



LICENCE 3 DE SCIENCES, MENTION INFORMATIQUE

RÉSEAUX ET PROTOCOLES

# MODÈLE DE DOCUMENT POUR UN RAPPORT D'ÉTUDE

Présenté par  
Julien MONTAVONT  
montavont@unistra.fr

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Concepts et utilisation</b>	<b>3</b>
2.1	En-tete IPv4 . . . . .	3
<b>3</b>	<b>Suite de protocole</b>	<b>5</b>
3.1	ARP . . . . .	5
3.1.1	Exemple . . . . .	5
3.1.2	Entête . . . . .	5
3.1.3	Fonctionnement . . . . .	5
3.1.4	ACD . . . . .	6
3.2	ICMP . . . . .	6
3.2.1	Message de type 3: Unreachable Destination . . . . .	6
3.2.2	Message de type 4: . . . . .	7
3.2.3	Message de type 11: Time Exceeded . . . . .	7
3.2.4	Message de type 5: . . . . .	7
3.2.5	Message de type 8 et 0: . . . . .	8
3.3	IGMP . . . . .	8
3.4	DHCP . . . . .	8
<b>4</b>	<b>Conclusion</b>	<b>10</b>
	<b>Références</b>	<b>10</b>

## 1 Introduction

A la fin des années 1960 il y eu une forte demande de la part des universités et centres de recherche aux Etats-Unis pour la création d'un réseau permettant d'une part, d'interconnecter les différentes structures afin de partager les informations et d'autre part, de faire des expérimentations sur les réseaux. C'est dans le but de faire ce réseau que l'ARPA a créé l'ARPANET qui est l'ancêtre d'internet. En effet, c'est à partir des principes de ce réseau qu'a été créé internet. L'ARPA (Advanced Research Project Agency ) est une agence de recherche créée par le département américain de la défense en 1957 afin de développer de nouvelles technologies à usage militaire. L'ARPA a mis en place en 1969 le premier réseau mondial qui a été appelé ARPANET ( Advanced Research Project Agency NETwork ). Ce réseau a été conçu de façon a ne pas dépendre d'un centre névralgique qui aurait pu être détruit en cas d'attaque nucléaire. Ce réseau a été constitué comme une toile reliant plusieurs serveurs. Chaque serveur est un noeud et peut stocker, traiter ou servir de relais. Ainsi, il existe plusieurs chemins pour accéder à un noeud et lorsqu'un noeud est hors service, il est toujours possible de rejoindre le noeud destinataire en passant par un autre chemin. Avant ARPANET, la communication réseau était également basée sur la communication par circuit électrique dont les informations étaient envoyées en continue dans un seul morceau. Ce réseau est le premier qui fonctionne sur la base de paquets. Le principe de communication par paquet est de découper l'information à transmettre en de plus petits paquets qui peuvent chacun prendre un chemin différent pour arriver à destination. Ce réseau se développa est il compta 23 noeuds en 1971 et en 1977 il en compta 111. Afin d'uniformiser ce réseau, Vint Cerf et Bob Kahn on introduit la première version du protocole TCP. Historiquement, les protocoles IP constituaient la partie du protocole TCP qui s'occupe de la transmission en mode sans connexion. La transmission en mode sans connexion est une transmission de donnée dans laquelle chaque paquet contient l'adresse de destination. Ceci permet une transmission du paquet sans que les deux hôtes soient obligés d'établir une connexion

auparavant. Cette version est ce qu'on aurait pu nommer l'IPv1 et elle est documentée dans la RFC 675. Cette version fut modifiée et publiée en 1977. Elle correspond à la deuxième version de TCP (IPv2). Initialement, le protocole TCP avait deux fonctions. (as a host level end to end protocol, and to serve as an internet packaging and routing protocol. These two things should be provided in a layered and modular way. I suggest that a new distinct internetwork protocol is needed, and that TCP be used strictly as a host level end to end protocol.”) Premièrement, il devait permettre une transmission fiable d'informations entre deux hôtes. Il devait également servir en tant que protocole de routage et de packaging. Cependant, pour être cohérent avec le modèle en couche, qui différencie la fiabilité (couche transport) et le routage (couche réseau), il fut décidé en 1978 de diviser le protocole TCP. Le protocole TCP ne s'occupe maintenant plus que de la partie transport. La partie réseau a été prise en charge par les protocoles IP. C'est finalement le 1er janvier 1983 que l'ARPANET adopte les protocoles TCP/IP et donc l'IPv4.

## 2 Concepts et utilisation

### 2.1 En-tête IPv4

Un packet IPv4 est précédé par un en-tête ayant une longueur minimale de 20 octets (dans le cas aucune option supplémentaire a été spécifiée). La figure suivante montre le contenu de l'en-tête d'un packet IPv4.

TODO FIGURE

Comme on peut voir dans la figure ci dessus, un en-tête IPv4 est composé par 13 champs. En réalité nous verrons plus loin que cet en-tête peut, quand il est nécessaire, contenir un champ additionnel qui servira à spécifier quelque option qui n'est pas présente dans les 13 champs ci dessus.

Commençons par voir plus en détail les 13 champs d'un en-tête IPv4 standard:

**Version** Cette champ occupe les premiers 4 bits de l'en-tête IPv4. Il est utilisé pour déterminer le type de protocole utilisé par la couche réseau (couche 3). Dans le cas de IPv4 cet champs contiendra toujours la valeur 4, qui justement identifie le protocole IPv4.

Cet champ n'est pas très utilisé, en tenant compte que le protocole à utiliser pour la couche 3 est presque toujours spécifié dans l'en-tête de la couche liaison.

**IHL** Le champ IHL spécifie la taille de l'en-tête IPv4, en fait IHL est l'acronyme de Internet Header Length. Bien entendu, en disant cela on souligne un concept important à propos du protocole IPv4: la taille de l'en-tête n'est pas fixe.

La taille de l'en-tête est exprimée en blocs de 32 bits. Étant donné une taille de 4 bits pour le champ IHL, la longueur maximale d'un en-tête IPv4 est de 15 blocs de 32 bits, qui correspond à 60 octets. Comme l'en-tête IPv4 a une taille minimale de 20 octets (160 bits), le champ IHL ne peut pas contenir une valeur inférieure à 5.

**Type of Service** Le champ Type of Service, mieux connu avec l'acronyme ToS, est utilisé pour spécifier la qualité de service souhaitée pour l'envoi d'un packet IPv4. Cet champ occupe un octet de l'en-tête et il se compose en trois parties. Une première partie de 3 bits permet d'indiquer la priorité avec laquelle le packet doit être traité, les 3 bits après sont utilisés pour spécifier certaines caractéristiques du service, notamment: le temps, le débit et la fiabilité. Enfin l'emploi des 2 derniers bits n'a pas été spécifié et leur usage a été laissé libre pour des implémentations futures.

En réalité l'histoire de ces champs est bien plus longue et complexe que ça, car en pratique la façon d'utiliser ces champs a été modifiée plusieurs fois au cours des années. <sup>1</sup> Cette

---

<sup>1</sup>L'utilisation des 8 bits du champ ToS a été redéfinie par cinq standards différents (plus divers standards

manque de stabilité a par fois cause une certaine confusion dans les implementations. <sup>2</sup>

Aujourd'hui les 8 bits du champ ToS sont utilisés par le mécanisme DiffServ (Differentiated Services). Cet système utilise les premières 6 bits du champ ToS (DSCP - Differentiated Services Code Point) pour marquer chaque paquet comme appartenant à un niveau de priorité et une classe de service. Chaque classe détermine le type de traitement que l'on souhaite demander pour le paquet aux routeurs au long du chemin (PHB - Per-Hop behaviour), toutefois le service offert par chaque routeur est fortement lié à sa configuration.

<sup>3</sup> Les dernières 2 bits du champ ToS sont utilisés pour l'extension ECN (*Explicit Congestion Notification*). Cette extension, proposée par RFC2481 et introduite deux ans après avec le RFC3168, ajoute un système de contrôle de la congestion du trafic réseau. Dans le cas d'une saturation du réseau ce champ est utilisé pour notifier ce problème et demander au dispositif émetteur une réduction du rythme auquel les paquets sont envoyés, avec l'objectif de réduire l'attente et la perte de paquets.

**Total length** Comme le suggère le nom, ce champ est utilisé pour indiquer la taille totale du paquet IPv4: en tête plus données. Le champ *Total length* est défini sur 16 bits, ceci permet de indiquer une valeur comprise entre 0 et 65,535 octets. Comme l'en-tête est compris dans la longueur totale d'un paquet cette valeur ne serait jamais inférieure à 20 (taille minimale d'un en-tête IPv4 en octets). RFC 791 impose à tous les dispositifs d'un réseau IPv4 la capacité de recevoir des paquets jusqu'à une taille de 576 octets, cette prérogative permet d'éviter une excessive fragmentation.

**Identification** Cet en-tête (sur 16 bits) permet d'identifier les fragments appartenant au même paquet.

**Flags** Les 3 bits du champ Flags sont utilisés pour gérer la fragmentation d'un paquet. Un de ces bits est employé pour indiquer si le paquet peut être fragmenté ou non. Ce bit, appelé DF (*Don't Fragment*), doit être pris en considération par les routeurs dans le chemin pour décider si un paquet trop grand pour être transmis peut être retransmis sous forme de fragments plus petits ou rejeté. Un autre bit, appelé MF (*More Fragments*), indique si le paquet est suivi par d'autres fragments. Le bit MF est mis à 0 dans le dernier fragment ou dans des paquets qui n'ont pas été fragmentés.

Un des trois bits de ce champ n'est pas actuellement utilisé mais il a été réservé pour applications futures possibles. <sup>4</sup>

**Fragment Offset** Lorsque un paquet a été fragmenté cet en-tête est utilisé pour déterminer la position (offset) d'un fragment par rapport aux données du paquet réassemblé. Le décalage de chaque fragment est exprimé en blocs de huit octets (ou 64 bits). Le champ Fragment Offset utilise 13 bits de l'en-tête IPv4, cela permet un offset maximal de 65,528 octets.<sup>5</sup> Étant donné que le flag MF (*More Fragments*) doit être mis à zéro lorsque si un

---

experimentals). Les documents présentent ces standards sont mentionnés dans le chapitre "Historical Definitions for the IPv4 TOS Octet" du RFC 3168

<sup>2</sup>Comme le souligne le RFC 3260 "At least one implementor has expressed confusion about the relationship of the DSField, as defined in RFC 2474, to the use of the TOS bits, as described in RFC 1349"

<sup>3</sup>"The DiffServ standard does not specify a precise definition of "low," "medium," and "high" drop probability. Not all devices recognize the DiffServ (DS2 and DS1) settings; and even when these settings are recognized, they do not necessarily trigger the same PHB forwarding action at each network node. Each node implements its own response based on how it is configured." - Implementing Quality of Service Policies with DSCP <http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html>

<sup>4</sup>Cet bit a été aussi le protagoniste d'un des plus connus poissons d'avril présentée par le IETF. Pour faciliter les tâches des systèmes de filtrage le RFC 3514 propose d'utiliser ce bit pour étiqueter paquets malveillants, à ce titre tous les paquets étant envoyés avec ce bit (renommé "Evil Bit") mis à 1 seront mis à la poubelle.

<sup>5</sup>En pratique un tel offset n'est jamais utilisé car, en ajoutant un en-tête minimal de 20 octets, la taille totale du paquet réassemblé dépasserait la longueur maximale d'un paquet IPv4.

paquet n'est pas fragmentée ou si il est le dernier fragment d'un paquet plus grand, l'unique différence entre ces deux types de paquets est la valeur de le champ Fragment Offset que, dans le cas d'un paquet pas fragmentée, est toujours zero.

**Time to Live** Cet champ determine le nombre maximal de fois qu'un paquet peut etre retransmis, il est utilise pour empecher que un paquet puisse etre retransmis a l'infini. Chaque router au long du chemin d'un paquet est tenu a detruire un paquet si la valeur du TTL (*Time to Live*) est zero ou decrements ce champs par le nombre de secondes que le paquet passe en attente d'etre transmis.

En theorie le TTL indique le nombre de secondes pendant le quels un paquet peut continuer a etre retransmis dans un reseau ,mais , etant chaque router toujours tenu a decrements ce champ de au moins 1 (meme si le paquet a ete retransmis en moins qu'une seconde) et considerant les performances des routers d'aujourd'hui, en pratique le TTL indique le nombre maximum de router que un paquet peut rencontrer au long de son chemin.

Le space reservee au TTL dans l'en-tete IPv4 est de un octet ce qui comporte un TTL maximum de 255.<sup>6</sup>

Quand un paquet a ete detruit ensuite a l'expiration du TTL, le router qui a detruit le paquet peut decider de envoyer un message d'erreur a l'emetteur du paquet detruit. Ce type de message (ICMP Time exceeded) est utilise par outils comme *traceroute* pour decouvrir, approximativement, le chemin d'un packet IP.

**Protocol** Chaque paquet IPv4 specifie le protocole utilise par les donnees transmises: cela est l'objectif de ce champs de 8 bits

**Header Checksum** Ce champ contient une somme de controle et est utilise pour detecter des erreurs dans l'en-tete IPv4. La valeur de ce champs est recalcule a chaque retransmission<sup>7</sup>: si il ne correspond pas avec celui presente dans l'en-tete le paquet est detruit.

## 3 Suite de protocole

### 3.1 ARP

ARP (Address resolution protocol) est un protocole à cheval sur la couche 2 et la couche 3. La fonction principale d'ARP est de faire la conversion entre les adresses de niveau 2 et de niveau 3. Cela est très utilisé étant donné que les hôtes connaissent souvent les adresses IP de leur destinataire, mais rarement l'adresse de niveau 2 de ce destinataire ou de la passerelle à contacter pour joindre le destinataire.

#### 3.1.1 Exemple

Dans la partie qui suit nous allons nous placer dans l'exemple suivant. TODO LAN exemple

#### 3.1.2 Entête

#### 3.1.3 Fonctionnement

Prenons l'exemple où A veut envoyer un message à B. A connaît l'adresse IP de B. Donc A va préparer son paquet qu'il va envoyer à B, avec son adresse IP en source et l'adresse IP de B en destination. Le paquet passe dans la couche liaison, il va être encapsulé dans une trame de niveau 2. Cette trame aura comme adresse source l'adresse de niveau 2 de A, mais à ce moment il

---

<sup>6</sup>Le RFC 1700 recommande une valeur par défaut de 64.

<sup>7</sup>Cela est nécessaire car le TTL est decrementé à chaque retransmission et un changement de l'en-tête comporte une valeur différente dans la somme de contrôle



### 3.2.2 Message de type 4:

### 3.2.3 Message de type 11: Time Exceeded

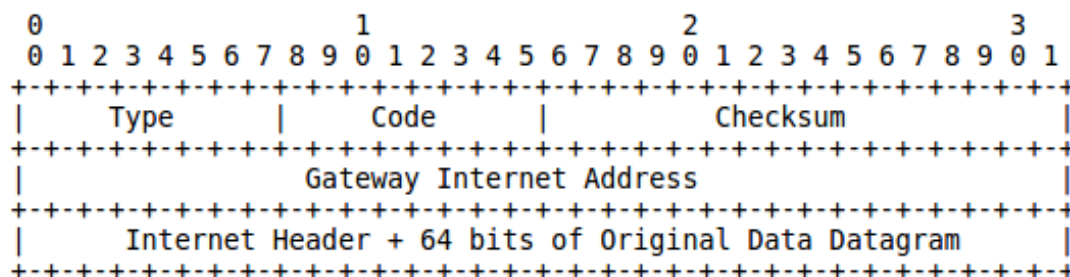
Ces messages sont envoyés lorsque le TTL d'un paquet à atteint 0. Une autre utilisation des ces messages est lorsque que le temps de ré-assemblage des fragments d'un paquet est dépassé. Ces deux cas sont distingé par le code. Ces messages ont pour destinataire l'hôte qui à envoyé le paquet qui à provoqué l'erreur.//TODO(vérifier) Le champ Internet header contient l'entête du paquet qui a été supprimé plus les 64 bits suivant celui-ci. Cela permet à l'émetteur de retrouver quel paquet à été supprimé.

**Code 0:** Le code 0 est utilisé pour indiquer que le TTL du paquet posant problème est arrivé à 0. Lorsque le TTL d'un paquet arrive à 0, celui-ci est supprimer et un message ICMP de type 11 et de code 0 est envoyer par le routeur qui à détecté le problème. Cela permet principalement d'éviter qu'un paquet sans dans une boucle et qu'il soit relayé à l'infini.

**Code 1:** Le code 1 est quant à lui utilisé pour indiquer //TODO

### 3.2.4 Message de type 5:

Les message de type 5 utilisent les entêtes ci-dessous et servent à faire de la redirection. En effet, lorsqu'un routeur détecte que le prochain routeur dans lequel va transiter le paquet se trouve dans le même réseau que l'émetteur de ce paquet, il va envoyer un message ICMP pour avertir cet hôte (et/ou le réseau) qu'il existe un chemin plus court en envoyant directement les paquets vers le prochain routeur. Ce message ICMP va avoir pour effet de modifier la table de routage interne à l'émetteur (et/ou des hôtes connecté au réseau). Concernant le paquet que le premier routeur à reçu, il va le transmettre vers sa destination.



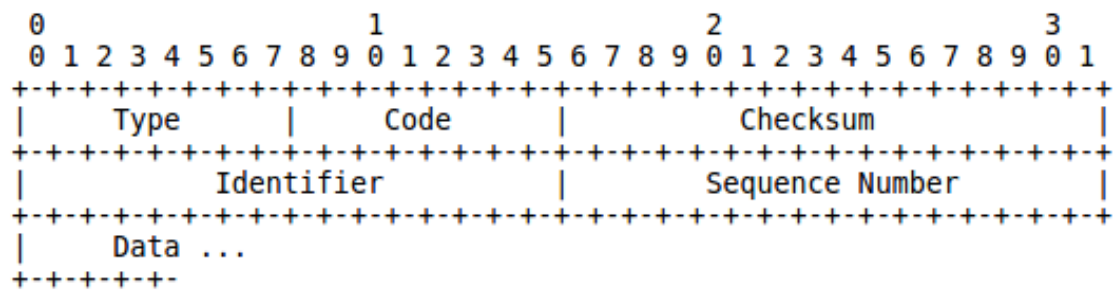
Le champ Gateway Internet Address contient la l'adresse du routeur auquel il faut faire transiter le trafic directement pour avoir un chemin de routage plus court. Le champ Internet Header contient toujours l'entête du message ayant porvoqué l'envoi du message ICMP plus les 64 bits suivant l'entête. Cela permet à (aux) hôte(s) de pouvoir modifier leur table de routage en fonction la destination que cherchait à atteindre le paquet.

**Code 0** Ce code indique que la redirection est adresser à tout le réseau de l'émetteur du paquet.

**Code 1** Ce code indique que la redirection est adresser à l'émetteur du paquet.

**Code 2** Ce code indique que la redirection est adresser à tout le réseau de l'émetteur du paquet et aux services(//TODO(préciser)).

**Code 3** Ce code indique que la redirection est adresser à l'émetteur du paquet(//TODO(préciser)).



### 3.2.5 Message de type 8 et 0:

Les messages de type 8 et 0 servent à faire des envoies et des renvoies d'information. Ils utilisent pour cela l'entête ci-dessus. Les messages de type 8 font des envoies d'informations, appelé echo request. Tandis que les messages de type 0 sont envoyés en réponse aux echo request et renvoie les informations reçus de ceux-ci; ils sont appelés echo reply. Etant donnée que les echo reply sont des réponses aux echo request, l'adresse destination des echo reply est l'adresse source des echo request. Ces deux messages peuvent envoyés et reçu aussi bien par un hôte que par un routeur. Ce sont notamment les message envoyés par la commande *ping* qui permet de vérifier si l'on peut communiquer avec un hôte ou un routeur. Les champs Identifier et Sequence Number aide l'émetteur de l'echo request à associer les echos request qu'il à envoyés avec les echos reply qu'il à reçus. //TODO(qui a t-il dans data?)

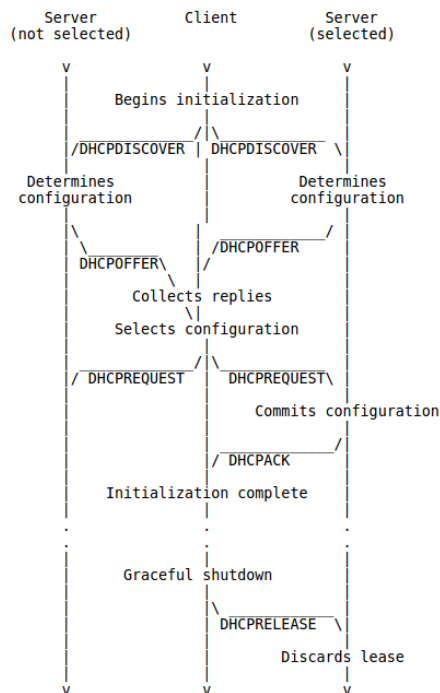
## 3.3 IGMP

## 3.4 DHCP

<sup>9</sup> Le protocole DHCP (Dynamic Host Configuration Protocol) sert à l'autoconfiguration des interfaces. Plus précisément, il permet d'attribuer une adresse IP à une interface et de lui faire parvenir d'autres information essentielle pour le fonctionnement de l'interface sur le réseau. Voyons comment une interface peut ce configurer auprès d'un serveur DHCP.

<sup>9</sup>RFC 2131: <https://tools.ietf.org/html/rfc2131>





Lorsqu'une interface, qui n'a pas d'adresse IP, souhaite en recevoir une, elle va émettre un message DHCPDISCOVER en broadcast sur son réseau. Des agents DHCP peuvent faire passer ce message DHCP sur un autre réseau si le serveur DHCP (qui distribue les adresses) ne se trouve pas sur le même réseau que l'hôte qui fait la demande.

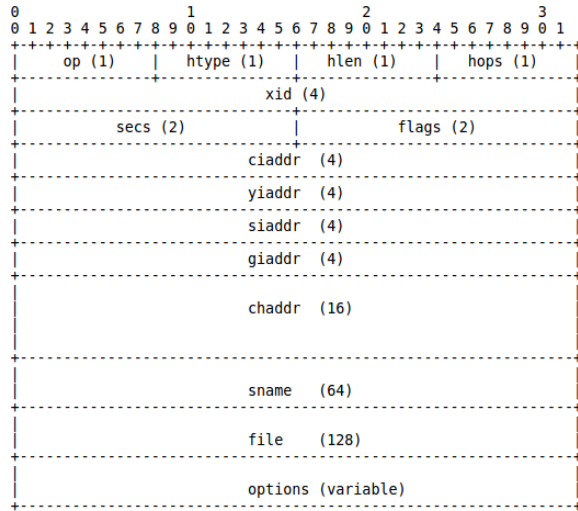
Étant donné que le message est envoyé en broadcast, tous les hôtes sur le réseau vont recevoir le message, et en particulier le ou les serveurs DHCP qui pourraient s'y trouver. Si cela est le cas, ceux-ci vont répondre avec un DHCPOFFER. Ce message contient entre autre l'adresse IP proposée pour le client souhaitant se configurer, ainsi que le masque de sous-réseau de l'adresse. À ce moment-là l'adresse n'est pas encore attribuée et réservée pour l'hôte étant donné qu'il peut refuser l'offre et accepter l'offre d'un autre serveur. Si jamais l'hôte ne reçoit aucun DHCPOFFER, il va ré-émettre un DHCPDISCOVERY. Si il reçoit un ou plusieurs DHCPOFFER, l'hôte va devoir choisir une configuration qui lui est proposée. Une fois ce choix fait, il va informer les serveurs DHCP de son choix à l'aide d'un message DHCPREQUEST émis en broadcast. Ce message va contenir l'identifiant du serveur DHCP retenu ainsi que la configuration souhaitée par l'hôte (adresse IP et masque de sous-réseau). Ce message peut être interprété de deux manières différentes selon le serveur :

- si ce n'est pas le serveur retenu, il considère le message comme une déclinaison de l'offre.
- si c'est le serveur retenu, il va sortir l'adresse attribuée à l'hôte de la plage d'adresse libre pour ne plus l'attribuer à un autre hôte. Il va ensuite émettre un message DHCPACK contenant la configuration effective de l'hôte avec notamment : l'adresse IP, le masque de sous-réseau, la durée du bail, l'adresse de la passerelle par défaut et l'adresse du serveur DNS. Si pour quelque raison le serveur n'est pas capable d'attribuer l'adresse proposée dans l'offre (par exemple si l'adresse a été attribuée entre temps), le serveur émet un DHCPNAK pour avertir l'hôte que l'adresse n'est plus disponible. L'hôte devra alors recommencer la procédure pour obtenir une adresse IP. Enfin si le serveur ne reçoit pas de message DHCPREQUEST, la procédure s'arrêtera à ce moment et l'adresse n'étant pas encore attribuée à l'hôte elle reste disponible pour être attribuée à d'autre hôte. Arrive la dernière étape. Si le client reçoit un message DHCPACK, il peut prendre en compte la configuration (adresse IP, masque de sous-réseau, DNS, passerelle par défaut et durée de bail). Il va effectuer une dernière vérification pour s'assurer que l'adresse qui lui a été attribuée est bien unique sur le réseau pour éviter d'avoir deux hôtes avec la même adresse. Il va pour cela utiliser le protocole ARP et la méthode de vérification vu plus haut. Si jamais l'adresse est

déjà utilisé par un autre hôte, il va envoyer un message DHCPDECLINE au serveur DHCP pour lui indiquer qu'il n'utilisera pas la configuration proposé par celui-ci, et il va recommencer la procédure pour pouvoir obtenir une nouvelle configuration.

Si jamais l'adresse proposé par le serveur est unique sur le réseau, la configuration est terminé et l'hôte peut utiliser l'adresse (durant la durée du bail de celle-ci). Dernier cas possible, si jamais le l'hôte ne reçoit pas de DHCPACK ou de DHCPNAK, il va rémettre le message DHCPREQUEST pour esperer recevoir une réponse du serveur.

//TODO algo de retransmission //TODO fonctionnement agent relais dhcp //client peut renoncer à son bail //identification des message faisant partit d'un meme echange avec client identifier, server identifier



## 4 Conclusion