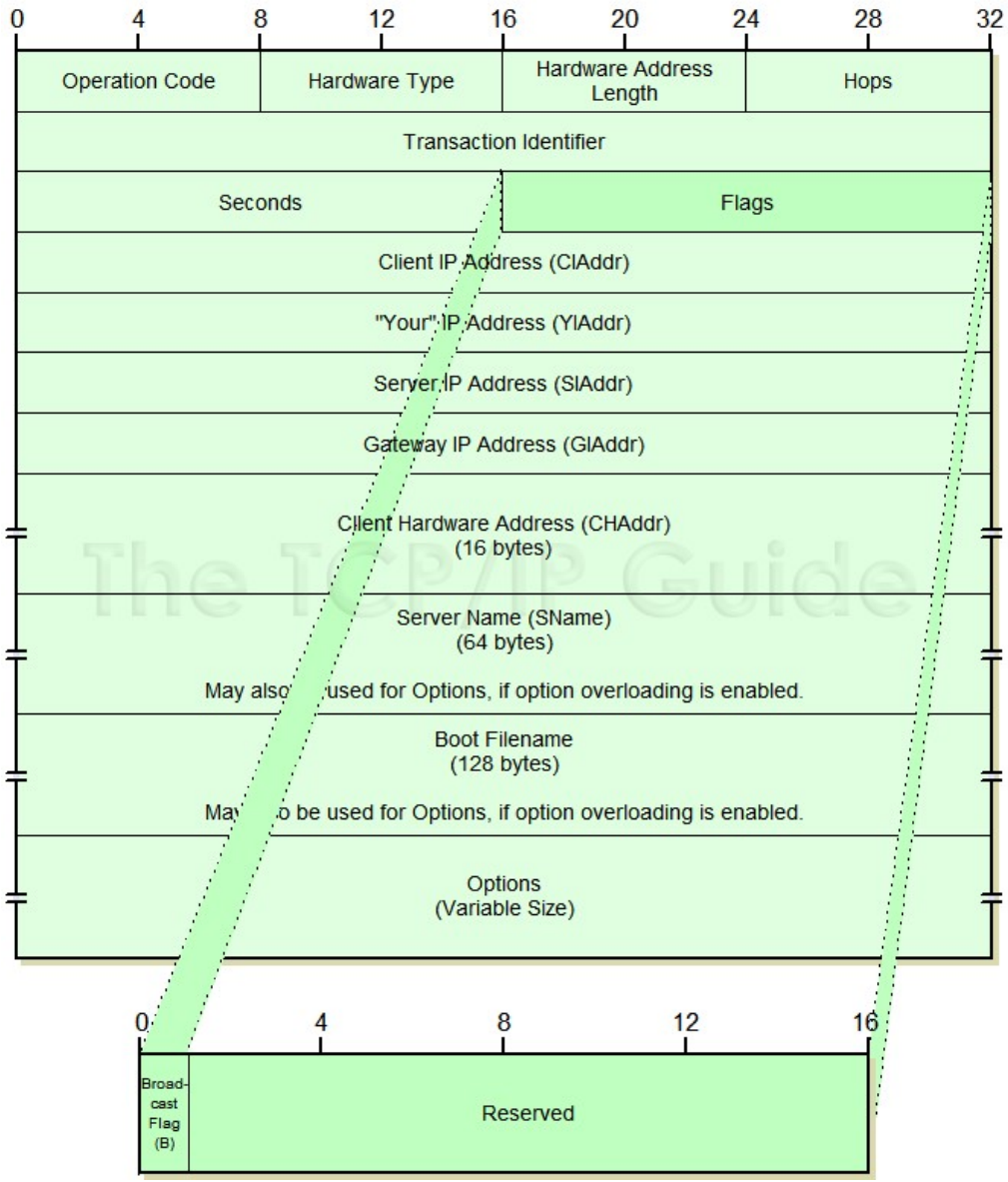
192.168.0.1 est le serveur DHCP, et 192.168.0.10 est le demandeur, enfin, le demandeur quand il aura obtenu cette adresse en fin de déroulement du protocole DHCP. On fait remarquer que DHCP est transporté dans des datagrammes UDP… sinon les adresses IP n'auraient pas de sens.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

Question 1
Compléter à l'aide du nom des requêtes indiqué dans la trace le diagramme d'échange du protocole DHCP suivant :



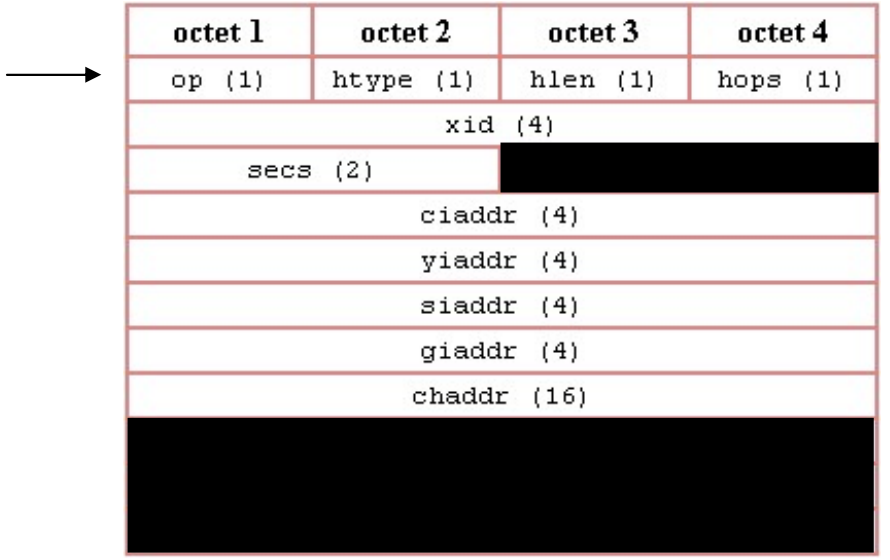
Question 2
Dans la suite du problème on va étudier plus en détail le protocole DHCP. Pour cela, on vous donne le format d'un message DHCP (source : http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm) ci-après :



Voici le détail du message DHCP_Offer tel que donné par Wireshark :

```
> Ethernet II, Src: Dell_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.10
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.10
    Next server IP address: 192.168.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  v Option: (1) Subnet Mask
      Length: 4
      Subnet Mask: 255.255.255.0
  v Option: (58) Renewal Time Value
      Length: 4
      Renewal Time Value: (1800s) 30 minutes
  v Option: (59) Rebinding Time Value
      Length: 4
      Rebinding Time Value: (3150s) 52 minutes, 30 seconds
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (3600s) 1 hour
  v Option: (54) DHCP Server Identifier
      Length: 4
      DHCP Server Identifier: 192.168.0.1
  > Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000...
```

Remplir les champs du message DHCP ci-dessous à partir de la flèche, sauf champs en noir, avec les informations données issues de la trace Wireshark.



octet 1	octet 2	octet 3	octet 4
op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)			
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			

Question 3

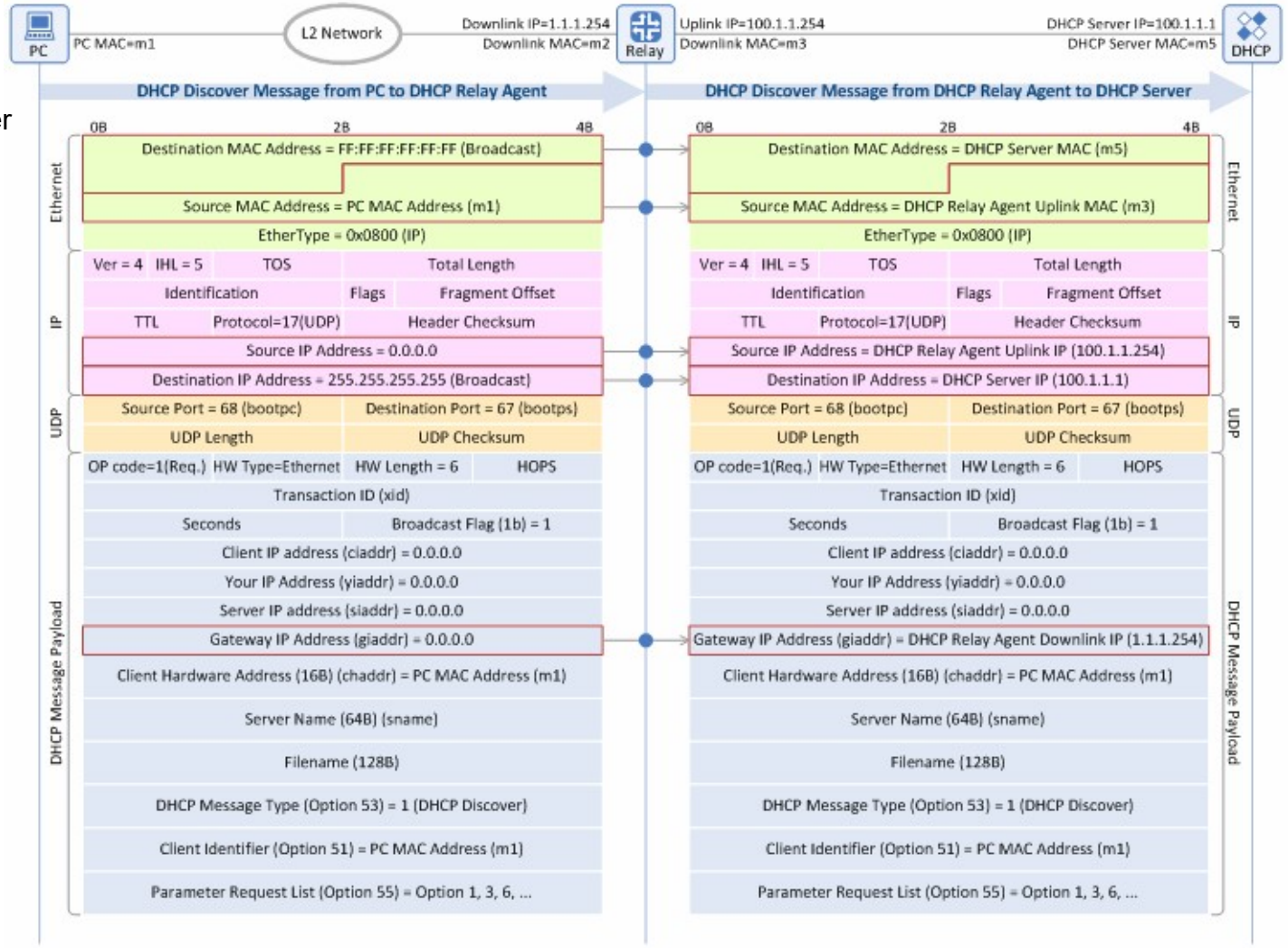
A l'issue des échanges, si le système d'exploitation du client DHCP est de type Windows, compléter les champs manquants du résultat de la commande `ipconfig` matérialisés par un "?"

```
Carte Ethernet eth0 :
   Suffixe DNS propre à la connexion. . . : myhome.fr
   Adresse physique . . . . . . . . . . . : ?
   Adresse IPv4. . . . . . . . . . . . . .: ?
   Masque de sous-réseau. . . . . . . . . : ?
   Passerelle par défaut. . . . . . . . . : 192.168.0.2
   Serveur DHCP . . . . . . . . . . . . . : ?
   Serveur DNS. . . . . . . . . . . . . . : 192.168.0.3
```

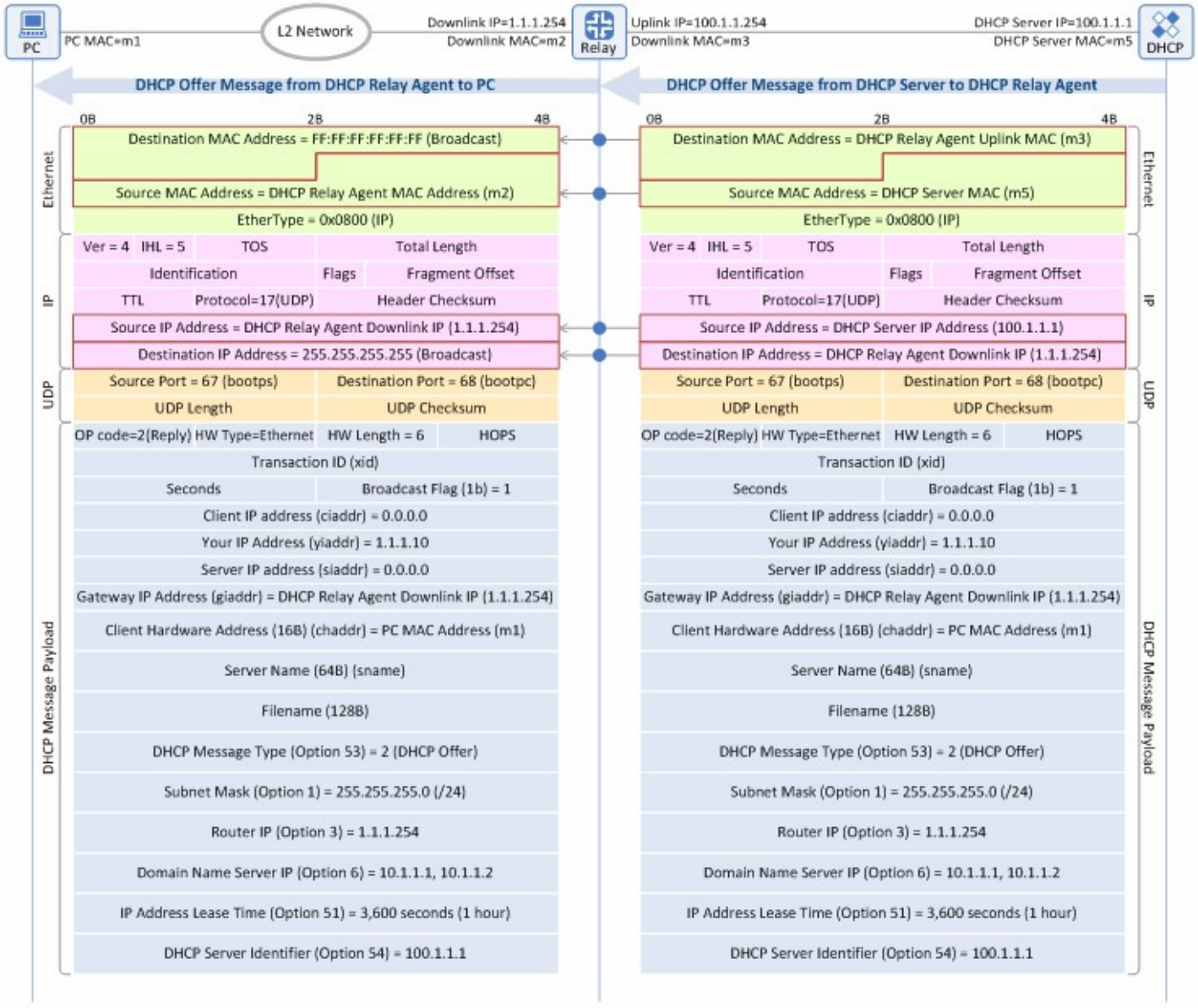
Question 4

On s'intéresse à DHCP mais avec une architecture utilisant un routeur/relais.

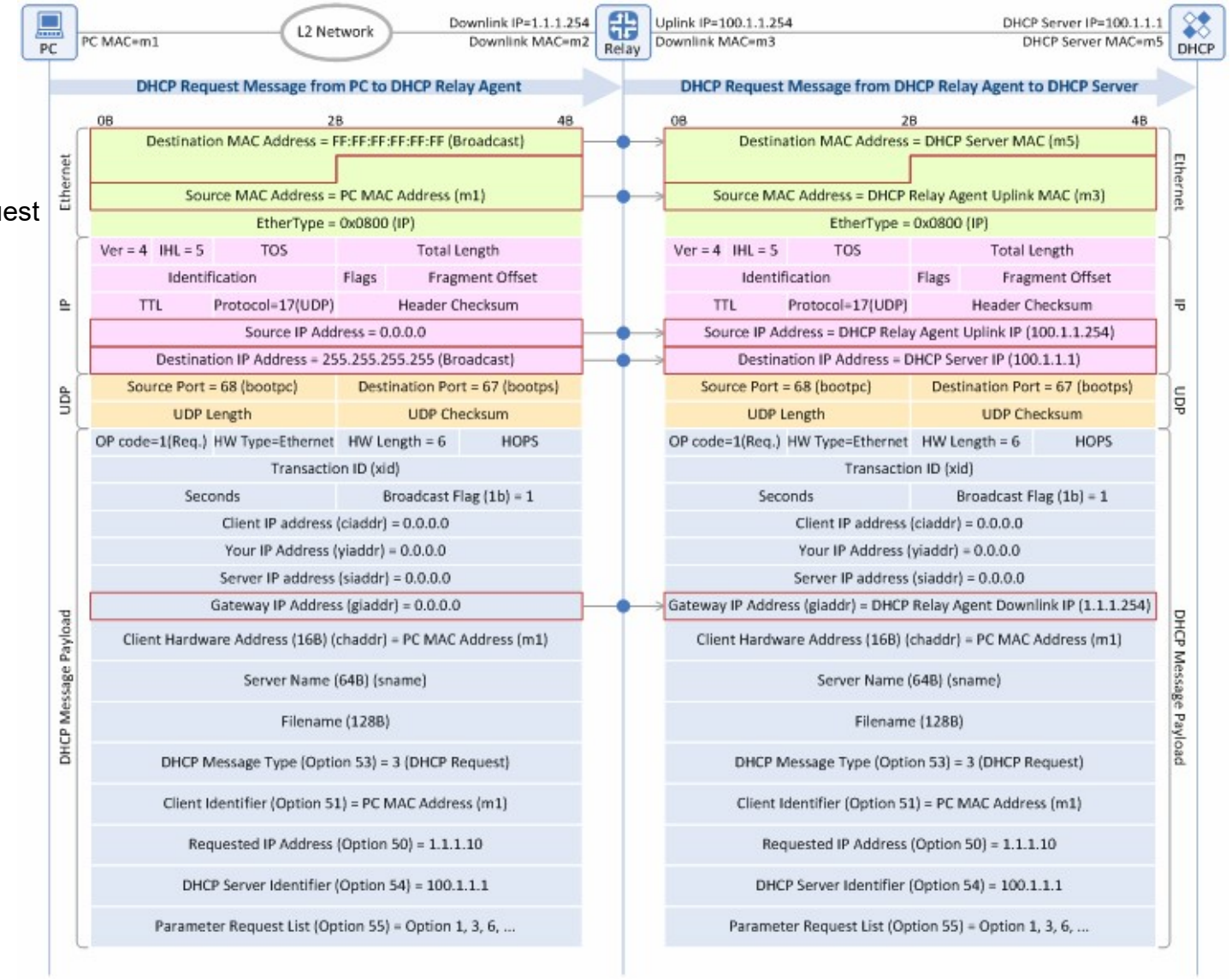
DHCP Discover



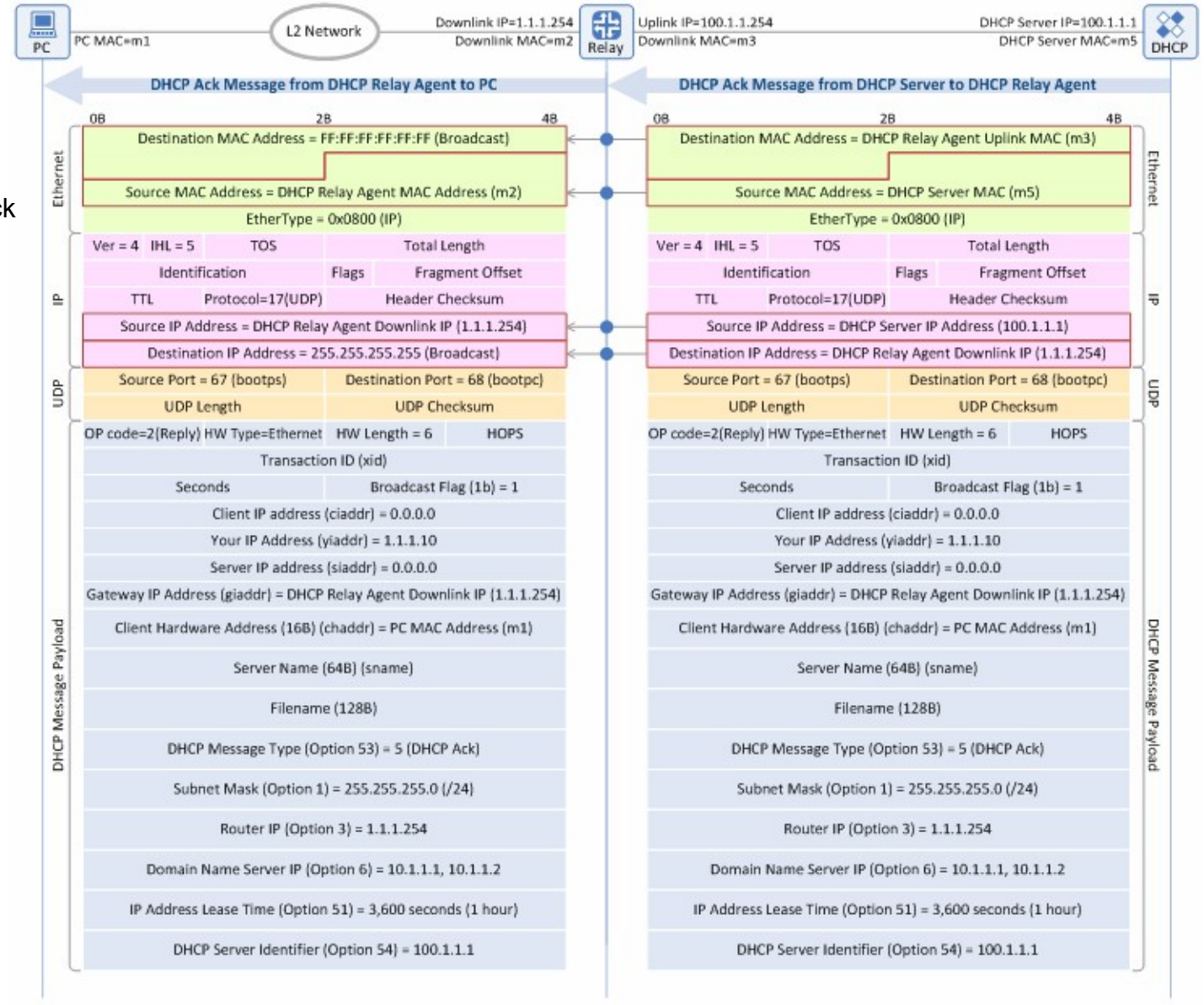
DHCP Offer



DHCP Request



DHCP Ack



Les schémas ci-avant sont issus de https://www.netmanias.com/en/post/techdocs/6000/dhcp-network-protocol/understanding-dhcp-relay-agents consulté le 13/11/2019 à 18h50.

Le serveur DHCP est sur le réseau 100.1.1.0/24 tandis que le client DHCP, le demandeur, est sur le réseau 1.1.1.0/24. Le broadcast du client ne peut atteindre le serveur, le relais DHCP a été introduit pour cette raison.
Expliquer, d'après vos observations pourquoi le protocole est différent.

Exercice 3 : Traduction d'adresses IPV4 (NAT), cours d'introduction sous forme d'exercice

La norme RFC 1631 (mai 1994) ('The IP Network Address Translator'), définit un principe général de traduction d'adresses IP. La dernière version, la plus récente de cette approche correspond à la RFC 3022 (janvier 2001) améliore différents points. La RFC 7857[2] effectue des mises à jour complémentaires sur la transformation d'adresses.
La traduction d'adresses peut être appliquée par différents types d'appareils dont la caractéristique principale est d'être situés entre un réseau IPV4 privé et le réseau IPV4 global, l'Internet. Typiquement la traduction est effectuée par un routeur, mais on peut aussi appliquer la traduction dans un hôte quelconque ou dans un filtre (pare-feux ou 'firewall').
La traduction au niveau des adresses IP s'applique à l'adresse source d'un datagramme IP en provenance du réseau privé (baptisé encore en NAT réseau interne) et à destination du réseau public (baptisé encore en NAT réseau externe). De manière symétrique, la traduction est effectuée sur les datagrammes en provenance du réseau public (ou externe) vers le réseau privé (ou interne).
La traduction d'adresses peut être réalisée de différentes façons qui sont examinées dans les questions suivantes.

Question 1
Dans le mode NAT statique l'adresse IPV4 source privée est traduite en une adresse IPV4 source publique qui est toujours la même. La correspondance dans ce cas est bijective (biunivoque) c'est-à-dire qu'à une adresse privée est associée, de manière statique, une adresse publique (selon une table de correspondance statiquement définie par un administrateur réseau).

Quelle utilisation peut-on faire d'un tel mode de traduction d'adresses IP ? Quels sont les inconvénients ?

Question 2
Dans le mode NAT dynamique, la traduction d'une adresse source IPV4 privée est effectuée vers une adresse source IPV4 publique qui est prise dans un bloc d'adresses publiques disponibles. L'adresse publique utilisée n'est donc pas toujours la même. Par exemple si l'on suppose que l'hôte d'adresse 172.16.40.17 émet un datagramme à un instant donné vers l'Internet global, son adresse est traduite dans la première adresse disponible d'un bloc. Par exemple, si l'adresse 212.19.50.63 du bloc disponible 212.19.50.0 à 212.19.50.255 est non utilisée au moment de l'émission du datagramme, on l'utilisera et on traduira 172.16.40.17 en 212.19.50.63. Cette correspondance est enregistrée dans une table.
De manière à éviter de bloquer indéfiniment une adresse attribuée dynamiquement, un temporisateur est utilisé pour révoquer l'attribution d'une adresse publique. A l'échéance, on récupère une adresse attribuée et l'on procède à une nouvelle attribution d'adresse si un nouvel échange à lieu (éventuellement on peut reprendre la même adresse pour un autre quantum de temps).

Quel avantage nouveau obtient-on d'un tel mode de traduction d'adresses IP ?

---

[2] Cette RFC parle de Network Address Translation, et non plus de Network Address Translator comme la RFC de base 3022.
Sinon consulter le blog de S. Bortzmyer à propos de cette RFC : https://www.bortzmeyer.org/7857.html

Question 3
Le troisième mode est connu sous différents noms (mode NAT avec surcharge NAT 'overloading' encore appelé NAT with PAT 'Port Address Translation'). Dans ce cas la traduction d'une adresse source IPV4 privée vers une adresse source IPV4 publique est complétée par la traduction du numéro de port. Le plus souvent, dans ce cas on suppose l'utilisation d'une seule adresse publique (par exemple une adresse publique comme 212.19.50.63 disponible). Si l'on suppose que l'hôte d'adresse 172.16.40.17 émet un datagramme selon le protocole TCP avec le numéro de port source 5032, alors son adresse IP est traduite en l'adresse IP publique (212.19.50.63) et le numéro de port source TCP est également traduit vers un numéro de port non utilisé (par exemple 4097 si ce port n'est pas déjà attribué à une autre communication). Comme dans le cas du NAT dynamique, les attributions sont associées à un temporisateur avec récupération à échéance. Ce mode de fonctionnement est le plus utilisé.

Quels en sont les avantages et les inconvénients ?

Exercice 4 : NAT et voix sur IP : la nécessité de STUN

STUN a évolué de "Simple Traversal of UDP through NATs", RFC3489 ou "classic STUN", à Session Traversal Utilities for NAT, RFC5389. Initialement dédié à la VoIP, et à des applications interactives qui s'appuient sur UDP, la nouvelle version autorise différents protocoles de transport. Wikipedia indique "STUN is a standardized set of methods, including a network protocol, for traversal of network address translator (NAT) gateways in applications of real-time voice, video, messaging, and other interactive communications." à https://en.wikipedia.org/wiki/STUN

L'approche NAT ('Network Address Translation') présente dans le cadre du protocole IPV4 de nombreux avantages. NAT pose aussi différents problèmes avec certaines applications Internet en particulier des applications d'actualité comme les communications de voix sur IP (VoIP 'Voice over IP').

En communication de voix sur IP on cherche à réaliser des communications vocales en utilisant le réseau Internet. L'analogue du numéro de téléphone est une adresse IPV4 d'interface d'accès à un appareil (un poste de travail qui possède un micro et un écouteur ou un téléphone IP). Cependant il n'a pas été retenu d'utiliser directement des adresses IP pour désigner un correspondant comme on le fait des numéros de téléphone. On rappelle que l'attribution d'adresse IP peut être statique ou dynamique.

Question 1 (facultative)
On s'intéresse au cas d'une attribution statique des adresses IP. Un émetteur peut-il utiliser l'adresse IP pour appeler un correspondant comme on le fait avec un numéro de téléphone ? Justifier votre réponse.

Question 2
On se place maintenant dans le cas d'une attribution dynamique d'adresses IP (DHCP, Dynamic Host Configuration Protocol)). Quel(s) problème(s) se posent en utilisation d'adresses IP dynamiques pour appeler un correspondant ?

Question 3
Dans le cas où l'on se trouve dans un réseau privé avec un routeur NAT, peut-on directement utiliser les adresses IP pour appeler un correspondant comme on le fait avec un numéro de téléphone ?

Question 4

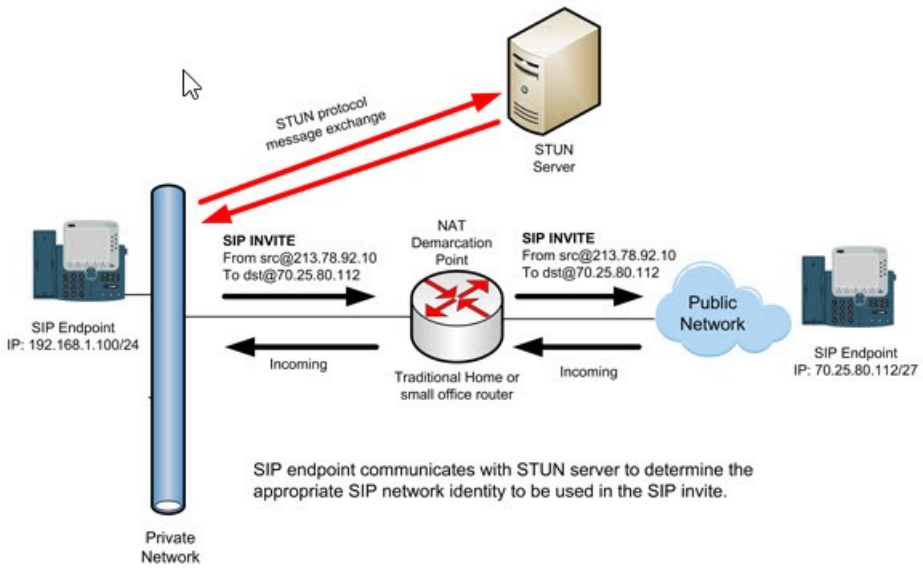
Dans les protocoles de voix sur IP on utilise une gestion d'annuaires. Les annuaires sont placés dans l'Internet public et sont accessibles en ligne en mode client-serveur ou peer-to-peer. C'est le cas de SIP ('Session Initiation Protocol' un protocole de signalisation sur réseau IP) ou de SKYPE (système de téléphonie Microsoft 'gratuite' utilisant la voix sur IP).
Rappelez le rôle d'un serveur d'annuaire, quelles sont les trois opérations principales réalisées par un serveur d'annuaire ?

Question 5
Dans certains protocoles d'application de l'Internet, certains messages protocolaires contiennent l'adresse IP V4 source de l'émetteur dans l'entête du datagramme IP et dans la partie donnée du message (dans la charge utile). Par exemple, en voix sur IP, dans quel cas peut-on trouver une adresse IP dans la partie charge utile d'un message?
Quel problème pose l'utilisation de NAT pour de tels protocoles ?

Question 6
Différentes solutions ont été proposées pour résoudre le problème précédent (adresses IP dans une charge utile). Une solution consiste à faire en sorte que les applications qui font de la voix sur IP reçoivent des adresses IP fixes publiques ou des traductions en adresses IP fixes publiques.
Discutez cette solution (évaluez les avantages et les inconvénients, la faisabilité de la solution) ?

Question 7
Une autre solution consiste à faire en sorte que les routeurs NAT connaissent la structure des messages des protocoles de voix sur IP comme SIP ou Skype.
Précisez et discutez cette solution ?

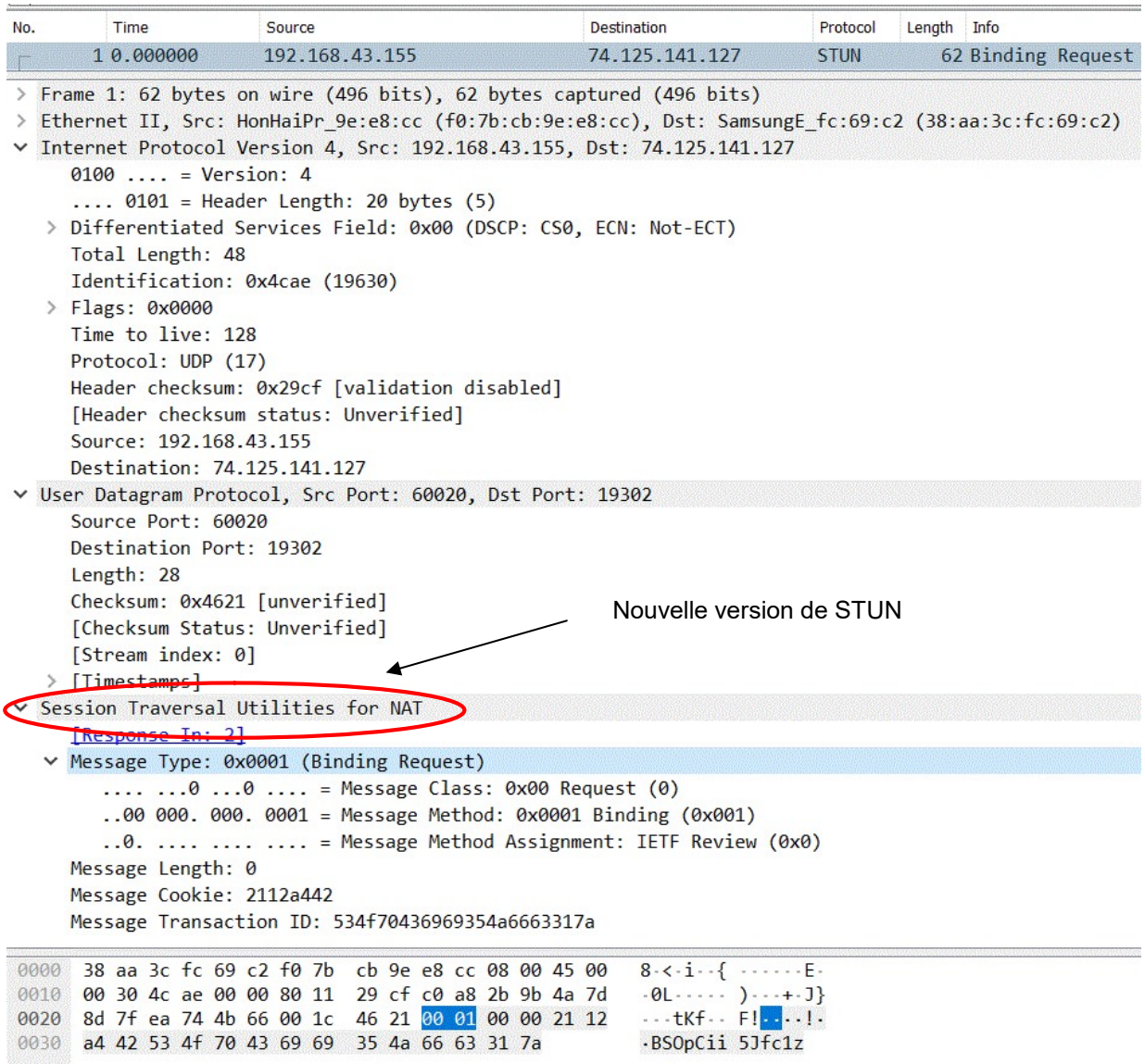
Question 8
Une troisième solution consiste à utiliser un protocole client/serveur baptisé STUN. Ce protocole a été conçu pour répondre aux problèmes des adresses IP contenues dans la partie charge utile des messages.
Un client STUN est associé à un utilisateur de l'Internet qui souhaite connaître son adresse IP et son numéro de port. Un serveur STUN est situé dans l'Internet global (celui des adresses publiques). Il possède un port de numéro réservé (port 'bien connu', 3478 pour UDP et TCP, et 5349 pour TLS).
Dans un message de requête un client STUN (typiquement un téléphone IP) émet une demande de son adresse IP et de son numéro de port vers un serveur STUN situé dans l'Internet global. Le serveur STUN analyse le datagramme reçu et répond en retournant au client l'adresse IP et le port public du client dans le message. L'architecture globale se résume sur la figure suivante :



source : https://www.vladan.fr/what-is-stun-server/ consulté le 15/11/2019 à 19h50

On se place dans le cas où les adresses sont traduites en sortie d'un domaine (traduction des adresses et port source sur les datagrammes en sortie et des adresses et ports destination sur les datagrammes en entrée). On fait l'hypothèse que le routeur NAT effectue toujours la même traduction pour tous les datagrammes ayant un couple adresse, numéro de port donné. Comment le serveur STUN peut-il connaître l'adresse IP et le numéro de port du demandeur dans l'Internet global?
Expliquez comment le client utilise les informations reçues pour résoudre le problème des adresses IP contenues dans les messages ?

Question 9
Ci-dessous un exemple de requête Bind dans le protocole STUN côté client (réseau privé) vers le serveur (Internet global).



Ci-après la réponse au Bind par le serveur (réseau public) vers le client (réseau privé).

```
    2 0.043685     74.125.141.127          192.168.43.155        STUN       74 Binding Success Response MAPPED-ADDRESS: 70.199.128.46:4604
> Ethernet II, Src: SamsungE_fc:69:c2 (38:aa:3c:fc:69:c2), Dst: HonHaiPr_9e:e8:cc (f0:7b:cb:9e:e8:cc)
v Internet Protocol Version 4, Src: 74.125.141.127, Dst: 192.168.43.155
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x3b72 (15218)
  > Flags: 0x0000
    Time to live: 43
    Protocol: UDP (17)
    Header checksum: 0x8fff [validation disabled]
    [Header checksum status: Unverified]
    Source: 74.125.141.127
    Destination: 192.168.43.155
> User Datagram Protocol, Src Port: 19302, Dst Port: 60020
v Session Traversal Utilities for NAT
    [Request In: 1]
    [Time: 0.043685000 seconds]
  v Message Type: 0x0101 (Binding Success Response)
      .... ...1 ...0 .... = Message Class: 0x10 Success Response (2)
      ..00 000. 000. 0001 = Message Method: 0x0001 Binding (0x001)
      ..0. .... .... .... = Message Method Assignment: IETF Review (0x0)
    Message Length: 12
    Message Cookie: 2112a442
    Message Transaction ID: 534f70436969354a6663317a
  v Attributes
    v MAPPED-ADDRESS: 70.199.128.46:4604
      > Attribute Type: MAPPED-ADDRESS (0x0001)
        Attribute Length: 8
        Reserved: 00
        Protocol Family: IPv4 (0x01)
        Port: 4604
        IP: 70.199.128.46

0000  f0 7b cb 9e e8 cc 38 aa  3c fc 69 c2 08 00 45 00   ·{····8· <·i···E·
0010  00 3c 3b 72 00 00 2b 11  8f ff 4a 7d 8d 7f c0 a8   ·<;r··+· ··J}····
0020  2b 9b 4b 66 ea 74 00 28  6c 01 01 01 00 0c 21 12   +·Kf·t·( l·····!·
0030  a4 42 53 4f 70 43 69 69  35 4a 66 63 31 7a 00 01   ·BSOpCii 5Jfc1z··
0040  00 08 00 01 11 fc 46 c7  80 2e                    ------F· ··

stun-ice-testcall.pcap                                                    Paquets: 108
```

A quel endroit du réseau la capture de la trace a été faite ? Quelle est l'adresse publique attribuée au Client dans le réseau privé ?

Question 10
A quelles phases de l'interaction entre 2 entité correspond l'utilisation d'un serveur STUN ?

Question 11
De nombreux routeurs NAT effectuent une traduction d'adresse IP et de numéro de port source qui dépend de la destination. Tous les datagrammes ayant même source et même destination sont traduits de la même façon. Mais deux datagrammes ayant même source (adresse IP et numéro de port) et deux destinations différentes (adresse IP ou numéro de port) voient l'adresse IP et le numéro de port source traduits de deux façons différentes.
Expliquez pourquoi dans ce cas, le protocole STUN ne marche plus.