

Groupe de travail sur les réseaux
Requête pour Commentaires : 2131
 Remplace : RFC 1541
 Catégorie : Standard

R. Droms
 Bucknell University
 mars 1997

Spécification du protocole de configuration dynamique d'hôte (DHCP)

Statut de ce document

Ce document spécifie un protocole standard d'Internet pour la communauté Internet, et ne sera éprouvé qu'après plusieurs discussions et suggestions. Merci de vous référer à l'édition courante des "Normes des protocoles officiels de l'Internet" (STD1) pour l'état de standardisation et le statut de ce protocole. La distribution de ce document est illimitée.

La présente RFC a depuis été mise à jour par les [RFC3396](#), [RFC4361](#), [RFC5494](#), [RFC6842](#)

Résumé

DHCP fournit un cadre de travail pour transférer des informations de configuration à des hôtes sur un réseau TCP/IP. DHCP est basé sur le protocole d'amorçage BOOTP [RFC0951], en y ajoutant la possibilité d'allocation automatique d'adresses réseaux réutilisables, ainsi que de nouvelles options de configuration [DYNPROT]. DHCP capture le comportement d'agents de relais BOOTP [RFC0951], [RFC1542] et les participants DHCP peuvent interagir avec des participants BOOTP [RFC1534].

Table des Matières

1. Introduction.....	2
1.1 Changements par rapport à la RFC1541.....	2
1.2 Travaux connexes.....	2
1.3 Définitions des problèmes et solutions.....	3
1.4 Exigences.....	3
1.5 Terminologie.....	4
1.6 But du projet.....	4
2. Résumé du protocole.....	5
2.1 Configuration des paramètres.....	7
2.2 Allocation dynamique des adresses réseau.....	7
3. Le protocole client - serveur.....	7
3.1 L'interaction client - serveur - allocation d'une adresse réseau.....	8
3.2 Interaction client serveur - Réutilisation d'une adresse réseau antérieurement attribuée.....	10
3.3 Interprétation et représentation des valeurs de temps.....	12
3.4 Obtenir des paramètres avec des adresses réseau configurées en externe.....	12
3.5 Paramètres client dans DHCP.....	12
3.6 Utilisation de DHCP chez des clients à plusieurs interfaces.....	13
3.7 Quand un client doit-il utiliser DHCP ?.....	13
4. Spécification du protocole client - serveur.....	13
4.1 Construire et envoyer des messages DHCP.....	13
4.2 Contrôles administratifs de serveur DHCP.....	15
4.3 Comportement du serveur DHCP.....	15
4.4 Comportement du client DHCP.....	19
5. Remerciements.....	23
6. Références.....	23
7. Considérations pour la sécurité.....	24
8. Adresse de l'auteur.....	24
A. Paramètres de configuration d'hôte.....	25

1. Introduction

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

DHCP est bâti sur le modèle client - serveur, où l'hôte désigné serveur DHCP alloue des adresses réseaux et délivre des paramètres de configuration à des hôtes configurés dynamiquement. Dans la suite de ce document, le terme "serveur" se réfère à un hôte fournissant des paramètres d'initialisation au travers du DHCP, et le terme "client" se réfère à un hôte qui demande des paramètres d'initialisation au serveur DHCP.

Un hôte ne devrait pas agir en tant que serveur DHCP à moins qu'il ne soit configuré à cela par l'administrateur du système. La diversité des mises en œuvre du matériel et des protocoles sur l'Internet conduirait à un manque de fiabilité au niveau des opérations si n'importe quel hôte était autorisé à répondre aux requêtes DHCP. Par exemple, IP nécessite le paramétrage de nombreux paramètres à l'intérieur du logiciel qui met en œuvre le protocole. Parce que IP peut être utilisé sur un grand nombre de matériels réseaux dissemblables, les valeurs par défaut de ces paramètres ne peuvent être devinées ou supposées avoir des valeurs par défaut correctes. De même, les schémas de distribution d'adresses reposent sur un mécanisme d'élection/défense pour la découverte des adresses déjà utilisées. Les hôtes IP ne peuvent pas toujours défendre leurs adresses réseaux, de sorte qu'un tel schéma réparti d'allocation d'adresses ne peut pas garantir qu'il évitera la duplication d'allocation des adresses.

DHCP supporte trois mécanismes pour l'allocation des adresses IP. Dans l'allocation automatique, DHCP assigne une adresse IP permanente à un client. Dans l'allocation dynamique, DHCP assigne une adresse IP à un client pour une durée déterminée (ou jusqu'à ce que le client renonce explicitement à son adresse). Dans l'allocation manuelle, une adresse IP d'un client 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 le seul des trois mécanismes qui permette la réutilisation automatiquement d'une adresse qui n'est plus nécessaire au client à qui elle a été attribuée. Donc, l'allocation dynamique est particulièrement utile pour assigner une adresse à un client qui ne se connectera au réseau que de manière temporaire, ou pour partager un réservoir limité d'adresses IP entre un groupe de clients qui ne nécessitent pas une adresse permanente. L'allocation dynamique peut aussi être 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 des hôtes 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.

Le format des messages DHCP est fondé sur le format des messages BOOTP, pour capturer le comportement de l'agent de relais BOOTP comme décrit dans la spécification BOOTP [RFC0951], [RFC1542] et pour autoriser l'interopérabilité des clients BOOTP existants avec les serveurs DHCP. L'utilisation des agents de relais BOOTP élimine la nécessité d'avoir un serveur DHCP sur chaque segment physique du réseau.

1.1 Changements par rapport à la RFC1541

Ce document met à jour la spécification du protocole DHCP donnée dans la [RFC1541]. Un nouveau type de message, DHCPINFORM, a été ajouté ; voir les paragraphes 3.4, 4.3 et 4.4 pour les détails. Le mécanisme de classement pour l'identification des clients DHCP aux serveurs DHCP a été étendu pour inclure les classes "fournisseurs" comme défini aux paragraphes 4.2 et 4.3. La restriction du temps de bail minimum a été enlevée. Enfin, de nombreux changements rédactionnels ont été faits pour clarifier le texte et sont le résultat d'expériences réussies dans des essais d'interopérabilité du DHCP.

1.2 Travaux connexes

Il y a plusieurs protocoles et mécanismes Internet liés qui s'adressent à quelques éléments du problème de la configuration dynamique d'hôte. Le protocole de résolution inverse d'adresse (RARP, *Reverse Address Resolution Protocol*) [RFC0903] (au travers des extensions définies dans le RARP dynamique (DRARP) [RFC1931]) s'adresse explicitement au problème de la découverte d'adresse réseau, et inclut un mécanisme d'attribution automatique d'adresse IP. Le protocole de transfert de fichiers

simplifié (TFTP, *Trivial File Transfer Protocol*) [RFC0783] pourvoit au transport d'une image d'amorce à partir d'un serveur d'amorçage. Le protocole de message de contrôle Internet (ICMP, *Internet Control Message Protocol*) [RFC0792] pourvoit à l'information des hôtes de la présence de routeurs supplémentaires via les messages "ICMP redirect". ICMP peut aussi fournir des informations sur le gabarit de sous réseau au travers du message "Demande de gabarit ICMP" et d'autres informations au travers du message (obsolète) "demande d'informations ICMP". Les hôtes peuvent localiser les routeurs au travers du mécanisme de découverte de routeur ICMP [RFC1256].

BOOTP est un mécanisme de transport pour une collection d'informations de configuration. BOOTP est également extensible, et les extensions officielles [RFC1497] ont été définies pour plusieurs paramètres de configuration. Morgan a proposé des extensions à BOOTP pour l'allocation dynamique d'adresses IP [DYNAM]. Le protocole d'informations réseau (NIP, *Network Information Protocol*) utilisé par le projet Athena au MIT, est un mécanisme réparti pour l'allocation dynamique d'adresses IP [DYNPROT]. Le protocole de localisation de ressource (RLP, *Ressource Location Protocol*) [RFC0887] pourvoit à la localisation des services de haut niveaux. Les stations sans disque de Sun Microsystems utilisent une procédure d'amorce qui emploie RARP, TFTP et un mécanisme RPC appelé "bootparams" pour délivrer les informations de configuration et le code du système d'exploitation aux hôtes sans disque, (Sun Micro Systems, Sun Workstation et SunOs sont des marques déposées de Sun Microsystems, Inc.) Quelques réseaux Sun utilisent aussi DRARP et un mécanisme d'auto-installation pour automatiser la configuration de nouveaux hôtes dans un réseau existant.

Dans d'autres travaux liés, l'algorithme de découverte de l'unité de transmission maximum (MTU, *Maximum Transmission Unit*) peut déterminer la MTU d'un chemin Internet arbitraire [RFC1191]. Le protocole de résolution d'adresse (ARP) a été proposé comme protocole de transport pour la localisation et la sélection de ressources [UAIDS]. Enfin, Les RFC des exigences pour les hôtes [RFC1122], [RFC1123] mentionnent les exigences spécifiques de la reconfiguration d'un hôte et suggèrent un scénario pour la configuration initiale d'un hôte sans disque.

1.3 Définitions des problèmes et solutions

DHCP est défini pour fournir aux clients DHCP les paramètres de configuration définis dans les RFC sur les exigences pour les hôtes. Après avoir obtenu les paramètres via DHCP, un client DHCP devrait être en mesure d'échanger des paquets avec n'importe quel autre hôte sur Internet. Les paramètres de la pile TCP/IP fournis par DHCP figurent à l'Appendice A.

Tout ces paramètres ne sont pas requis pour un client nouvellement initialisé. Un client et un serveur peuvent négocier la transmission des seuls paramètres demandés par le client ou spécifiques d'un certain sous réseau.

DHCP permet, mais n'exige pas, la configuration des paramètres client qui ne sont pas directement liés au protocole IP. DHCP ne s'occupe pas non plus de l'enregistrement des clients nouvellement configurés auprès du service des noms de domaine (DNS) [RFC1034], [RFC1035].

DHCP n'est pas destiné à la configuration des routeurs.

1.4 Exigences

Tout au long de ce document, les mots qui sont utilisés pour définir la signification d'exigences particulières seront mis en majuscules. Ces mots sont :

- o "DOIT" : Ce mot ou l'adjectif "OBLIGATOIRE" signifie que l'élément est une nécessité absolue de cette spécification.
- o "NE DOIT PAS" : Cette phrase signifie que l'élément est absolument prohibé par cette spécification.
- o "DEVRAIT" : Ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer cet élément, mais les implications complètes devront être comprises et le cas soigneusement étudié avant de choisir un chemin différent.
- o "NE DEVRAIT PAS" : Cette phrase signifie qu'il peut exister des raisons valides dans des circonstances particulières quand le comportement de l'élément est acceptable ou même utile, mais les implications complètes devront être comprises et le cas soigneusement étudié avant de mettre en œuvre un comportement décrit avec cette étiquette.
- o "PEUT" : Ce mot ou l'adjectif "OPTIONNEL" signifie que cet élément est vraiment optionnel. Par exemple, un distributeur peut choisir d'inclure l'élément parce qu'un marché particulier l'exige ou parce qu'il améliore le produit; un autre distributeur peut omettre le même élément.

1.5 Terminologie

Ce document utilise les termes suivants :

- o "client DHCP" : Un client DHCP est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration tels qu'une adresse réseau.
- o "serveur DHCP" : Un serveur DHCP est un hôte Internet qui retourne des paramètres de configuration à un client DHCP.
- o "agent de relais BOOTP" : Un agent de relais BOOTP ou agent de relais est un hôte ou routeur Internet qui transmet des messages DHCP entre clients et serveurs DHCP. DHCP est conçu pour utiliser le même comportement d'agent de relais que spécifié dans la spécification du protocole BOOTP.
- o "lien" : Un lien est une collection de paramètres de configuration, incluant au moins une adresse IP, associée ou liée à un client DHCP. Les liens sont gérées par les serveurs DHCP.

1.6 But du projet

La liste suivante donne les objectifs de conception générale de DHCP.

- o DHCP devrait être un mécanisme plutôt qu'une stratégie. DHCP doit permettre à l'administrateur système de contrôler les paramètres de configuration là où ils sont désirés, par exemple l'administrateur d'un système local devrait être capable de mettre en application la politique locale concernant les allocations et l'accès aux ressources locales là où elles sont désirées.
- o Les clients ne devraient pas exiger de configurations manuelles. Chaque client devrait être capable de découvrir les paramètres de configuration locaux appropriés sans l'intervention de l'utilisateur et d'incorporer ces paramètres dans sa propre configuration.
- o Les réseaux ne devraient pas exiger de configuration manuelle pour les clients individuels. Dans des circonstances normales, le gestionnaire de réseau ne devrait pas à avoir à entrer les paramètres de configuration pour chaque client.
- o DHCP ne devrait pas exiger un serveur sur chaque sous réseau. Pour permettre une meilleure adaptabilité et économie, DHCP doit fonctionner au travers des routeurs ou via l'intervention des agents de relais BOOTP.
- o Un client DHCP doit être prêt à recevoir plusieurs réponses à une demande de paramètres de configuration. Quelques installations peuvent inclure plusieurs serveurs DHCP se chevauchant pour améliorer la fiabilité et augmenter les performances.
- o DHCP doit coexister avec des hôtes à configuration statique et non participants ainsi qu'avec les mises en œuvre de protocole réseau déjà en place.
- o DHCP doit interagir avec le comportement d'agent de relais BOOTP comme décrit dans les [RFC0951] et [RFC1542].
- o DHCP doit fournir un service aux clients BOOTP existants.

La liste suivante donne les objectifs de conception spécifiques de la transmission des paramètres de couche réseau. DHCP doit :

- o Garantir que toute adresse réseau spécifique ne sera pas utilisée par plusieurs clients DHCP en même temps.
- o Conserver la configuration d'un client DHCP malgré un redémarrage du client DHCP. Un client DHCP devrait, chaque fois que possible, se voir assigner les mêmes paramètres de configuration (par exemple: une adresse réseau) en réponse à chaque demande.
- o Conserver la configuration d'un client DHCP au travers des redémarrages du serveur, et chaque fois que possible, un client DHCP devrait se voir assigner les mêmes paramètres de configuration malgré les redémarrages du mécanisme DHCP,
- o Permettre une attribution automatique de paramètres de configuration aux nouveaux clients pour éviter la configuration manuelle de ces nouveaux clients,

DHCP définit une nouvelle option 'identifiant client' qui est utilisée pour transmettre un identifiant client explicite à un serveur DHCP. Ce changement élimine la surcharge du champ 'chaddr' dans les messages BOOTP, où 'chaddr' est utilisé à la fois comme adresse de matériel pour la transmission des messages de réponse BOOTP et comme identifiant client. L'identifiant client est une clé opaque, qui n'est pas à interpréter par le serveur ; par exemple, l'identifiant client peut contenir une adresse de matériel, identique au contenu du champ 'chaddr', ou bien il peut contenir un autre type d'identifiant, comme un nom DNS. L'identifiant client, choisit par un client DHCP, DOIT être propre à ce client à l'intérieur du sous réseau auquel il est rattaché. Si le client utilise un 'identifiant client' dans un message, il DOIT utiliser le même identifiant dans tous les messages suivants, pour garantir que le serveur identifie correctement le client. DHCP précise l'interprétation du champ 'siaddr' comme étant l'adresse du serveur à utiliser dans l'étape suivante du processus de démarrage du client. Un serveur DHCP peut retourner sa propre adresse dans le champ 'siaddr', si le serveur est prêt à fournir le prochain service de démarrage (par exemple, la livraison d'une image exécutable par le système d'exploitation). Un serveur DHCP retourne toujours sa propre adresse dans l'option 'identifiant serveur'.

Champ	Octets	Description
op	1	Code opération du message / type du message. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Type d'adresse de matériel, voir la section ARP dans la RFC "Numéros alloués" ; par ex., '1' = Ethernet 10Mb.
hlen	1	Longueur de l'adresse du matériel (par exemple, '6' pour Ethernet 10Mb).
bonds	1	Mis à zéro par le client, utilisé de manière optionnelle par les agents de relais quand on démarre via un agent de relais
xid	4	Identifiant de transaction, un nombre aléatoire choisi par le client, utilisé par le client et le serveur pour associer les messages et les réponses entre un client et un serveur
secondes	2	Rempli par le client, les secondes écoulées depuis le début du processus d'acquisition ou de renouvellement d'adresse
fanions	2	Fanions (voir figure 2).
ciaddr	4	Adresse IP du client, rempli seulement si le client est dans un état AFFECTÉ, RENOUELEMENT ou RÉAFFECTATION et peut répondre aux demandes ARP
yiaddr	4	'votre' adresse IP (de client).
siaddr	4	Adresse IP du prochain serveur à utiliser pour le démarrage ; retournée par le serveur dans DHCP OFFER et DHCPACK.
giaddr	4	Adresse IP de l'agent de relais, utilisée pour démarrer via un agent de relais.
chaddr	16	Adresse du matériel du client.
sname	64	Nom d'hôte facultatif du serveur, chaîne terminée par des zéros.
fichier	128	Nom du fichier de démarrage, chaîne terminée par des zéros ; nom "générique" ou nul dans DHCPDISCOVER, nom pleinement qualifié du chemin du répertoire dans DHCP OFFER.
options	var	Champ des paramètres facultatifs. Voir les documents d'options pour une liste des options définies.

Tableau 1 : Description des champs dans un message DHCP

Le champ 'options' est maintenant de longueur variable. Un client DHCP doit être prêt à recevoir des messages DHCP avec un champ 'options' d'au moins 312 octets. Cette exigence implique qu'un client DHCP doit être prêt à recevoir un message jusqu'à 576 octets, taille minimum de datagramme IP qu'un hôte IP doit être prêt à accepter [RFC1122]. Les clients DHCP peuvent négocier l'utilisation de messages DHCP plus grands à l'aide de l'option 'taille maximum de message DHCP'. Le champ Options peut être étendu d'avantage dans les champs 'fichier' et 'sname'.

Dans le cas où un client utilise DHCP pour une configuration initiale (avant que le logiciel TCP/IP du client n'ait été complètement configuré), DHCP nécessite une utilisation créative des logiciels TCP/IP du client et une interprétation libérale de la [RFC1122]. Le logiciel TCP/IP DEVRAIT accepter et faire suivre à la couche IP tout paquet IP délivré à l'adresse de matériel du client avant que l'adresse IP ne soit configurée ; les serveurs DHCP et les agents de relais BOOTP peuvent n'être pas capables de livrer des messages DHCP aux clients qui ne peuvent pas accepter les datagrammes en envoi individuel à l'adresse du matériel avant que le logiciel TCP/IP ne soit configuré.

Pour travailler avec des clients qui ne peuvent pas accepter les datagrammes IP en envoi individuel avant que le logiciel TCP/IP soit configuré comme mentionné dans le paragraphe ci-dessus, DHCP utilise le champ 'fanions' [RFC1542]. Le bit le plus à gauche est défini comme le fanion diffusion (B, *Broadcast*). La sémantique de ce fanion est exposée au paragraphe 4.1 de ce document. Les bits restants de ce fanion sont réservés pour utilisation ultérieure. Ils DOIVENT être mis à zéro par les clients et ignorés par les serveurs et les agents de relais. La figure 2 donne le format du champ 'fanions'

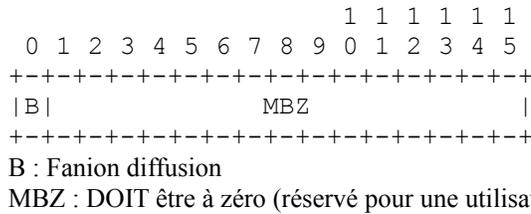


Figure 2: Format du champ 'fanions'

2.1 Configuration des paramètres

Le premier service assuré par DHCP est de fournir un espace de mémorisation persistante des paramètres réseau pour les clients du réseau. Le modèle DHCP de mémorisation persistante est que le service DHCP conserve une entrée de valeur de clé pour chaque client, et cette clé est un identifiant univoque (par exemple un numéro de sous réseau IP et un identifiant unique au sein du sous réseau) et la valeur contient les paramètres de configuration du client.

Par exemple, la clé peut être la paire (numéro du sous réseau IP, adresse du matériel) (noter que l'adresse du matériel devrait être caractérisée par le type du matériel pour faire face aux possibles duplications d'adresses de matériel résultant d'un problème de réarrangement des bits dans un réseau ponté comportant des supports mixtes) permettant une réutilisation à la suite ou concurrente d'une adresse de matériel sur des sous réseaux différents, et à des adresses de matériel qui peuvent n'être pas uniques au monde. Autrement, la clé peut être la paire (numéro de sous réseau IP, nom d'hôte) permettant au serveur d'assigner des paramètres de manière intelligente à un client DHCP qui a été déplacé sur un sous réseau différent ou qui a changé d'adresse de matériel (peut-être parce que l'interface réseau a été remplacée à cause d'une défaillance). Le protocole définit que la clé sera (numéro de sous réseau IP, adresse de matériel) sauf si le client fournit explicitement un identifiant utilisant l'option 'identifiant client'. Un client peut interroger le service DHCP pour récupérer ses paramètres de configuration. L'interface client avec le dépôt des paramètres de configuration consiste en des messages de protocole pour demander les paramètres de configuration et en des réponses du serveur qui portent les paramètres de configuration.

2.2 Allocation dynamique des adresses réseau

Le second service fourni par DHCP est l'allocation d'adresses réseau (IP) temporaires ou permanentes aux clients. Le mécanisme de base pour l'allocation dynamique d'adresses réseau est simple : un client demande l'utilisation d'une adresse pour une certaine période. Le mécanisme d'allocation (la collection des serveurs DHCP) garantit de ne pas réallouer l'adresse pendant le temps demandé et tente de retourner la même adresse réseau à chaque client qui en fait la demande. Dans ce document, la période pendant laquelle une adresse réseau est allouée à un client est nommée "bail" [LEASES]. Le client peut étendre ce bail avec des requêtes. Le client peut émettre un message pour libérer l'adresse quand il ne l'utilise plus. Le client peut demander une allocation permanente en demandant un bail permanent, un serveur peut choisir de donner un bail très long mais pas infini pour permettre la détection qu'un client s'est retiré du réseau.

Dans certains environnements il sera nécessaire de réallouer des adresses réseau du fait de l'épuisement des adresses disponibles. Dans un tel cas le mécanisme d'allocation réutilisera les adresses dont le bail aura expiré. Le serveur devrait utiliser toute information disponible dans le répertoire des informations de configuration pour choisir une adresse à réutiliser. Par exemple, le serveur peut utiliser l'adresse allouée le moins récemment. Comme contrôle de cohérence, le serveur allocataire DEVRAIT vérifier l'adresse réutilisée avant d'allouer l'adresse, par exemple, par une demande d'écho ICMP, et le client DEVRAIT vérifier la nouvelle adresse reçue, par exemple, avec ARP.

3. Le protocole client - serveur

DHCP utilise les messages BOOTP définis dans la [RFC0951] et donnés dans le tableau 1 et la figure 1. Le champ 'op' de chaque message DHCP envoyé par un client à un serveur contient BOOTREQUEST. BOOTREPLY est utilisé dans le champ 'op' de chaque message DHCP d'un serveur à un client. Les quatre premiers octets du champ 'options' d'un message DHCP contiennent les valeurs (en décimal) 99, 130, 83 et 99, (il s'agit du même cookie magique que celui défini dans la [RFC1497]). Le reste du champ 'options' consiste en une liste de paramètres étiquetés qui sont appelés "options". Toutes les "extensions fournisseur" listées dans la RFC1497 sont aussi des options DHCP. La RFC1533 donne la liste complète des options utilisables dans DHCP.

Plusieurs options ont déjà été définies. Une option particulière - l'option "type de message DHCP" doit être incluse dans chaque message DHCP. Cette option définit le "type" du message DHCP. Des options supplémentaires peuvent être permises, requises ou non permises, selon le type du message DHCP.

Dans tout ce document, les messages DHCP qui contiennent une option 'Type de message DHCP' seront désignées par ce type de message ; par exemple, un message DHCP avec une option 'type de message DHCP' de 1 sera considéré comme un message DHCPDISCOVER.

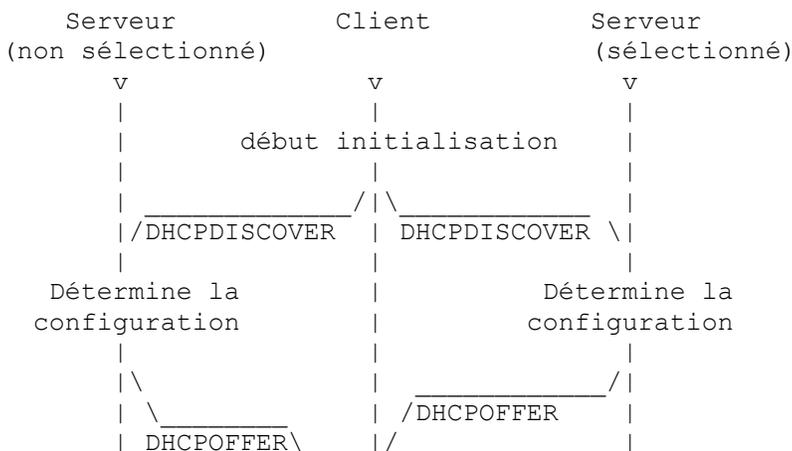
3.1 L'interaction client - serveur - allocation d'une adresse réseau

Le résumé suivant des échanges de protocole entre clients et serveurs se réfère aux messages DHCP décrits dans le tableau 2. Le diagramme temporel de la figure 3 montre les relations temporelles dans une interaction normale entre un client et un serveur. Si le client connaît déjà son adresse, certaines étapes peuvent être omises ; cette interaction réduite est décrite au paragraphe 3.2

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.
2. Chaque serveur peut répondre avec un message DHCPOFFER 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 fonctionne 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 exemple, le serveur devrait vérifier les adresses offertes par une demande d'écho ICMP. Les serveurs DEVRAIENT être mis en œuvre de manière à ce que les administrateurs réseaux puissent choisir de désactiver les vérifications d'adresses nouvellement allouées. Le serveur transmet un message DHCPOFFER au client, en utilisant l'agent de relais BOOTP si nécessaire.

Message	Utilisation
DHCPDISCOVER	Diffusion du client pour localiser les serveurs disponibles
DHCPOFFER	Du serveur au client pour répondre au DHCPDISCOVER avec les paramètres de configuration.
DHCPREQUEST	Message client aux serveurs soit (a) qui demande les paramètres à un serveur et décline implicitement les offres de tous les autres, (b) qui confirme la validité des adresses précédemment allouées, par exemple, un redémarrage système, ou (c) qui étend le bail sur une adresse réseau en particulier.
DHCPACK	Du serveur au client avec les paramètres de configuration et qui inclut l'adresse réseau déjà attribuée.
DHCNACK	Du serveur au client indiquant que la notion d'un client pour les adresses réseau est incorrecte. (par exemple, si un client est déplacé sur un nouveau sous réseau) ou que le bail du client a expiré.
DHCPDECLINE	Client vers serveur indiquant que l'adresse réseau est déjà utilisée.
DHCPRELEASE	Client vers serveur libérant l'adresse réseau et annulant le bail.
DHCPINFORM	Client vers serveur, demandant seulement les paramètres de configuration locaux ; le client possède déjà une adresse réseau attribuée de manière externe.

Tableau 2 : Messages DHCP



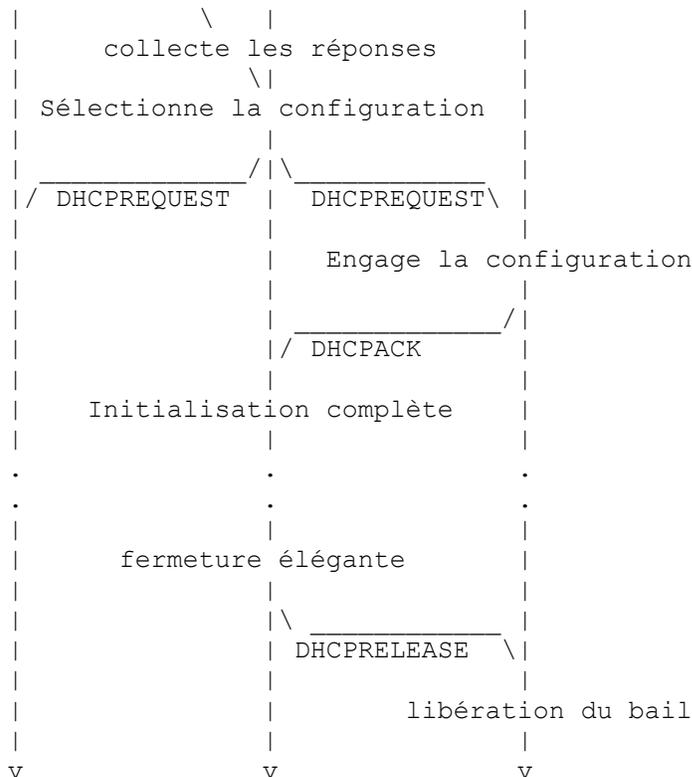


Figure 3 : diagramme temporel des messages échangés entre clients et serveurs DHCP quand on alloue une nouvelle adresse

- Le client reçoit un ou plusieurs messages DHCPPOFFER d'un ou plusieurs serveurs. Le client peut choisir d'attendre d'avoir plusieurs réponses. Le client choisit un serveur auquel demander ses paramètres de configuration, sur la base de la configuration présente dans les messages DHCPPOFFER. Le client diffuse un message DHCPREQUEST qui DOIT inclure l'option 'identifiant serveur' pour indiquer quel serveur il a choisi et qui PEUT inclure d'autres options spécifiant les valeurs de configuration désirées. L'option 'adresse IP demandée' DOIT être réglée sur la valeur de 'yiaddr' du message DHCPPOFFER provenant du serveur. Ce DHCPREQUEST est diffusé et relayé par les agents de relais DHCP/BOOTP. Pour s'assurer que tout agent de relais fait suivre le message DHCPREQUEST au même ensemble de serveurs DHCP qui a reçu le message DHCPDISCOVER original, le DHCPREQUEST DOIT utiliser la même valeur dans le champ 'secs' de l'en-tête du message DHCP et être envoyé à la même adresse IP de diffusion que le message DHCPDISCOVER original. Le client attend l'expiration du temporisateur et retransmet le message DHCPDISCOVER si il ne reçoit pas de message DHCPPOFFER.
- Les serveurs reçoivent les diffusions DHCPREQUEST des clients. Les serveurs qui ne sont pas sélectionnés par le message DHCPREQUEST utilisent le message comme notification que le client décline leur offre. Le serveur sélectionné dans le message DHCPREQUEST engage une liaison pour le client dans sa mémoire permanente et répond avec un message DHCPACK qui contient la configuration pour le client demandeur. La combinaison d'un 'identifiant client' ou 'chaddr' et de l'adresse réseau allouée constitue un identifiant univoque pour le bail du client et est utilisé par à la fois le client et le serveur pour identifier un bail auquel il sera fait référence dans tous les messages DHCP. Aucun paramètre de configuration dans le message DHCPACK NE DEVRAIT produire de conflit avec ceux du précédent message DHCPPOFFER auquel le client répond. Le serveur NE DEVRAIT PAS vérifier à ce stade l'adresse réseau offerte. Le champ 'yiaddr' du DHCPACK est rempli avec l'adresse réseau sélectionnée.

Si le serveur sélectionné est incapable de satisfaire au message DHCPREQUEST (par exemple, 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 DHCPPOFFER. Le serveur DEVRAIT marquer comme disponible une adresse offerte à un client dans un message DHCPPOFFER si le serveur ne reçoit pas de message DHCPREQUEST de ce client.

- Le client reçoit le message DHCPACK avec les paramètres de configuration. Le client DEVRAIT faire une vérification finale sur les paramètres (par exemple, ARP pour l'allocation de l'adresse réseau) et noter la durée du bail spécifiée dans le

DHCPACK. À ce moment, le client est configuré. Si le client détecte que l'adresse est déjà utilisée (par exemple, via l'utilisation de ARP) le client DOIT envoyer un DHCPDECLINE au serveur et recommencer le processus de configuration. Le client DEVRAIT attendre un minimum de dix secondes avant de recommencer la configuration pour éviter un trafic réseau excessif dans le cas d'un bouclage.

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

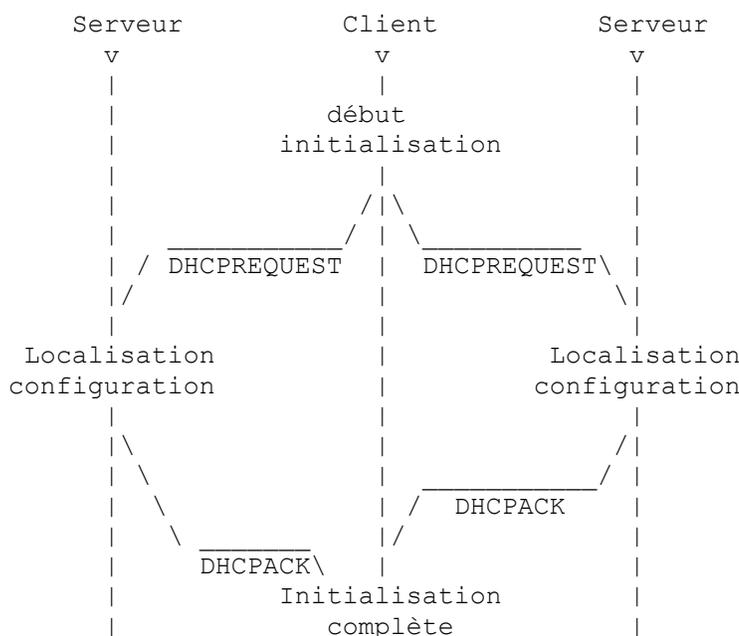
Le client arrive en fin de temporisation et retransmet le message DHCPREQUEST si le client ne reçoit ni DHCPACK ni DHCPNACK. Le client retransmet le DHCPREQUEST conformément à l'algorithme de retransmission du paragraphe 4.1. Le client devrait choisir de retransmettre le DHCPREQUEST suffisamment de fois 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 exemple, un client retransmettant comme décrit au paragraphe 4.1 pourrait retransmettre le DHCPREQUEST quatre fois sur un total de 60 secondes, avant de recommencer 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 recommence le processus d'initialisation. Le client DEVRAIT notifier à l'utilisateur que le processus d'initialisation a échoué et qu'il recommence.

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

3.2 Interaction client serveur - Réutilisation d'une adresse réseau antérieurement attribuée.

Si un client se souvient d'une adresse réseau antérieurement attribuée et souhaite la réutiliser, il peut choisir d'omettre certaines des étapes décrites au paragraphe précédent. Le diagramme temporel de la figure 4 montre la relation temporelle dans une interaction classique client - serveur pour un client réutilisant une adresse réseau antérieurement 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'. 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 aux serveurs DHCP qui ne sont pas sur le même sous réseau. Si le client a utilisé 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 au client par un DHCPACK. 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.



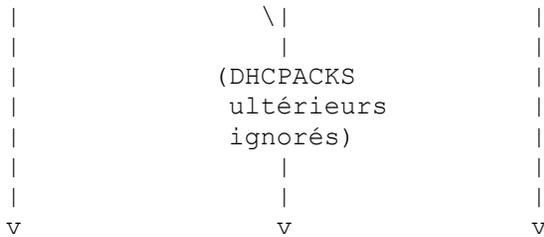


Figure 4 : Diagramme temporel des messages échangés entre le client DHCP et les serveurs quand il réutilise une adresse ayant été précédemment attribuée.

Si la requête du client est invalide (par exemple, 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 allocation 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 la cohérence entre eux.

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 gabarit de sous réseau, et le client peut ne pas répondre aux demandes ARP. Autrement, le serveur DOIT envoyer le message DHCPNAK à l'adresse IP de l'agent de relais BOOTP, comme enregistré dans le 'giaddr'. L'agent de relais va, à son tour, faire suivre le message directement à l'adresse de matériel 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 (comme au paragraphe 3.1) et note la durée du bail spécifiée dans '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 recommencer le processus de configuration en faisant la demande d'une nouvelle adresse réseau. Cette action correspond au passage du client à l'état INIT dans le diagramme d'états DHCP, décrit au paragraphe 4.4.

Si le client reçoit un message DHCPNAK, il ne peut pas réutiliser l'adresse dont il se souvient. Il doit à la place demander une nouvelle adresse en recommençant le processus de configuration, cette fois en utilisant la procédure (non abrégée) décrite au paragraphe 3.1. Cette action correspond également à un client qui passe dans l'état INIT du diagramme d'état DHCP.

Le client arrive à l'expiration du temporisateur et retransmet le message DHCPREQUEST si il ne reçoit ni un DHCPACK ni un DHCPNAK. Le client retransmet le DHCPREQUEST selon l'algorithme de retransmission du paragraphe 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 exemple, un client retransmettant comme décrit au paragraphe 4.1 pourrait retransmettre le DHCPREQUEST quatre fois sur un total de 60 secondes, avant de recommencer 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 allouée précédemment et les paramètres de configuration pour les baux non expirés. Ceci correspond à un déplacement vers l'état AFFECTÉ dans le diagramme de la figure 5.

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 à libérer par son 'identifiant client' ou 'chaddr' et l'adresse réseau dans le message DHCPRELEASE.

Noter que dans ce cas, où le client conserve son adresse réseau en local, le client ne va normalement pas renoncer à son bail durant un arrêt en douceur. C'est uniquement dans le cas où le client doit explicitement renoncer à son bail, par exemple, le client va passer sur un autre sous réseau, que le client va envoyer un message DHCPRELEASE.

3.3 Interprétation et représentation des valeurs de temps

Un client acquiert un bail pour une adresse réseau pour une période fixée (qui peut être infinie). Dans ce protocole, l'unité de temps est la seconde. La valeur temps 0xffffffff est réservée pour infini. Comme clients et serveurs n'ont pas forcément des horloges

synchronisées, les temps sont représentés dans les messages en temps relatifs, à interpréter par rapport à l'horloge locale du client. Représenter les temps relatifs en secondes dans un mot de 32 bits non signé donne une plage de temps relatif de 0 à environ 100 ans, ce qui est suffisant pour les temps relatifs mesurés dans DHCP.

L'algorithme pour l'interprétation de la durée du bail donné dans le paragraphe précédent considère que les horloges du client et du serveur sont relativement stables. Si il y a un décalage entre les deux horloges, le serveur peut considérer que le bail a expiré avant que le client ne le fasse. Pour compenser, le serveur peut retourner au client un bail d'une durée plus courte que celle assignée dans sa base de donnée locale d'informations de client.

3.4 Obtenir des paramètres avec des adresses réseau configurées en externe

Si un client a obtenu une adresse réseau grâce à d'autres moyens (par exemple, 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 tous paramètres de configuration locale appropriés pour le client sans : allouer une nouvelle adresse, vérifier une liaison existante, remplir le 'yiaddr' ou inclure des paramètres de durée de bail. Les serveurs DEVRAIENT faire une réponse DHCPACK en envoi individuel à l'adresse donnée dans le champs 'ciaddr' du message DHCPINFORM.

Le serveur DEVRAIT vérifier la cohérence de 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.

3.5 Paramètres client dans DHCP

Tous les clients ne requièrent pas l'initialisation de tous les paramètres listés dans l'appendice A. Deux techniques sont utilisées pour réduire le nombre de paramètres transmis du serveur au client. Premièrement, la plupart des paramètres ont des valeurs par défaut définies dans les RFC sur les exigences pour les hôtes, si un client ne reçoit pas d'un serveur des paramètres qui se substituent à ces valeurs par défaut, il utilise ces valeurs par défaut. Deuxièmement, dans son message initial DHCPDISCOVER ou DHCPREQUEST, un client peut fournir au serveur une liste de paramètres spécifiques qui intéressent le client. Si le client inclut une liste de paramètres dans un message DHCPDISCOVER, il DOIT inclure cette liste de paramètres dans tout message DHCPREQUEST ultérieur.

Le client DEVRAIT inclure l'option 'taille maximum des messages DHCP' pour faire savoir au serveur la taille que peuvent prendre ses messages DHCP. Les paramètres retournés à un client peuvent quand même dépasser l'espace alloué aux options dans un message DHCP. Dans ce cas, deux fanions facultatifs supplémentaires (qui doivent apparaître dans le champ 'options' du message) indiquent que les champs 'fichier' et 'sname' doivent être utilisés pour les options.

Le client peut informer le serveur des paramètres de configuration qui l'intéressent en incluant l'option 'liste des paramètres demandés'. La partie données de cette option fait la liste explicite par numéros d'étiquette des options demandés.

De plus le client peut suggérer des valeurs pour l'adresse réseau et la durée de bail dans le message DHCPDISCOVER. Le client peut inclure l'option 'Adresse IP demandée' pour suggérer qu'une adresse IP soit attribuée, et peut inclure l'option 'durée de bail de l'adresse IP' pour suggérer la durée de bail qu'il désire. D'autres options, qui sont des suggestions pour les paramètres de configuration, sont permises dans un DHCPDISCOVER ou un DHCPREQUEST. Cependant, les options supplémentaires peuvent être ignorées par les serveurs, et des serveurs différents peuvent donc ne pas retourner des valeurs identiques pour certaines options. L'option 'Adresse IP demandée' n'est à remplir dans un message DHCPREQUEST que quand le client vérifie les paramètres réseau obtenus précédemment. Le client ne remplit le champ 'ciaddr' que quand il est correctement configuré avec une adresse IP dans l'état AFFECTÉ, RENOUVELLEMENT, ou REAFFECTATION.

Si un serveur reçoit un message DHCPREQUEST avec une 'Adresse IP demandée' invalide, le serveur DEVRAIT répondre au client avec un DHCPNAK et peut choisir de rapporter le problème à l'administrateur du système. Le serveur peut inclure un message d'erreur dans l'option 'message'.

3.6 Utilisation de DHCP chez des clients à plusieurs interfaces

Un client avec des interfaces réseaux multiples doit utiliser DHCP de manière indépendante sur chacune de ses interfaces pour obtenir les paramètres d'information de configuration pour chacune de ces interfaces.

3.7 Quand un client doit-il utiliser DHCP ?

Un client DEVRAIT utiliser DHCP pour obtenir de nouveau ou vérifier son adresse IP et les paramètres réseau chaque fois que les paramètres de réseau local peuvent avoir changé ; par exemple au moment de l'amorçage du système ou après une déconnexion du réseau local, car la configuration du réseau local peut avoir changé sans que le client ou l'utilisateur en ait connaissance.

Si le client a connaissance d'une précédente adresse réseau et est incapable de contacter un serveur DHCP local, le client peut continuer d'utiliser l'adresse réseau précédente jusqu'à ce que le bail de cette adresse soit expiré. Si le bail expire avant que le client ait eu le temps de contacter le serveur DHCP, le client doit immédiatement stopper l'utilisation de l'adresse réseau et peut informer les utilisateurs locaux du problème.

4. Spécification du protocole client - serveur

Dans cette section on suppose que le serveur DHCP possède un bloc d'adresses réseau à partir desquelles il peut satisfaire les demandes de nouvelles adresses. Chaque serveur maintient également, dans un espace de stockage local permanent, une base de données des adresses allouées et des baux.

4.1 Construire et envoyer des messages DHCP

Les clients et serveurs DHCP construisent tout deux des messages DHCP en remplissant les champs de la partie de format fixe des messages et ajoutant des éléments de données étiquetés dans la zone option de longueur variable. La zone des options inclut d'abord un 'cookie magique' de quatre octets (qui a été décrit dans la section 3) suivi par les options. La dernière option doit toujours être 'end'

DHCP utilise le protocole de transport UDP. Les messages DHCP d'un client à un serveur sont envoyés à l'accès 'serveur DHCP' 67 et les messages d'un serveur à un client sont envoyés à l'accès 'client DHCP' 68. Un serveur avec plusieurs adresses réseau (par exemple, un hôte multi rattachements) PEUT utiliser n'importe laquelle de ses adresses réseau dans les messages DHCP sortants.

Le champ 'identifiant serveur' est utilisé à la fois pour identifier un serveur DHCP dans un message DHCP et comme adresse de destination des clients aux serveurs. Un serveur avec plusieurs adresses réseau DOIT être prêt à accepter que n'importe laquelle de ses adresses réseau serve d'identifiant de ce serveur dans un message DHCP. Pour s'accommoder d'une connectivité réseau potentiellement incomplète, un serveur DOIT choisir une adresse comme 'identifiant serveur' qui, à la connaissance du serveur, soit accessible à partir du client. Par exemple, si le serveur DHCP et le client DHCP sont connectés sur le même sous-réseau (c'est-à-dire, si le champ 'giaddr' dans le message du client est à zéro) le serveur DEVRAIT sélectionner l'adresse IP que le serveur utilise pour communiquer sur ce sous-réseau comme 'identifiant serveur'. Si le serveur utilise des plusieurs adresses sur ce sous-réseau, n'importe laquelle de ces adresses peut être utilisée. Si le serveur a reçu un message par un agent de relais DHCP, le serveur DEVRAIT choisir une adresse de l'interface sur laquelle il a reçu le message comme 'identifiant serveur' (à moins que le serveur n'ait de meilleures informations sur lesquelles fonder son choix). Les clients DHCP DOIVENT utiliser l'adresse IP fournie dans l'option 'identifiant serveur' pour toutes les demandes en envoi individuel au serveur DHCP.

Les messages DHCP diffusés par un client avant qu'il n'ait obtenu son adresse IP doivent avoir mis à 0 leur champ d'adresse de source de l'en-tête IP.

Si le champ 'giaddr' dans un message DHCP d'un client n'est pas à zéro, le serveur envoie tous les messages de réponse à l'accès 'serveur DHCP' de l'agent de relais BOOTP dont l'adresse apparaît dans le 'giaddr'. Si le 'giaddr' est à zéro et si le champ 'ciaddr' n'est pas à zéro, alors le serveur adresse les messages DHCPOFFER et DHCPACK en envoi individuel à l'adresse contenue dans 'ciaddr'. Si 'giaddr' est à zéro et 'ciaddr' est à zéro, et si le bit Diffusion est établi, alors le serveur diffuse les messages DHCPOFFER et DHCPACK à 0xffffffff. Si le bit Diffusion n'est pas établi, et si 'giaddr' et 'ciaddr' sont à zéro, alors le serveur adresse DHCPOFFER et DHCPACK en envoi individuel à l'adresse de matériel du client et à l'adresse 'yiaddr'. Dans tout les cas

quand 'giaddr' est à zéro, le serveur diffuse tout message DHCPNAK à 0xffffffff.

Si les options dans un message DHCP s'étendent dans les champs 'sname' et 'fichier', l'option 'surcharge d'option' DOIT apparaître dans le champ 'options' avec pour valeur 1, 2 ou 3 comme spécifié dans la RFC1533. Si l'option 'surcharge d'option' est présente dans le champ 'options', les options du champ 'options' DOIVENT se terminer par l'option 'end', et PEUVENT contenir un ou plusieurs options 'bourrage' pour remplir le champ d'options. Les options dans les champs 'sname' et 'fichier' (si utilisés comme indiqué par l'option 'surcharge d'option') DOIVENT commencer par le premier octet du champ, DOIVENT être terminées par l'option 'end', et DOIVENT être suivies par les options 'bourrage' pour remplir le reste du champ. Toute option individuelle dans les champs 'options', 'sname' et 'fichier' DOIT être entièrement contenue dans ce champ. Les options dans le champ 'options' DOIVENT être interprétées en premier, de manière à ce que toute option 'surcharge d'option' puisse être interprétée. Le champ 'fichier' DOIT être interprété ensuite (si l'option 'surcharge d'option' indique que le champ 'fichier' contient des options DHCP) suivi par le champ 'sname'.

Les valeurs à passer dans une étiquette 'option' peuvent être trop longues pour tenir sur les 255 octets disponibles pour une seule option (par exemple, une liste de routeurs dans l'option 'routeurs' [RFC1542]). Les options ne peuvent apparaître qu'une seule fois, à moins qu'il en soit spécifié autrement dans le document de définition de l'option. Le client enchaîne les valeurs de plusieurs instances de la même option dans une seule liste de paramètres pour la configuration.

Les clients DHCP sont responsables de toutes les retransmissions de messages. Le client DOIT adopter une stratégie de retransmission qui incorpore un algorithme aléatoire de retard exponentiel pour déterminer le délai entre les retransmissions. Le délai entre les retransmission DEVRAIT être choisi de manière à laisser suffisamment de temps pour que les réponses venant du serveur soient livrées sur la base des caractéristiques de l'inter-réseau entre le client et le serveur. Par exemple, dans un réseau Ethernet à 10 Mbit/s, le délai avant la première retransmission DEVRAIT être de quatre secondes modifié de manière aléatoire par la valeur d'un nombre aléatoire uniforme choisi entre -1 et +1. Les clients avec des horloges qui fournissent une granularité de résolution de moins d'une seconde peuvent choisir une valeur d'aléation non entière. Le délai avant la retransmission suivante DEVRAIT être de 8 secondes rendu aléatoire par la valeur d'un nombre uniforme choisi entre -1 et +1. Le délai de retransmission DEVRAIT être doublé pour les retransmission ultérieures jusqu'à un délai maximum de 64 secondes. Le client PEUT fournir une indication sur les tentatives de retransmission à l'utilisateur sous la forme d'un indicateur de progression du processus de configuration.

Le champ 'xid' est utilisé par le client pour associer les messages DHCP entrants avec les requêtes en cours. Un client DHCP DOIT choisir 'xid' de manière à minimiser les risques d'avoir un 'xid' identique à celui utilisé par un autre client. Par exemple, un client peut choisir un 'xid' initial aléatoire différent à chaque fois que le client redémarre, et ensuite utiliser des 'xid' en séquence jusqu'au prochain redémarrage. Choisir un nouvel 'xid' pour chaque retransmission est un choix de la mise en œuvre. Un client peut choisir de réutiliser le même 'xid' ou choisir un nouvel 'xid' pour chaque message retransmis.

Normalement les serveurs DHCP et les agents de relais BOOTP tentent de délivrer les messages DHCP OFFER, DHCPACK, et DHCPNAK directement au client en utilisant la livraison en envoi individuel. L'adresse IP de destination (dans l'en-tête IP) est réglée sur l'adresse DHCP 'yiaddr' et l'adresse de destination couche liaison est réglée sur l'adresse DHCP 'chaddr'. Malheureusement, quelques mises en œuvre de client ne sont pas capables de recevoir de tels datagrammes IP en envoi individuel tant que la mise en œuvre n'a pas été configurée avec une adresse IP valide (conduisant à un blocage dans lequel l'adresse IP du client ne peut être livrée tant que le client n'a pas été configuré avec une adresse IP).

Un client qui ne peut recevoir les datagrammes IP en envoi individuel tant que son logiciel de protocole n'a pas été configuré avec une adresse IP DEVRAIT établir le bit Diffusion dans le champ 'fanions' à 1 dans tous les messages DHCPDISCOVER ou DHCPREQUEST qu'il émet. Le bit Diffusion va fournir un indice au serveur DHCP et à l'agent de relais BOOTP pour diffuser tout message au client sur le sous-réseau du client. Un client qui peut recevoir des datagrammes IP en envoi individuel avant que son logiciel de protocole ait été configuré DEVRAIT mettre le bit diffusion à 0. Le document de clarification BOOTP expose les ramifications de l'utilisation du bit Diffusion [RFC1542].

Un serveur ou agent de relais qui envoie ou relaye un message DHCP directement à un client DHCP (c'est-à-dire, pas à un agent de relais spécifié dans le champ 'giaddr') DEVRAIT examiner le bit Diffusion dans le champ 'fanions'. Si ce bit est à un, le message DHCP DEVRAIT être envoyé comme diffusion IP en utilisant une adresse de diffusion IP (de préférence 0xffffffff) comme adresse de destination IP et l'adresse de diffusion de couche liaison comme adresse destination de couche liaison. Si le bit Diffusion est à 0, le message DEVRAIT être envoyé comme envoi individuel IP à l'adresse IP spécifiée dans le champ 'yiaddr' et à l'adresse de couche liaison spécifiée dans le champ 'chaddr'. S'il est impossible de faire un envoi individuel, le message PEUT être envoyé comme diffusion IP en utilisant l'adresse IP de diffusion (de préférence 0xffffffff) comme adresse IP de destination et l'adresse de diffusion de couche liaison comme adresse de destination de couche liaison.

4.2 Contrôles administratifs de serveur DHCP

Les serveurs DHCP ne sont pas obligés de répondre à chaque message DHCPDISCOVER et DHCPREQUEST qu'ils reçoivent. Par exemple, un administrateur réseau, pour avoir un contrôle strict sur les clients rattachés au réseau, peut choisir de configurer les serveurs DHCP pour qu'ils répondent seulement aux clients qui ont été précédemment enregistrés au travers d'un mécanisme externe. La spécification DHCP décrit seulement les interactions entre clients et serveurs quand les clients et les serveurs choisissent d'interagir ; il sort du domaine d'application de la spécification DHCP de décrire tous les contrôles administratifs que les administrateurs de systèmes peuvent vouloir utiliser. Les mises en œuvre particulières de serveur DHCP peuvent incorporer tous les contrôles ou politiques désirés par un administrateur de réseau.

Dans certains environnements, un serveur DHCP devra considérer les valeurs des options de la classe 'fournisseur' incluses dans les messages DHCPDISCOVER ou DHCPREQUEST quand il détermine les paramètres corrects pour un client particulier.

Un serveur DHCP a besoin d'utiliser des identifiants univoques pour associer un client avec son bail. Le client PEUT choisir de fournir de manière explicite l'identifiant au travers de l'option 'identifiant client'. Si le client fournit un 'identifiant client', le client DOIT utiliser le même 'identifiant client' dans tout les messages qui suivront, et le serveur DOIT utiliser cet identifiant pour identifier le client. Si le client ne propose pas l'option 'identifiant client', le serveur DOIT utiliser le contenu du champ 'chaddr' pour identifier le client. Il est crucial pour un client DHCP d'utiliser un identifiant univoque à l'intérieur d'un sous-réseau auquel il est rattaché dans l'option 'identifiant client'. L'utilisation de 'chaddr' comme identifiant univoque du client peut conduire à des résultats inattendus, car cet identifiant peut être associé à une interface matérielle qui pourrait être déplacée vers un autre client. Certains sites peuvent choisir d'utiliser le numéro de série d'un fabricant comme 'identifiant client', pour éviter des changements inattendus des adresses réseaux dus au transfert d'interfaces matérielles entre des ordinateurs. Des sites peuvent aussi choisir d'utiliser un nom DNS comme 'identifiant client', provoquant un bail d'adresse associé au nom DNS plutôt qu'à un matériel spécifique.

Les clients sont libre d'utiliser n'importe quelle stratégie de sélection d'un serveur DHCP parmi ceux dont le client reçoit le message DHCPDISCOVER. La mise en œuvre de client DHCP DEVRAIT fournir un mécanisme à l'utilisateur afin qu'il puisse sélectionner directement des valeurs de 'identifiant de classe de fournisseur'

4.3 Comportement du serveur DHCP

Un serveur DHCP traite les messages DHCP entrants provenant d'un client selon l'état courant de la liaison pour ce client. Un serveur DHCP peut recevoir les messages suivants d'un client :

- o DHCPDISCOVER
- o DHCPREQUEST
- o DHCPDECLINE
- o DHCPRELEASE
- o DHCPINFORM

Le tableau 3 donne l'utilisation par un serveur des champs et options dans un message DHCP. Le reste de cette section décrit l'action du serveur DHCP pour chaque message entrant possible.

4.3.1 Message DHCPDISCOVER

Quand un serveur reçoit un message DHCPDISCOVER d'un client, le serveur choisit une adresse réseau pour le client demandeur. Si aucune adresse n'est disponible, le serveur peut choisir de rapporter le problème à l'administrateur système. Si une adresse est disponible, la nouvelle adresse DEVRAIT être choisie comme suit :

- o L'adresse courante du client telle qu'elle a été enregistrée dans l'affectation du client, SINON
- o L'adresse précédente du client telle qu'elle a été enregistrée dans l'affectation du client (maintenant périmée ou libérée) si cette adresse est dans le réservoir d'adresses disponibles du serveur, et pas encore allouée, SINON
- o L'adresse demandée dans l'option 'adresse IP demandée' si cette adresse est valide et n'est pas déjà allouée, SINON

- o Une nouvelle adresse allouée à partir du réservoir d'adresses disponibles ; l'adresse est sélectionnée en fonction du sous réseau à partir duquel le message a été reçu (si 'giaddr' est 0) ou en fonction de l'adresse de l'agent de relais qui a transmis le message ('giaddr' quand il est différent de 0).

Comme décrit au paragraphe 4.2, un serveur PEUT, pour des raisons administratives, allouer une adresse autre que celle demandée, ou peut refuser d'allouer une adresse à un client particulier même si des adresses sont disponibles.

Noter que dans certaines architectures réseau (par exemple, des internets avec plus d'un sous réseau IP affecté à un segment physique de réseau) il peut se trouver que le client DHCP devrait se voir allouer une adresse d'un sous-réseau différent plutôt que celle enregistrée dans 'giaddr'. Donc, DHCP n'exige pas que le client se voit allouer une adresse provenant du sous-réseau indiqué dans 'giaddr'. Un serveur est libre de choisir un autre sous-réseau, et il sort du domaine d'application de la spécification DHCP de décrire les manières de choisir l'adresse IP allouée.

Bien que cela ne soit pas requis pour le bon fonctionnement de DHCP, le serveur NE DEVRAIT PAS réutiliser l'adresse réseau sélectionnée avant que le client réponde au message DHCPOFFER du serveur. Le serveur peut choisir d'enregistrer l'adresse telle qu'offerte au client.

Le serveur doit aussi choisir un délai d'expiration pour le bail, comme suit :

- o Si le client n'a pas demandé un bail spécifique dans le message DHCPDISCOVER et si le client possède déjà une adresse réseau, le serveur retourne le temps d'expiration du bail défini précédemment pour cette adresse (noter que le client doit explicitement demander un bail spécifique pour étendre le délai d'expiration sur une adresse précédemment attribuée), SINON
- o Si le client n'a pas fait la demande d'un bail spécifique dans le message DHCPDISCOVER et si le client n'a pas d'adresse réseau attribuée, le serveur alloue un temps de bail par défaut configuré localement, SINON
- o Si le client a demandé un bail spécifique dans le message DHCPDISCOVER (sans considérer si le client a une adresse réseau allouée) le serveur peut choisir soit de retourner le bail demandé (si le bail est compatible avec la politique locale) ou de sélectionner un autre bail.

Champ	DHCPOFFER	DHCPACK	DHCPNAK
'op'	BOOTREPLY	BOOTREPLY	BOOTREPLY
'htype'	(de la RFC "Numéros alloués")		
'hlen'	(longueur de l'adresse de matériel en octets)		
'hops'	0	0	0
'xid'	'xid' du message client DHCPDISCOVER	'xid' du message client DHCPREQUEST	'xid' du message client DHCPREQUEST
'secs'	0	0	0
'ciaddr'	0	'ciaddr' du DHCPREQUEST ou 0	0
'yiaddr'	adresse IP offerte au client	adresse IP assignée au client	0
'siaddr'	adresse IP du serveur d'amorçage suivant	adresse IP du serveur d'amorçage suivant	0
'fanions'	fanions du message client DHCPDISCOVER	fanions du message client DHCPREQUEST	fanions du message client DHCPREQUEST
'giaddr'	'giaddr' du message client DHCPDISCOVER	'giaddr' du message client DHCPREQUEST	'giaddr' du message client DHCPREQUEST
'chaddr'	'chaddr' du message client DHCPDISCOVER	'chaddr' du message client DHCPREQUEST	'chaddr' du message client DHCPREQUEST
'sname'	nom d'hôte serveur ou options	nom d'hôte serveur ou options	(inutilisé)
'fichier'	nom du fichier démarrage client ou options	nom du fichier démarrage client ou options	(inutilisé)
'options'	options	options	

Option	DHCPOFFER	DHCPACK	DHCPNAK
adresse IP demandée	NE DOIT PAS	NE DOIT PAS	NE DOIT PAS
Durée du bail de l'adresse IP	DOIT	DOIT (DHCPREQUEST) NE DOIT PAS (DHCPINFORM)	NE DOIT PAS
Utilisation des champs 'fichier'/'sname'	PEUT	PEUT	NE DOIT PAS

Type du message DHCP	DHCPOFFER	DHCPACK	DHCPNAK
Liste des Paramètres requis	NE DOIT PAS	NE DOIT PAS	NE DOIT PAS
Message	DEVRAIT	DEVRAIT	DEVRAIT
Identifiant client	NE DOIT PAS	NE DOIT PAS	PEUT
Identifiant de classe fournisseur	PEUT	PEUT	PEUT
Identifiant serveur	DOIT	DOIT	DOIT
Taille maximum de message	NE DOIT PAS	NE DOIT PAS	NE DOIT PAS
Toutes les autres	PEUT	PEUT	NE DOIT PAS

Tableau 3 : Champs et options utilisés par les serveurs DHCP

Une fois que l'adresse réseau et le bail ont été déterminés, le serveur construit un message DHCPOFFER avec les paramètres de configurations offerts. Il est important pour tous les serveurs DHCP qu'ils retournent les mêmes paramètres (à l'exception possible d'une adresse réseau nouvellement allouée) pour assurer que le client aura un comportement prévisible quel que soit le serveur choisi par le client. Les paramètres de configuration DOIVENT être sélectionnés en appliquant les règles dans l'ordre donné ci dessous. L'administrateur réseau est chargé de configurer plusieurs serveurs DHCP pour s'assurer de l'uniformité des réponses de ces serveurs. Le serveur DOIT retourner au client :

- o L'adresse réseau du client, comme déterminé par les règles données plus haut dans cette section,
- o Le délai d'expiration pour le bail du client, comme déterminé dans les règles données plus haut dans cette section,
- o Les paramètres requis par le client, en fonction des règles suivantes :
 - SI le serveur a été explicitement configuré avec une valeur par défaut pour le paramètre, le serveur DOIT inclure cette valeur dans une option appropriées du champ 'option', SINON
 - SI le serveur reconnaît le paramètre comme paramètre défini dans le document 'Exigences pour les hôtes', le serveur DOIT inclure la valeur par défaut pour ce paramètre comme donné dans le document 'Exigences pour les hôtes' dans une option approprié du champ 'option' SINON
 - Le serveur NE DOIT PAS retourner de valeur pour ce paramètre.

Le serveur doit fournir autant des paramètres demandés que possible et DOIT omettre tous les paramètres qu'il ne peut pas fournir. Le serveur DOIT inclure chaque paramètre requis une fois seulement à moins que cela ne soit explicitement permis dans le document définissant les options DHCP et extensions fournisseur BOOTP.

- o Tout paramètre de l'affectation existante qui diffère des valeurs par défaut du document 'Exigences pour les hôtes',
- o Tout paramètre spécifique de ce client (comme identifié par le contenu de 'chaddr' ou de 'identifiant client' dans le message DHCPDISCOVER ou DHCPREQUEST) par exemple, comme configuré par l'administrateur réseau.
- o Tous paramètres spécifique de cette classe de client (comme identifié par le contenu de l'option 'identifiant de classe de fournisseur' dans le message DHCPDISCOVER ou DHCPREQUEST) par exemple, comme configuré par l'administrateur réseau ; les paramètres DOIVENT être identifiés par une correspondance exacte entre l'identifiant de 'classe de fournisseur' du client et les classes clients identifiées par le serveur,
- o Les paramètres avec des valeurs qui ne sont pas celles par défaut sur le sous-réseau du client.

Le serveur PEUT choisir de retourner le 'identifiant de classe de fournisseur' utilisé pour déterminer les paramètres dans le message DHCPOFFER pour assister le client dans son choix du DHCPDISCOVER qu'il va accepter. Le serveur insère le champ 'xid' du message DHCPDISCOVER dans le champ 'xid' du message DHCPOFFER et envoie le message DHCPOFFER au client demandeur.

4.3.2 Message DHCPREQUEST

Un message DHCPREQUEST peut venir d'un client répondant à un message DHCPOFFER du serveur, d'un client vérifiant une adresse IP précédemment allouée ou d'un client qui rallonge le bail sur une adresse réseau. Si le message DHCPREQUEST contient une option 'identifiant serveur' le message est la réponse à un DHCPOFFER. Sinon, le message est une demande pour vérifier ou étendre un bail existant. Si le client utilise un 'identifiant client' dans un message DHCPREQUEST, il DOIT utiliser le même 'identifiant client' dans tous les messages suivants. Si le client inclut une liste de paramètres requis dans un message DHCPDISCOVER, il DOIT inclure cette liste dans tous les messages suivants.

Aucun paramètre de configuration dans le message DHCPACK NE DEVRAIT créer de conflit avec ceux définis précédemment

dans le message DHCPPOFFER auquel le client répond. Le client DEVRAIT utiliser les paramètres du message DHCPACK pour la configuration.

Les clients envoient les messages DHCPREQUEST comme suit :

- o DHCPREQUEST généré durant l'état SELECTION :
 Les clients insèrent l'adresse du serveur choisit dans 'identifiant serveur', 'ciaddr' DOIT être à 0, 'Adresse IP demandée' DOIT être rempli avec la valeur de 'yiaddr' du DHCPPOFFER choisi.
 Noter que le client peut choisir de collecter plusieurs DHCPPOFFER et choisir la meilleure offre. Le client indique sa sélection en identifiant le serveur offreur dans le message DHCPREQUEST. Si le client ne reçoit aucune offre acceptable, il peut choisir d'essayer un autre message DHCPPOFFER. Donc, les serveurs peuvent ne pas recevoir de DHCPREQUEST spécifique à partir duquel ils peuvent décider si le client a ou non accepté l'offre. Parce que les serveurs ne se sont engagé sur aucune allocation d'adresse réseau sur la base d'un DHCPPOFFER, les serveurs sont libres de réutiliser les adresses réseau offertes en réponse à des demandes ultérieures. En tant que détail de mise en œuvre, les serveurs NE DEVRAIENT PAS réutiliser les adresses offertes et pourraient utiliser un mécanisme de temporisation spécifique de la mise en œuvre, pour décider quand réutiliser une adresse offerte.
- o DHCPREQUEST généré pendant l'état INIT-REBOOT :
 'identifiant serveur' NE DOIT PAS être rempli, l'option 'adresse IP demandée' DOIT être remplie avec l'adresse client précédemment assignée. 'ciaddr' doit être à 0. Le client cherche à vérifier une adresse précédemment allouée, une configuration en antémémoire. Le serveur DEVRAIT envoyer un message DHCPNAK au client si l'adresse IP demandée est incorrecte, ou est sur un mauvais réseau.
 La détermination de si un client, dans l'état INIT-REBOOT, est sur le bon réseau est faite grâce à l'examen du 'giaddr', de l'option 'adresse IP demandée' et une recherche dans la base de données. Si le serveur DHCP détecte que le client est sur le mauvais réseau (c'est-à-dire, le résultat de l'application du gabarit de sous-réseau local ou d'un gabarit de sous-réseau distant (si 'giadr' n'est pas zéro) sur la valeur de l'option 'adresse IP demandée' ne correspond pas à la réalité) alors le serveur DEVRAIT envoyer un message DHCPNAK au client.
 Si le réseau est correct, alors le serveur DHCP devrait vérifier si la notion qu'a le client de son adresse IP est correcte. Sinon, le serveur POURRAIT alors envoyer un message DHCPNAK au client. Si le serveur DHCP n'a pas de trace de ce client, il DOIT alors rester silencieux, et PEUT produire un avertissement à l'administrateur réseau. Ce comportement est nécessaire pour la coexistence pacifique de serveurs DHCP non communicants sur le même réseau.
 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 la bonne adresse réseau ou le bon gabarit de sous-réseau, et le client peut ne pas répondre aux requêtes ARP.
 Si 'giaddr' est établi dans le message DHCPREQUEST, le client est sur un sous-réseau différent. Le serveur DOIT établir le bit Diffusion dans le DHCPNAK, afin que les agents de relais diffusent le DHCPNAK au client, parce que le client peut ne pas avoir une adresse réseau ou un gabarit de sous-réseau correct, et le client peut ne pas répondre aux requêtes ARP.
- o DHCPREQUEST généré pendant l'état RENOUVELLEMENT :
 'identifiant serveur' NE DOIT PAS être rempli, 'adresse IP demandée' NE DOIT PAS être rempli, 'ciaddr' DOIT être rempli avec l'adresse IP du client. Dans cette situation, le client est complètement configuré et essaie d'étendre son bail. Ce message sera en envoi individuel, donc aucun agent de relais ne sera impliqué dans sa transmission. Parce que 'giaddr' n'est pas rempli, le serveur DHCP fera confiance à la valeur 'ciaddr' et l'utilisera quand il répondra à ce client.
 Un client peut choisir de renouveler ou étendre son bail jusqu'à l'expiration de T1. Le serveur peut choisir de ne pas étendre le bail (c'est une décision de politique de l'administrateur réseau), mais devrait quand même retourner un message DHCPACK.
- o DHCPREQUEST généré pendant l'état REAFFECTATION :
 'identifiant serveur' NE DOIT PAS être rempli, 'adresse IP demandée' NE DOIT PAS être rempli, 'ciadr' DOIT être rempli par l'adresse IP du client. Dans cette situation, le client est complètement configuré et essaie d'étendre son bail. Ce message DOIT être diffusé à l'adresse de diffusion IP 0xffffffff. Le serveur DHCP DEVRAIT vérifier que 'ciaddr' est correct avant de répondre au DHCPREQUEST.
 Le DHCPREQUEST d'un client en REAFFECTATION est destiné à satisfaire les sites qui possèdent plusieurs serveurs DHCP et un mécanisme pour maintenir une certaine cohérence entre les différents baux gérés par les divers serveurs. Un serveur DHCP ne PEUT étendre le bail d'un client que si il a l'autorisation administrative locale de le faire.

4.3.3 Message DHCPDECLINE

Si le serveur reçoit un message DHCPDECLINE, le client a découvert par d'autres moyens que l'adresse réseau suggérée est déjà

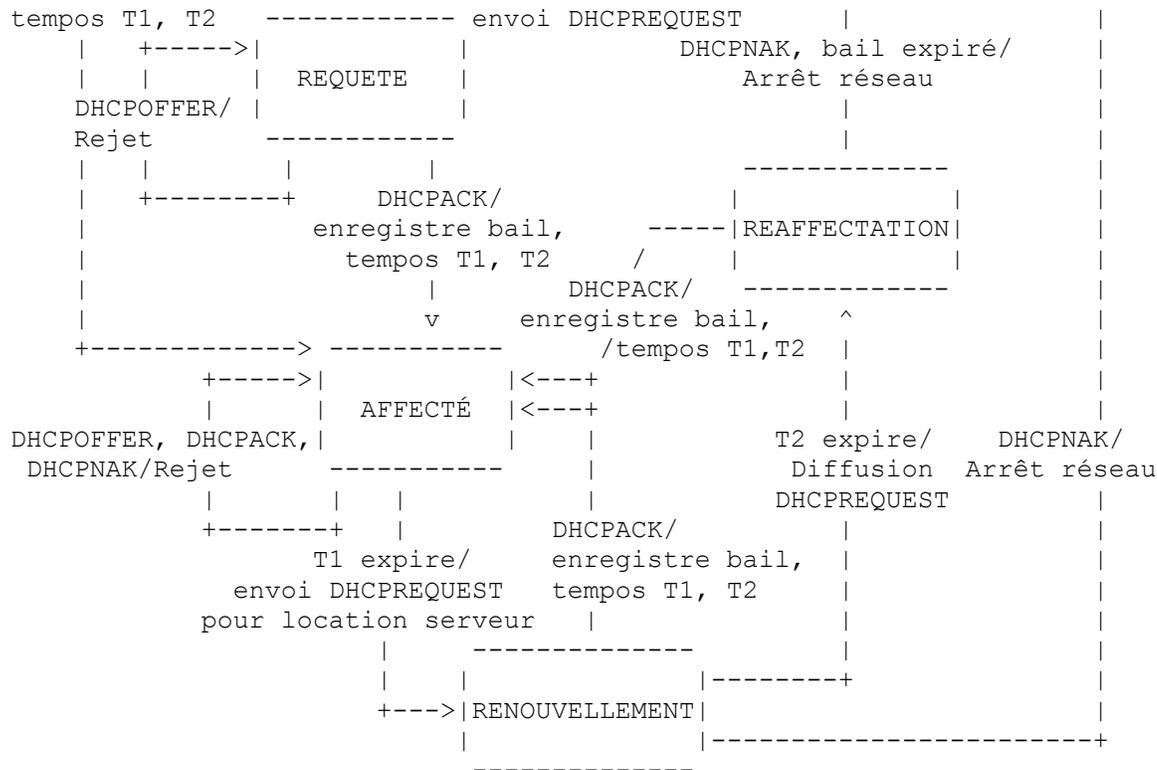


Figure 5 : Diagramme des transitions d'état pour les clients DHCP

4.4.1 Initialisation et allocation des adresses réseau

Le client commence par un état INIT et formule un message DHCPDISCOVER. Le client DEVRAIT attendre une durée aléatoire comprise entre une et dix secondes pour désynchroniser l'utilisation du DHCP au lancement. Le client règle 'ciaddr' sur 0x00000000. Le client PEUT demander des paramètres spécifiques en incluant l'option 'liste des paramètres demandés'. Le client PEUT suggérer une adresse réseau et/ou une durée de bail en incluant les options 'adresse IP demandée' et 'durée du bail de l'adresse IP'. Le client DOIT inclure son adresse de matériel dans le champ 'chaddr' si elle est nécessaire pour la livraison des réponses au message DHCP. Le client PEUT inclure un identifiant univoque différent dans l'option 'identifiant client' comme vu au paragraphe 4.2. Si le client a inclure une liste des paramètres demandés dans un message DHCPDISCOVER, il DOIT inclure cette liste dans tous les messages suivants.

Le client génère et enregistre un identifiant de transaction aléatoire et insère cet identifiant dans le champ 'xid'. Le client enregistre sa propre heure locale pour calculer ultérieurement l'expiration de son bail. Le client diffuse ensuite le DHCPDISCOVER sur l'adresse de diffusion du matériel à l'adresse IP de diffusion 0xffffffff et à l'accès UDP du serveur DHCP.

Si le 'xid' d'un message DHCPOFFER entrant ne correspond pas au 'xid' du plus récent message DHCPDISCOVER reçu, le DHCPOFFER doit être rejeté en silence. Tout message DHCPACK entrant doit être éliminé en silence.

Le client collecte les messages DHCPOFFER sur une période de temps, choisit un message DHCPOFFER parmi les (éventuellement plusieurs) messages DHCPOFFER entrants (par exemple, le premier DHCPOFFER arrivant ou celui du serveur précédemment utilisé) et extrait l'adresse du serveur de l'option 'identifiant serveur' du message DHCPOFFER. Le temps pendant lequel le client collecte les messages et le mécanisme utilisé pour choisir un DHCPOFFER dépendent de la mise en œuvre.

Champ	DHCPDISCOVER DHCPINFORM	DHCPREQUEST	DHCPDECLINE, DHCPRELEASE
'op'	BOOTREQUEST	BOOTREQUEST	BOOTREQUEST
'htype'	(De la RFC "Numéros alloués")		
'hlen'	(Longueur de l'adresse du matériel en octets)		
'hops'	0	0	0
'xid'	choisi par le client	'xid' du message DHCPOFFER du serveur	choisi par le client
'secs'	0 ou secondes depuis le début du processus DHCP	0 ou secondes depuis le début du processus DHCP	0

'fanions'	Fanion 'BROADCAST' établi si le client demande une réponse diffusée	Fanion 'BROADCAST' établi si le client demande une réponse diffusée	0
'ciaddr'	0 (DHCPDISCOVER) adresse réseau du client (DHCPINFORM)	0 ou adresse réseau du client (BOUND/RENEW/REBIND)	0 (DHCPDECLINE) adresse réseau du client (DHCPRELEASE)
'yiaddr'	0	0	0
'siaddr'	0	0	0
'giaddr'	0	0	0
'chaddr'	adresse du matériel du client	adresse du matériel du client	adresse du matériel du client
'sname'	options, si indiqué dans l'option 'sname/fichier' sinon inutilisé	options, si indiqué dans l'option 'sname/fichier' sinon inutilisé	(inutilisé)
'fichier'	options, si indiqué dans option 'sname/fichier' sinon inutilisé	options, si indiqué dans option 'sname/fichier' sinon inutilisé	(inutilisé)
'options'	options	options	(inutilisé)

Option	DHCPDISCOVER DHCPINFORM	DHCPREQUEST	DHCPDECLINE, DHCPRELEASE
Adresse IP demandée	PEUT (DISCOVER) NE DOIT PAS (INFORM)	DOIT (dans SELECTION ou INIT-REBOOT) NE DOIT PAS (dans AFFECTATION ou RENOUELEMENT)	DOIT (DHCPDECLINE) NE DOIT PAS (DHCPRELEASE)
Durée du bail IP	PEUT (DISCOVER) NE DOIT PAS (INFORM)	PEUT	NE DOIT PAS
Utilisation des champs 'fichier'/'sname'	PEUT DHCPDISCOVER/ DHCPINFORM	PEUT DHCPREQUEST	PEUT DHCPDECLINE/ DHCPRELEASE
Identifiant client	PEUT	PEUT	PEUT
Identifiant classe fournisseur	PEUT	PEUT	NE DOIT PAS
Identifiant serveur	NE DOIT PAS	DOIT (après SELECTION) NE DOIT PAS (après INIT-REBOOT, AFFECTÉ, RENOUELEMENT ou REAFFECTATION)	DOIT
Liste des paramètres requis	PEUT	PEUT	NE DOIT PAS
Taille maximum des messages	PEUT	PEUT	NE DOIT PAS
Message	NE DEVRAIT PAS	NE DEVRAIT PAS	DEVRAIT
Spécifique du site	PEUT	PEUT	NE DOIT PAS
Toutes les autres	PEUT	PEUT	NE DOIT PAS

Tableau 5 : Champs et options utilisés par les clients DHCP

Si les paramètres sont acceptables, le client enregistre l'adresse du serveur qui a fourni les paramètres à partir du champ 'identifiant serveur' et envoie cette adresse dans le champ 'identifiant serveur' d'un message diffusé DHCPREQUEST. Une fois qu'arrive le message DHCPACK d'un serveur, le client est initialisé et passe à l'état AFFECTÉ. Le message DHCPREQUEST contient le même 'xid' que le message DHCPPOFFER. Le client enregistre le délai d'expiration du bail comme étant la somme de l'heure à laquelle la demande originale a été envoyée et la durée du bail à partir du message DHCPACK. Le client DEVRAIT faire une vérification sur l'adresse suggérée pour s'assurer que l'adresse n'est pas déjà utilisée. Par exemple, si le client est sur un réseau qui prend en charge l'ARP, il peut émettre une demande ARP pour l'adresse suggérée. Quand on diffuse une demande ARP pour l'adresse suggérée, le client doit mettre sa propre adresse de matériel comme adresse de matériel de l'envoyeur, et 0 pour l'adresse IP de l'envoyeur, pour éviter la confusion chez les antémémoires ARP des autres hôtes sur le même sous-réseau. Si l'adresse réseau semble être utilisée, le client DOIT envoyer un message DHCPDECLINE au serveur. Le client DEVRAIT diffuser une réponse ARP pour annoncer la nouvelle adresse IP du client et vider toutes les entrées de l'antémémoire ARP périmées chez les hôtes de son sous-réseau.

4.4.2 Initialisation avec une adresse réseau connue

Le client commence dans l'état INIT-REBOOT et envoie un message DHCPREQUEST. Le client DOIT insérer son adresse réseau connue comme option 'adresse IP demandée' dans le message DHCPREQUEST. Le client peut demander des paramètres de configurations spécifiques en incluant l'option 'liste des paramètres demandés'. Le client génère et enregistre un identifiant de

transaction aléatoire et insère cet identifiant dans le champ 'xid'. Le client enregistre sa propre heure locale pour le calcul ultérieur de l'expiration du bail. Le client NE DOIT PAS inclure un 'identifiant serveur' dans le message DHCPREQUEST. Le client diffuse ensuite le DHCPREQUEST sur l'adresse de diffusion de matériel local à l'accès UDP 'serveur DHCP'.

Une fois qu'arrive d'un serveur quelconque un message DHCPACK avec un champ 'xid' correspondant à celui du message DHCPREQUEST du client, le client est initialisé et passe à l'état AFFECTÉ. Le client enregistre l'heure d'expiration du bail comme étant la somme de l'heure à laquelle le message DHCPREQUEST a été envoyé et de la durée du bail tirée du message DHCPACK.

4.4.3 Initialisation avec une adresse réseau allouée en externe

Le client envoie un message DHCPINFORM. Le client peut demander des paramètres de configuration spécifiques en incluant l'option 'liste des paramètres demandés'. Le client génère et enregistre un identifiant de transaction aléatoire et insère cet identifiant dans le champ 'xid'. Le client place sa propre adresse réseau dans le champ 'ciaddr'. Le client NE DEVRAIT PAS demander de paramètres de durée de bail.

Le client envoie alors le message DHCPINFORM en envoi individuel au serveur DHCP si il connaît l'adresse du serveur ; autrement il diffuse le message à l'adresse de diffusion limitée (toute de 1). Les messages DHCPINFORM DOIVENT être dirigés sur l'accès UDP 'serveur DHCP'.

Une fois qu'arrive de n'importe quel serveur un message DHCPACK avec un champ 'xid' correspondant à celui du message DHCPINFORM du client, le client est initialisé.

Si le client ne reçoit pas un DHCPACK dans un délai raisonnable (60 secondes ou 4 essais si on utilise la temporisation définie au paragraphe 4.1) il DEVRAIT alors afficher un message informant l'utilisateur du problème, et DEVRAIT ensuite commencer un processus réseau en utilisant des valeurs par défaut convenables selon l'Appendice A.

4.4.4 Utilisation de la diffusion et de l'envoi individuel

Le client DHCP diffuse les message DHCPDISCOVER, DHCPREQUEST et DHCPINFORM, à moins que le client ne connaisse l'adresse d'un serveur DHCP. Le client adresse les messages DHCPRELEASE en envoi individuel au serveur. Parce que le client décline l'utilisation de l'adresse IP fournie par le serveur, le client diffuse les messages DHCPDECLINE.

Quand le client DHCP connaît l'adresse d'un serveur DHCP, dans l'état INIT ou REBOOT, le client peut utiliser cette adresse dans le DHCPDISCOVER ou DHCPREQUEST plutôt que l'adresse IP de diffusion. Le client peut aussi utiliser l'envoi individuel pour envoyer des messages DHCPINFORM à un serveur DHCP connu. Si le client ne reçoit aucune réponse aux messages DHCP envoyés à l'adresse IP d'un serveur DHCP connu, le client DHCP revient à l'utilisation de l'adresse IP de diffusion.

4.4.5 Réacquisition et expiration

Le client entretient 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 dans l'état RENOUVELLEMENT et tente de contacter le serveur qui a produit à l'origine l'adresse réseau du client. T2 est le temps au bout duquel le client entre dans l'état REAFFECTATION et tente de contacter un serveur. T1 DOIT être plus tôt que T2, qui doit à son tour être plus tôt que l'heure à laquelle expire le bail.

Pour éviter le besoin d'horloges synchronisées, T1 et T2 sont exprimés dans les options comme des temps relatifs [RFC1533].

Au temps T1 le client passe à l'état RENOUVELLEMENT et envoie (en envoi individuel) un message DHCPREQUEST au serveur pour étendre son bail. Le client règle le champ 'ciaddr' dans le DHCPREQUEST avec son adresse réseau actuelle. Le client enregistre l'heure locale à laquelle le message DHCPREQUEST a été envoyé pour calculer l'heure de fin du bail. Le client NE DOIT PAS inclure un 'identifiant de serveur' dans le message DHCPREQUEST.

Tout message DHCPACK qui arrive avec un 'xid' qui ne correspond pas au 'xid' du message DHCPREQUEST du client est rejeté en silence. Quand le client reçoit un DHCPACK du serveur, le client calcule l'heure d'expiration du bail en faisant la somme de l'heure à laquelle le client a envoyé le message DHCPREQUEST et de la durée du bail dans le message DHCPACK. Le client réussit à acquérir de nouveau son adresse réseau, et retourne à l'état AFFECTÉ et peut continuer son processus réseau.

Si aucun DHCPACK n'arrive avant l'heure T2, le client passe à l'état REAFFECTATION et envoie (via diffusion) un message DHCPREQUEST pour étendre son bail. Le client règle le champ 'ciaddr' dans le DHCPREQUEST à son adresse réseau actuelle. Le client NE DOIT PAS inclure un 'identifiant de serveur' dans le message DHCP.

Les temps 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 d'une valeur fixée, pour éviter la synchronisation de la réacquisition du client.

Un client PEUT choisir de renouveler ou étendre son bail avant T1. Le serveur PEUT choisir d'étendre le bail en accord avec la politique établie par l'administrateur du 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.

Dans les deux état RENOUVELLEMENT et REAFFECTATION, si le client ne reçoit pas de réponse à son message DHCPREQUEST, le client DEVRAIT attendre la moitié du temps restant avant T2 (dans l'état RENOUVELLEMENT) et la moitié du temps de bail restant (dans l'état REAFFECTATION) jusqu'à un minimum de 60 secondes, avant de retransmettre le message DHCPREQUEST.

Si le bail expire avant que le client reçoive un DHCPACK, le client passe à l'état INIT ; il DOIT immédiatement arrêter tout autre processus réseau et demander les paramètres d'initialisation du réseau comme si le client n'était pas initialisé. Si le client reçoit alors un DHCPACK allouant à ce client sa précédente adresse réseau, il DEVRAIT continuer son processus réseau. Si le client obtient une nouvelle adresse réseau, il NE DOIT PAS continuer à utiliser l'adresse réseau précédente et DEVRAIT avertir l'utilisateur local du problème.

4.4.6 DHCPRELEASE

Si le client n'a plus besoin d'utiliser l'adresse réseau qui lui est allouée (par exemple, le client est arrêté normalement) le client envoie un message DHCPRELEASE au serveur. Noter que le fonctionnement correct de DHCP ne dépend pas de la transmission des messages DHCPRELEASE.

5. Remerciements

L'auteur remercie les nombreux membres (trop nombreux pour être mentionnés ici) du groupe de travail 'DHC' pour leurs efforts inlassables et continus dans le développement du DHCP et de ce document.

Les efforts de J Allard, Mike Carney, Dave Lapp, Fred Lien et John Mendonca dans l'organisation des sessions d'essais d'interopérabilité du DHCP sont particulièrement reconnus.

Le développement de ce document a été en partie soutenu par des subventions du CNRI (Corporation for National Research Initiatives), de l'université Bucknell et par Sun Microsystems.

6. Références

[DYNAM] Morgan, R., "Dynamic IP Address Assignment for Ethernet Attached Hosts", *Non publiée*

[DYNPROT] Jeffrey Schiller and Mark Rosenstein. "A Protocol for the Dynamic Assignment of IP Addresses for use on an Ethernet". (Disponible auprès de Athena Project, MIT), 1989.

[LEASES] Gray C., and D. Cheriton, "Leases: An Efficient Fault-Tolerant Mechanism for Distributed File Cache Consistency", Dans le compte rendu du Twelfth ACM Symposium on Operating Systems Design, 1989.

[RFC0783] K. Sollins, "Protocole TFTP (révision 2)", juin 1981. (*Osolète, voir la RFC1350*)

[RFC0792] J. Postel, "Protocole du [message de contrôle Internet](#) – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. (*MàJ par la RFC6633*)

[RFC0887] M. Acceta, "Protocole de [localisation de ressource](#)", décembre 1983.

- [RFC0903] R. Finlayson, T. Mann, J. Mogul et M. Theimer, "Protocole de [résolution inverse d'adresse](#)", STD 38, juin 1984.
- [RFC0951] B. Croft et J. Gilmore, "[Protocole BOOTSTRAP](#) (BOOTP)", septembre 1985.
- [RFC1034] P. Mockapetris, "Noms de domaines - [Concepts et facilités](#)", STD 13, novembre 1987.
- [RFC1035] P. Mockapetris, "Noms de domaines – [Mise en œuvre](#) et spécification", STD 13, novembre 1987. (*MàJ par la RFC6604*)
- [RFC1122] R. Braden, "[Exigences pour les hôtes Internet](#) – couches de communication", STD 3, octobre 1989. (*MàJ par la RFC6633*)
- [RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – [Application et prise en charge](#)", STD 3, octobre 1989.
- [RFC1191] J. Mogul et S. Deering, "[Découverte de la MTU](#) de chemin", novembre 1990.
- [RFC1256] S. Deering, éditeur, "Messages ICMP de [découverte de routeur](#)", septembre 1991.
- [RFC1497] J. Reynolds, "Extensions Informations de fabricant BOOTP", août 1993. (*Remplacée par la RFC1533*)
- [RFC1533] S. Alexander et R. Droms, "Options DHCP et extensions de fabricant BOOTP", octobre 1993. (*Obsolète, voir 2132*)
- [RFC1534] R. Droms, "Interfonctionnement entre DHCP et BOOTP", octobre 1993. (*D.S.*)
- [RFC1542] W. Wimer, "Précisions et extensions au protocole Bootstrap", octobre 1993. (*D.S.*)
- [RFC1700] J. Reynolds et J. Postel, "[Numéros alloués](#)", STD 2, octobre 1994. (*Historique, voir www.iana.org*)
- [RFC1931] D. Brownell, "Extensions RARP dynamiques pour l'acquisition automatique d'adresse réseau", avril 1996. (*Information*)
- [UAIDS] Comer, D., and R. Droms, "Uniform Access to Internet Directory Services", Proc. of ACM SIGCOMM '90 (Numéro spécial de Computer Communications Review) 20(4):50--59, 1990.

7. Considérations pour la sécurité

DHCP est construit directement sur UDP et IP qui sont par nature peu sécurisés. De plus DHCP est généralement destiné à rendre plus aisée la maintenance des hôtes distants et/ou sans disques. Bien que peut-être pas impossible, la configuration de tels hôtes avec des mots de passe ou des clés peut être difficile voire gênante. Donc, DHCP dans sa forme actuelle est assez peu sécurisé.

Des serveurs DHCP non autorisés peuvent facilement être montés. De tels serveurs peuvent envoyer des informations fausses et potentiellement dommageables aux clients, comme des adresses IP incorrectes ou dupliquées, des informations d'acheminement incorrectes (y compris des routeurs factices, etc.) des serveurs de noms de domaine incorrects (comme des serveurs de noms factices) et autres. Clairement, une fois que ces germes d'informations sont mis en place, un attaquant peut compromettre les systèmes affectés.

Des clients DHCP malveillants peuvent se faire passer pour des clients légitimes et récupérer des informations destinées aux clients légitimes. Là où l'allocation dynamique de ressources est utilisée, un client malveillant peut demander toute les ressources pour lui-même, et ainsi dénier l'accès aux ressources aux clients légitimes.

8. Adresse de l'auteur

Ralph Droms
Computer Science Department
323 Dana Engineering
Bucknell University
Lewisburg, PA 17837

téléphone : (717) 524-1145
 mél : droms@bucknell.edu

A. Paramètres de configuration d'hôte

Paramètres de couche IP, par hôte :

Être un routeur	marche/arrêt	HRC 3.1
Acheminement de source non local	marche/arrêt	HRC 3.3.5
Filtres de politique pour acheminement de source non local	(liste)	HRC 3.3.5
Taille maximum de réassemblage	entier	HRC 3.3.2
TTL par défaut	entier	HRC 3.2.1.7
Temporisation de péremption de PMTU	entier	MTU 6.6
Tableau de lissage de MTU	(liste)	MTU 7

Paramètres de couche IP, par interface :

Adresse IP	(adresse)	HRC 3.3.1.6
Gabarit de sous-réseau	(gabarit d'adresse)	HRC 3.3.1.6
MTU	entier	HRC 3.3.3
MTU tous sous-réseaux	marche/arrêt	HRC 3.3.3
Nuance d'adresse de diffusion	0x00000000/0xffffffff	HRC 3.3.6
Effectuer la découverte de gabarit	marche/arrêt	HRC 3.2.2.9
Être un fournisseur de gabarit	marche/arrêt	HRC 3.2.2.9
Effectuer la découverte de routeur	marche/arrêt	RD 5.1
Adresse de sollicitation de routeur	(adresse)	RD 5.1
Routeurs par défaut, liste des :		
Adresse de routeur	(adresse)	HRC 3.3.1.6
Niveau de préférence	entier	HRC 3.3.1.6
Routeurs statiques, liste des :		
Destination	(host/subnet/net)	HRC 3.3.1.2
Gabarit de destination	(gabarit d'adresse)	HRC 3.3.1.2
Type de service	entier	HRC 3.3.1.2
Routeur de premier bond	(adresse)	HRC 3.3.1.2
Ignorer les redirections	marche/arrêt	HRC 3.3.1.2
PMTU	entier	MTU 6.6
Effectuer la découverte de PMTU	marche/arrêt	MTU 6.6

Paramètres de couche liaison, par interface :

En-queues	marche/arrêt	HRC 2.3.1
Temporisation d'antémémoire ARP	entier	HRC 2.3.2.1
Ethernet encapsulation	(RFC894/RFC1042)	HRC 2.3.3

TCP_parameters_per_host:

TTL	entier	HRC 4.2.2.19
Intervalle de garder-en-vie	entier	HRC 4.2.3.6
Taille des données de garder-en-vie	0/1	HRC 4.2.3.6

Clés :

MTU = Découverte de la MTU de chemin (RFC1191, Norme proposée)

RD = Découverte de routeur (RFC1256, Norme proposée)