

# 1. Le service DHCP.

## 1.1. Introduction.

Le DHCP fournit des paramètres de configuration pour des machines Internet. DHCP est constitué de 2 parties : Un protocole pour la livraison de paramètres de configuration de machines spécifiques à partir d'un serveur DHCP et un mécanisme d'allocation d'adresses réseaux à des machines.

DHCP est bâti sur le modèle client - serveur, où la machine désignée serveur DHCP alloue des adresses réseaux et délivre des paramètres de configuration à des machines configurées dynamiquement. D'un bout à l'autre de ce document, le terme "serveur" se réfère à une machine fournissant des paramètres d'initialisation au travers du DHCP, et le terme "client" se réfère à une machine qui demande des paramètres d'initialisation au serveur DHCP.

Une machine ne devrait pas agir en tant que serveur DHCP à moins que cela ne soit spécifié par l'administrateur du système. La diversité des implantations du matériel et des protocoles sur l'Internet conduirait à un manque de fiabilité au niveau des opérations si n'importe quelle machine était autorisée à répondre aux requêtes DHCP. Par exemple, IP nécessite le paramétrage de nombreux paramètres à l'intérieur du logiciel qui implante le protocole. Parce qu'IP peut être utilisé sur un grand nombre de matériels réseaux, les valeurs par défaut de ces paramètres ne peuvent être devinées ou présupposées pour être correctes. De même, les schémas de distribution d'adresses reposent sur un mécanisme d'élection/défense pour la découverte des adresses déjà utilisées. Les machines IP ne peuvent pas toujours défendre leurs adresses réseaux, ainsi un tel schéma d'allocation d'adresse ne peut garantir que les adresses allouées ne se dupliquent.

DHCP supporte 3 mécanismes pour l'allocation des adresses IP. L'allocation automatique : DHCP assigne une adresse IP permanente à un client. L'allocation dynamique : DHCP assigne une adresse IP à un client pour une durée déterminée (ou jusqu'à ce que le client renonce à son adresse). L'allocation manuelle, une adresse IP est assignée par l'administrateur réseau, et DHCP est simplement utilisé pour convoier les adresses désignées jusqu'au client. Un réseau spécifique utilisera un ou plusieurs de ces mécanismes, cela dépend de la stratégie de l'administrateur réseau.

L'allocation dynamique est la seule des 3 mécanismes qui réutilise automatiquement une adresse qui n'est plus utilisée par un client. De plus, l'allocation dynamique est particulièrement utile pour assigner une adresse à un client qui se connectera au réseau de manière temporaire, ou pour partager une liste limitée d'adresses IP entre un groupe de clients qui ne nécessitent pas une adresse permanente. L'allocation dynamique est aussi un bon choix pour assigner une adresse IP à un nouveau client qui se connectera de manière permanente au réseau où les adresses IP sont suffisamment rares pour qu'il soit important de les récupérer quand les anciens clients sont hors connexion. L'allocation manuelle permet à DHCP d'être utilisé pour éliminer les processus enclins à l'erreur de configuration manuelle de machines avec une adresse IP dans des environnements où (pour diverses raisons) il est préférable de gérer l'attribution des adresses IP en dehors des mécanismes de DHCP.

DHCP utilise le protocole de transport UDP. Les messages DHCP d'un client vers un serveur sont envoyés au port (67) du 'serveur DHCP' et les messages d'un serveur vers un client sont envoyés au port (68) 'client DHCP'. Un serveur avec de multiples adresses réseau (par ex : une machine multi-sites) peut utiliser n'importe laquelle de ses adresses dans un message DHCP sortant.

### Avantages de DHCP dans l'administration d'un réseau ?

1. Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.

2. Economie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité. Ainsi grâce à DHCP, seules les machines connectées en ligne ont une adresse IP. En effet, imaginons un fournisseur d'accès qui a plus de 1000 clients. Il lui faudrait 5 réseaux de classe C, s'il voulait donner à chaque client une adresse IP particulière. S'il se dit que chaque client utilise en moyenne un temps de connexion de 10 mn par jour, il peut s'en sortir avec une seule classe C, en attribuant, ce que l'on pourrait appeler des "jetons d'accès" en fonction des besoins des clients.
3. Les postes itinérants sont plus faciles à gérer
4. Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

Avec DHCP, il suffit d'attribuer une adresse au serveur. Lorsqu'un ordinateur client DHCP demande l'accès au réseau en TCP-IP, son adresse est allouée dynamiquement à l'intérieur d'une plage d'adresses définie sur le serveur.

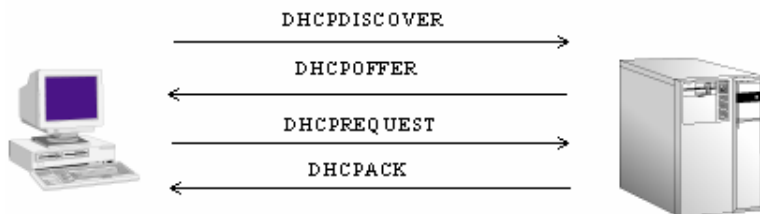
L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'hôte peut utiliser une configuration IP attribuée, avant de devoir solliciter le renouvellement du bail auprès du serveur DHCP.

**L'inconvénient :**

Le client utilise des trames de broadcast pour rechercher un serveur DHCP sur le réseau, cela charge le réseau. Si vous avez une entreprise avec plusieurs centaines de personnes qui ouvrent leur session le matin à 8 h ou l'après midi à 14 h, il peut s'en suivre de graves goulets d'étranglement sur le réseau. L'administrateur devra donc réfléchir sérieusement à l'organisation de son réseau.

**1.2. Allocation d'une adresse réseau.**

Nous aborderons dans ce paragraphe l'interaction entre un client et un serveur DHCP dans le cas où le client n'a pas encore reçu un bail précédent pour une adresse IP. Si le client connaît déjà son adresse, certaines étapes peuvent être omises, cette interaction réduite est décrite dans la section suivante.



Octet1	Octet2	Octet3	Octet4
op(1)	htype(1)	hlen(1)	hops(1)
xid(4)			
secs(2)		flags(2)	
ciaddr(4)			
yiaddr(4)			
siaddr(4)			
giaddr(4)			
chaddr(4)			
sname(16)			
file(128)			
options (dépend de la norme RFC 2132)			

Format d'un paquet de type DHCP.

Pour le champ des options, nous retrouvons le format suivant :

Octet1	Octet2	Octet3
Code de l'option	Longueur	Données

1. Le client diffuse un message DHCPDISCOVER sur son réseau local physique. Le message DHCPDISCOVER peut inclure des options qui suggèrent des valeurs pour les adresses réseau et la durée du bail. Les agents de relais BOOTP peuvent passer le message sur des serveurs DHCP qui ne se trouvent pas sur le même sous réseau physique. Nous reviendrons ultérieurement sur la raison d'exister des agents de relais BOOTP.

Dans le paquet DHCP, nous retrouverons les informations de champs suivants :

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client (uniquement si le client a déjà une adresse)
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	0.0.0.0	Adresse IP de l'agent DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	0.0.0.
Adresse IP de destination	255.255.255.255
Adresse MAC source	ex : 00 11 2F 50 66 A1 (adresse MAC du client)
Adresse MAC de destination	FF FF FF FF FF FF
Au niveau UDP	Port source 68, port de destination 67

Nous retrouvons un champ d'options reprises dans le protocole RFC 2132 et nous nous limiterons aux options les plus courantes. Dans le champ d'options, nous retrouverons :

DHCP option 53	DHCP Discover
----------------	---------------

2. Chaque serveur peut répondre avec un message DHCP OFFER qui inclut une adresse réseau valide dans le champ 'yiaddr' (et d'autres paramètres de configuration des options DHCP). Le serveur n'a pas besoin de réserver l'adresse réseau offerte, bien que le protocole fonctionnera de manière optimale si le serveur évite d'allouer les adresses offertes à un autre client. Quand on alloue une nouvelle adresse les serveurs doivent vérifier que l'adresse réseau offerte n'est pas déjà utilisée ; par ex : le serveur devrait vérifier les adresses offertes par une requête d'écho ICMP. Les serveurs devraient être implantés de manière à ce que les administrateurs réseaux puissent choisir de désactiver les vérifications des adresses nouvellement allouées. Le serveur transmet un message DHCP OFFER au client, en utilisant l'agent de relais BOOTP si nécessaire.

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	0.0.0.0	Adresse IP de l'agent DHCP
yiaddr	192.168.1.100	Adresse IP proposée par le serveur DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	192.168.1.2 (adresse IP du serveur DHCP)
Adresse IP de destination	255.255.255.255 (adresse pas encore connue du client)
Adresse MAC source	ex : 00 0F 66 C8 A1 38 (adresse MAC du serveur DHCP)
Adresse MAC de destination	ex : 00 11 2F 50 66 A1 (adresse MAC du client)
Au niveau UDP	Port source 67, port de destination 68

Nous retrouvons un champ d'options reprises dans le protocole RFC 2132 et nous nous limiterons aux options les plus courantes. Dans le champ d'options, nous retrouverons :

DHCP option 53	DHCP Offer
DHCP option 1	Masque de sous réseau. Ex : 255.255.255.0
DHCP option 3	Routeur par défaut. Ex : 192.168.1.1
DHCP option 51	Durée de location de l'adresse IP. Ex : 1 jour
DHCP option 54	Adresse du serveur DHCP. Ex : 192.168.1.2

3. Le client reçoit un ou plusieurs messages DHCP OFFER d'un ou plusieurs serveurs. Le client peut choisir d'attendre des réponses multiples. Le client choisit un serveur pour ses paramètres de configuration, basé sur la configuration présente dans le DHCP OFFER. Le client diffuse un message DHCP REQUEST qui doit inclure l'option 'identifiant serveur' indiquant quel serveur il a sélectionné et qui peut inclure d'autres options spécifiant les valeurs de configuration désirées. L'option 'adresse IP demandée' doit être réglée sur la même valeur que 'yiaddr' du message DHCP OFFER provenant du serveur. Ce DHCP REQUEST est diffusé et relayé au travers de l'agent de relais DHCP/BOOTP. Pour s'assurer que n'importe quel agent de relais fasse suivre le message DHCP REQUEST au même serveur DHCP qui a reçu le message DHCP DISCOVER original, le DHCP REQUEST doit utiliser les mêmes valeurs dans l'en-tête du champ 'secs' du message DHCP et être envoyé à la même adresse IP de diffusion que le message DHCP DISCOVER original. Le client clôture à la fin d'un délai d'attente et retransmet le message DHCP DISCOVER si le client ne reçoit pas de messages DHCP OFFER.

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client (pas encore définie car le serveur doit confirmer ce choix)
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	0.0.0.0	Adresse IP de l'agent DHCP
yiaddr	0.0.0.0	Adresse IP proposée par le serveur DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	0.0.0.0
Adresse IP de destination	255.255.255.255
Adresse MAC source	ex : 00 11 2F 50 66 A1 (adresse MAC du client)
Adresse MAC de destination	ex : 00 0F 66 C8 A1 38 (adresse MAC du serveur DHCP)
Au niveau UDP	Port source 68, port de destination 67

Nous retrouvons un champ d'options reprises dans le protocole RFC 2132 et nous nous limiterons aux options les plus courantes. Dans le champ d'options, nous retrouverons :

DHCP option 53	DHCP Request
DHCP option 50	Adresse demandée. Ex : 192.168.1.100

4. Les serveurs reçoivent les diffusions DHCP REQUEST des clients. Les serveurs qui ne sont pas sélectionnés par le message DHCP REQUEST utilisent le message comme notification que le client décline leur offre. Le serveur sélectionné dans le message DHCP REQUEST engage une liaison pour le client dans sa mémoire permanente et répond avec un message DHCP ACK qui contient la configuration pour le client demandeur. La combinaison entre 'identifiant client' ou 'chaddr' et l'adresse réseau assignée constitue un identifiant unique pour le bail du client et sont utilisés à la fois par le client et le serveur pour identifier un bail auquel il sera fait référence dans tous les messages DHCP. N'importe quel paramètre de configuration dans le message DHCP ACK ne devrait pas produire de conflit avec ceux du précédent message DHCP OFFER auquel le client répond. Le serveur ne devrait pas vérifier l'adresse réseau offerte à ce stade. Le 'yiaddr' du DHCP ACK est rempli avec l'adresse réseau sélectionnée.

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client
siaddr	0.0.0.0	Adresse IP du serveur DHCP

giaddr	0.0.0.0	Adresse IP de l'agent DHCP
yiaddr	192.168.1.100	Adresse IP proposée par le serveur DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	192.168.1.2 (adresse IP du serveur DHCP)
Adresse IP de destination	255.255.255.255 (adresse pas encore connue du client)
Adresse MAC source	ex : 00 0F 66 C8 A1 38 (adresse MAC du serveur DHCP)
Adresse MAC de destination	ex : 00 11 2F 50 66 A1 (adresse MAC du client)
Au niveau UDP	Port source 67, port de destination 68

Si le serveur sélectionné est indisponible pour satisfaire au message DHCPREQUEST (par ex : l'adresse réseau demandée a été allouée), le serveur devrait répondre par un message DHCPNAK.

Un serveur peut choisir de marquer comme indisponibles les adresses offertes aux clients dans un message DHCPOFFER. Le serveur devrait marquer comme disponible une adresse offerte à un client dans un message DHCPOFFER si le serveur ne reçoit pas de message DHCPREQUEST de ce client.

5. Le client reçoit un message DHCPACK avec les paramètres de configuration. Le client devrait faire une vérification finale sur les paramètres (par ex : ARP pour l'allocation de l'adresse réseau), et noter la durée du bail spécifié dans le DHCPACK. A ce moment, le client est configuré. Si le client détecte que l'adresse est déjà utilisée (par ex : via l'utilisation de ARP) le client doit envoyer un DHCPDECLINE au serveur et relancer le processus de configuration. Le client devrait attendre un minimum de dix seconde avant de relancer la configuration pour éviter un trafic réseau excessif dans le cas d'un bouclage.

Nous retrouvons un champ d'options reprises dans le protocole RFC 2132 et nous nous limiterons aux options les plus courantes. Dans le champ d'options, nous retrouverons :

DHCP option 53	DHCP ACK
DHCP option 1	Masque de sous réseau. Ex : 255.255.255.0
DHCP option 3	Routeur par défaut. Ex : 192.168.1.1
DHCP option 51	Durée de location de l'adresse IP. Ex : 1 jour
DHCP option 54	Adresse du serveur DHCP. Ex : 192.168.1.2

Si le client reçoit un DHCPNACK, le client relance le processus de configuration.

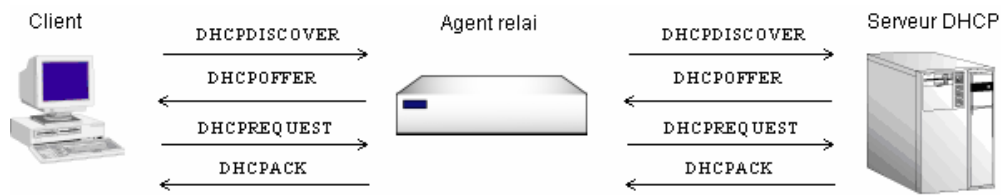
Le client clôture à la fin d'un délai d'attente et retransmet le message DHCPREQUEST si le client ne reçoit ni DHCPACK ni DHCPNACK. Le client retransmet le DHCPREQUEST conformément à l'algorithme de retransmission de la section 4.1. Le client devrait choisir de retransmettre le DHCPREQUEST suffisamment de fois pour espérer contacter le serveur sans faire en sorte que le client (et l'utilisateur du client) n'attende trop longtemps avant d'abandonner; par ex : un client retransmettant comme décrit dans la section 4.1 pourrait retransmettre le DHCPREQUEST 4 fois sur un total de 60 seconds, avant de relancer la procédure d'initialisation. Si le client ne reçoit ni DHCPACK ni DHCPNAK après l'utilisation de l'algorithme de retransmission, il retourne à l'état INIT et relance le processus d'initialisation. Le client DEVRAIT notifier à l'utilisateur que le processus d'initialisation n'a pas abouti et qu'il est relancé.

6. Le client peut choisir de renoncer au bail sur une adresse réseau en envoyant un DHCPRELEASE au serveur. Le client identifie le bail qu'il libère avec son 'identifiant client' ou 'chaddr' et l'adresse réseau dans le message DHCPRELEASE. Si le client utilise un 'identifiant client' quand il obtient le bail il DOIT utiliser le même 'identifiant client' dans le message DHCPRELEASE.

### ***1.3. Agent de relai BOOTP.***

Lorsqu'un réseau est composé de plusieurs segments séparés par des routeurs ou des switchs, ceux-ci ne sont pas configurés pour laisser passer des paquets de diffusion qui doivent rester local au segment dans lequel ils sont

généérés. Cela peut nous obliger à utiliser plusieurs serveurs DHCP, un par segment ce qui augment le coût et la maintenance. Nous pouvons envisager aussi de prévoir au niveau des routeurs des agents de relai BOOTP dont le seul rôle sera de faire passer les paquets de diffusion de type DHCP.



Nous reprendrons uniquement le cas de figure ou le client n'a pas encore reçu de bail pour une adresse IP comme évoqué au paragraphe 1.2. L'agent relai doit pouvoir accepter tout paquet de diffusion utilisant les ports 67 et 68 du protocole de transport UDP. Nous mettrons en évidence l'utilisation du champ 'giaddr'. Les différentes adresses MAC et adresses IP seront les suivantes :

Rôle	Adresse matérielle	Adresse IP
Client	00 11 2F 50 66 A1	Sur le segment 192.168.2.0/24
Agent relai DHCP	00 10 DB 57 DA 26	192.168.2.100/24
Serveur DHCP	00 0F 66 C8 A1 38	192.168.1.2/24

1. Le client diffuse un message DHCPDISCOVER sur son réseau local physique. L'agent relai va intercepter ce paquet de diffusion sur son port 68 et le rediriger par son port 67 vers le serveur DHCP. A ce niveau, l'accès au serveur DHCP ne se fera plus par diffusion mais directement vers l'adresse du serveur connue de l'agent relai.

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client (uniquement si le client a déjà une adresse)
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	192.168.2.100	Adresse IP de l'agent DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	192.168.2.100
Adresse IP de destination	192.168.1.2
Adresse MAC source	00 10 DB 57 DA 26 (celle de l'agent)
Adresse MAC de destination	00 0F 66 C8 A1 38 (celle du serveur)

2. A ce stade, il n'est pas possible que plusieurs serveurs puissent répondre à la demande puisque l'agent relai a transmis le paquet vers un seul serveur. Celui-ci pourra donc transmettre une offre, non pas directement vers le client mais vers l'agent relai dont il connaît l'adresse MAC. Il est à noter que le serveur DHCP retrouve l'adresse IP de l'agent relai au travers du champ 'giaddr' et qu'il peut donc attribuer une adresse dans le bon pool à savoir dans notre cas 192.168.2.0/24. Ce serveur, dans notre exemple, se situe sur le segment 192.168.1.0/24 et peut donc disposer d'un deuxième pool d'adresse qui serait 192.168.1.0/24.

Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	0.0.0.0	Adresse IP de l'agent DHCP
yiaddr	192.168.2.10	Adresse IP proposée par le serveur DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	192.168.1.2 (adresse IP du serveur DHCP)
Adresse IP de destination	255.255.255.255 (adresse pas encore connue du client)
Adresse MAC source	00 0F 66 C8 A1 38 (adresse MAC du serveur DHCP)
Adresse MAC de destination	00 10 DB 57 DA 26 (adresse MAC de l'agent relai)

3. L'agent relai va donc maintenant rediriger ce paquet vers le client qui n'a pas encore d'adresse. Cette redirection va donc devoir s'effectuer via une diffusion et nous retrouverons donc les paquets suivants :

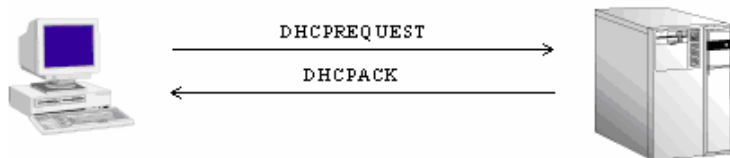
Nom du champ	Valeur	Description
xid	Nombre aléatoire	Nombre aléatoire généré par le client
ciaddr	0.0.0.0	Adresse IP du client
siaddr	0.0.0.0	Adresse IP du serveur DHCP
giaddr	0.0.0.0	Adresse IP de l'agent DHCP
yiaddr	192.168.2.10	Adresse IP proposée par le serveur DHCP
chaddr	00 11 2F 50 66 A1	Adresse matérielle du client

Au niveau UDP, IP et ARP, nous retrouverons les informations suivantes :

Adresse IP source	192.168.2.100 (adresse IP de l'agent DHCP)
Adresse IP de destination	255.255.255.255 (adresse pas encore connue du client)
Adresse MAC source	00 10 DB 57 DA 26 (adresse MAC de l'agent relai)
Adresse MAC de destination	FF FF FF FF FF FF (adresse MAC de diffusion)

De manière similaire, nous retrouverons les étapes 4 et 5 à savoir le paquet DHCPREQUEST et DHCPACK.

#### ***1.4. Réutilisation d'une adresse réseau anciennement attribuée.***



Si un client se souvient et souhaite réutiliser une adresse réseau anciennement attribuée, il peut choisir d'omettre les étapes décrites précédemment. Le diagramme montre la relation dans une interaction classique client - serveur pour un client réutilisant une adresse réseau anciennement attribuée.

1. Le client diffuse un message DHCPREQUEST sur son sous - réseau local. Le message inclut l'adresse réseau du client dans l'option 'adresse IP demandée' (option 50). Comme le client n'a pas encore reçu son adresse réseau, il ne doit pas remplir le champ 'ciaddr'. Les agents de relais BOOTP transmettent le message au serveur DHCP qui n'est pas sur le même sous réseau. Si le client utilise un 'identifiant client' pour obtenir son adresse, le client doit utiliser le même 'identifiant client' dans le message DHCPREQUEST.

2. Les serveurs qui connaissent les paramètres de configuration du client répondent avec un DHCPACK au client. Les serveurs ne devraient pas vérifier que l'adresse réseau du client est déjà utilisée; le client peut répondre à une demande d'écho ICMP à cet instant.

Si la requête du client est invalide (par ex : le client a changé de sous réseau), les serveurs devraient répondre par un message DHCPNAK au client. Les serveurs ne devraient pas répondre si l'exactitude de leurs informations n'est pas garantie. Par exemple, un serveur qui identifie une requête pour une affectation périmée qui est détenue par un autre serveur ne devrait pas répondre avec un DHCPNAK à moins que les serveurs n'utilisent un mécanisme explicite pour maintenir une cohérence entre les serveurs.

Si 'giaddr' est 0x0 dans le message DHCPREQUEST, le client est sur le même sous réseau que le serveur. Le serveur DOIT diffuser le message DHCPNAK à l'adresse de diffusion 0xffffffff parce que le client peut ne pas

avoir d'adresse réseau correcte ou le bon masque de sous réseau, et le client ne peut pas répondre à une requête ARP. De plus, le serveur DOIT envoyer le message DHCPNAK à l'adresse de l'agent de relais BOOTP, comme enregistré dans le 'giaddr'. L'agent de relais pourra, en retour, faire suivre le message directement, à l'adresse matérielle du client, de manière à ce que le DHCPNAK puisse être délivré même si le client s'est déplacé vers un nouveau réseau.

3. Le client reçoit le message DHCPACK avec les paramètres de configuration. Le client effectue une vérification finale sur les paramètres, et note la durée du bail spécifiée dans l'identifiant client ou 'chaddr' et l'adresse réseau. A ce stade, le client est configuré.

Si le client détecte que l'adresse IP dans le message DHCPACK est déjà utilisée, le client DOIT envoyer un message DHCPDECLINE au serveur et relancer le processus de configuration en faisant la requête d'une nouvelle adresse réseau. L'action correspond à un déplacement du client vers l'état INIT dans le diagramme DHCP.

Si le client reçoit un message DHCPNAK, il ne peut réutiliser l'adresse dont il se souvient. Il doit faire la requête d'une nouvelle adresse en relançant le processus de configuration, cette fois en utilisant la procédure (non abrégée). Le client clôture à la fin d'un délai d'attente et retransmet le message DHCPREQUEST si le client ne reçoit ni un DHCPACK ni un DHCPNAK. Le client retransmet le DHCPREQUEST en accord avec l'algorithme de retransmission précédemment abordé. Le client devrait choisir de retransmettre le DHCPREQUEST suffisamment de fois pour espérer contacter le serveur sans faire en sorte que le client (et l'utilisateur du client) n'attende trop longtemps avant d'abandonner; par ex : un client pourrait retransmettre le DHCPREQUEST 4 fois sur un total de 60 secondes, avant de relancer la procédure d'initialisation. Si le client ne reçoit ni DHCPACK ni DHCPNAK après avoir employé l'algorithme de retransmission, le client peut choisir d'utiliser une adresse réseau alloué précédemment et les paramètres de configurations pour les baux non expirés. Ceci correspond à un déplacement vers l'état AFFECTÉ.

4. Le client peut choisir de renoncer à son bail sur une adresse réseau en envoyant un message DHCPRELEASE au serveur. Le client identifie le bail dont il veut se défaire avec l'identifiant client ou 'chaddr' et l'adresse réseau dans le message DHCPRELEASE.

Notez que dans ce cas, le client retient son adresse réseau localement, normalement le client ne renonce pas à son bail lors d'un arrêt normal. Uniquement dans le cas où le client doit explicitement renoncer à son bail, par ex : le client va être déplacé sur un autre sous réseau, le client enverra un message DHCPRELEASE.

## ***1.5. Interprétation et représentation des valeurs de temps***

Un client acquiert un bail pour une adresse réseau pour une période fixe (qui peut être infinie). Dans ce protocole, l'unité de temps est la seconde. La valeur temps 0xffffffff est réservée pour infini. Comme un client et un serveur n'ont pas forcément une horloge synchronisée et pour être interprété correctement par les horloges des clients locaux, le temps est représenté dans les messages par des données relatives. Le temps relatif, représenté en secondes dans un mot de 32 bit non signé, donne une plage de temps relatif de 0 à environ 100 ans, ce qui est suffisant pour les temps mesurés dans DHCP.

## ***1.6. Obtenir des paramètres avec des adresses réseau déjà configurées.***

Si un client a obtenu une adresse réseau grâce à d'autres moyens (par ex. configuration manuelle) il peut utiliser une requête DHCPINFORM pour obtenir d'autres paramètres locaux de configuration. Les serveurs recevant un message DHCPINFORM construisent un message DHCPACK avec n'importe quels paramètres de configuration appropriés pour le client sans : allouer d'adresse, vérifier une liaison existante, remplir le 'yiaddr' ou inclure des durées de bail. Les serveurs devraient faire une réponse adressée DHCPACK à l'adresse donnée dans le champ 'ciaddr' du message DHCPINFORM.

Le serveur devrait vérifier l'adresse réseau dans un message DHCPINFORM, mais il ne doit pas vérifier l'existence d'un bail. Le serveur formule un message DHCPACK contenant les paramètres de configurations pour le client ayant émis la requête et envoie le message DHCPACK directement au client.

## ***1.7. Acquisition et expiration.***

Le client maintient deux temporisateurs, T1 et T2 qui spécifient les temps auxquels le client essaie d'étendre son bail sur son adresse réseau. T1 est le temps au bout duquel le client entre en état RENOUELEMENT et tente de contacter le serveur qui a émis l'adresse réseau du client. T2 est le temps au bout duquel le client entre en état REAFFECTATION et tente de contacter un serveur. T1 doit être plus récent que T2, qui doit être plus récent que la date à laquelle expire le bail.

Pour éviter le besoin d'horloge synchronisée, T1 et T2 sont exprimés dans les options comme temps relatifs.

Au temps T1 le client passe en RENOUELEMENT et envoie (par message adressé) un message DHCPREQUEST au serveur pour étendre son bail. Le client met 'ciaddr' dans le DHCPREQUEST avec sa propre adresse réseau. Le client enregistre l'heure locale à laquelle le DHCPREQUEST a été envoyé pour calculer la durée du bail. Le client ne doit pas inclure un 'identifiant serveur' dans le message DHCPREQUEST.

Tout message DHCPACK qui arrive avec un 'xid' qui ne correspond pas avec le 'xid' du DHCPREQUEST client est rejeté silencieusement. Quand le client reçoit un DHCPACK du serveur, le client calcule la durée du bail en faisant la somme du temps auquel le client envoie le message DHCPREQUEST et la durée du bail obtenu dans le message DHCPACK. Le client a fait de nouveau l'acquisition de son adresse réseau, et retourne en état AFFECTÉ et peut continuer son processus réseau.

Si aucun DHCPACK n'arrive avant T2, le client passe en REAFFECTATION et envoie (via diffusion) un message DHCPREQUEST pour étendre son bail. Le client règle le champ 'ciaddr' du DHCPREQUEST avec sa propre adresse réseau. Le client ne doit pas inclure de 'identifiant serveur' dans le message DHCP. T1 et T2 sont configurables par le serveur via les options. La valeur par défaut de T1 est  $(0.5 * \text{durée\_du\_bail})$  et celle de T2 =  $(0.875 * \text{durée\_du\_bail})$ . Les temps T1 et T2 devraient être choisis avec une petite notion de " hasard " autour de la valeur par défaut, pour éviter la synchronisation de la ré acquisition du client.

Un client PEUT choisir de renouveler ou étendre son bail sur T1. Le serveur peut choisir d'attendre le bail en accord avec la stratégie de l'administrateur réseau. Le serveur devrait retourner T1 et T2 et leurs valeurs devraient être ajustées à partir de leurs valeurs d'origine pour prendre en compte le temps de bail restant.

Que ce soit en RENOUELEMENT ou en REAFFECTATION si le client ne reçoit pas de réponse à son message DHCPREQUEST, le client devrait attendre la moitié du temps restant avant T2 (pour RENOUELEMENT) et la moitié du temps de bail restant (pour REAFFECTATION), jusqu'à un minimum de 60 secondes, avant de retransmettre le message DHCPREQUEST.

Si le bail expire avant que le client ne reçoive un DHCPACK, le client passe en état INIT, il doit alors immédiatement stopper tout processus réseau et nécessite une initialisation des paramètres réseau comme si le client n'était pas initialisé. Si le client reçoit alors un DHCPACK allouant la précédente adresse réseau du client il devrait continuer son processus réseau. Si le client obtient une nouvelle adresse réseau, il ne doit pas continuer à utiliser l'adresse préalable et devrait avertir l'utilisateur local du problème.

## ***1.8. Installation et configuration d'un serveur sous Linux.***