Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8415
RFC rendues obsolètes : 3315, 3633, 3736, 4242, 7083, 7283, 7550
Catégorie : Sur la voie de la normalisation
ISSN : 2070-1721

Traduction Claude Brière de L'Isle

T. Mrugalski, ISC
M. Siodelski, ISC
B. Volz, Cisco
A. Yourtchenko, Cisco
M. Richardson, SSW
S. Jiang, Huawei
T. Lemon, Nibbhaya Consulting
T. Winters, UNH-IOL
novembre 2018

Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)

Résumé
Le présent document décrit le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) : un mécanisme extensible pour configurer les nœuds avec les paramètres de configuration du réseau, les adresses IP, et les préfixes. Les paramètres peuvent être fournis sans état, ou en combinaison avec une allocation à état plein d'une ou plusieurs adresses IPv6 et/ou préfixes IPv6. DHCPv6 peut fonctionner soit à la place, soit en plus de l'auto configuration d'adresse sans état (SLAAC, *stateless address autoconfiguration*).

Le présent document met à jour le texte de la RFC 3315 (la spécification originale de DHCPv6) et incorpore la délégation de préfixe (RFC 3633), DHCPv6 sans état (RFC 3736) une option pour spécifier une limite supérieure à la durée pendant laquelle un client devrait attendre avant de rafraîchir les informations (RFC 4242) un mécanisme pour ralentir les clients DHCPv6 quand le service DHCPv6 n'est pas disponible (RFC 7083) et le traitement par les agent de relais des messages inconnus (RFC 7283). De plus, le présent document précise les interactions entre les modèles de fonctionnement (RFC7550). À ce titre, le présent document rend obsolètes les RFC 3315, RFC 3633, RFC 3736, RFC 4242, RFC 7083, RFC 7283, et RFC 7550.

Table des matières

1. Introduction

Le présent document décrit DHCP pour IPv6 (DHCPv6) un protocole client/serveur qui traite de la gestion de la configuration des appareils. Le fonctionnement de base de DHCPv6 assure la configuration des clients connectés à la même liaison que le serveur. La fonction d'agent de relais est aussi définie pour permettre la communication entre clients et serveurs qui ne sont pas sur la même liaison.

DHCPv6 peut fournir à un appareil des adresses allouées par un serveur DHCPv6 et d'autres informations de configuration ; ces données sont portées dans des options. DHCPv6 peut être étendu par la définition de nouvelles options pour porter des informations de configuration non spécifiées dans le présent document.

DHCPv6 fournit aussi un mécanisme pour la délégation automatique de préfixes IPv6 en utilisant DHCPv6, comme spécifié à l'origine dans la [RFC3633]. Par ce mécanisme, un routeur délégant peut déléguer des préfixes aux routeurs demandeurs. L'utilisation de ce mécanisme est spécifiée au titre de la [RFC7084] et par [TR-187].

DHCP peut aussi être utilisé juste pour fournir d'autres options de configuration (c'est-à-dire, pas des adresses ou préfixes). Cela implique que le serveur n'a pas à tracer les états ; donc, ce mode est appelé "DHCPv6 sans état". Les mécanismes nécessaires à la prise en charge de DHCPv6 sans état sont bien plus réduits que les mécanismes nécessaires pour prendre en charge DHCPv6 à états pleins. La [RFC3736] a été écrite pour documenter les portions de DHCPv6 nécessaires pour la prise en charge du fonctionnement de DHCPv6 sans état.

Le reste de cette introduction résume les relations avec les précédentes normes DHCPv6 (paragraphe 1.1) et précise la position à l'égard de DHCPv4 (paragraphe 1.2). La Section 5 décrit les mécanismes d'échange de messages pour illustrer le fonctionnement de DHCP plutôt que de fournir une liste exhaustive de toutes les interactions possibles, et la Section 6 donne une vue d'ensemble des modèles de fonctionnement courants. La Section 18 explique en détails le fonctionnement du client et du serveur.

1.1 Relations avec les précédentes normes DHCPv6

La spécification DHCPv6 initiale était définie dans la [RFC3315], et un certain nombre de documents ont été publiés à la suite au fil des ans :

- [RFC3633] ("Options de préfixe IPv6 pour le protocole de configuration dynamique d'hôte (DHCP) version 6")
- [RFC3736] ("Service sans état du protocole de configuration dynamique d'hôte (DHCP) pour IPv6")
- [RFC4242] ("Option Heure de rafraîchissement d'informations pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)")
- [RFC7083] ("Modification des valeurs par défaut de SOL_MAX_RT et INF_MAX_RT")
- [RFC7283] ("Traitement des messages DHCPv6 inconnus")
- [RFC7550] ("Problèmes et recommandations avec plusieurs options DHCPv6 à états pleins")

Le présent document fournit une définition unifiée, corrigée, et nettoyée de DHCPv6 qui couvre aussi tous les errata applicables aux plus anciennes RFC (voir la liste à l'Appendice A). À ce titre, il rend obsolète les RFC dont la liste est donnée ci-dessus. Aussi, il y a quelques mécanismes qui deviennent obsolètes ; voir la Section 25 et l'Appendice A.

1.2 Relations avec DHCPv4

Les modèles de fonctionnement et les informations de configuration pertinentes pour DHCPv4 [RFC2131], [RFC2132] et DHCPv6 sont suffisamment différentes pour que l'intégration entre les deux services ne soit pas incluse dans le présent document. La [RFC3315] suggérait qu'un futur travail pourrait être d'étendre DHCPv6 à porter des adresses et informations de configuration IPv4. Cependant, le consensus actuel de l'IETF est que DHCPv4 devrait être utilisé plutôt que DHCPv6 quand on transporte des informations de configuration IPv4 aux nœud. Pour les réseaux seulement IPv6, la [RFC7341] décrit un mécanisme de transport pour porter les messages DHCPv4 en utilisant le protocole DHCPv6 pour le provisionnement dynamique des adresses et informations de configuration IPv4.

Fusionner les configuration DHCPv4 et DHCPv6 n'est pas dans le domaine d'application du présent document. La [RFC4477] discute certaines questions et les stratégies possibles pour faire fonctionner ensemble les services DHCPv4 et DHCPv6. Bien que la [RFC4477] soit un peu dépassée, elle fournit une bonne vue d'ensemble des problèmes en cause.

2. Exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

Le présent document utilise aussi des variables conceptuelles internes pour décrire le comportement du protocole, et des variables externes qu'une mise en œuvre doit permettre aux administrateurs de système de changer. Les noms spécifiques des variables, comment leurs valeurs changent, et comment leurs réglages influencent le comportement du protocole sont fournis pour montrer le comportement du protocole. Une mise en œuvre n'est pas obligée de les avoir dans la forme exacte décrite ici, pour autant que son comportement externe soit cohérent avec celui décrit dans le présent document.

3. Fondements

La [RFC8200] ("Spécification du protocole Internet, version 6 (IPv6)") donne l'architecture et la conception de base de IPv6. En plus de la [RFC8200], les travaux en relation avec IPv6 qu'un développeur serait bien inspiré d'étudier incluent :
- [RFC4291] ("Architecture d'adressage de IPv6")
- [RFC4862] ("Auto configuration d'adresse IPv6 sans état")
- [RFC4861] ("Découverte de voisin pour IP version 6 (IPv6)")

Ces spécifications permettent à DHCP de s'appuyer sur les travaux de IPv6 pour fournir une auto configuration robuste à états pleins.

La [RFC4291] définit la portée d'adresse qui peut être utilisée dans une mise en œuvre de IPv6 et donne aussi diverses lignes directrices d'architecture de configuration pour les concepteurs de réseau de l'espace d'adresses IPv6. Deux avantages de IPv6 sont que la prise en charge de la diffusion groupée est exigée et que les nœuds peuvent créer des adresses de liaison locale durant l'initialisation. La disponibilité de ces caractéristiques signifie qu'un client peut utiliser son adresse de liaison locale et une adresse bien connue de diffusion groupée pour découvrir et communiquer avec les serveurs DHCP ou les agents de relais sur sa liaison.

La [RFC4862] spécifie les procédures par lesquelles un nœud peut auto configurer les adresses sur la base des annonces de routeur [RFC4861] et l'utilisation d'une durée de vie valide pour prendre en charge le re-numérotage des adresses sur l'Internet. La compatibilité avec l'auto configuration d'adresse sans état est une exigence de conception de DHCP.

La découverte de voisin IPv6 [RFC4861] est le protocole de découverte de nœuds dans IPv6 qui remplace et améliore les fonctions de ARP [RFC0826]. Pour comprendre IPv6 et l'auto configuration d'adresse sans état, il est fortement recommandé que les développeurs comprennent la découverte de voisin IPv6.

4. Terminologie

Cette Section définit la terminologie spécifique de IPv6 et DHCP utilisée dans le présent document.

4.1 Terminologie IPv6

La terminologie IPv6 des [RFC8200], [RFC4291], et [RFC4862] pertinente pour cette spécification est donnée ci-après.

adresse : identifiant de couche IP pour une interface ou ensemble d'interfaces.

GUA *(Global Unicast Address)* : adresse mondiale d'envoi individuel (voir la [RFC4291]).

hôte : tout nœud qui n'est pas un routeur.

IP : protocole Internet version 6 (IPv6). Les termes "IPv4" et "IPv6" ne sont utilisés que dans les contextes où il est nécessaire d'éviter l'ambiguïté.

interface : rattachement d'un nœud à une liaison.

liaison : facilité ou support de communication sur lequel les nœuds peuvent communiquer à la couche de liaison, c'est-à-dire, la couche immédiatement en-dessous de IP. Des exemples sont les liaisons Ethernet (simples ou pontées) les liaisons du protocole point à point (PPP) et PPP sur Ethernet (PPPoE) et les "tunnels" de couche Internet (ou supérieure) comme les tunnels sur IPv4 ou IPv6 lui-même.

identifiant de couche de liaison : identifiant de couche de liaison pour une interface -- par exemple, les adresses IEEE 802 pour les interfaces de réseau Ethernet ou d'anneau à jetons.

adresse de liaison locale : adresse IPv6 qui a une portée de seulement une liaison, indiquée par le préfixe (fe80::/10), qui peut être utilisée pour joindre les nœuds du voisinage sur la même liaison. Chaque interface IPv6 sur laquelle DHCPv6 peut raisonnablement être utile a une adresse de liaison locale.

adresse de diffusion groupée : identifiant pour un ensemble d'interfaces (appartenant normalement à des nœuds différents). Un paquet envoyé à une adresse de diffusion groupée est livré à toutes les interfaces identifiées par cette adresse.

voisin : nœud rattaché à la même liaison.

nœud : appareil qui met en œuvre IP.

paquet : un en-tête IP plus une charge utile.

préfixe : bits initiaux d'une adresse, ou ensemble d'adresses IP qui partagent les mêmes bits initiaux.

longueur de préfixe : nombre de bits dans un préfixe.

routeur : nœud qui transmet les paquets IP non explicitement adressés à lui-même.

ULA (*Unique Local Address)* : adresse locale unique (voir la [RFC4193]).

adresse d'envoi individuel : identifiant pour une seule interface. Un paquet envoyé à une adresse d'envoi individuel est livré à l'interface identifié par cette adresse.

4.2 Terminologie DHCP

On donne ci-dessous la terminologie spécifique de DHCP.

approprié à la liaison : une adresse est "appropriée à la liaison" quand l'adresse est cohérente avec la connaissance du serveur DHCP de la topologie du réseau, de l'allocation de préfixe, et des politiques d'allocation d'adresses.

lien : un lien (ou lien de client) est une groupe d'enregistrements de données de serveur contenant les informations qu'a le serveur sur les adresses ou les préfixes délégués dans une association d'identité (IA, *Identity Association*) ou des informations de configuration explicitement allouées au client. Les informations de configuration qui ont été retournées à un client par une politique, comme les informations retournées à tous les clients sur la même liaison, n'exigent pas un lien. Un lien contenant des informations sur une IA est indexé par le triplet <DUID, type d'IA, IAID> (où le type d'IA est le type de prêt dans l'IA -- par exemple, temporaire). Un lien contenant des informations de configuration pour un client est indexé par <DUID>. Voir ci-dessous les définitions de DUID, IA, et IAID.

paramètre de configuration : un élément des informations de configuration réglées sur le serveur et livré au client en utilisant DHCP. De tels paramètres peuvent être utilisés pour porter des informations à utiliser par un nœud pour configurer son sous système réseau et permettre la communication sur une liaison ou un inter réseaux, par exemple.

option conteneur : une option qui encapsule d'autres options (par exemple, l'option IA_NA (paragraphe 21.4) peut contenir des options Adresse d'IA (paragraphe 21.6)).

routeur délégant : routeur qui agit comme un serveur DHCP et répond aux demandes de délégation de préfixes. Le présent document utilise principalement le terme "serveur DHCP" ou "serveur" quand il discute de la fonction de "routeur délégant" de délégation de préfixe (voir la Section 1).

DHCP : protocole de configuration dynamique d'hôte pour IPv6. Les termes "DHCPv4" et "DHCPv6" ne sont utilisés que

dans des contextes où il est nécessaire d'éviter des ambiguïtés.

client DHCP : aussi appelé "client". Un nœud qui initie des demandes sur une liaison pour obtenir les paramètres de configuration d'un ou plusieurs serveurs DHCP. Le nœud peut agir comme un routeur demandeur (voir ci-dessous) si il prend en charge la délégation de préfixe.

domaine DHCP : ensemble des liaisons gérées par DHCP et que fait fonctionner une seule entité administrative.

agent de relais DHCP : aussi appelé "agent de relais". Un nœud qui agit comme intermédiaire pour livrer les messages DHCP entre les clients et les serveurs. Dans certaines configurations, il peut y avoir plus d'un agent de relais entre les clients et les serveurs, de sorte qu'un agent de relais peut envoyer des messages DHCP à un autre agent de relais.

serveur DHCP : aussi appelé "serveur". Un nœud qui répond aux demandes des clients. Il peut ou non être sur la même liaison que le ou les clients. Selon ses capacités, si il prend en charge la délégation de préfixe, il peut aussi assurer la fonction de routeur délégant.

DUID : identifiant DHCP unique pour un participant à DHCP. Chaque client et serveur DHCP a exactement un DUID. Voir à la Section 11 les détails de la façon dont un DUID peut être construit.

option encapsulée : option DHCP qui est généralement seulement contenue dans une autre option. Par exemple, l'option Adresse d'IA est contenue dans les options IA_NA ou IA_TA (paragraphe 21.5). Voir à la Section 9 de la [RFC7227] une définition plus complète.

IA *(Identity Association)* : association d'identité, une collection de prêts alloués à un client. Chaque IA a un IAID associé (voir ci-dessous). Un client peut avoir plus d'une IA allouée -- par exemple, une pour chacune de ses interfaces. Chaque IA détient un type de prêt ; par exemple, une association d'identité pour les adresses temporaires (IA_TA) détient des adresses temporaires, et une association d'identité pour une délégation de préfixe (IA_PD) détient les préfixes délégués. Dans le présent document, "IA" est utilisé pour se référer à une association d'identité sans identifier le type de prêt dans l'IA. Au moment de la rédaction du présent document, trois types d'IA sont définis : IA_NA, IA_TA, et IA_PD. De nouveaux types d'IA pourront être définis à l'avenir.

options d'IA : au moment de la rédaction du présent document, une ou plusieurs options IA_NA, IA_TA, et/ou IA_PD. De nouveaux types d'IA pourront être définis à l'avenir.

IAID *(Identity Association Identifier)* : identifiant d'association d'identité. Identifiant d'une IA, choisi par le client. Chaque IA a un IAID, qui est choisi pour être unique parmi les IAID pour les IA d'un type spécifique qui appartient à ce client.

IA_NA *(Identity Association for Non-temporary Addresses)* : association d'identité pour adresses non temporaires. C'est une IA qui porte des adresses allouées qui ne sont pas des adresses temporaires (voir "IA_TA"). Voir au paragraphe 21.4 les détails de l'option IA_NA.

IA_PD *(Identity Association for Prefix Delegation)* : association d'identité qui porte des préfixes délégués. Voir au paragraphe 21.21 les détails de l'option IA_PD.

IA_TA *(Identity Association for Temporary Addresses)* : association d'identité qui porte des adresses temporaires ([RFC4941]). Voir au paragraphe 21.5 les détails de l'option IA_TA.

prêt : contrat par lequel le serveur concède l'utilisation d'une adresse ou d'un préfixe délégué au client pour une période spécifiée.

message : unité de données portée comme charge utile d'un datagramme UDP, échangée entre les serveurs DHCP, les agents de relais, et les clients.

clé de reconfiguration : clé fournie à un client par un serveur. Utilisée pour assurer la sécurité des messages Reconfigure (voir au paragraphe 7.3 la liste des types de messages disponibles).

relais : un agent de relais DHCP relaye les messages DHCP entre les participants à DHCP.

routeur demandeur : routeur qui agit comme client DHCP et demande qu'un ou des préfixes lui soient alloués. Le présent document utilise principalement le terme "client DHCP" ou "client" quand il discute de la fonction de "routeur demandeur" de délégation de préfixe (voir la Section 1).

retransmission : autre tentative d'envoi du même message DHCP par un client ou serveur, par suite de la non réception d'une réponse valide aux messages envoyés précédemment. Le message retransmis est normalement modifié avant l'envoi, comme exigé par les spécifications DHCP. En particulier, le client met à jour la valeur de l'option Temps écoulé dans le message retransmis.

RKAP *(Reconfiguration Key Authentication Protocol)* : protocole d'authentification de clé de reconfiguration (paragraphe 20.4).

option singleton : option à qui il n'est permis d'apparaître qu'une fois comme option de niveau supérieur ou à tout niveau d'encapsulation. La plupart des options sont des singletons.

T1 : intervalle de temps après lequel le client est supposé contacter le serveur qui a fait l'allocation pour étendre (renouveler) les durées de vie des adresses allouées (via les options IA_NA et/ou des préfixes délégués (via les options IA_PD) au client. T1 est exprimé par une valeur absolue (en secondes) dans les messages, est convoyé dans des conteneurs IA (actuellement les options IA_NA et IA_PD) et est interprété comme un intervalle de temps depuis la réception du paquet. La valeur mémorisée dans le champ T1 dans les options IA est appelée la valeur T1. L'heure réelle où le temporisateur expire est appelée le temps T1.

T2 : intervalle de temps après lequel le client est supposé contacter tout serveur disponible pour étendre (lier à nouveau) les durées de vie des adresses allouées (via la ou les options IA_NA) et/ou préfixes délégués (via la ou les options IA_PD) au client. T2 est exprimé comme une valeur absolue (en secondes) dans les messages, est convoyée dans des conteneurs IA (actuellement les options IA_NA et IA_PD) et est interprété comme un intervalle de temps depuis la réception du paquet. La valeur mémorisée dans le champ T2 dans les options IA est appelée la valeur T2. L'heure réelle à laquelle le temporisateur expire est appelée le temps T2.

option de niveau supérieur : option convoyée directement dans un message DHCP, c'est-à-dire, non encapsulée dans une autre option, comme décrit à la Section 9 de la [RFC7227].

Identifiant de transaction : valeur opaque utilisée pour faire correspondre les réponses avec les répliques initiées par un client ou un serveur.

5. Échanges client/serveur

Les clients et les serveurs échangent des messages DHCP en utilisant UDP (voir la [RFC0768] et le BCP 145 [RFC8085]). Le client utilise une adresse de liaison locale ou des adresses déterminées par d'autres mécanismes pour émettre et recevoir les messages DHCP.

Un client DHCP envoie la plupart des messages en utilisant une adresse de destination réservée de diffusion groupée à portée de liaison afin que le client n'ait pas besoin d'être configuré avec la ou les adresses des serveurs DHCP.

Pour permettre à un client DHCP d'envoyer un message à un serveur DHCP qui n'est pas rattaché à la même liaison, un agent de relais DHCP sur la liaison du client va relayer les messages entre le client et le serveur. L'opération de l'agent de relais est transparente pour le client. La discussion des échanges de messages dans le reste de cette section va omettre la description du relais des messages par les agents de relais.

Une fois que le client a déterminé l'adresse d'un serveur, il peut, dans certaines circonstances, envoyer les messages directement au serveur en utilisant l'envoi individuel.

5.1 Échanges client/serveur impliquant deux messages

Quand un client DHCP n'a pas besoin d'avoir un serveur DHCP qui lui alloue des adresses IP ou des préfixes délégués, il peut obtenir d'autres informations de configuration comme une liste de serveurs DNS disponibles [RFC3646] ou de serveurs NTP [RFC5908] par un seul échange de message et réponse avec un serveur DHCP. Pour obtenir d'autres informations de configuration, le client envoie d'abord un message Demande d'informations à l'adresse de diffusion groupée Tous_agents_de_relais_et_serveurs_DHCP. Les serveurs répondent par un message contenant les autres informations de configuration pour le client.

Un client peut aussi demander au serveur d'expédier une allocation d'adresse et/ou une délégation de préfixe en utilisant un échange de deux messages au lieu de l'échange normal de quatre messages comme expliqué au paragraphe suivant. L'allocation expédiée peut être demandée par le client, et les serveurs peuvent ou non honorer la demande (voir aus paragraphes 18.3.1 et 21.14 plus de détails et pourquoi les serveurs peuvent ne pas honorer cette demande). Les clients peuvent demander ce service expédié dans des environnements où il est probable qu'il y a seulement un serveur disponible sur une liaison et pas d'espoir qu'un second serveur devienne disponible, ou quand l'achèvement aussi vite que possible du processus de configuration est une priorité.

Pour demander l'échange de deux messages expédiés, le client envoie un message Solicit à l'adresse de diffusion groupée Tous_agents_de_relais_et_serveurs_DHCP demandant l'allocation des adresses et/ou préfixes délégués et autres informations de configuration. Ce message comporte une indication (l'option Engagement rapide ; voir au paragraphe 21.14) que le client veut accepter un message de réponse immédiat du serveur. Le serveur qui veut s'engager à l'allocation des adresses et/ou préfixes délégués au client répond immédiatement par un message de réponse. Les informations de configuration et les adresses et/ou préfixes délégués dans le message de réponse sont alors immédiatement disponibles pour que le client les utilise.

Chaque adresse ou préfixe délégué alloué au client a des durées de vie associées préférées et valides spécifiées par le serveur. Pour demander une extension des durées de vie allouées à une adresse ou préfixe délégué, le client envoie un message Renouvellement au serveur.
Le serveur envoie un message Réponse au client avec les nouvelles durées de vie, ce qui permet au client de continuer d'utiliser l'adresse ou préfixe délégué sans interruption. Si le serveur est incapable d'étendre la durée de vie d'une adresse ou préfixe délégué, il l'indique en retournant l'adresse ou préfixe délégué avec une durée de vie de 0. En même temps, le serveur peut allouer d'autres adresses ou préfixes délégués.

Voir à la Section 18 les descriptions d'échanges de deux messages supplémentaires entre client et serveur.

5.2 Échanges client/serveur impliquant quatre messages

Pour demander l'allocation d'une ou plusieurs adresses et/ou préfixes délégués, un client localise d'abord un serveur DHCP et ensuite demande l'allocation des adresses et/ou préfixes délégués et autres informations de configuration au serveur. Le client envoie un message Solicit à l'adresse de diffusion groupée Tous_agents_de_relais_et_serveurs_DHCP pour trouver les serveurs DHCP disponibles. Tout serveur qui peut satisfaire les exigences du client répond par un message Advertise. Le client choisit alors un des serveurs et envoie un message Request au serveur lui demandant de confirmer l'allocation des adresses et/ou préfixes délégués et autres informations de configuration. Le serveur répond par un message Reply qui contient les adresses, préfixes délégués, et informations de configuration confirmées.

Comme décrit au paragraphe précédent, le client peut demander une extension des durées de vie allouées aux adresses ou préfixes délégués (c'est un échange à deux messages).

5.3 Échanges serveur/client

Un serveur qui a précédemment communiqué avec un client et négocié que le client écoute les messages Reconfigure peut envoyer au client un message Reconfigure pour initier par le client une mise à jour de sa configuration par l'envoi d'un message Demande d'informations, de Renouvellement, ou Réinitialisation. Le client effectue alors l'échange à deux messages comme décrit précédemment. Ceci peut être utilisé pour expédier des changements de configuration à un client, comme le besoin de renuméroter un réseau (voir la [RFC6879]).

6. Modèles de fonctionnement

Cette Section décrit les modèles de fonctionnement les plus courants de DHCP. Les modèles décrits ne sont pas mutuellement exclusifs et sont parfois utilisés ensembles. Par exemple, un appareil peut commencer en mode à états pleins pour obtenir une adresse et, ensuite, quand une application est lancée, demander des paramètres supplémentaires en utilisant le mode sans état.

Le présent document suppose que les serveurs et le client DHCP, communiquant avec les serveurs via une interface spécifique, appartiennent à un seul domaine de provisionnement.

DHCP peut être étendu pour prendre en charge des services à états pleins supplémentaires qui peuvent interagir avec un ou

plusieurs des modèles décrits ci-dessous. Une telle interaction devrait être considérée et documentée au titre de toute future extension du protocole.

6.1 DHCP sans état

DHCP sans état [RFC3736] est utilisé quand DHCP n'est pas utilisé pour obtenir un prêt mais qu'un nœud (client DHCP) désire un ou plusieurs paramètres "autre configuration" DHCP, comme une liste des serveurs de noms DNS récurrents ou des listes de recherche de domaines DNS [RFC3646]. DHCP sans état peut être utilisé quand un nœud s'amorce initialement ou à tout moment où le logiciel sur le nœud exige des informations manquantes ou expirés de configuration qui sont disponibles via DHCP.

C'est le fonctionnement le plus simple et le plus basique pour DHCP et qui exige d'un client (et d'un serveur) de prendre seulement en charge deux messages – Demande d'informations et Réponse. Noter que les serveurs et agents de relais DHCP ont normalement aussi besoin de prendre en charge les messages Relay-forward et Relay-reply pour s'accommoder du fonctionnement où les clients et les serveurs ne sont pas sur la même liaison.

6.2 DHCP pour allocation d'adresse non temporaire

Ce modèle de fonctionnement était la motivation d'origine de DHCP. Il est approprié pour les situations où l'auto configuration d'adresse sans état seule est impraticable, par exemple, à cause de la politique du réseau, des exigences supplémentaires comme une mise à jour dynamique du DNS, ou des exigences spécifiques du client.

Le modèle de fonctionnement pour l'allocation non temporaire d'adresse est comme suit. Des préfixes sont fournis au serveur à partir desquels il peut allouer des adresses aux clients, ainsi que toutes les informations relatives à la topologie du réseau sur quels préfixes sont présents sur quelles liaisons. Un client demande qu'une adresse non temporaire lui soit allouée par le serveur. Le serveur alloue une ou des adresses appropriées pour la liaison sur laquelle le client est connecté. Le serveur retourne la ou les adresses allouées au client.

Chaque adresse a une durée de vie associée préférée et valide, qui constitue un accord sur la durée pendant laquelle il est permis au client d'utiliser l'adresse. Un client peut demander une extension de la durée de vie d'une adresse et est obligé de terminer l'utilisation d'une adresse si la durée de vie valide de l'adresse arrive à expiration.

Normalement, les clients demandent d'autres paramètres de configuration, comme les adresses de serveur de noms du DNS et les listes de rechercher de domaines, quand ils demandent des adresses.

Les clients peuvent aussi demander plus d'une adresse ou ensemble d'adresses (voir le paragraphe 6.6 et la Section 12).

6.3 DHCP pour délégation de préfixe

Le mécanisme de délégation de préfixe, décrit à l'origine dans la [RFC3633], est un autre mode de fonctionnement à états pleins et était à l'origine destiné à une simple délégation de préfixes à partir d'un routeur de délégation (serveur DHCP) pour les routeurs demandeurs (clients DHCP). Il est approprié pour les situations dans lesquelles le routeur délégant (1) n'a pas connaissance de la topologie des réseaux auxquels le routeur demandeur est rattaché et (2) n'exige pas d'autres informations en dehors de l'identité du routeur demandeur pour choisir un préfixe à déléguer. Ce mécanisme est approprié pour l'utilisation par un fournisseur d'accès Internet (FAI) pour déléguer un préfixe à un abonné, où le préfixe délégué va éventuellement être dans un sous réseau et alloué aux liaisons au sein du réseau de l'abonné. Les [RFC7084] et [RFC7368] décrivent cette utilisation en détails.

La conception de ce mécanisme de délégation de préfixe satisfait aux exigences de délégation de préfixe de la [RFC3769].

Alors que la [RFC3633] suppose que le client DHCP est un routeur (d'où l'expression de "routeur demandeur") et que le serveur DHCP est un routeur (d'où l'utilisation de "routeur délégant") la délégation de préfixe DHCP elle-même n'exige pas que le client transmette les paquets IP qui ne sont pas adressés à lui-même et donc n'exige pas que le client (ou serveur) soit un routeur comme défini dans la [RFC8200]. Aussi, dans de nombreux cas (comme le rattachement ou l'hébergement de machines virtuelles) les hôtes transmettent déjà les paquets IP et opèrent donc comme routeurs comme défini dans la [RFC8200]. Donc, le présent document remplace le plus souvent "routeur demandeur" par "client" et "routeur délégant" par "serveur".

Le modèle de fonctionnement pour la délégation de préfixe est comme suit. Un serveur est provisionné avec des préfixes à

déléguer aux clients. Un client demande un ou des préfixes au serveur, comme décrit à la Section 18. Le serveur choisit le ou les préfixes à déléguer et répond avec le ou les préfixes au client. Le client est alors responsable du ou des préfixes délégués. Par exemple, le client pourrait allouer à un sous réseau un préfixe délégué à une de ses interfaces et commencer à envoyer des annonces de routeur pour le préfixe sur cette liaison.

Chaque préfixe a une durée de vie associée préférée et une durée de vie valide, qui constituent un accord sur la durée pendant laquelle il est permis au client d'utiliser le préfixe. Un client peut demander une extension des durées de vie sur un préfixe délégué et est obligé de terminer l'utilisation d'un préfixe délégué si la durée de vie valide du préfixe expire.

La Figure 1 illustre une architecture de réseau dans laquelle on pourrait utiliser une délégation de préfixe.

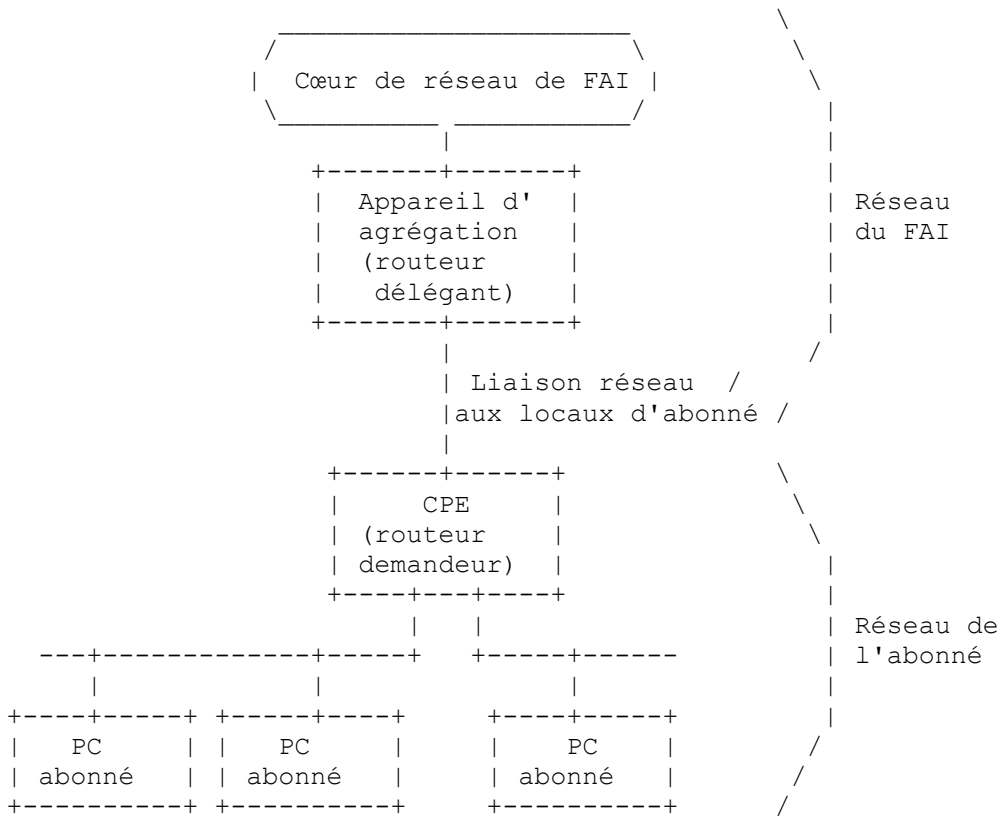


Figure 1 : Réseau à délégation de préfixe

Dans cet exemple, le serveur (routeur délégant) est configuré avec un ensemble de préfixes à utiliser pour les allouer aux consommateurs au moment de la première connexion de chaque consommateur au service du FAI. Le processus de délégation de préfixe commence quand le client (routeur demandeur) demande les informations de configuration par DHCP. Les messages DHCP provenant du client sont reçus par le serveur dans l'appareil d'agrégation. Quand le serveur reçoit la demande, il choisit un ou des préfixes disponibles pour les déléguer au client. Le serveur retourne ensuite le ou les préfixes au client.

Le client met en sous réseau le préfixe délégué et alloue les plus longs préfixes aux liaisons dans le réseau de l'abonné. Dans un scénario normal fondé sur le réseau montré à la Figure 1, le client met en sous réseau un seul préfixe /48 délégué dans des préfixes /64 et alloue un préfixe /64 à chaque liaison du réseau de l'abonné.

Les options de délégation de préfixe peuvent être utilisées en conjonction avec les autres options DHCP qui portent d'autres informations de configuration au client.

Le client peut, à son tour, fournir le service DHCP aux nœuds rattachés au réseau interne. Par exemple, le client peut obtenir les adresses des serveurs DNS et NTP du serveur du FAI et passer ensuite ces informations de configuration aux hôtes abonnés à travers un serveur DHCP chez le client (routeur demandeur).

Si le client utilise un préfixe délégué pour configurer les adresses sur ses interfaces ou d'autres nœuds derrière lui, les durées de vie préférées et valides de ces adresses DOIVENT être pas plus longues que les durées de vie, respectivement

préférées et valides restantes pour le préfixe délégué à tout moment. En particulier, si le préfixe délégué ou un préfixe qui en est déduit est annoncé pour l'auto configuration d'adresse sans état [RFC4862], les durées de vie annoncées préférée et valide NE DOIVENT PAS excéder les durées de vie correspondantes restantes du préfixe délégué.

6.4 DHCP pour routeurs côté consommateur

Les exigences de DHCP et l'architecture de réseau pour les routeurs côté consommateur sont décrites dans la [RFC7084]. Ce modèle de fonctionnement combine l'allocation d'adresse (voir au paragraphe 6.2) et la délégation de préfixe (voir au paragraphe 6.3). En général, ce modèle suppose qu'un seul ensemble de transactions entre client et serveur va allouer ou étendre les adresses et préfixes délégués non temporaires du client.

6.5 DHCP pour adresses temporaires

Les adresses temporaires ont été introduites à l'origine pour éviter des problèmes de confidentialité avec l'auto configuration d'adresse sans état, qui fondait 64 bits de l'adresse sur le EUI-64 (voir la [RFC4941]). Elles ont été ajoutées à DHCP pour fournir un soutien complémentaire quand l'allocation d'adresse à états pleins est utilisée.

L'allocation d'adresse temporaire fonctionne à peu près comme l'allocation d'adresse non temporaire (paragraphe 6.2) ; cependant, ces adresses sont généralement destinées à être utilisées pour un court instant et n'ont pas leurs durées de vie étendues, bien qu'elles puissent l'être si nécessaire.

6.6 Adresses et préfixes multiples

DHCP permet à un client de recevoir plusieurs adresses. En fonctionnement normal, un client envoie une instance d'une option IA_NA et le serveur alloue au plus une adresse à partir de chaque préfixe alloué à la liaison à laquelle le client est rattaché. En particulier, le serveur peut être configuré à servir des adresses à partir de plusieurs préfixes pour une certaine liaison. Ceci est utile dans des cas comme celui d'un événement de renumérotation de réseau en cours. Dans un déploiement normal, le serveur va accorder une adresse pour chaque option IA_NA (voir au paragraphe 21.4).

Un client peut explicitement demander plusieurs adresses en envoyant plusieurs options IA_NA (et/ou options IA_TA ; voir au paragraphe 21.5). Un client peut envoyer plusieurs options IA_NA (et/ou IA_TA) dans ses transmissions initiales. Autrement, il peut envoyer un message Request supplémentaire avec de nouvelles options IA_NA (et/ou IA_TA) (ou les inclure dans un message Renew).

Le même principe s'applique aussi à la délégation de préfixe. En principe, DHCP permet à un client de demander que de nouveaux préfixes soient délégués en envoyant des options IA_PD supplémentaires (voir au paragraphe 21.21). Cependant, un opérateur normal va généralement préférer déléguer un seul préfixe, plus grand. Dans la plupart des déploiements, il est recommandé que le client demande un plus grand préfixe dans ses transmissions initiales plutôt que de demander des préfixes supplémentaires plus tard.

Le comportement exact du serveur (accorder ou non des adresses et préfixes supplémentaires) dépend de la politique du serveur et sort du domaine d'application du présent document.

Voir à la Section 12 plus d'informations sur la façon dont le serveur distingue entre les instances d'option IA.

7. Constantes DHCP

Cette section décrit diverses constantes de programme et de réseautage utilisées par DHCP.

7.1 Adresses de diffusion groupée

DHCP utilise les adresses de diffusion groupée suivantes :

Tous_agents_de_relais_et_serveurs_DHCP (ff02::1:2)
C'est une adresse de diffusion groupée de portée de liaison qui est utilisée par un client pour communiquer avec les agents de relais et les serveurs du voisinage (c'est-à-dire, en liaison). Tous les serveurs et agents de relais sont membres de ce groupe de diffusion groupée.

Tous_serveurs_DHCP (ff05::1:3)
Adresse de diffusion groupée à portée de site utilisée par un agent de relais pour communiquer avec les serveurs, soit parce que l'agent de relais veut envoyer des messages à tous les serveurs, soit parce qu'il ne connaît pas les adresses d'envoi individuel des serveurs. Noter qu'afin qu'un agent de relais utilise cette adresse, il doit avoir une adresse de portée suffisante pour être accessible par les serveurs. Tous les serveurs au sein du site sont membres de ce groupe de diffusion groupée sur les interfaces qui sont dans le site.

7.2 Accès UDP

Les clients écoutent les messages DHCP sur l'accès UDP 546. Les serveurs et agents de relais écoutent les messages DHCP sur l'accès UDP 547.

7.3 Types de messages DHCP

DHCP définit les types de messages suivants. Le format de ces messages est fourni aux Sections 8 et 9. Des types de messages supplémentaires ont été définis et pourront être définis à l'avenir ; voir <https://www.iana.org/assignments/dhcpv6-parameters>. Le codage numérique de chaque type de message est montré entre parenthèses.

SOLICIT (1) : un client envoie un message Solicit pour localiser les serveurs.

ADVERTISE (2) : un serveur envoie un message Advertise pour indiquer qu'il est disponible pour le service DHCP, en réponse à un message Solicit reçu d'un client.

REQUEST (3) : un client envoie un message Request pour demander des paramètres de configuration, incluant des adresses et/ou préfixes délégués, à un serveur spécifique.

CONFIRM (4) : un client envoie un message Confirm à tout serveur disponible pour déterminer si les adresses qui lui ont été allouées sont toujours appropriées pour la liaison à laquelle le client est connecté.

RENEW (5) : un client envoie un message Renew au serveur qui a à l'origine fourni les prêts et paramètres de configuration au client pour étendre les durées de vie sur les prêts alloués au client et pour mettre à jour d'autres paramètres de configuration.

REBIND (6) : un client envoie un message Rebind à tout serveur disponible pour étendre les durées de vie sur les prêts alloués au client et pour mettre à jour d'autres paramètres de configuration ; ce message est envoyé après qu'un client n'a pas reçu de réponse à un message Renew.

REPLY (7) : un serveur envoie un message Reply contenant les prêts et paramètres de configuration alloués en réponse à un message Solicit, Request, Renew, ou Rebind reçu d'un client. Un serveur envoie un message Reply contenant des paramètres de configuration en réponse à un message Demande d'informations. Un serveur envoie un message Reply en réponse à un message Confirm confirmant (ou niant) que les adresses allouées au client sont appropriées pour la liaison à laquelle le client est connecté. Un serveur envoie un message Reply pour accuser réception d'un message Release ou Decline.

RELEASE (8) : un client envoie un message Release au serveur qui a alloué les prêts au client pour indiquer que le client ne va plus utiliser un ou plusieurs des prêts alloués.

DECLINE (9) : un client envoie un message Decline à un serveur pour indiquer que le client a déterminé qu'une ou plusieurs des adresses allouées par le serveur sont déjà utilisées sur la liaison à laquelle le client est connecté.

RECONFIGURE (10) : un serveur envoie un message Reconfigure à un client pour l'informer que le serveur a des paramètres de configuration nouveaux ou mis à jour et que le client doit initier une transaction Renew/Reply, Rebind/Reply, ou Information-request/Reply avec le serveur afin de recevoir la mise à jour des informations.

INFORMATION-REQUEST (11) : un client envoie un message Demande d'informations à un serveur pour demander des paramètres de configuration sans l'allocation d'aucun prêt au client.

RELAY-FORW (12) : un agent de relais envoie un message Relay-forward pour relayer des messages aux serveurs, soit directement, soit à travers un autre agent de relais. Le message reçu – message de client ou message Relay-forward provenant d'un autre agent de relais -- est encapsulé dans une option dans le message Relay-forward.

RELAY-REPL (13) : un serveur envoie un message Relay-reply à un agent de relais contenant un message que l'agent de relais livre à un client. Le message Relay-reply peut être relayé par d'autres agents de relais pour être livré à l'agent de relais de destination. Le serveur encapsule le message du client comme une option dans le message Relay-reply, que l'agent de relais extrait et relaie au client.

7.4 Codes d'option DHCP

DHCP fait un large usage des options dans les messages ; certains d'entre eux sont définis à la Section 21. Des options supplémentaires sont définies dans d'autres documents ou pourront être définies à l'avenir (voir dans la [RFC7227] des conseils pour la définition de nouvelles options).

7.5 Codes d'état

DHCP utilise des codes d'état pour communiquer la réussite ou l'échec des opérations demandées dans les messages provenant des clients et des serveurs et pour fournir des informations supplémentaires sur les causes spécifiques de l'échec d'un message. Les codes d'état sont définis au paragraphe 21.13.
Si l'option Code d'état (voir au paragraphe 21.13) n'apparaît pas dans un message dans lequel l'option pourrait apparaître, l'état du message est supposé être Succès.

7.6 Paramètres de transmission et retransmission

Ce paragraphe présente un tableau des valeurs utilisées pour décrire le comportement de transmission de messages des clients et des serveurs. Certaines des valeurs sont ajustées d'un facteur aléatoire et par des facteurs de réduction (voir la Section 15). Les transmissions peuvent aussi être influencées par une limitation de débit (voir au paragraphe 14.1).

Paramètre	Valeur par défaut	Description
SOL_MAX_DELAY	1 s	délai maximum de la première sollicitation
SOL_TIMEOUT	1 s	temporisation de sollicitation initiale
SOL_MAX_RT	3 600 s	valeur maximale de temporisation de sollicitation
REQ_TIMEOUT	1 s	temporisation de demande initiale
REQ_MAX_RT	30 s	valeur maximale de temporisation de demande
REQ_MAX_RC	10	nombre maximum de tentative d'essai de demande
CNF_MAX_DELAY	1 s	délai maximum de première confirmation
CNF_TIMEOUT	1 s	temporisation de confirmation initiale
CNF_MAX_RT	4 s	temporisation maximale de confirmation
CNF_MAX_RD	10 s	durée maximale de confirmation
REN_TIMEOUT	10 s	temporisation de renouvellement initial
REN_MAX_RT	600 s	valeur maximale de temporisation de renouvellement
REB_TIMEOUT	10 s	temporisation de réinitialisation initiale
REB_MAX_RT	600 s	valeur maximale de temporisation de réinitialisation
INF_MAX_DELAY	1 s	délai maximal de la première demande d'informations
INF_TIMEOUT	1 s	temporisation de demande 'informations initiale
INF_MAX_RT	3 600 s	valeur maximale de temporisation de demande d'informations
REL_TIMEOUT	1 s	temporisation de libération initiale
REL_MAX_RC	4	nombre maximum de tentatives d'essai de libération
DEC_TIMEOUT	1 s	temporisation de refus initial
DEC_MAX_RC	4	nombre maximum de tentatives d'essais de refus
REC_TIMEOUT	2 s	temporisation de reconfiguration initiale
REC_MAX_RC	8	nombre maximum de tentatives de reconfiguration
HOP_COUNT_LIMIT	8	compte maximum de bonds dans un message de transmission-relais
IRT_DEFAULT	86 400 s (24 h)	délai par défaut de rafraîchissement des informations
IRT_MINIMUM	600 s	délai minimum de rafraîchissement des informations
MAX_WAIT_TIME	60 s	Délai maximum obligatoire d'attente d'une réponse

Tableau 1 : Paramètres de transmission et retransmission

7.7 Représentation des valeurs de temps et "Infini" comme valeur de temps

Toutes les valeurs de temps pour les durées de vie, T1, et T2 sont des entiers de 32 bits non signés et sont exprimées en unités de secondes. La valeur 0xffffffff est prise pour signifier "infini" quand elle est utilisée comme durée de vie (comme dans la [RFC4861]) ou une valeur pour T1 ou T2.

Régler la durée de vie valide d'une adresse ou d'un préfixe délégué à 0xffffffff ("infini") revient à une allocation permanente d'une adresse ou délégation à un client et ne devrait être utilisé que dans des cas où des allocations permanentes sont désirées.

Il faut faire attention quand on règle T1 ou T2 à 0xffffffff ("infini"). Un client ne va jamais tenter d'étendre la durée de vie d'une adresse dans une IA avec T1 réglé à 0xffffffff. Un client ne va jamais tenter d'utiliser un message Rebind pour localiser un serveur différent pour étendre les durées de vie d'adresses dans une IA avec T2 réglé à 0xffffffff.

8. Format des messages client/serveur

Tous les messages DHCP envoyés entre clients et serveurs partagent un en-tête identique de format fixe et une zone de format variable pour les options.

Toutes les valeurs dans l'en-tête de message et dans les options sont dans l'ordre des octets du réseau.

Les options sont mémorisées en série dans le champ "options", sans bourrage entre les options. Les options sont alignées sur l'octet mais ne sont pas alignées d'autre façon (comme sur des limites de 2 ou 4 octets).

Le diagramme suivant illustre le format des messages DHCP envoyés entre clients et serveurs :

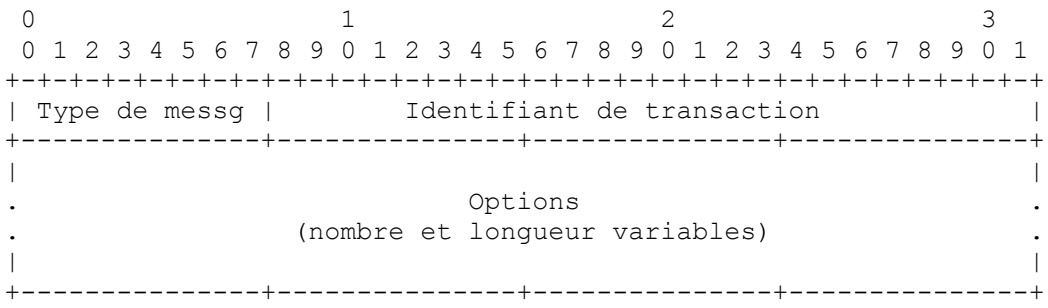


Figure 2 : Format des messages client/serveur

Type de message : identifie le type de message DHCP ; la liste des types de messages disponibles figure au paragraphe 7.3. Champ d'un octet.

Identifiant de transaction : identifiant de transaction pour cet échange de messages. Champ de 3 octets.

Options : options portées dans ce message ; les options sont décrites à la Section 21. Champ de longueur variable (4 octets de moins que la taille du message).

9. Format des messages d'agent de relais/serveur

Les agents de relais échangent des messages avec les autres agents de relais et les serveurs pour relayer les messages entre les clients et les serveurs qui ne sont pas connectés à la même liaison.

Toutes les valeurs dans l'en-tête de message et dans les options sont dans l'ordre des octets du réseau.

Les options sont mémorisées en série dans le champ "options", sans bourrage entre les options. Les options sont alignées sur l'octet mais ne sont pas alignées d'autre façon (comme sur des limites de 2 ou 4 octets).

Il y a deux messages d'agent de relais (Relay-forward et Relay-reply) qui partagent le format suivant :

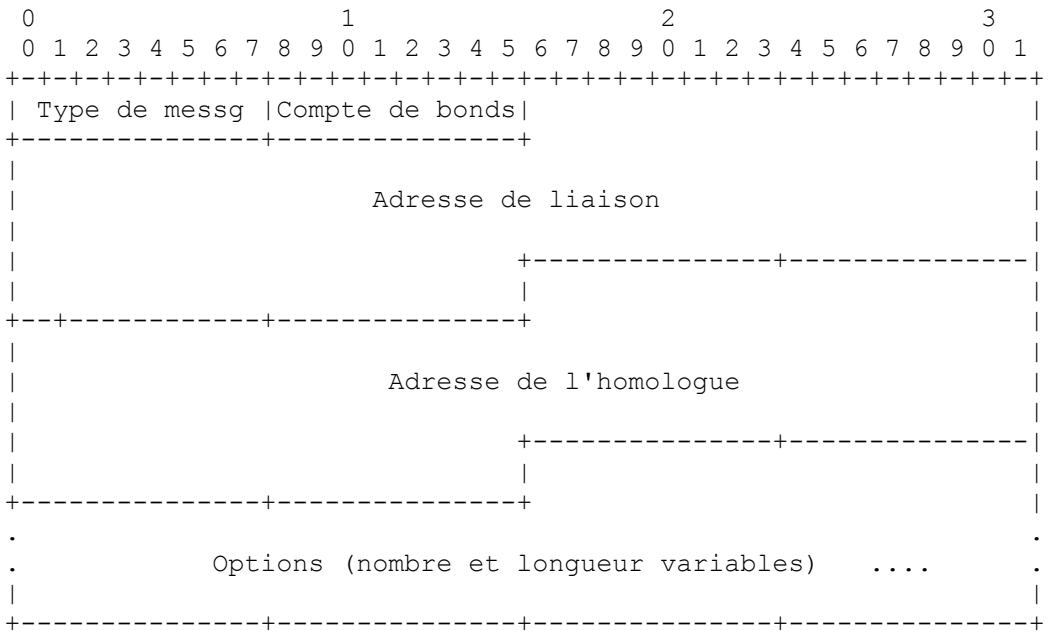


Figure 3 : Format de message d'agent de relais/serveur

Les paragraphes qui suivent décrivent l'utilisation de l'en-tête de message d'agent de relais.

9.1 Message Relay-forward

L'usage des champs de message suivants dans un message Relay-forward est :

Type de message : RELAY-FORW (12). Champ d'un octet.

Compte de bonds : nombre d'agents de relais qui ont déjà relayé ce message. Champ d'un octet.

Adresse de liaison : adresse qui peut être utilisée par le serveur pour identifier la liaison sur laquelle est situé le client. C'est normalement une adresse d'envoi individuel de portée mondiale (c'est-à-dire, GUA ou ULA) mais voir la discussion du paragraphe 19.1.1. Champ de 16 octets.

Adresse de l'homologue : adresse du client ou agent de relais d'où le message à relayer a été reçu. Champ de 16 octets.

Options : DOIT inclure une option Relais de message (paragraphe 21.10) ; PEUT inclure d'autres options, comme l'option Identifiant d'interface (paragraphe 21.18) ajoutées par l'agent de relais. Champ de longueur variable (34 octets de moins que la taille du message).

Voir au paragraphe 13.1 l'explication de la façon dont le champ Adresse de liaison est utilisé.

9.2 Message Relay-reply

L'usage des champs de message suivants dans un message Relay-reply est :

Type de message : RELAY-REPL (13). Champ d'un octet.

Compte de bonds : copié du message Relay-forward. Champ d'un octet.

Adresse de liaison : copiée du message Relay-forward. Champ de seize octets.

Adresse de l'homologue : copiée du message Relay-forward. Champ de seize octets.

Options : DOIT inclure une option Message de relais (paragraphe 21.10) ; PEUT inclure d'autres options, comme une option Identifiant d'interface (paragraphe 21.18). Champ de longueur variable (34 octets de moins que la taille du message).

10. Représentation et usage des noms de domaines

De même façon que les noms de domaines peuvent être codés uniformément, un nom de domaine ou une liste de noms de domaines est codé en utilisant la technique décrite au paragraphe 3.1 de la [RFC1035]. Un nom de domaine, ou liste de noms de domaines, dans DHCP NE DOIT PAS être mémorisé en forme compressée comme décrit au paragraphe 4.1.4 de la [RFC1035].

11. Identifiant univoque DHCP (DUID)

Chaque client et serveur DHCP a un identifiant univoque DHCP (DUID, *DHCP Unique Identifier*). Les serveurs DHCP utilisent des DUID pour identifier les clients pour le choix des paramètres de configuration et dans l'association des IA avec les clients. Les clients DHCP utilisent les DUID pour identifier un serveur dans les messages où un serveur a besoin d'être identifié. Voir aux paragraphes 21.2 et 21.3 les détails concernant la représentation d'un DUID dans un message DHCP.

Les clients et les serveurs DOIVENT traiter les DUID comme des valeurs opaques et DOIVENT seulement comparer les DUID pour égalité. Les clients et les serveurs NE DEVRAIENT PAS interpréter les DUID de quelque autre façon. Les clients et les serveurs NE DOIVENT PAS restreindre les DUID aux types définis dans le présent document, car des types de DUID supplémentaires pourront être définis à l'avenir. On devrait noter qu'une tentative d'analyser un DUID pour obtenir l'adresse de couche de liaison d'un client n'est pas fiable, car il n'est pas garanti que le client utilise encore la même adresse de couche de liaison que quand il a généré son DUID. Aussi, une telle tentative va être de moins en moins fiable à mesure que plus de clients adoptent des mesures de confidentialité comme celles définies dans la [RFC7844]. Si cette capacité est requise, il est recommandé de s'appuyer plutôt sur l'option Adresse de couche de liaison de client [RFC6939].

Le DUID est porté dans une option parce qu'il peut être de longueur variable et parce qu'il n'est pas exigé dans tous les messages DHCP. Le DUID est conçu pour être unique parmi tous les clients et les serveurs DHCP, et stable pour tout client ou serveur spécifique. C'est-à-dire que le DUID utilisé par un client ou serveur NE DEVRAIT PAS changer avec le temps si c'est possible ; par exemple, le DUID d'un appareil ne devrait pas changer par suite d'un changement du matériel réseau de l'appareil ou de changements des interfaces virtuelles (par exemple, interfaces logiques PPP (sur Ethernet) qui peuvent aller et venir dans les routeurs d'équipement dans les locaux d'utilisateur). Le client peut changer son DUID comme spécifié dans la [RFC7844].

La motivation d'avoir plus d'un type de DUID est qu'il doit être unique au monde et doit aussi être facile à générer. La sorte d'identifiant unique au monde facile à générer pour tout appareil peut différer assez largement. Aussi, certains appareils peuvent ne pas contenir de mémorisation persistante. Conserver un DUID généré dans un tel appareil n'est pas possible, de sorte que le schéma de DUID doit s'accommoder de tels appareils.

11.1 Contenu du DUID

Un DUID consiste en un code de type de 2 octets représentés dans ordre des octets du réseau, suivi par un nombre variable d'octets qui constituent l'identifiant réel. La longueur du DUID (non inclus le code de type) fait au moins 1 octet et au plus 128 octets. Les types suivants sont actuellement définis :

Type	Description
1	adresse de couche de liaison plus l'heure
2	identifiant univoque alloué par le fabricant sur la base du numéro d'entreprise
3	adresse de couche de liaison
4	identifiant unique universel (UUID) [RFC6355]

Tableau 2 : Types de DUID

Les formats pour les champs variables du DUID pour les trois premiers types ci-dessus sont montrés ci-dessous. Le quatrième type, DUID-UUID [RFC6355], peut être utilisé dans des situations où un UUID est mémorisé dans les réglages

d'usine de l'appareil.

11.2 DUID fondé sur l'adresse de couche liaison plus l'heure (DUID-LLT)

Ce type de DUID consiste en un champ de type de 2 octets contenant la valeur 1, un code de type de matériel de 2 octets, et 4 octets contenant une valeur d'heure, suivis par l'adresse de couche de liaison de toute interface réseau qui est connectée à l'appareil DHCP au moment où le DUID est généré. La valeur de l'heure est celle de la génération du DUID, représentée en secondes depuis minuit (UTC) le 1er janvier 2000, modulo 2^32. Le type de matériel DOIT être un type de matériel valide alloué par l'IANA ; voir [IANA-HARDWARE-TYPES]. L'heure et le type de matériel sont tous deux mémorisés dans l'ordre des octets du réseau. Pour les types de matériel Ethernet, l'adresse de couche de liaison est mémorisée en forme canonique, comme décrit dans la [RFC2464].

Le diagramme suivant illustre le format d'un DUID-LLT :

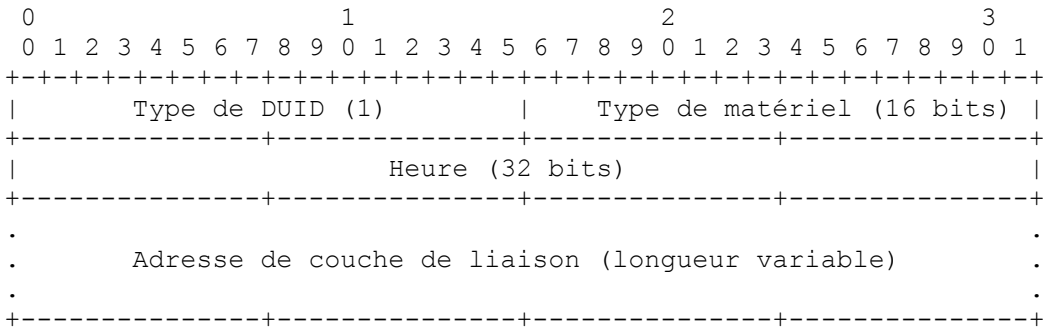


Figure 4 : Format de DUID-LLT

Le choix de l'interface réseau peut être complètement arbitraire, pour autant que l'interface fournisse une adresse de couche de liaison unique au monde pour le type de liaison ; le même DUID-LLT DEVRAIT être utilisé pour configurer toutes les interfaces réseau connectées à l'appareil, sans considération de quelle adresse de couche de liaison de l'interface a été utilisée pour générer le DUID-LLT.

Les clients et les serveurs qui utilisent ce type de DUID DOIVENT mémoriser le DUID-LLT dans une mémorisation stable et DOIVENT continuer d'utiliser ce DUID-LLT même si l'interface réseau utilisée pour générer le DUID-LLT est supprimée. Les clients et les serveurs qui n'ont pas de mémorisation stable NE DOIVENT PAS utiliser ce type de DUID.

Les clients et les serveurs qui utilisent ce DUID DEVRAIENT tenter de configurer l'heure avant de générer le DUID, si c'est possible, et DOIVENT utiliser une sorte de source horaire (par exemple, une horloge en temps réel) pour générer le DUID, même si cette source horaire n'a pas pu être configurée avant de générer le DUID. L'utilisation d'une source horaire rend improbable que deux DUID-LLT identiques soient générés si l'interface réseau est retirée du client et qu'un autre client utilise alors la même interface réseau pour générer un DUID-LLT. Une collision entre deux DUID-LLT est très improbable même si les horloges n'ont pas été configurées avant de générer le DUID.

Cette méthode de génération de DUID est recommandée pour tous les appareils informatiques d'usage général comme les ordinateurs de bureau et les ordinateurs portables, et aussi pour des appareils comme des imprimantes, des routeurs, etc., qui contiennent des formes de mémorisation écrivables non volatiles.

Il est possible que cet algorithme pour générer un DUID puisse résulter en une collision d'identifiants de client. Un client DHCP qui génère un DUID-LLT en utilisant ce mécanisme DOIT fournir une interface administrative qui remplace le DUID existant par un DUID-LLT nouvellement généré.

11.3 DUID alloué par fabricant sur la base du numéro d'entreprise (DUID-EN)

Le fabricant alloue cette forme de DUID à l'appareil. Ce DUID consiste en les 4 octets du numéro d'entrepris privée enregistré du fabricant tel que tenu par l'IANA [IANA-PEN] suivi par un identifiant univoque alloué par le fabricant. Le diagramme suivant résume la structure d'un DUID-EN :

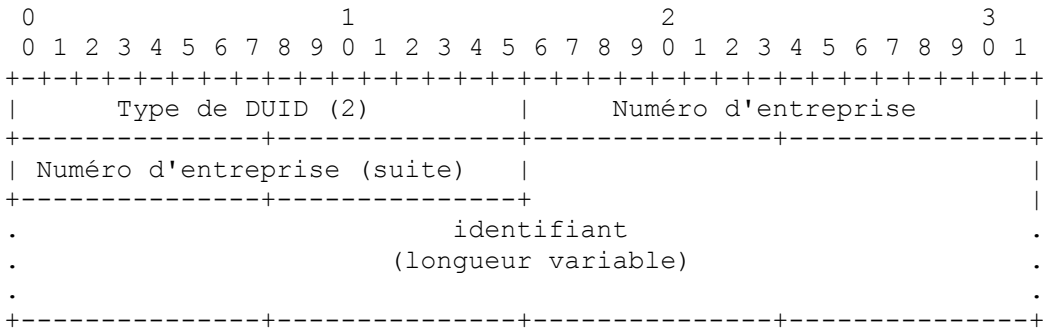


Figure 5 : Format de DUID-EN

La source de l'identifiant est à l'initiative du fabricant qui le définit, mais chaque partie de l'identifiant de chaque DUID-EN DOIT être unique pour l'appareil qui l'utilise, et DOIT être alloué à l'appareil pas plus tard qu'au premier usage, et mémorisé dans une forme non volatile de mémorisation. Cela signifie normalement d'être alloué durant le processus de fabrication dans le cas d'appareils physiques ou, dans le cas de machines virtuelles, quand l'image est créée ou amorcée pour la première fois. Le DUID généré DEVRAIT être enregistré dans une mémorisation non écrasable. Le numéro d'entreprise est le numéro d'entreprise privé enregistré du fabricant comme tenu par l'IANA [IANA-PEN]. Le numéro d'entreprise est mémorisé comme un nombre de 32 bits non signé.

Un exemple de DUID de ce type pourrait ressembler à :

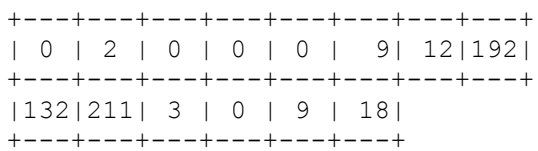


Figure 6 : Exemple de DUID-EN

Cet exemple inclut les deux octets de type de 2 et le numéro d'entreprise (9), suivi par 8 octets de données d'identifiant (0x0CC084D303000912).

11.4 DUID fondé sur l'adresse de couche liaison (DUID-LL)

Ce type de DUID consiste en 2 octets contenant un type de DUID de 3 et un code de type de matériel réseau de 2 octets, suivi par l'adresse de couche de liaison de toute interface réseau qui est connectée de façon permanente à l'appareil client ou serveur. Par exemple, un nœud qui a une interface réseau mise en œuvre dans une puce qui ne peut probablement pas être retirée et utilisée ailleurs pourrait utiliser un DUID-LL. Le type de matériel DOIT être un type valide de matériel alloué par l'IANA ; voir [IANA-HARDWARE-TYPES]. Le type de matériel est mémorisé dans l'ordre des octets du réseau. L'adresse de couche de liaison est mémorisée en forme canonique, comme décrit dans la [RFC2464]. Le diagramme suivant illustre le format d'un DUID-LL :

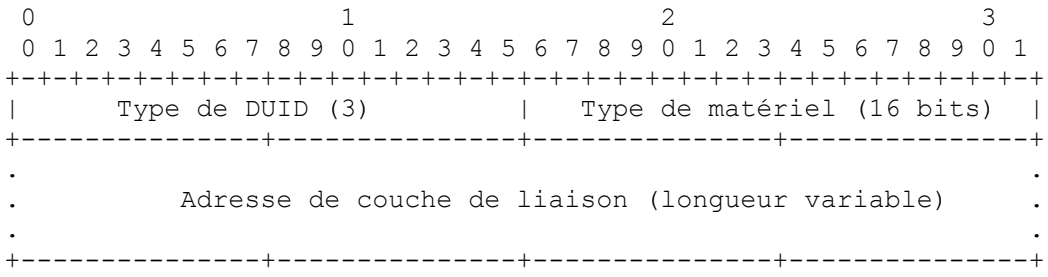


Figure 7 : Format de DUID-LL

Le choix de l'interface réseau peut être complètement arbitraire, pour autant que l'interface fournisse une adresse univoque de couche de liaison et soit rattachée de façon permanente à l'appareil sur lequel le DUID-LL est généré. Le même DUID-LL DEVRAIT être utilisé pour configurer toutes les interfaces réseau connectées à l'appareil, sans considération de

l'adresse de couche de liaison de l'interface qui a été utilisée pour générer le DUID.

Un DUID-LL est recommandé pour les appareils qui ont une interface réseau connectée de façon permanente à une adresse de couche de liaison et n'ont pas une mémorisation écrivable stable non volatile. Un DUID-LL NE DEVRAIT PAS être utilisé par les clients ou les serveurs DHCP qui ne peuvent pas dire si une interface réseau est ou non rattachée de façon permanente à l'appareil sur lequel fonctionne le client DHCP.

11.5 DUID fondé sur un identifiant unique au monde (DUID-UUID)

Ce type de DUID consiste en 16 octets contenant un UUID de 128 bits. La [RFC6355] précise quand utiliser ce type et comment prendre une source appropriée de UUID.

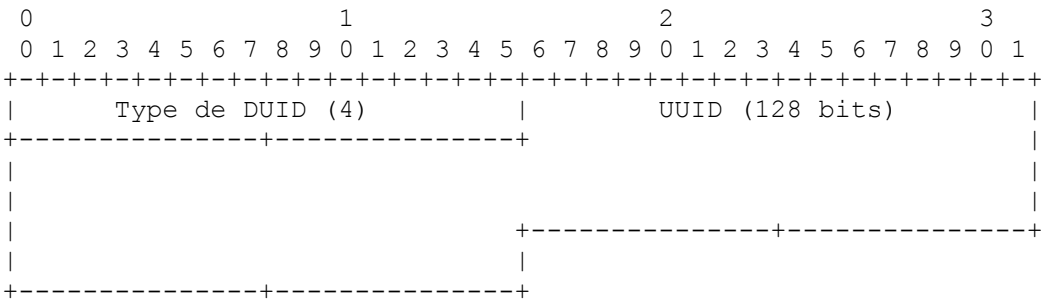


Figure 8 : Format de DUID-UUID

12. Association d'identité

Une association d'identité (IA, *Identity Association*) est une construction par laquelle un serveur et un client peuvent identifier, grouper, et gérer un ensemble d'adresses ou préfixes délégués IPv6 en rapport. Chaque IA consiste en un identifiant d'association d'identité (IAID) et des informations de configuration associées.

L'IAID identifie de façon univoque l'IA et DOIT être choisi comme étant unique parmi les IAID pour ce type d'IA chez le client (par exemple, un IA_NA avec un IAID de 0 et un IA_PD avec un IAID de 0 sont chacun considérés comme uniques). L'IAID est choisi par le client. Pour toute utilisation d'un IA par le client, l'IAID pour cette IA DOIT être cohérent à travers les redémarrages du client DHCP. Le client peut garder la cohérence soit en mémorisant l'IAID dans une mémoire non volatile, soit en utilisant un algorithme qui va régulièrement produire le même IAID tant que la configuration du client ne change pas. Il peut n'y avoir pas de moyen pour un client de garder la cohérence des IAID si il n'a pas de mémoire non volatile et si la configuration de matériel du client change. Si le client utilise seulement un IAID, il peut utiliser une valeur bien connue, par exemple, zéro.

Si le client souhaite obtenir une nouvelle adresse ou préfixe distinct et ne fait plus confiance à l'existant, il envoie un message Release au serveur pour les IA en utilisant l'IAID d'origine. Le client crée alors un nouvel IAID, à utiliser dans les futurs messages pour obtenir des prêts pour la nouvelle IA.

12.1 Associations d'identité pour allocation d'adresse

Un client doit associer au moins une IA distincte avec chacune de ses interfaces réseau pour lesquelles il va demander l'allocation d'adresses IPv6 à un serveur DHCP. Le client utilise les IA allouées à une interface pour obtenir des informations de configuration d'un serveur pour cette interface. Chacune de ces IA doit être associée à exactement une interface.

Les informations de configuration dans une option IA_NA consistent en une ou plusieurs adresses IPv6 avec les valeurs T1 et T2 pour l'IA. Voir au paragraphe 21.4 les détails concernant la représentation d'une IA_NA dans un message DHCP.

Les informations de configuration dans une option IA_TA consistent en une ou plusieurs adresses IPv6. Voir au paragraphe 21.5 les détails concernant la représentation d'une IA_TA dans un message DHCP.

Chaque adresse dans une IA a une durée de vie préférée et une durée de vie valide, comme défini dans la [RFC4862]. Les

durées de vie sont transmises du serveur DHCP au client dans l'option Adresse d'IA (voir au paragraphe 21.6). Les durées de vie s'appliquent à l'utilisation des adresses ; voir au paragraphe 5.5.4 de la [RFC4862].

12.2 Associations d'identité pour délégation de préfixe

Une IA_PD est différente d'une IA pour l'allocation d'adresse en ce qu'elle n'a pas besoin d'être associée à exactement une interface. Une IA_PD peut être associée au client, avec un ensemble d'interfaces, ou avec exactement une interface. Un client configuré pour demander des préfixes délégués doit créer au moins une IA_PD distincte. Il peut associer une IA_PD distincte à chacune de ses interfaces réseau en aval et utiliser cette IA_PD pour obtenir du serveur un préfixe pour cette interface.

Les informations de configuration dans une option IA_PD consistent en un ou plusieurs préfixes avec les valeurs T1 et T2 pour l'IA_PD. Voir au paragraphe 21.21 les détails concernant la représentation d'une IA_PD dans un message DHCP.

Chaque préfixe délégué dans une IA a une durée de vie préférée et une durée de vie valide, comme défini dans la [RFC4862]. Les durées de vie sont transmises du serveur DHCP au client dans l'option Préfixe d'IA (voir au paragraphe 21.22). Les durées de vie s'appliquent à l'utilisation des préfixes délégués ; voir au paragraphe 5.5.4 de la [RFC4862].

13. Allocation à une IA

13.1 Choix des adresses pour l'allocation à une IA_NA

Un serveur choisit les adresses à allouer à une IA_NA en accord avec les politiques d'allocation d'adresses déterminées par l'administrateur du serveur et les informations spécifiques que le serveur détermine au sujet du client à partir d'une combinaison des sources suivantes :

- La liaison à laquelle le client est rattaché. Le serveur détermine la liaison comme suit :
  * Si le serveur reçoit le message directement du client et si l'adresse de source dans le datagramme IP dans lequel le message a été reçu est une adresse de liaison locale, le client est alors sur la même liaison que celle à laquelle est rattachée l'interface sur laquelle le message a été reçu.
  * Si le serveur reçoit le message d'un agent de relais transmetteur, le client est alors sur la même liaison que celle à laquelle l'interface, identifiée par le champ Adresse de liaison dans le message provenant de l'agent de relais, est rattachée. Selon la [RFC6221], le serveur DOIT ignorer tout champ Adresse de liaison dont la valeur est zéro. L'adresse de liaison dans ce cas peut venir de tout message Relay-forward encapsulé dans le Relay-forward reçu, et en général le plus encapsulé (le plus proche du Relay-forward pour le client) a la valeur la plus utile.
  * Si le serveur reçoit le message directement du client et si l'adresse de source dans le datagramme IP dans lequel le message a été reçu n'est pas une adresse de liaison locale, le client est alors sur la liaison identifiée par l'adresse de source dans le datagramme IP (noter que cette situation ne peut se produire que si le serveur a activé l'utilisation de la livraison de message en envoi individuel par le client et que le client a envoyé un message pour lequel la livraison en envoi individuel est permise).

- Le DUID fourni par le client.

- D'autres informations dans les options fournies par le client, par exemple, des options Adresse IA (paragraphe 21.6) qui incluent des demandes du client pour des adresses spécifiques.

- D'autres informations dans des options fournies par l'agent de relais.

Par défaut, les mises en œuvre de serveur DHCP NE DEVRAIENT PAS générer des adresses prévisibles (voir au paragraphe 4.7 de la [RFC7721]). Les mises en œuvre de serveurs sont encouragées à revoir les [RFC4941], [RFC7824], et [RFC7707] sur de possibles considérations sur comment générer des adresses.

Un serveur NE DOIT PAS allouer une adresse qui est par ailleurs réservée pour un autre objet. Par exemple, un serveur NE DOIT PAS allouer une adresse qui utilise un identifiant d'interface IPv6 réservé [RFC5453], [RFC7136], [IANA-RESERVED-IID].

Voir dans la [RFC7969] un exposé plus détaillé de la façon dont les serveurs déterminent la localisation d'un client sur le réseau.

13.2 Allocation d'adresses temporaires

Un client peut demander l'allocation d'adresses temporaires (voir dans la [RFC4941] la définition des adresses temporaires). Le traitement par DHCP des allocations d'adresses n'est pas différent pour les adresses temporaires.

Les clients demandent des adresses temporaires, et les serveurs les leur alloent. Les adresses temporaires sont portées dans l'option IA_TA (voir au paragraphe 21.5). Chaque option IA_TA contient normalement au moins une adresse temporaire pour chacun des préfixes sur la liaison à laquelle le client est rattaché.

La durée de vie de l'adresse temporaire allouée est réglée dans l'option Adresse d'IA (voir au paragraphe 21.6) encapsulée dans l'option IA_TA. Il est RECOMMANDÉ d'établir de courtes durées de vie, normalement plus courtes que TEMP_VALID_LIFETIME et TEMP_PREFERRED_LIFETIME (voir la Section 5 de la [RFC4941]).

Une mise en œuvre de serveur DHCP PEUT générer des adresses temporaires, en se référant à l'algorithme défini au paragraphe 3.2.1 de la [RFC4941], avec la condition supplémentaire que toute nouvelle adresse ne soit pas la même que toute adresse allouée

Le serveur PEUT mettre à jour le DNS pour une adresse temporaire, comme décrit à la Section 4 de la [RFC4941].

Chez les clients, par défaut, les adresses temporaires sont préférées dans le choix d'adresse de source, conformément à la règle 7 de la Section 5 de la [RFC6724]. Cependant, cette politique peut être outrepassée.

Une des propriétés les plus importantes d'une adresse temporaire est de rendre difficile de lier l'adresse à différentes actions au fil du temps. Donc, il N'EST PAS RECOMMANDÉ qu'un client renouvelle les adresses temporaires, bien que DHCP fournisse une telle possibilité (voir au paragraphe 21.5).

13.3 Allocation de préfixes pour IA_PD

Le mécanisme par lequel le serveur choisit un ou des préfixes pour les déléguer n'est pas spécifié dans le présent document. Des exemples de façons dont le serveur pourrait choisir des préfixes pour un client incluent des allocations statiques fondées sur l'abonnement à un FAI, une allocation dynamique à partir d'un réservoir de préfixes disponibles, et un choix fondé sur une autorité externe comme un serveur RADIUS utilisant l'option Framed-IPv6-Prefix comme décrit dans la [RFC3162].

14. Transmission de messages par un client

Sauf autrement spécifié dans le présent document ou dans un document qui décrit comment IPv6 est porté sur un type spécifique de liaison (pour les types de liaisons qui ne prennent pas en charge la diffusion groupée) un client envoie les messages DHCP à l'adresse de diffusion groupée Tous_Agents_de_Relais et_Serveurs_DHCP.

Les serveurs DHCP NE DEVRAIENT PAS vérifier si l'adresse de couche 2 utilisée était ou non de diffusion groupée, pour autant que l'adresse de couche 3 est correcte.

Un client utilise la diffusion groupée pour joindre tous les serveurs ou un serveur individuel. Un serveur individuel est indiqué en spécifiant le DUID du serveur dans une option Identifiant de serveur (voir au paragraphe 21.3) dans le message du client. (Tous les serveurs vont recevoir ce message, mais seul le serveur indiqué va répondre.) Tous les serveurs sont indiqués quand cette option n'est pas fournie.

Un client peut envoyer des messages directement à un serveur en utilisant l'envoi individuel, comme décrit au paragraphe 21.12.

14.1 Limitation de taux

Afin d'éviter des salves prolongées de messages qui peuvent être causées par de possibles boucles logiques, un client DHCP DOIT limiter le taux de messages DHCP qu'il transmet ou retransmet. Un exemple est qu'un client obtient une adresse ou préfixe délégué mais n'aime pas la réponse, donc il revient à la procédure Solicit, découvre le même (le seul) serveur, demande une adresse ou préfixe délégué, et obtient la même adresse ou préfixe délégué que précédemment (car le serveur avait alloué ce prêt demandé précédemment à ce client). Cette boucle peut se répéter indéfiniment si il n'y a pas un

mécanisme d'abandon/arrêt. Donc, un client ne doit pas initier des transmissions trop fréquemment.

Une méthode recommandée pour mettre en œuvre la fonction de limitation de taux est un baquet de jetons (voir l'Appendice A de la [RFC3290]) limitant le taux moyen de transmission à un certain nombre dans un certain intervalle de temps. Cette méthode d'encadrement de la sporadicité garantit aussi que le taux de transmission à long terme ne sera pas dépassé.

Une limite du taux de transmission DEVRAIT être configurable. Elle pourrait par défaut être de 20 paquets en 20 secondes.

Pour un appareil qui a plusieurs interfaces, la limite DOIT être appliquée par interface.

La limitation en taux des messages DHCP transmis et des messages côté serveur sort du domaine d'application de la présente spécification.

14.2 Comportement du client quand T1 et/ou T2 sont 0

Dans certains cas, les valeurs T1 et/ou T2 peuvent être réglées à 0. Actuellement, il y a trois cas :
1. un client a reçu une option IA_NA (voir au paragraphe 21.4) avec une valeur de zéro ;
2. un client a reçu une option IA_PD (voir au paragraphe 21.21) avec une valeur de zéro ;
3. un client a reçu une option IA_TA (voir au paragraphe 21.5) (qui ne contient pas de champ T1 et T2 et ces prêts ne sont généralement pas renouvelés).

C'est une indication que les heures de renouvellement et de réinitialisation sont laissées à la discrétion du client. Cependant, elles ne sont pas complètement discrétionnaires.

Quand les valeurs T1 et/ou T2 sont réglées à 0, le client DOIT choisir un moment pour éviter les tempêtes de paquets. En particulier, il NE DOIT PAS transmettre immédiatement. Si le client a reçu plusieurs options IA, il DEVRAIT prendre les heures de transmission de renouvellement et/ou réinitialisation de telle façon que toutes les options IA soient traitées en un échange, si possible. Le client DOIT choisir de heures de renouvellement et réinitialisation qui ne violent pas les restrictions de limitation de taux définies au paragraphe 14.1.

15. Fiabilité des échanges de messages initiés par le client

Les clients DHCP sont responsables de la livraison fiable des messages dans les échanges de messages initiés par le client décrits à la Section 18. Si un client DHCP manque à recevoir une réponse attendue d'un serveur, le client doit retransmettre son message conformément à la stratégie de retransmission décrite dans cette section.

Noter que la procédure décrite dans cette section est légèrement modifiée quand elle est utilisé avec le message Solicit. La procédure modifiée est décrite au paragraphe 18.2.1.

Le client commence l'échange de messages en transmettant un message au serveur. L'échange de messages se termine quand (1) le client reçoit la ou les réponses appropriées d'un ou des serveurs ou (2) l'échange de messages est considéré avoir échoué conformément au mécanisme de retransmission décrit ci-dessous.

Le client DOIT mettre à jour une valeur de "temps écoulé" au sein d'une option Temps écoulé (voir au paragraphe 21.9) dans le message retransmis. Dans certains cas, le client peut aussi avoir besoin de modifier les valeurs dans les options Adresse d'IA (voir au paragraphe 21.6) ou les options Préfixe d'IA (voir au paragraphe 21.22) si une durée de vie valide pour un des prêts du client arrive à expiration avant la retransmission. Donc, chaque fois que le présent document se réfère à une "retransmission" d'un message de client, il se réfère à la fois à la modification du message original et à l'envoi de cette nouvelle instance de message au serveur.

Le comportement de retransmission du client est contrôlé et décrit par les variables suivantes :

RT *(Retransmission timeout)* temporisation de retransmission
IRT *(Initial retransmission time)* heure de retransmission initiale
MRC *(Maximum retransmission count)* compte de retransmission maximum
MRT *(Maximum retransmission time)* temps de retransmission maximum
MRD *(Maximum retransmission duration)* durée de retransmission maximum
RAND *(Randomization factor)* facteur d'aléation

Les valeurs spécifique de chacun de ces paramètres relevant des divers messages sont données dans les sous paragraphes du paragraphe 18.2, en utilisant les valeurs définie au Tableau 1 du paragraphe 7.6. L'algorithme pour RAND est commun à toutes les transmissions de messages.

Avec chaque transmission ou retransmission de message, le client règle RT conformément aux règles données ci-dessous. Si RT expire avant la fin de l'échange de messages, le client recalcule RT et retransmet le message.

Chacun des calculs d'une nouvelle RT inclut un facteur d'aléation (RAND) qui est un nombre aléatoire choisi avec une distribution uniforme entre -0,1 et +0,1. Le facteur d'aléation est inclus pour minimiser la synchronisation des messages transmis par les clients DHCP.

L'algorithme de choix d'un nombre aléatoire n'a pas besoin d'être cryptographiquement fondé. L'algorithme DEVRAIT produire une séquence différente de nombres aléatoires à chaque invocation du client DHCP.

La RT pour la première transmission de message est fondée sur IRT : RT = IRT + RAND*IRT

La RT pour chaque transmission de message suivante est fondée sur la précédente valeur de RT : RT = 2*RTprev + RAND*RTprev

MRT spécifie une limite supérieure à la valeur de RT (sans tenir compte du facteur d'aléation ajouté par l'utilisation de RAND). Si MRT a une valeur de 0, il n'y a pas de limite supérieure à la valeur de RT. Autrement :

si (RT > MRT) : RT = MRT + RAND*MRT

MRC spécifie une limite supérieure au nombre de fois qu'un client peut retransmettre un message. Sauf si MRC est zéro, l'échange de messages échoue une fois que le client a transmis le message MRC fois.

MRD spécifie une limite supérieure à la durée pendant laquelle un client peut retransmettre un message. Sauf si MRD est zéro, l'échange de messages échoue une fois que MRD secondes se sont écoulées depuis la première transmission du message par le client.

Si MRC et MRD sont tous deux non à zéro, l'échange de messages échoue chaque fois qu'une des conditions spécifiées aux deux alinéas précédents est satisfaite.

Si MRC et MRD sont tous deux à zéro, le client continue de transmettre message jusqu'à ce qu'il reçoive une réponse.

Un client n'est pas supposé écouter pour une réponse durant la période RT entière et peut désactiver les capacités d'écoute après avoir attendu au moins le plus court de RT et MAX_WAIT_TIME à cause d'économies d'énergie ou autre raison. Bien sûr, un client DOIT écouter pour un Reconfigure si il a négocié son utilisation avec le serveur.

16. Validation du message

Cette Section décrit quelles options sont valides dans quels types de messages et explique que faire quand un client ou serveur reçoit un message qui contient des options connues invalides pour ce message. Par exemple, une option IA n'est pas autorisée à apparaître dans un message Demande d'information.

Les clients et les serveurs PEUVENT choisir soit (1) d'extraire les informations d'un tel message si elles sont utiles au receveur, soit (2) d'ignorer complètement un tel message et de juste l'éliminer.

Si un serveur reçoit un message qu'il considère invalide, il PEUT envoyer un message Réponse (ou Annonce, comme approprié) avec une option Identifiant de serveur (paragraphe 21.3) une option Identifiant de client (paragraphe 21.2) (si il en était une incluse dans le message) et une option Code d'état (paragraphe 21.13) avec l'état 1.

Les clients, agents de relais, et les serveurs NE DOIVENT PAS éliminer les messages qui contiennent des options inconnues (ou des instances d'options de fabricant avec des valeurs de numéro d'entreprise inconnues). Elles devraient être ignorées comme si elles n'étaient pas présentes. Ceci est critique pour prévoir de futures extensions de DHCP.

Un serveur DOIT éliminer tout message Solicit, Confirm, Rebind, ou Information-request qu'il reçoit avec une adresse de

destination en envoi individuel de couche 3.

Un client ou serveur DOIT éliminer tout message DHCP reçu avec un type de message inconnu.

16.1 Utilisation des identifiants de transaction

Le champ "Identifiant de transaction" contient une valeur utilisée par les clients et les serveurs pour synchroniser les réponses du serveur aux messages du client. Un client DEVRAIT générer un nombre aléatoire qui ne puisse pas être deviné ou prédit facilement pour l'utiliser comme identifiant de transaction pour chaque nouveau message qu'il envoie. Noter que si un client génère des identifiants de transaction facilement prévisibles, il peut devenir plus vulnérable à certaines formes d'attaques de la part d'intrus. Un client DOIT laisser l'identifiant de transaction inchangé dans les retransmissions d'un message.

16.2 Message Solicit

Les clients DOIVENT éliminer tout message Solicit reçu.

Les serveurs DOIVENT éliminer tout message Solicit qui ne comporte pas d'option Identifiant de client ou qui comporte une option Identifiant de serveur.

16.3 Message Advertise

Les clients DOIVENT éliminer tout message Advertise reçu qui satisfait une des conditions suivantes :
- le message n'inclut pas d'option Identifiant de serveur (paragraphe 21.3).
- le message n'inclut pas d'option Identifiant de client (paragraphe 21.2).
- le contenu de l'option Identifiant de client ne correspond pas au DUID du client.
- la valeur du champ "Identifiant de transaction" ne correspond pas à la valeur que le client a utilisée dans son message Solicit.

Les serveurs et agents de relais DOIVENT éliminer tout message Advertise reçu.

16.4 Message Request

Les clients DOIVENT éliminer tout message Request reçu.

Les serveurs DOIVENT éliminer tout message Request reçu qui satisfait une des conditions suivantes :
- le message n'inclut pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le contenu de l'option Identifiant de serveur ne correspond pas au DUID du serveur.
- le message n'inclut pas d'option Identifiant de client (voir au paragraphe 21.2).

16.5 Message Confirm

Les clients DOIVENT éliminer tout message Confirm reçu.

Les serveurs DOIVENT éliminer tout message Confirm reçu qui ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2) ou qui comporte une option Identifiant de serveur (voir au paragraphe 21.3).

16.6 Message Renew

Les clients DOIVENT éliminer tout message Renew reçu.

Les serveurs DOIVENT éliminer tout message Renew reçu qui satisfait une des conditions suivantes :
- le message n'inclut pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le contenu de l'option Identifiant de serveur ne correspond pas à l'identifiant du serveur.
- le message ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2).

16.7 Message Rebind

Les clients DOIVENT éliminer tout message Rebind reçu.

Les serveurs DOIVENT éliminer tout message Rebind reçu qui ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2) ou qui comporte une option Identifiant de serveur (voir au paragraphe 21.3).

16.8 Message Decline

Les clients DOIVENT éliminer tout message Decline reçu.

Les serveurs DOIVENT éliminer tout message Decline reçu qui satisfait une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le contenu de l'option Identifiant de serveur ne correspond pas à l'identifiant du serveur.
- le message ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2).

16.9 Message Release

Les clients DOIVENT éliminer tout message Release reçu.

Les serveurs DOIVENT éliminer tout message Release reçu qui satisfait à une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le contenu de l'option Identifiant de serveur ne correspond pas à l'identifiant du serveur.
- le message ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2).

16.10 Message Reply

Les clients DOIVENT éliminer tout message Reply reçu qui satisfait à une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le champ "Identifiant de transaction" dans le message ne correspond pas à la valeur utilisée dans le message original.

Si le client a inclus une option Identifiant de client (voir au paragraphe 21.2) dans le message original, le message Reply DOIT inclure une option Identifiant de client, et le contenu de l'option Identifiant de client DOIT correspondre au DUID du client. Si le client n'a pas inclus d'option Identifiant de client dans le message original, le message Reply NE DOIT PAS inclure d'option Identifiant de client.

Les serveurs et agents de relais DOIVENT éliminer tout message Reply reçu.

16.11 Message Reconfigure

Les serveurs et agents de relais DOIVENT éliminer tout message Reconfigure reçu.

Les clients DOIVENT éliminer tout message Reconfigure qui satisfait à une des conditions suivantes :
- le message n'est pas en envoi individuel au client.
- le message ne comporte pas d'option Identifiant de serveur (voir au paragraphe 21.3).
- le message ne comporte pas d'option Identifiant de client (voir au paragraphe 21.2) qui contienne le DUID du client.
- le message ne comporte pas d'option Reconfiguration de message (voir au paragraphe 21.19).
- le type de message d'option Reconfiguration de message n'est pas une valeur valide.
- le message ne comporte pas d'authentification (comme RKAP ; voir au paragraphe 20.4) ou échoue à la validation d'authentification.

16.12 Message Demande d'informations

Les clients DOIVENT éliminer tout message Demande d'informations reçu.

Les serveurs DOIVENT éliminer tout message Demande d'informations reçu qui satisfait à une des conditions suivantes :
- le message comporte une option Identifiant de serveur (voir au paragraphe 21.3) et le DUID dans l'option ne correspond pas au DUID du serveur.

- le message comporte une option IA.

16.13 Message Relay-forward

Les clients DOIVENT éliminer tout message Relay-forward reçu.

16.14 Message Relay-reply

Les clients et les serveurs DOIVENT éliminer tout message Relay-reply reçu.

17. Choix de l'adresse de source et de l'interface par le client

Le comportement du client concernant le choix de l'interface est différent selon l'objet de la configuration.

17.1 Choix de l'adresse de source et de l'interface pour l'allocation d'adresse

Quand un client envoie un message DHCP à l'adresse de diffusion groupée Tous_Agents_De_Relais_Et_Serveurs_DHCP, il DEVRAIT envoyer le message à travers l'interface pour laquelle les informations de configuration (incluant les adresses) sont demandées. Cependant, le client PEUT envoyer le message à travers une autre interface si l'interface pour laquelle la configuration est demandée est une interface logique dans la liaison de rattachement direct ou si le client est certain que deux interfaces sont rattachées à la même liaison.

Quand un client envoie un message DHCP directement à un serveur en utilisant l'envoi individuel (après avoir reçu l'option Serveur en envoi individuel (paragraphe 21.12) de ce serveur) l'adresse de source dans l'en-tête du datagramme IPv6 DOIT être une adresse allouée à l'interface pour laquelle le client est intéressé à obtenir la configuration et qui convient à l'utilisation par le serveur pour répondre au client.

17.2 Choix de l'adresse de source et de l'interface pour la délégation de préfixe

Les préfixes délégués ne sont pas associés à une interface particulière de la même façon que les adresses le sont pour l'allocation d'adresse comme mentionné au paragraphe 17.1.

Quand un client envoie un message DHCP pour une délégation de préfixe, il DEVRAIT être envoyé sur l'interface associée au routeur en amont (normalement connecté au réseau d'un FAI) ; voir la [RFC7084]. L'interface amont est normalement déterminée par configuration. Cette règle s'applique même dans le cas où une IA_PD séparée est utilisée pour chaque interface en aval.

Quand un client envoie un message DHCP directement à un serveur en utilisant l'envoi individuel (après avoir reçu l'option Serveur en envoi individuel (voir au paragraphe 21.12) de ce serveur) l'adresse de source DEVRAIT être une adresse qui provient de l'interface en amont et qui convient pour l'utilisation par le serveur pour répondre au client.

18. Échanges de configuration DHCP

Un client initie un échange de messages avec un ou des serveurs pour acquérir ou mettre à jour les informations de configuration qui l'intéressent. Un client a de nombreuses raisons pour initier l'échange de configuration. Les plus courantes sont :

1. au titre du processus de configuration/amorçage du système d'exploitation,
2. quand il lui est demandé de le faire par la couche application (à travers une API spécifique du système d'exploitation),
3. quand une annonce de routeur indique que DHCPv6 est disponible pour la configuration d'adresse (voir au paragraphe 4.2 de la [RFC4861]),
4. comme nécessaire pour étendre la durée de vie de la ou des adresses et/ou préfixes délégués, en utilisant les messages Renew et Rebind, ou
5. à réception d'un message Reconfigure, quand il lui est demandé de le faire par un serveur.

Le client est chargé de créer les IA et de demander qu'un serveur alloue des adresses et/ou préfixes délégués aux IA. Le

client crée d'abord les IA et leur alloue les IAID. Le client transmet ensuite un message Solicit contenant les options d'IA qui décrivent les IA. Le client NE DOIT PAS être en train d'utiliser une des adresses ou un des préfixes délégués pour lesquels il essaye d'obtenir les liens par l'envoi du message Solicit. En particulier, si le client a des liens valides et a choisi de commencer le processus de découverte de serveur pour obtenir les mêmes liens à partir d'un serveur différent, le client DOIT arrêter d'utiliser les adresses et préfixes délégués pour les liens qu'il a obtenus du précédent serveur (voir au paragraphe 18.2.7 plus de détails sur ce que "arrêter d'utiliser" signifie dans ce contexte) et qu'il essaye maintenant d'obtenir d'un nouveau serveur.

Un client DHCP qui n'a pas besoin qu'un serveur DHCP lui alloue des adresses IP ou préfixes délégués peut obtenir des informations de configuration comme une liste de serveurs DNS disponibles [RFC3646] ou de serveurs NTP [RFC5908] par un seul échange de message et réponse avec un serveur DHCP. Pour obtenir des informations de configuration, le client envoie d'abord un message Demande d'information (voir au paragraphe 18.2.6) à l'adresse de diffusion groupée Tous_Agents_de_Relais_et_Serveurs_DHCP. Les serveurs répondent par un message Reply contenant les informations de configuration pour le client (voir au paragraphe 18.3.6).

Pour demander l'allocation d'une ou plusieurs adresses ou préfixes délégués, un client localise d'abord un serveur DHCP et demande ensuite l'allocation des adresses/préfixes et autres informations de configuration au serveur. Le client fait cela en envoyant le message Solicit (paragraphe 18.2.1) à l'adresse de diffusion groupée Tous_Agents_de_Relais_et_Serveurs _DHCP et en collectant les messages Advertise provenant des serveurs qui répondent au message du client ; le client choisit alors un serveur dont il veut obtenir les informations de configuration. Ce processus est appelé la découverte de serveur. Quand le client a choisi le serveur, il envoie un message Request à ce serveur comme décrit au paragraphe 18.2.2.

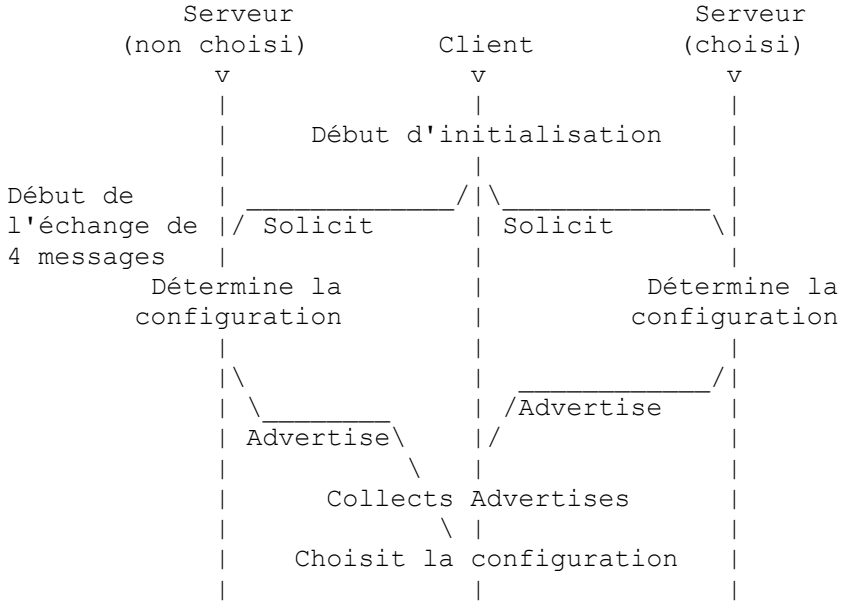
Un client qui veut effectuer l'échange de messages Solicit/Reply décrit au paragraphe 18.2.1 inclut une option Rapid Commit *(engagement rapide)* (voir au paragraphe 21.14) dans son message Solicit.

Les serveurs qui peuvent allouer des adresses ou préfixes délégués aux IA répondent au client par un message Advertise ou un message Reply si le client a inclus une option Rapid Commit et si le serveur est configuré à l'accepter.

Si le serveur répond par un message Advertise, le client initie un échange de configuration comme décrit au paragraphe 18.2.2.

Un serveur peut initier un échange de messages avec un client en envoyant un message Reconfigure pour causer l'envoi par le client d'un message Renew, Rebind, ou Demande d'information pour rafraîchir ses informations de configuration aussitôt que le message Reconfigure est reçu par le client.

La Figure 9 montre un diagramme de la succession dans le temps des messages échangés entre un client et deux serveurs pour le cycle de vie typique d'un ou plusieurs prêts. Cela commence par l'échange de quatre messages Solicit/Advertise/Request/Reply pour obtenir le ou les prêts, suivi par un échange des deux messages Renew/Reply pour étendre la durée de vie du ou des prêts, et se termine ensuite par un échange de deux messages Release/Reply pour terminer l'utilisation du prêt par le client.



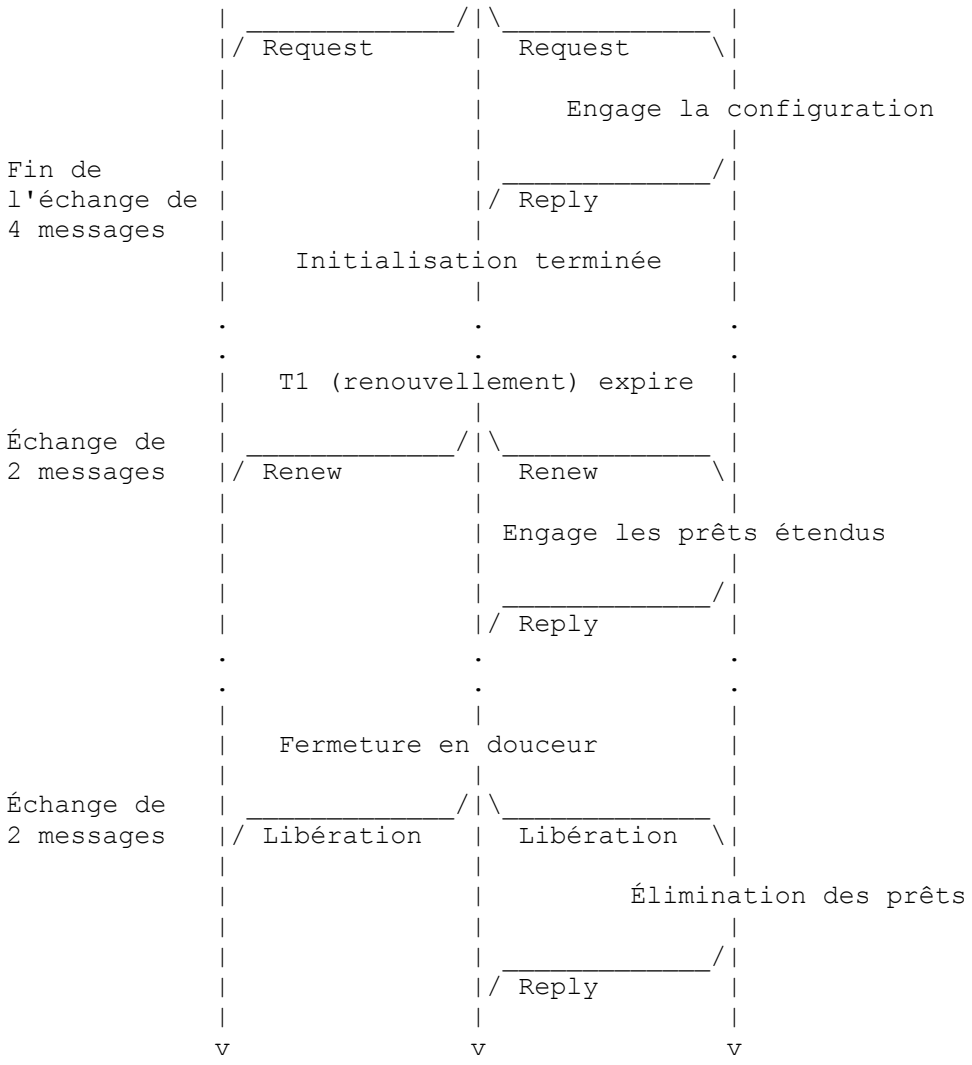


Figure 9 : Diagramme des messages échangés entre un client et deux serveurs pour le cycle de vie normal d'un ou plusieurs prêts

18.1 Un seul échange pour plusieurs options d'IA

Le présent document suppose qu'un client DEVRAIT utiliser une seule transaction pour toutes les options d'IA requises sur une interface ; cela simplifie la mise en œuvre de client et réduit le nombre potentiel de transactions nécessaires (pour les fondements de ce choix de conception, se reporter à la Section 4 de la [RFC7550]). Pour faciliter l'utilisation par un client d'une seule transaction pour toutes les options d'IA, les serveurs DOIVENT retourner les mêmes valeurs de T1/T2 pour toutes les options d'IA dans une Reply (voir les paragraphes 18.3.2, 18.3.4, et 18.3.5) afin que le client génère une seule transaction quand il renouvelle ou réinitialise ses prêts. Cependant, parce que certains serveurs ne peuvent pas encore se conformer à cette exigence, un client DOIT être prêt à choisir des temps T1/T2 appropriés comme décrit au paragraphe 18.2.4.

18.2 Comportement du client

Un client utilise le message Solicit pour découvrir les serveurs DHCP configurés pour allouer des prêts ou retourner d'autres paramètres de configuration sur la liaison à laquelle le client est rattaché.

Un client utilise les messages Request, Renew, Rebind, Release, et Decline durant le cycle de vie normal des adresses et préfixes délégués.

Quand un client détecte qu'il peut s'être déplacé sur une nouvelle liaison, il utilise Confirm si il a seulement des adresses et Rebind si il a des préfixes délégués (et des adresses). Il utilise les messages Demande d'information quand il a besoin

d'informations de configuration mais pas d'adresses ni de préfixes.

Quand un client demande plusieurs types d'option d'IA ou plusieurs instances des mêmes types d'IA dans un message Solicit, Request, Renew, ou Rebind, il est possible que le ou les serveurs disponibles puissent seulement être configurés à en offrir un sous ensemble. Quand c'est possible, le client DEVRAIT utiliser la meilleure configuration disponible et continuer de demander les IA supplémentaires dans les messages suivants. Cela permet au client de conserver une seule session et automate à états. En pratique, en particulier dans le cas du traitement des demandes IA_NA et IA_PD [RFC7084], cette situation devrait être rare ou le résultat d'une erreur de fonctionnement temporaire. Donc, il est plus probable que le client va obtenir toute la configuration si il continue, dans chaque échange de configuration suivant, de demander toutes les informations de configuration qu'il est programmé à essayer d'obtenir, incluant toute option de configuration à état pleins pour laquelle aucun résultat n'a été retourné dans les précédents échanges de messages.

À réception d'un message Reconfigure du serveur, un client répond par un message Renew, Rebind, ou Demande d'information comme indiqué par l'option Reconfiguration de message (voir au paragraphe 21.19). Le client DEVRAIT être soupçonneux sur le message Reconfigure (il pourrait être un faux) et il NE DOIT PAS abandonner des ressources qu'il pourrait avoir déjà obtenues. Le client DEVRAIT traiter le message Reconfigure comme si le temporisateur T1 avait expiré. Le client va attendre que le serveur envoie les IA et/ou autres informations de configuration au client dans un message Reply.

Si le client a une adresse de source de portée suffisante qui peut être utilisée par le serveur comme adresse de retour et si le client a reçu du serveur une option Envoi individuel de serveur (voir au paragraphe 21.12) le client DEVRAIT envoyer tout message Request, Renew, Release, et Decline en envoi individuel au serveur.

L'utilisation de l'envoi individuel peut éviter des délais dus au relais des messages par les agents de relais, ainsi qu'éviter de surcharger les serveurs avec la livraison des messages du client à plusieurs serveurs. Cependant, exiger du client qu'il relaye tous les messages DHCP à travers un agent de relais permet l'inclusion des options d'agent de relais dans tous les messages envoyés par le client. Le serveur devrait ne permettre l'utilisation de l'envoi individuel que quand les options d'agent de relais ne vont pas être utilisées.

18.2.1 Création et transmission des messages Solicit

Le client règle le champ "type de message" à SOLICIT. Le client génère un identifiant de transaction et insère sa valeur dans le champ "Identifiant de transaction".

Le client DOIT inclure une option Identifiant de client (voir au paragraphe 21.2) pour s'identifier auprès du serveur. Le client inclut des options d'IA pour toutes les IA auxquelles il veut que le serveur alloue des prêts.

Le client DOIT inclure un option Temps écoulé (voir au paragraphe 21.9) pour indiquer pendant combien de temps le client a essayé d'achever l'échange de messages DHCP en cours.

Le client utilise des options IA_NA (voir au paragraphe 21.4) pour demander l'allocation d'adresses non temporaires, des options IA_TA (voir au paragraphe 21.5) pour demander l'allocation d'adresses temporaires, et des options IA_PD (voir au paragraphe 21.21) pour demander une délégation de préfixe. Les options IA_NA, IA_TA, ou IA_PD, ou une combinaison de toutes, peuvent être incluses dans les messages DHCP. De plus, plusieurs instances de tout type d'option d'IA peuvent être incluses.

Le client PEUT inclure des adresses dans les options Adresse d'IA (voir au paragraphe 21.6) encapsulées dans les options IA_NA et IA_TA comme indication au serveur sur les adresses pour lesquelles le client a une préférence.

Le client PEUT inclure des valeurs dans des options Préfixe d'IA (voir au paragraphe 21.22) encapsulées dans les options IA_PD comme indication sur le préfixe délégué et/ou la longueur de préfixe pour qui le client a une préference. Voir au paragraphe 18.2.4 les indications de longueur de préfixes.

Le client DOIT inclure une option Demande d'option (ORO) (voir au paragraphe 21.7) pour demander l'option SOL_MAX_RT (voir au paragraphe 21.24) et toute autre options que le client est intéressé à recevoir. Le client PEUT de plus inclure des instances de ces options qui sont identifiées dans l'option Demande d'option, avec des valeurs de données comme indication au serveur sur les valeurs de paramètres que le client aimerait voir retournées.

Le client inclut une option Accepte Reconfigure (voir au paragraphe 21.20) si il veut accepter les messages Reconfigure provenant du serveur.

Le client NE DOIT PAS inclure d'autre option dans le message Solicit, sauf si spécifiquement permis dans la définition des options individuelles.

Le premier message Solicit du client sur l'interface DEVRAIT être retardé d'un délai aléatoire entre 0 et SOL_MAX_DELAY. Ce délai aléatoire aide à désynchroniser les clients qui commencent une session DHCP au même moment, comme après une récupération d'une panne de courant ou après une panne de routeur, ayant vu que DHCP est disponible dans des messages Annonce de routeur (voir au paragraphe 4.2 de la [RFC4861]).

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : SOL_TIMEOUT
MRT : SOL_MAX_RT
MRC : 0
MRD : 0

Un client qui souhaite utiliser l'échange de deux messages Engagement rapide inclut une option Rapid Commit (voir au paragraphe 21.14) dans son message Solicit. Le client peut recevoir un certain nombre de différentes réponses de différents serveurs. Le client va prendre note de tous les messages Advertise valides qu'il reçoit. Le client va éliminer tous les messages Reply qui ne contiennent pas l'option Rapid Commit.

À réception d'une réponse valide avec l'option Rapid Commit, le client traite le message comme décrit au paragraphe 18.2.10.

À la fin de la première période de RT, si aucun message Reply convenable n'est reçu mais si le client a des messages Advertise valides, il traite alors le Advertise comme décrit au paragraphe 18.2.9.

Si le client reçoit ensuite un message Reply valide qui inclut une option Rapid Commit, il fait une des choses suivantes :

- il traite le message Reply comme décrit au paragraphe 18.2.10 et élimine tout message Reply reçu en réponse au message Request
- il traite tout message Reply reçu en réponse au message Request et élimine le message Reply qui inclut l'option Rapid Commit.

Si le client attend un message Advertise, le mécanisme décrit à la Section 15 est modifié comme suit pour la transmission des messages Solicit. L'échange de messages n'est pas terminé par la réception d'un Advertise avant l'écoulement du premier RT. Le client collecte plutôt les messages Advertise valides jusqu'à l'écoulement du premier RT. Aussi, le premier RT DOIT être choisi comme étant strictement supérieur à l'IRT en choisissant RAND comme strictement supérieur à 0.

Un client DOIT collecter les messages Advertise valides pendant les RT premières secondes, sauf si il reçoit un message Advertise valide avec une valeur de préférence de 255. La valeur de préférence est portée dans l'option Préférence (voir au paragraphe 21.8). Tout Advertise valide qui ne comporte pas d'option Préférence est considéré comme ayant une valeur de préférence de 0. Si le client reçoit un message Advertise valide qui comporte une option Préférence avec une valeur de préférence de 255, le client commence immédiatement un échange de messages initié par le client (comme décrit au paragraphe 18.2.2) en envoyant un message Request au serveur de qui le message Advertise a été reçu. Si le client reçoit un message Advertise valide qui ne comporte pas d'option Préférence avec une valeur de préférence de 255, il continue d'attendre jusqu'à l'écoulement du premier RT. Si le premier RT s'écoule et que le client a reçu un message Advertise valide, le client DEVRAIT continuer avec un échange de messages initié par le client en envoyant un message Request.

Si le client ne reçoit pas de message Advertise valide avant l'écoulement du premier RT, il applique alors le mécanisme de retransmission décrit à la Section 15. Le client termine le processus de retransmission aussitôt qu'il reçoit un message Advertise valide, et le client agit sur le message Advertise reçu sans attendre de message Advertise supplémentaire.

Un client DHCP DEVRAIT choisir des valeurs de MRC et MRD de 0. Si le client DHCP est configuré avec un MRC ou MRD réglé à une valeur autre que 0, il DOIT arrêter d'essayer de configurer l'interface si l'échange de messages échoue. Après que le client DHCP a arrêté d'essayer de configurer l'interface, il DEVRAIT recommencer le processus de reconfiguration après un événement externe, comme une entrée de l'utilisateur, un redémarrage du système, ou quand le client est rattaché à une nouvelle liaison.

18.2.2 Création et transmission des messages Request

Le client utilise un message Request pour remplir les IA avec de prêts et obtenir d'autres informations de configuration. Le

client inclut une ou plusieurs options d'IA dans le message Request. Le serveur retourne alors les prêts et autres informations sur les IA au client dans les options IA d'un message Reply.

Le client règle le champ "type de message" à REQUEST. Le client génère un identifiant de transaction et insère sa valeur dans le champ "Identifiant de transaction".

Le client DOIT inclure l'identifiant du serveur de destination dans une option Identifiant de serveur (paragraphe 21.3).

Le client DOIT inclure une option Identifiant de client (paragraphe 21.2) pour s'identifier auprès du serveur. Le client ajoute toutes les autres options appropriées, incluant une ou plusieurs options d'IA.

Le client DOIT inclure une option Temps écoulé (paragraphe 21.9) pour indiquer pendant combien de temps le client a essayé de terminer l'échange de messages DHCP en cours.

Le client DOIT inclure une option Demande d'option (paragraphe 21.7) pour demander l'option SOL_MAX_RT (voir au paragraphe 21.24) et toutes les autres options que le client est intéressé à recevoir. Le client PEUT de plus inclure des instances des options qui sont identifiées dans l'option Demande d'option, avec des valeurs de données comme indications au serveur sur les valeurs de paramètres qu'il aimerait voir retournées.

Le client inclut une option Reconfigure Accept (paragraphe 21.20) si le client veut accepter les messages Reconfigure du serveur.

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : REQ_TIMEOUT
MRT : REQ_MAX_RT
MRC : REQ_MAX_RC
MRD : 0

Si l'échange de messages échoue, le client agit selon sa politique locale. Des exemples d'actions que le client pourrait prendre incluent :

- de choisir un autre serveur dans une liste des serveurs connus du client -- par exemple, les serveurs qui ont répondu avec un message Advertise,
- d'initier le processus de découverte de serveur décrit au début de la Section 18,
- terminer le processus de configuration et rapporter l'échec.

18.2.3 Création et transmission des messages Confirm

Le client utilise un message Confirm quand il a seulement des adresses (pas de préfixes délégués) allouées par un serveur DHCP pour déterminer si il est toujours connecté à la même liaison quand le client détecte un changement des informations de réseau comme décrit au paragraphe 18.2.12.

Le client règle le champ "type de message" à CONFIRM. Le client génère un identifiant de transaction et insère sa valeur dans le champ "transaction-id".

Le client DOIT inclure une option Identifiant de client (voir au paragraphe 21.2) pour s'identifier auprès du serveur.

Le client DOIT inclure une option Temps écoulé (voir au paragraphe 21.9) pour indiquer pendant combien de temps il a essayé d'achever l'échange de messages DHCP en cours.

Le client inclut des options d'IA pour toutes les IA allouées à l'interface pour laquelle le message Confirm est envoyé. Les options d'IA incluent toutes les adresses que le client a actuellement associées à ces IA. Le client DEVRAIT régler les champs T1 et T2 dans toutes les options IA_NA (voir au paragraphe 21.4) et les champs Durée de vie préférée et Durée de vie valide dans les options Adresse d'IA (voir au paragraphe 21.6) à 0, car le serveur va ignorer ces champs.

Le premier message Confirm provenant du client sur l'interface DOIT être retardé d'une durée aléatoire entre 0 et CNF_MAX_DELAY. Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : CNF_TIMEOUT
MRT : CNF_MAX_RT
MRC : 0
MRD : CNF_MAX_RD

Si le client ne reçoit pas de réponse avant la fin du processus de transmission de message, comme décrit à la Section 15, il DEVRAIT continuer d'utiliser tous les prêts, en utilisant les dernières durées de vie connues pour ces prêts, et DEVRAIT continuer d'utiliser tous les autres paramètres de configuration obtenus précédemment.

18.2.4 Création et transmission des messages Renew

Pour étendre les durées de vie préférées et valides pour les prêts alloués aux IA et obtenir de nouvelles adresses ou préfixes délégués pour les IA, le client envoie un message Renew au serveur de qui les prêts ont été obtenus ; le message Renew inclut des options d'IA pour les IA dont les durées de vie de prêts sont à étendre. Le client inclut des options Adresse d'IA (paragraphe 21.6) au sein des options IA_NA (paragraphe 21.4) et IA_TA (paragraphe 21.5) pour les adresses allouées aux IA. Le client inclut des options Préfixe d'IA (paragraphe 21.22) au sein des options IA_PD (paragraphe 21.21) pour les préfixes délégués alloués aux IA.

Le serveur contrôle l'heure à laquelle le client devrait contacter le serveur pour étendre les durées de vie sur les prêts alloués par les valeurs de T1 et T2 allouées à une IA. Cependant, comme le client DEVRAIT renouveler/réinitialiser toutes les IA sur le serveur au même moment, le client DOIT choisir des instants T1 et T2 pour toutes les options d'IA qui vont garantir que le client initie les transmissions des messages Renew/Rebind pas plus tard que l'heure de T1/T2 associée à tous liens du client (T1/T2 au plus tôt).

À l'instant T1, le client initie un échange de messages Renew/Reply pour étendre les durées de vie de tout prêt dans l'IA.

Un client DOIT aussi initier un échange de messages Renew/Reply avant le temps T1 si l'adresse de liaison locale du client utilisée dans les précédentes interactions avec le serveur n'est plus valide et si il veut recevoir des messages Reconfigure.

Si T1 ou T2 avait été réglé à 0 par le serveur (pour une IA_NA ou IA_PD) ou si il n'y a pas de valeur de T1 ou T2 (pour une IA_TA) dans un Reply précédant, le client peut, à sa discrétion, envoyer, respectivement un message Renew ou Rebind. Le client DOIT suivre les règles définies au paragraphe 14.2.

Le client règle le champ "type de message" à RENEW. Le client génère un identifiant de transaction et insère sa valeur dans le champ "transaction-id".

Le client DOIT inclure une option Identifiant de serveur (voir au paragraphe 21.3) dans le message Renew, identifiant le serveur avec lequel le client a communiqué le plus récemment.

Le client DOIT inclure une option Identifiant de client (voir au paragraphe 21.2) pour s'identifier auprès du serveur. Le client ajoute toutes les options appropriées, incluant une ou plusieurs options d'IA.

Le client DOIT inclure une option Temps écoulé (voir au paragraphe 21.9) pour indiquer pendant combien de temps le client a essayé d'achever l'échange de messages DHCP en cours.

Pour les IA auxquelles des prêts ont été alloués, le client inclut une option d'IA correspondante contenant une option Adresse d'IA pour chaque adresse allouée à l'IA et une option Préfixe d'IA pour chaque préfixe alloué à l'IA. Le client NE DOIT PAS inclure d'adresses et préfixes dans une option d'IA que le client n'a pas obtenue du serveur ou qui ne sont plus valides (qui ont une durée de vie valide de 0).

Le client PEUT inclure une option d'IA pour chaque lien qu'il désire mais n'a pas pu obtenir. Dans ce cas, si le client inclut l'option IA_PD pour demander une délégation de préfixe, le client PEUT inclure l'option Préfixe d'IA encapsulée au sein de l'option IA_PD, avec le champ "IPv6-prefix" réglé à 0 et le champ "longueur de préfixe" réglé à la longueur désirée du préfixe à déléguer. Le serveur PEUT utiliser cette valeur comme conseil pour la longueur du préfixe. Le client NE DEVRAIT PAS inclure une option Préfixe d'IA avec le champ "Préfixe IPv6" réglé à 0 sauf si il fournit une indication pour la longueur du préfixe.

Le client inclut une option Demande d'option (voir au paragraphe 21.7) pour demander l'option SOL_MAX_RT (voir au paragraphe 21.24) et toute autre option que le client est intéressé à recevoir. Le client PEUT inclure des options avec des valeurs de données comme indications au serveur sur les valeurs de paramètres que client aimerait se voir retournées.

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : REN_TIMEOUT
MRT : REN_MAX_RT

MRC : 0
MRD : temps restant jusqu'au prochain T2

L'échange de messages est terminé quand le prochain instant T2 est atteint. Lorsque le client répond à un Reconfigure, il ignore et élimine tout message Reconfigure supplémentaire qu'il peut recevoir.

L'échange de messages est terminé quand le prochain instant T2 est atteint, point auquel le client commence l'échange de messages Rebind (voir au paragraphe 18.2.5).

18.2.5 Création et transmission des messages Rebind

À l'instant T2 (qui ne sera atteint que si le serveur auquel le message Renew a été envoyé et commençant à l'instant T1 n'a pas répondu) le client initie un échange de messages Rebind/Reply avec tout serveur disponible.

Un Rebind est aussi utilisé pour vérifier les liens de préfixe délégué mais avec des paramètres de retransmission différents, comme décrit au paragraphe 18.2.3.

Le client construit le message Rebind comme décrit à la Section 18.2.4, avec les différences suivantes :
- Le client règle le champ "type de message" à REBIND.
- Le client n'inclut pas d'option Identifiant de serveur (voir au paragraphe 21.3) dans le message Rebind.

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :
IRT : REB_TIMEOUT
MRT : REB_MAX_RT
MRC : 0
MRD : temps restant jusqu'à ce que les durées de vie valides de tous les prêts dans toutes les IA aient expiré.

Si tous les prêts pour une IA ont expiré, le client peut choisir d'inclure cette IA dans les messages Rebind suivants pour indiquer que le client est intéressé à l'allocation de prêts à cette IA.

L'échange de messages est terminé quand les durées de vie valides de tous les prêts à travers toutes les IA ont expiré, moment auquel le client utilise le message Solicit pour localiser un nouveau serveur DHCP et envoie un message Request pour les IA expirées au nouveau serveur. Si l'échange Rebind terminé a été initié suite à la réception d'un message Reconfigure, le client ignore et élimine le message Reconfigure.

18.2.6 Création et transmission des messages Demande d'information

Le client utilise un message Demande d'information pour obtenir des informations de configuration sans que lui soient allouées des adresses et/ou préfixes délégués.

Le client règle le champ "type de message" à INFORMATION-REQUEST. Le client génère un identifiant de transaction et insère sa valeur dans le champ "transaction-id".

Le client DEVRAIT inclure une option Identifiant de client (voir au paragraphe 21.2) pour s'identifier auprès du serveur (cependant, voir au paragraphe 4.3.1 de la [RFC7844] les raisons pour lesquelles un client peut ne pas vouloir inclure cette option). Si le client ne comporte pas d'option Identifiant de client, le serveur ne sera pas capable de retourner d'options spécifiques du client au client, ou le serveur peut choisir de ne pas répondre du tout au message.

Le client DOIT inclure une option Temps écoulé (voir au paragraphe 21.9) pour indiquer pendant combien de temps le client a essayé d'achever l'échange de messages DHCP en cours.

Le client DOIT inclure une option Demande d'option (voir au paragraphe 21.7) pour demander l'option INF_MAX_RT (voir au paragraphe 21.25) l'option Heure de rafraîchissement d'informations (voir au paragraphe 21.23) et toutes les autres options que le client est intéressé à recevoir. Le client PEUT inclure des options avec des valeurs de données comme indications au serveur sur les valeurs de paramètres que le client aimerait se voir retourner.

Quand il répond à un Reconfigure, le client inclut une option Identifiant de serveur (voir au paragraphe 21.3) avec l'identifiant provenant du message Reconfigure auquel répond le client.

Le premier message Demande d'information du client sur l'interface DOIT être retardé d'une durée aléatoire entre 0 et INF_MAX_DELAY. Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : INF_TIMEOUT
MRT : INF_MAX_RT
MRC : 0
MRD : 0

18.2.7 Création et transmission des messages Release

Pour libérer un ou plusieurs prêts, un client envoie un message Release au serveur.

Le client règle le champ "type de message" à RELEASE. Le client génère un identifiant de transaction et place sa valeur dans le champ "transaction-id".

Le client place l'identifiant du serveur qui a alloué le ou les prêts dans une option Identifiant de serveur (paragraphe 21.3).

Le client DOIT inclure une option Identifiant de client (paragraphe 21.2) pour s'identifier auprès du serveur.

Le client DOIT inclure une option Temps écoulé (paragraphe 21.9) pour indiquer depuis combien de temps il essaye d'achever l'échange de messages DHCP en cours.

Le client inclut des options contenant les IA pour les prêts qu'il libère dans le champ "options". Les prêts à libérer DOIVENT être inclus dans les IA. Aucun prêt pour les IA que le client souhaite continuer d'utiliser NE DOIT être ajouté aux IA.

Le client DOIT arrêter d'utiliser tous les prêts qu'il libère avant qu'il commence le processus d'échange de messages Release. Pour une adresse, cela signifie qu'elle DOIT avoir été retirée de l'interface. Pour un préfixe délégué, cela signifie qu'il DOIT avoir été annoncé avec une durée de vie préférée et une durée de vie valide de 0 dans un message Annonce de routeur comme décrit au point (e) du paragraphe 5.5.3 de la [RFC4862] ; voir aussi l'exigence L-13 du paragraphe 4.3 de la [RFC7084].

Le client NE DOIT utiliser aucune des adresses qu'il libère comme adresse de source dans le message Release ou tout message transmis ultérieurement.

Parce que les messages Release peuvent être perdus, le client devrait retransmettre le Release si aucune réponse n'est reçue. Cependant, il y a des scénarios où le client peut ne pas souhaiter attendre la fin normale du temporisateur de retransmission avant d'abandonner (par exemple, avec une batterie faible). Les mises en œuvre DEVRAIENT retransmettre une ou plusieurs fois mais PEUVENT choisir de terminer précocement la procédure de retransmission.

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : REL_TIMEOUT
MRT : 0
MRC : REL_MAX_RC
MRD : 0

Si les prêts sont libérés mais la réponse du serveur DHCP est perdue, le client va retransmettre le message Release, et le serveur peut répondre avec un Reply indiquant un état de NoBinding *(pas de lien)*. Donc, le client ne traite pas un message Reply qui a un état de NoBinding dans un échange de messages Release comme si il indiquait une erreur.

Noter que si le client manque à libérer le prêt, chaque prêt alloué à l'IA va être réclamé par le serveur quand la durée de vie valide de ce prêt aura expiré.

18.2.8 Création et transmission des messages Decline

Si un client détecte que une ou plusieurs adresses qui lui sont allouées par un serveur sont déjà utilises par un autre nœud, le client envoie un message Decline au serveur pour l'informer que cette adresse est suspecte.

Le message Decline n'est pas utilisé dans la délégation de préfixe ; donc, le client NE DOIT PAS inclure d'options IA_PD (voir au paragraphe 21.21) dans le message Decline.

Le client règle le champ "type de message" à DECLINE. Le client génère un identifiant de transaction et place sa valeur dans le champ "transaction-id".

Le client place l'identifiant du serveur qui a alloué la ou les adresses dans une option Identifiant de serveur (voir au paragraphe 21.3).

Le client DOIT inclure une option Identifiant de client (voir au paragraphe 21.2) pour s'identifier au serveur.

Le client DOIT inclure une option Temps écoulé (voir au paragraphe 21.9) pour indiquer depuis combien de temps le client essaye d'achever l'échange de messages DHCP en cours.

Le client inclut des options contenant les IA pour les adresses qu'il refuse dans le champ "options". Les adresses à refuser DOIVENT être incluses dans les IA. Aucune adresse pour les IA que le client souhaite continuer d'utiliser ne devrait être ajoutée aux IA.

Le client NE DOIT utiliser aucune des adresses qu'il refuse comme adresse de source dans le message Decline ou dans aucun message transmis ultérieurement.

Le client transmet le message conformément à la Section 15, en utilisant les paramètres suivants :

IRT : DEC_TIMEOUT
MRT : 0
MRC : DEC_MAX_RC
MRD : 0

Si des adresses sont refusées mais que le Reply provenant d'un serveur DHCP est perdu, le client va retransmettre le message Decline, et le serveur peut répondre avec un Reply indiquant un état de NoBinding. Donc, le client ne traite pas un message Reply avec un état de NoBinding dans un échange de messages Decline comme si il indiquait une erreur.

Le client NE DEVRAIT PAS envoyer de message Release pour d'autres liens qu'il pourrait avoir reçu juste parce qu'il a envoyé un message Decline. Le client DEVRAIT conserver les liens non conflictuels. Le client DEVRAIT traiter l'échec de l'acquisition d'un lien (à cause du conflit) comme équivalent à n'avoir pas reçu le lien, comme il se comporte quand il envoie des messages Renew et Rebind.

18.2.9 Réception des messages Advertise

À réception d'un ou plusieurs messages Advertise valides, le client choisit un ou plusieurs messages Advertise sur la base des critères suivants :

- Les messages Advertise qui ont la plus haute valeur de préférence de serveur DEVRAIT être préférés à tous les autres messages Advertise. Le client PEUT choisir un serveur moins préféré si ce serveur a un meilleur ensemble de paramètres annoncés, comme l'ensemble d'IA disponibles, ainsi que l'ensemble d'autres options de configuration annoncées.
- Au sein d'un groupe de messages Advertise avec la même valeur de préférence de serveur, un client PEUT choisir les serveurs dont les messages Advertise annoncent des informations qui intéressent le client.

Une fois qu'un client a choisi un ou des messages Advertise, il va normalement mémoriser les informations sur chaque serveur, comme la valeur de préférence du serveur, les adresses annoncées, quand l'annonce a été reçue, etc..

En pratique, cela signifie que le client va conserver des automates à états indépendants par IA pour chaque serveur sélectionné.

Si le client a besoin de choisir un serveur de remplacement pour le cas où un serveur choisi ne répondrait pas, le client choisit le prochain serveur conformément aux critères ci-dessus.

Le client DOIT traiter toute option SOL_MAX_RT (paragraphe 21.24) et INF_MAX_RT (paragraphe 21.25) présente dans un message Advertise, même si le message contient une option Code d'état (paragraphe 21.13) indiquant un échec, et le message Advertise va être éliminé par le client. Un client DEVRAIT ne mettre à jour ses valeurs de SOL_MAX_RT et INF_MAX_RT que si tous les messages Advertise reçus qui contenaient l'option correspondante spécifiaient la même valeur ; autrement, il devrait utiliser la valeur par défaut (voir au paragraphe 7.6).

Le client DOIT ignorer tout message Advertise qui ne contient pas d'adresse (options Adresse d'IA (paragraphe 21.6) encapsulée dans des options IA_NA (paragraphe 21.4) ou IA_TA (paragraphe 21.5)) et pas de préfixe délégué (options Préfixe d'IA (paragraphe 21.22) encapsulées dans des options IA_PD (paragraphe 21.21)) avec l'exception que le client :
- DOIT traiter une option SOL_MAX_RT incluse et
- DOIT traiter une option INF_MAX_RT incluse.

Un client peut enregistrer dans un journal d'activité ou afficher à l'utilisateur tous messages d'état associés.

Le client qui ignore un message Advertise NE DOIT PAS redémarrer le temporisateur de retransmission de Solicit.

18.2.10 Réception des messages Reply

À réception d'un message Reply valide en réponse à un message Solicit avec une option Rapid Commit (paragraphe 21.14) Request, Confirm, Renew, Rebind, ou Demande d'information, le client extrait l'option Code d'état de niveau supérieur (voir au paragraphe 21.13) si elle est présente.

Le client DOIT traiter toute option SOL_MAX_RT (voir au paragraphe 21.24) et INF_MAX_RT (voir au paragraphe 21.25) présente dans un message Reply, même si le message contient une option Code d'état indiquant un échec.

Si le client reçoit un message Reply avec un code d'état de UnspecFail, le serveur indique qu'il a été incapable de traiter le message du client à cause d'une condition d'échec non spécifiée. Si le client retransmet le message original au même serveur pour réessayer l'opération désirée, le client DOIT limiter le taux de retransmission du message et limiter la durée pendant laquelle il retransmet le message (voir au paragraphe 14.1).

Si le client reçoit un message Reply avec un code d'état de UseMulticast *(utiliser la diffusion groupée)* le client enregistre la réception du message et envoie les messages suivants au serveur à travers l'interface sur laquelle le message a été reçu en utilisant la diffusion groupée. Le client renvoie le message original en utilisant la diffusion groupée.

Autrement (pas de code d'état ou un autre code d'état) le client traite la réponse comme décrit ci-dessous sur la base du message original pour lequel la réponse a été reçue.

Le client PEUT choisir de rapporter tout code d'état ou message à partir de l'option Code d'état dans le message Reply.

Quand un client a reçu une option de configuration dans un Reply antérieur et envoie ensuite un Renew, Rebind, ou Demande d'information et que l'option demandée n'est pas présente dans le Reply, le client DEVRAIT arrêter d'utiliser les informations de configuration reçues précédemment. En d'autres termes, le client devrait se comporter comme si il n'avait jamais reçu cette option de configuration et retourner à l'état par défaut pertinent. Si il n'y a pas de moyen viable d'arrêter d'utiliser les informations de configuration reçues, les valeurs reçues/configurées à partir de l'option PEUVENT persister si il n'y a pas d'autre source pour ces données et si elles n'ont pas d'impact externe. Par exemple, un client qui a précédemment reçu une option FQDN de client (voir la [RFC4704]) et l'a utilisée pour établi son nom d'hôte est autorisé à continuer de l'utiliser si il n'y a pas de moyen raisonnable pour le nœud de désétablir son nom d'hôte et si ce n'a pas d'impact externe. Comme contre exemple, un client qui a précédemment reçu une adresse de serveur NTP du serveur DHCP et ne le reçoit plus DOIT arrêter d'utiliser l'adresse de serveur NTP configurée. Le client DEVRAIT être ouvert aux autres sources des mêmes informations de configuration. Ce comportement ne s'applique pas aux options d'IA, car leur traitement est décrit en détails dans la prochaine section.

Quand un client reçoit une option demandée qui a une valeur mise à jour par rapport à celle précédemment reçue, le client DEVRAIT utiliser cette valeur mise à jour aussitôt que possible pour ses informations de configuration.

18.2.10.1 Réponse pour Solicit (avec engagement rapide) Request, Renew, ou Rebind

Si le client reçoit un état NotOnLink *(pas sur la liaison)* du serveur en réponse à un Solicit (avec une option Engagement rapide ; voir au paragraphe 21.14) ou un Request, le client peut soit réitérer le message sans spécifier d'adresse, soit redémarrer le processus de découverte de serveur DHCP (voir le début de la Section 18).

Si le Reply a été reçu en réponse à un message Solicit (avec une option Engagement rapide) Request, Renew, ou Rebind, le client met à jour les informations qu'il a enregistrées sur les IA à partir des options d'IA contenues dans le message Reply :
- Il calcule les temps T1 et T2 (sur la base des valeurs de T1 et T2 envoyées dans le paquet et de l'heure de réception du paquet) si c'est approprié pour le type d'IA.

- Ajoute tous nouveaux prêts dans l'option d'IA à l'IA comme enregistré par le client.
- Met à jour les durées de vie pour tous les prêts dans l'option d'IA que le client a déjà enregistrés dans l'IA.
- Élimine tous les prêts de l'IA, comme enregistré par le client, qui ont une durée de vie valide de 0 dans l'option Adresse d'IA ou Préfixe d'IA.
- Laisse inchangées toutes les information sur les prêts que le client a enregistrés dans l'IA mais qui n'étaient pas inclus dans l'IA provenant du serveur.

Si le client peut fonctionner avec les adresses et/ou préfixes obtenus du serveur :
- Le client utilise les adresses, préfixes délégués, et autres informations provenant de toutes les IA qui ne contiennent pas une option Code d'état avec le code d'état NoAddrsAvail *(pas d'adresse disponible)* ou NoPrefixAvail. Le client PEUT inclure des IA pour lesquelles il a reçu le code d'état NoAddrsAvail ou NoPrefixAvail, sans adresse ou préfixe, dans les messages Renew et Rebind envoyés au serveur, pour réessayer d'obtenir les adresses ou préfixes pour ces IA.
- Le client DOIT effectuer la détection d'adresse dupliquée conformément au paragraphe 5.4 de la [RFC4862], qui fait la liste de quelques exceptions, sur chaque adresse reçue dans toute IA sur laquelle il n'a pas effectué la détection d'adresse dupliquée durant le traitement de tout message Reply précédent provenant du serveur. Le client effectue la détection d'adresse dupliquée avant d'utiliser pour tout trafic les adresses reçues. Si des adresses se trouvent être utilisées sur la liaison, le client envoie un message Decline au serveur pour ces adresses comme décrit au paragraphe 18.2.8.
- Pour chaque adresse allouée qui n'a pas d'informations d'accessibilité associées (voir la définition de "en liaison" au paragraphe 2.1 de la [RFC4861]) afin d'éviter les problèmes décrits dans la [RFC4943], le client NE DOIT PAS supposer qu'aucune adresse soit accessible en liaison par suite de la réception d'une IA_NA ou IA_TA. Les adresses obtenues d'une IA_NA ou IA_TA NE DOIVENT PAS être utilisées pour former un préfixe implicite d'une longueur autre que 128.
- Pour chaque préfixe délégué, le client alloue un sous réseau à chacune des liaisons auxquelles les interfaces associées sont rattachées.

Quand un client met en sous réseau un préfixe délégué, il doit allouer des bits supplémentaires au préfixe pour générer de plus longs préfixes uniques. Par exemple, si le client de la Figure 1 a reçu une délégation de 2001:db8:0::/48, il pourrait générer 2001:db8:0:1::/64 et 2001:db8:0:2::/64 pour l'allocation aux deux liaisons dans le réseau de l'abonné. Si le client a eu une délégation de 2001:db8:0::/48 et 2001:db8:5::/48, il pourrait allouer 2001:db8:0:1::/64 et 2001:db8:5:1::/64 à une des liaisons, et 2001:db8:0:2::/64 et 2001:db8:5:2::/64 à l'autre liaison.

Si le client utilise un préfixe délégué pour configurer des adresses sur des interfaces sur lui-même ou d'autres nœuds derrière lui, les durées de vie préférées et valides de ces adresses DOIVENT ne pas être à tout moment plus longues que les durées de vie, respectivement préférées et valides restantes pour le préfixe délégué. En particulier, si le préfixe délégué ou un préfixe dérivé de lui est annoncé pour l'auto configuration d'adresse sans état [RFC4862], les durées de vie préférées et valides annoncées NE DOIVENT PAS excéder les durées de vie correspondantes restantes du préfixe délégué.

La gestion des informations de configuration spécifiques est détaillée dans la définition de chaque option à la Section 21.

Si le message Reply contient des IA mais si le client ne trouve d'adresse et/ou préfixe délégué utilisable dans aucune de ces IA, il peut soit essayer un autre serveur (peut-être en redémarrant le processus de découverte de serveur DHCP) soit utiliser le message Demande d'information pour obtenir seulement d'autres informations de configuration.

Quand le client reçoit un message Reply en réponse à un message Renew ou Rebind :
- Il envoie un message Request au serveur qui a répondu si une des IA dans le message Reply contient le code d'état NoBinding. Le client place des options d'IA dans ce message pour toutes les IA. Le client continue d'utiliser les autres liens pour lesquels le serveur n'a pas retourné une erreur.
- Il envoie un Renew/Rebind si des IA ne sont pas dans le message Reply, mais comme cela indique probablement que le serveur qui a répondu ne prend pas en charge ce type d'IA, cet envoi immédiat va probablement produire le même résultat. Donc, le client DOIT limiter le débit de ses transmissions (voir au paragraphe 14.1) et PEUT juste attendre l'heure normale de retransmission (comme si le message Reply n'avait pas été reçu). Le client continue d'utiliser les autres liens pour lesquels le serveur a retourné des informations.
- Autrement, il accepte les informations dans l'IA.

Chaque fois qu'un client redémarre le processus de découverte de serveur DHCP ou choisit un autre serveur comme décrit au paragraphe 18.2.9, le client DEVRAIT arrêter d'utiliser toutes les adresses et préfixes délégués pour lesquels il a des liens et essayer d'obtenir tous les prêts nécessaire à partir du nouveau serveur. Cala facilite l'utilisation d'un seul automate à état par le client pour tous les liens.

18.2.10.2 Réponse pour Release et Decline

Quand le client reçoit un message Reply valide en réponse à un message Release, il considère l'événement Release comme achevé, sans considération de l'option Code d'état (voir au paragraphe 21.13) retournée par le serveur.

Quand le client reçoit un message Reply valide en réponse à un message Decline, il considère l'événement Decline comme achevé, sans considération de l'option Code d'état retournée par le serveur.

18.2.10.3 Réponse pour Confirm

Si le client reçoit des messages Reply qui indiquent un état de Succès (explicite ou implicite) le client peut utiliser les adresses dans l'IA et ignorer tout message qui indique un état NotOnLink. Quand le client reçoit seulement un ou plusieurs messages Reply avec l'état NotOnLink en réponse à un message Confirm, le client effectue la découverte de serveur DHCP comme décrit à la Section 18.

18.2.10.4 Réponse pour Demande d'information

Se reporter au paragraphe 21.23 pour les détails de la façon dont l'option Heure de rafraîchissement des informations (qu'elle soit ou non présente dans la réponse) devrait être traitée par le client.

18.2.11 Réception des messages Reconfigure

Un client reçoit les messages Reconfigure envoyés à l'accès UDP 546 sur les interfaces pour lesquelles il a acquis des informations de configuration par DHCP. Ces messages peuvent êtres envoyés à tout moment. Comme le résultat d'un événement de reconfiguration peut affecter des programmes de niveau application, le client DEVRAIT enregistrer ces événements et PEUT notifier le changement à ces programmes à travers une interface spécifique de la mise en œuvre.

À réception d'un message Reconfigure valide, le client répond par un message Renew, un message Rebind, ou un message Demande d'information comme indiqué par l'option Reconfiguration de message (voir au paragraphe 21.19). Le client ignore le champ "transaction-id" dans le message Reconfigure reçu. Lorsque la transaction est en cours, le client élimine tous les messages Reconfigure qu'il reçoit.

Le message Reconfigure agit comme un déclencheur qui signale au client d'achever un échange de messages réussi. Une fois que le client a reçu un Reconfigure, il procède à l'échange de messages (retransmission du message Renew, Rebind, ou Demande d'information si nécessaire) ; le client DOIT ignorer tout message Reconfigure supplémentaire jusqu'à ce que l'échange soit achevé.

Les messages dupliqués seront ignorés parce que le client va commencer l'échange après la réception du premier Reconfigure. Les messages retransmis vont soit (1) déclencher l'échange (si le premier Reconfigure n'a pas été reçu par le client) soit (2) être ignorés. Le serveur PEUT arrêter la retransmission des messages Reconfigure au client une fois que le serveur reçoit le message Renew, Rebind, ou Demande d'information du client.

Il serait possible qu'un Reconfigure dupliqué ou retransmis soit suffisamment retardé (et non livré dans l'ordre) pour qu'il arrive chez le client après la fin de l'échange (initié par le Reconfigure original). Dans ce cas, le client va initier un échange redondant. La probabilité d'une livraison retardée et hors ordre est assez petite pour être ignorée. La conséquence de l'échange redondant est l'inefficacité plutôt qu'un fonctionnement incorrect.

18.2.12 Rafraîchissement des informations de configuration

Chaque fois qu'un client peut être passé à une nouvelle liaison, les préfixes/adresses alloués aux interfaces sur cette liaison ne peuvent plus être appropriés pour la liaison à laquelle le client est rattaché. Des exemples de fois où un client peut s'être déplacé sur une nouvelle liaison incluent les suivantes :

- Le client réamorce (et a une mémorisation stable et un état DHCP persistent).
- Le client est reconnecté à une liaison sur laquelle il a obtenu des prêts.
- Le client retourne d'un mode dormant.
- Le client change de points d'accès (par exemple, si il utilise une technologie Wi-Fi).

Quand le client détecte qu'il peut s'être déplacé sur une nouvelle liaison et qu'il a obtenu des adresses et pas de préfixe délégué d'un serveur, le client DEVRAIT initier un échange de messages Confirm/Reply. Le client inclut toutes les IA allouées à l'interface qui peuvent avoir être déplacés à une nouvelle liaison, ainsi que les adresses associés à ces IA, dans

son message Confirm. Tout serveur qui répond va indiquer si ces adresses sont appropriées pour la liaison à laquelle le client est rattaché avec l'état dans le message Reply qu'il retourne au client.

Si le client a des préfixes délégués valides obtenus du serveur DHCP, le client DOIT initier un échange de messages Rebind/Reply comme décrit au paragraphe 18.2.5, à l'exception que les paramètres de retransmission devraient être réglés comme pour le message Confirm (voir au paragraphe 18.2.3). Le client inclut des IA_NA, IA_TA, et IA_PD, avec les prêts associés, dans son message Rebind.

Si le client a seulement obtenu des informations de réseau en utilisant les échanges de messages Demande d'information/Reply, il DOIT initier un échange de messages Demande d'information/Reply comme décrit au paragraphe 18.2.6.

Si il n'est pas associé à une des conditions sus mentionnées, un client DEVRAIT initier un échange Renew/Reply (comme si le temporisateur T1 avait expiré) comme décrit au paragraphe 18.2.4 ou échange Demande d'information/Reply comme décrit au paragraphe 18.2.6 si le client détecte un changement significatif concernant les préfixes disponibles sur la liaison (quand de nouveaux préfixes sont ajoutés ou que des préfixes existants sont déconseillés) car cela peut indiquer un changement de configuration. Cependant, un client DOIT limiter le taux de telles tentatives pour éviter d'inonder un serveur avec des demandes quand il y a des problèmes de liaison (par exemple, de ne faire cela qu'au plus toutes les 30 secondes).

18.3 Comportement du serveur

Pour cette discussion, le serveur est supposé avoir été configuré d'une manière spécifique de la mise en œuvre avec les configurations qui intéressent les clients.

Un serveur envoie un message Advertise en réponse à chaque message Solicit valide qu'il reçoit pour annoncer la disponibilité du serveur au client.

Dans la plupart des cas, le serveur va envoyer un Reply en réponse à un message Request, Confirm, Renew, Rebind, Decline, Release, et Demande d'information envoyé par un client. Le serveur va aussi envoyer un Reply en réponse à un Solicit avec une option Engagement rapide (paragraphe 21.14) quand le serveur est configuré à répondre avec des engagements d'allocation de prêts.

Ces messages Advertise et Reply DOIVENT toujours contenir l'option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur et l'option Identifiant de client (paragraphe 21.2) provenant du message du client si il en est une présente.

Dans la plupart des messages de réponse, le serveur inclut des options contenant des informations de configuration pour le client. Le serveur doit être conscient des recommandations sur les tailles de paquet et l'utilisation de la fragmentation exposées à la Section 5 de la [RFC8200]. Si le client inclut une option Demande d'option (paragraphe 21.7) dans son message, le serveur inclut les options dans le message de réponse contenant les paramètres de configuration pour toutes les options identifiées dans l'option Demande d'option que le serveur a été configuré à retourner au client. Le serveur PEUT retourner des options supplémentaires au client si il a été configuré à le faire.

Tout message envoyé d'un client peut arriver au serveur encapsulé dans un ou plusieurs messages Relay-forward. Le serveur DOIT utiliser le message reçu pour construire le message Relay-reply approprié pour permettre que la réponse au message reçu soit relayée à travers les mêmes agents de relais (en ordre inverse) que le message original du client ; voir plus de détails au paragraphe 19.3. Le serveur peut aussi avoir besoin d'enregistrer ces informations avec chaque client au cas où il serait nécessaire d'envoyer un message Reconfigure ultérieurement, sauf si le serveur a été configuré avec des adresses qui peuvent être utilisées pour envoyer des messages Reconfigure directement au client (paragraphe 18.3.11). Noter que les serveurs qui prennent en charge leasequery [RFC5007] ont aussi besoin d'enregistrer ces informations.

En envoyant des messages Reconfigure, le serveur PEUT initier un échange de configuration pour causer l'obtention par les clients DHCP de nouvelles adresses, nouveaux préfixes, et autres informations de configuration. Par exemple, un administrateur peut utiliser un échange de configuration initié par le serveur quand les liaisons dans le domaine DHCP doivent être renumérotées ou quand d'autres options de configuration sont mises à jour, peut-être parce que les serveurs sont déplacés, ajoutés, ou supprimés.

Quand un client reçoit un message Reconfigure du serveur, le client initie l'envoi d'un message Renew, Rebind, ou Demande d'information comme indiqué par le type de message dans l'option Reconfiguration de message (voir au paragraphe 21.19). Le serveur envoie des IA et/ou autres informations de configuration au client dans un message Reply. Le serveur PEUT inclure des options contenant les IA et les nouvelles valeurs pour les autres paramètres de configuration

dans le message Reply, même si ces IA et paramètres n'étaient pas demandés dans le message du client.

18.3.1 Réception des messages Solicit

Voir au paragraphe 18.4 les détails du traitement des messages Solicit reçus via envoi individuel. La transmission en envoi individuel des messages Solicit n'est pas permise, sans considération de si l'option Serveur en envoi individuel (voir au paragraphe 21.12) est configurée ou non.

Le serveur détermine les informations sur le client et sa localisation comme décrit à la Section 13 et vérifie sa politique administrative sur les réponses au client. Si il n'est pas permis au serveur de répondre au client, il élimine le message Solicit. Par exemple, si la politique administrative du serveur est qu'il peut seulement répondre à un client qui veut accepter un message Reconfigure, si le client ne comporte pas d'option Accepte Reconfigure (paragraphe 21.20) dans le message Solicit, le serveur élimine le message Solicit.

Si (1) il est permis au serveur de répondre au client, (2) le client n'a pas inclus une option Engagement rapide (paragraphe 21.14) dans le message Solicit, ou (3) le serveur n'a pas été configuré à répondre avec des engagements d'allocation de prêts et autres ressources, le serveur envoie un message Advertise au client comme décrit au paragraphe 18.3.9.

Si le client a inclus une option Engagement rapide dans le message Solicit et si le serveur a été configuré à répondre avec des engagements d'allocation de prêts et autres ressources, le serveur répond au Solicit par un message Reply. Le serveur produit le message Reply bien qu'il ait reçu un message Request comme décrit au paragraphe 18.3.2. Le serveur transmet le message Reply comme décrit au paragraphe 18.3.10. Le serveur DOIT engager l'allocation de toutes adresses et préfixes délégués ou autres informations de configuration avant d'envoyer un message Reply au client. Dans ce cas, le serveur inclut une option Engagement rapide dans le message Reply pour indiquer que le Reply est en réponse à un message Solicit.

Discussion : Quand il utilise l'échange de messages Solicit/Reply, le serveur engage l'allocation de tous les prêts avant d'envoyer le message Reply. Le client peut supposer que les prêts lui ont été alloués dans le message Reply et n'a pas besoin d'envoyer un message Request pour ces prêts.

Normalement, les serveurs qui sont configurés pour utiliser l'échange de messages Solicit/Reply vont être déployés de telle façon qu'un seul serveur réponde à un message Solicit. Si plus d'un serveur répond, le client va seulement utiliser les prêts d'un des serveurs, tandis que les prêts des autres serveurs vont être engagés au client mais non utilisés par le client.

18.3.2 Réception des messages Request

Voir au paragraphe 18.4 les détails du traitement des messages Request reçus via envoi individuel.

Quand le serveur reçoit un message Request valide, il crée les liens pour ce client conformément à la politique du serveur et aux informations de configuration, et il enregistre les IA et autres informations demandées par le client.

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Request dans le champ "transaction-id".

Le serveur DOIT inclure dans le message Reply une option Identifiant de serveur (voir au paragraphe 21.3) contenant le DUID du serveur et l'option Identifiant de client (voir au paragraphe 21.2) provenant du message Request.

Le serveur examine toutes les IA dans le message du client.

Pour chaque option IA_NA (paragraphe 21.4) et IA_TA (paragraphe 21.5) dans le message Request, le serveur vérifie si les préfixes des adresses incluses sont appropriées pour la liaison à laquelle le client est connecté. Si un des préfixes des adresses incluses n'est pas approprié pour la liaison à laquelle le client est connecté, le serveur DOIT retourner l'IA au client avec une option Code d'état (paragraphe 21.13) avec la valeur NotOnLink. Si le serveur n'envoie pas le code d'état NotOnLink mais ne peut pas allouer du tout d'adresses IP à une IA, il DOIT retourner l'option d'IA dans le message Reply sans adresse dans l'IA et une option Code d'état contenant le code d'état NoAddrsAvail dans l'IA.

Pour toute option IA_PD (paragraphe 21.21) dans le message Request auquel le serveur ne peut pas allouer de préfixe délégué, le serveur DOIT retourner l'option IA_PD dans le message Reply sans préfixe dans le IA_PD et avec une option Code d'état contenant le code d'état NoPrefixAvail dans le IA_PD.

Le serveur PEUT allouer à une IA des adresses et/ou préfixes délégués différents de ceux inclus dans l'IA du message Request du client.

Pour toutes les IA auxquelles le serveur peut allouer des adresses ou préfixes délégués, le serveur inclut les IA avec les adresses (pour les IA_NA et IA_TA) les préfixes (pour les IA_PD) et les autres paramètres de configuration, et il enregistre l'IA comme un nouveau lien de client. Le serveur NE DOIT PAS inclure dans l'IA d'adresses ou préfixes délégués qu'il n'alloue pas au client.

Les temps T1/T2 réglés dans chaque option d'IA applicable pour un Reply DOIVENT avoir les mêmes valeurs sur toutes les IA. Le serveur DOIT déterminer les temps T1/T2 à travers tous les liens de client applicables dans le Reply. Cela facilite la capacité du client à renouveler tous les liens en même temps.

Le serveur DEVRAIT inclure une option Accepte Reconfigure (paragraphe 21.20) si la politique du serveur permet le mécanisme de reconfiguration et si le client le prend en charge. Actuellement, l'envoi de cette option dans un Reply est techniquement redondant, car l'utilisation du mécanisme de reconfiguration exige l'authentification ; à présent, le seul mécanisme défini est RKAP (paragraphe 20.4) et la présence de la clé de reconfiguration signale la prise en charge de l'acceptation des messages Reconfigure. Cependant, de meilleurs mécanismes de sécurité pourraient être définis à l'avenir qui causeraient l'abandon de RKAP.

Le serveur inclut d'autres options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.3.

Si le serveur trouve que le client a inclus dans le message Request une IA pour laquelle le serveur a déjà un lien qui associe l'IA au client, le serveur envoie un message Reply avec le lien existant, éventuellement avec des durées de vie mises à jour. Le serveur peut mettre à jour les liens conformément à sa politique locale, mais le serveur DEVRAIT générer à nouveau la réponse et pas simplement retransmettre les informations envoyées précédemment, même si le champ "transaction-id" correspond à une transmission précédente. Le serveur NE DOIT PAS mettre ses réponses en antémémoire.

Discussion : Les réponses mises en antémémoire sont mauvaises parce que les durées de vie ont besoin d'être mises à jour (en diminuant les temporisateurs du temps écoulé depuis la transmission d'origine ou en gardant les valeurs de durée de vie et en mettant à jour les informations de prêt dans la base de données du serveur). Aussi, si le message utilise une protection de sécurité (comme la méthode de détection de répétition (RDM, *Replay Detection Method*) décrite au paragraphe 20.3) sa valeur doit être mise à jour. De plus, tous les résumés doivent être mis à jour. Tout cela fait que la mise en antémémoire des réponses est beaucoup plus complexe que de simplement envoyer la même mémoire tampon que précédemment, et il est facile de manquer une de ces étapes.

18.3.3 Réception des messages Confirm

Voir au paragraphe 18.4 les détails du traitement des messages Confirm reçus via l'envoi individuel. La transmission en envoi individuel des messages Confirm n'est pas permise, sans considération de si l'option Serveur en envoi individuel (paragraphe 21.12) est configurée ou non.

Quand le serveur reçoit a message Confirm, il détermine si les adresses dans le message Confirm sont appropriées pour la liaison à laquelle le client est rattaché. Si toutes les adresses dans le message Confirm réussissent cet examen, le serveur retourne un état de Succès. Si une des adresses ne passe pas l'essai, le serveur retourne un état de NotOnLink. Si le serveur est incapable d'effectuer cet essai (par exemple, le serveur n'a pas d'informations sur les préfixes sur la liaison à laquelle le client est connecté) ou il n'y avait d'adresse dans aucune des IA envoyées par le client, le serveur NE DOIT PAS envoyer de Reply au client.

Le serveur ignore les champs T1 et T2 dans les options d'IA et les champs Durée de vie préférée et Durée de vie valide dans les options Adresse d'IA (paragraphe 21.6).

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Confirm dans le champ "transaction-id".

Le serveur DOIT inclure dans le message Reply une option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur et l'option Identifiant de client (paragraphe 21.2) provenant du message Confirm. Le serveur inclut une option Code d'état (paragraphe 21.13) indiquant l'état du message Confirm.

18.3.4 Réception des messages Renew

Voir au paragraphe 18.4 les détails du traitement des messages Renew reçus via l'envoi individuel.

Pour chaque IA dans le message Renew provenant d'un client, le serveur localise le lien du client et vérifie que les informations dans l'IA provenant du client correspondent aux informations mémorisées pour ce client.

Si le serveur trouve l'entrée du client pour l'IA, il renvoie l'IA au client avec de nouvelles durées de vie et, si applicable, de nouveaux temps T1/T2. Si le serveur est incapable d'étendre les durées de vie d'une adresse ou préfixe délégué dans l'IA, il PEUT choisir de ne pas inclure l'option Adresse d'IA (paragraphe 21.6) pour cette adresse ou option Préfixe d'IA (paragraphe 21.22) pour ce préfixe délégué. Si le serveur choisit d'inclure l'option Adresse d'IA ou Préfixe d'IA pour une telle adresse ou préfixe délégué, le serveur DEVRAIT régler les valeurs T1 et T2 à la durée de vie valide pour l'option d'IA sauf si le serveur inclut aussi d'autres adresses ou préfixes délégués que le serveur est capable d'étendre pour l'IA. Régler T1 et T2 à des valeurs égales à la durée de vie valide informe le client que les prêts associés à ladite IA ne seront pas étendus, de sorte que ce n'est pas la peine d'essayer. Aussi, cela évite de générer du trafic inutile car la durée de vie restante approche de 0.

Le serveur peut choisir de changer la liste des adresses ou préfixes délégués et des durées de vie dans les IA qui sont retournées au client.

Si le serveur trouve qu'une des adresses dans l'IA n'est pas appropriée pour la liaison à laquelle le client est rattaché, le serveur retourne l'adresse au client avec une durée de vie de 0.

Si le serveur trouve qu'un des préfixes délégués dans l'IA n'est pas approprié pour la liaison à laquelle le client est rattaché, le serveur retourne le préfixe délégué au client avec une durée de vie de 0.

Pour chaque IA pour laquelle le serveur ne peut pas trouver d'entrée de client, le serveur a le choix suivant, selon la politique du serveur et les informations de configuration :

- Si le serveur est configuré à créer de nouveaux liens par suite du traitement des messages Renew, le serveur DEVRAIT créer un lien et retourner l'IA avec les adresses ou préfixes délégués alloués avec des durées de vie et, si applicable, des temps de T1/T2 et autres informations demandées par le client. Si le client inclut l'option Préfixe d'IA dans l'option IA_PD (paragraphe 21.21) avec une valeur de zéro dans le champ "Préfixe IPv6" et une valeur non de zéro dans le champ "Longueur de préfixe", le serveur PEUT utiliser la valeur de "Longueur de préfixe" comme une indication de la longueur des préfixes à allouer (voir dans la [RFC8168] les détails des conseils de longueur de préfixe).

- Si le serveur est configuré à créer de nouveaux liens par suite du traitement des messages Renew mais ne veut pas allouer de prêt à une IA, le serveur retourne l'option d'IA contenant une option Code d'état (paragraphe 21.13) avec le code d'état NoAddrsAvail ou NoPrefixAvail et un message d'état pour un utilisateur.

- Si le serveur ne prend pas en charge la création de nouveaux liens pour le client envoyant un message Renew ou si ce comportement est désactivé conformément à la politique du serveur ou aux informations de configuration, le serveur retourne l'option d'IA contenant une option Code d'état avec le code d'état NoBinding et un message d'état pour un utilisateur.

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Renew dans le champ "transaction-id".

Le serveur DOIT inclure dans le message Reply une option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur et l'option Identifiant de client (paragraphe 21.2) provenant du message Renew.

Le serveur inclut d'autres options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.3.

Le serveur PEUT inclure des options contenant les IA et les valeurs des autres paramètres de configuration, même si ces paramètres n'étaient pas demandés dans le message Renew.

Les valeurs T1/T2 réglées dans chaque option d'IA applicable pour un Reply DOIVENT être les mêmes sur toutes les IA. Le serveur DOIT déterminer les valeurs de T1/T2 sur tous les liens applicables du client dans le Reply. Cela facile la

capacité du client à renouveler tous les liens en une seule fois.

18.3.5 Réception des messages Rebind

Voir au paragraphe 18.4 les détails du traitement des messages Rebind reçus via l'envoi individuel. La transmission en envoi individuel des messages Rebind n'est pas permise, sans considération de si l'option Serveur en envoi individuel (paragraphe 21.12) est configurée ou non.

Quand le serveur reçoit un message Rebind qui contient une option d'IA provenant d'un client, il localise le lien du client et vérifie que les informations dans l'IA provenant du client correspondent aux information mémorisées pour ce client.

Si le serveur trouve l'entrée du client pour l'IA et si il détermine que les adresses ou préfixes délégués dans l'IA sont appropriés pour la liaison à laquelle l'interface du client est rattachée conformément aux informations de configuration explicites du serveur, celui-ci DEVRAIT renvoyer l'IA au client avec de nouvelles durées de vie et, si applicable, de nouvelles valeurs de T1/T2. Si le serveur est incapable d'étendre les durées de vie d'une adresse dans l'IA, le serveur PEUT choisir de ne pas inclure l'option Adresse d'IA (paragraphe 21.6) pour cette adresse. Si le serveur est incapable d'étendre les durées de vie d'un préfixe délégué dans l'IA, le serveur PEUT choisir de ne pas inclure l'option Préfixe d'IA (paragraphe 21.22) pour ce préfixe.

Si le serveur trouve que l'entrée de client pour l'IA et qu'une des adresses ou un des préfixes délégués ne sont plus appropriés pour la liaison à laquelle est rattachée l'interface du client, conformément aux informations de configuration, le serveur retourne ces adresses ou préfixes délégués au client avec des durées de vie de 0.

Si le serveur ne peut pas trouver une entrée du client pour l'IA, il vérifie si l'IA contient des adresses (pour les IA_NA et IA_TA) ou des préfixes délégués (pour les IA_PD). Le serveur vérifie si les adresses et préfixes délégués sont appropriés pour la liaison à laquelle est rattachée l'interface du client, conformément aux informations de configuration explicites du serveur. Pour toute adresse qui n'est pas appropriée pour la liaison à laquelle est rattachée l'interface du client, le serveur PEUT inclure l'option Adresse d'IA avec des durées de vie de 0. Pour tout préfixe délégué qui n'est pas approprié pour la liaison à laquelle est rattachée l'interface du client, le serveur PEUT inclure l'option Préfixe d'IA avec une durée de vie de 0. Le Reply avec des durées de vie de 0 constitue une notification explicite au client que les adresses et préfixes délégués spécifiques ne sont plus valides et NE DOIVENT PAS être utilisés par le client. Si le serveur choisit de ne pas inclure d'IA contenant les options Adresse d'IA ou Préfixe d'IA avec des durées de vie de 0 et si le serveur n'inclut aucune autre IA avec des prêts et/ou codes d'état, le serveur n'envoie pas un message Reply. Dans cette situation, le serveur élimine le message Rebind.

Autrement, pour chaque IA pour laquelle le serveur ne peut pas trouver une entrée de client, le serveur a le choix suivant, selon la politique du serveur et les informations de configuration :

- Si le serveur est configuré pour créer de nouveaux liens par suite du traitement des messages Rebind (voir aussi la note ci-dessous sur l'option Engagement rapide (paragraphe 21.14)) le serveur DEVRAIT créer un lien et retourner l'IA avec les prêts alloués avec des durées de vie et, si applicable, des valeurs de T1/T2 et les autres informations demandées par le client. Le serveur NE DOIT PAS retourner dans l'IA des adresses ou préfixes délégués que le serveur n'alloue pas au client.
- Si le serveur est configuré à créer de nouveaux liens par suite du traitement des messages Rebind mais si il ne veut pas allouer de prêt à une IA, le serveur retourne l'option d'IA contenant une option Code d'état (paragraphe 21.13) avec le code d'état NoAddrsAvail ou NoPrefixAvail et un message d'état pour un usager.
- Si le serveur ne prend pas en charge la création de nouveaux liens pour le client qui envoie un message Rebind ou si ce comportement est désactivé conformément à la politique du serveur ou aux informations de configuration, le serveur retourne l'option d'IA contenant une option Code d'état avec le code d'état NoBinding et un message d'état pour un usager.

Quand le serveur crée de nouveaux liens pour l'IA, il est possible que d'autres serveurs créent aussi des liens par suite de la réception du même message Rebind ; voir le texte de la "Discussion" au paragraphe 21.14. Donc, le serveur DEVRAIT ne créer de nouveaux liens durant le traitement d'un message Rebind que si le serveur est configuré à répondre par un message Reply à un message Solicit contenant l'option Engagement rapide.

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Rebind dans le champ "transaction-id".

Le serveur DOIT inclure dans le message Reply une option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur et l'option Identifiant de client (paragraphe 21.2) provenant du message Rebind.

Le serveur inclut d'autres options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.3.

Le serveur PEUT inclure des options contenant les IA et les valeurs des autres paramètres de configuration, même si ces IA et paramètres n'étaient pas demandés dans le message Rebind.

Les valeurs de T1 ou T2 réglées dans chaque option d'IA applicable pour un Reply DOIVENT être les mêmes à travers toutes les IA. Le serveur DOIT déterminer les valeurs de T1 ou T2 à travers tous les liens applicables au client dans le Reply. Cela facilite pour le client la capacité de renouveler tous les liens en même temps.

18.3.6 Réception des messages Demande d'information

Voir au paragraphe 18.4 les détails du traitement des messages Demande d'information reçus via l'envoi individuel.

Quand le serveur reçoit un message Demande d'information, le client demande des informations de configuration qui n'incluent l'allocation d'aucun prêt. Le serveur détermine tous les paramètres de configuration appropriés pour le client, sur la base des politiques de configuration connues du serveur.

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Demande d'information dans le champ "transaction-id".

Le serveur DOIT inclure une option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur dans le message Reply. Si le client inclut une option Identifiant de client (paragraphe 21.2) dans le message Demande d'information, le serveur copie cette option dans le message Reply.

Le serveur inclut des options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.3. Le serveur PEUT inclure des options supplémentaires qui n'étaient pas demandées par le client dans le message Demande d'information.

Si le message Demande d'information reçu du client n'incluait pas d'option Identifiant de client, le serveur DEVRAIT répondre avec un message Reply contenant tous les paramètres de configuration qui ne sont pas déterminés par l'identité du client. Si le serveur choisit de ne pas répondre, le client peut continuer de retransmettre indéfiniment le message Demande d'information.

18.3.7 Réception des messages Release

Voir au paragraphe 18.4 les détails du traitement des messages Release reçus via l'envoi individuel.

Le serveur construit un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction du message Release dans le champ "transaction-id".

À réception d'un message Release valide, le serveur examine la validité des IA et des prêts dans les IA. Si les IA dans le message sont dans un lien pour le client et si les prêts dans les IA ont été alloués par le serveur à ces IA, le serveur supprime les prêts des IA et rend les prêts disponibles pour une allocation à d'autres clients. Le serveur ignore les prêts non alloués aux IA, bien qu'il puisse choisir d'enregistrer une erreur.

Après le traitement de tous les prêts, le serveur génère un message Reply et inclut une option Code d'état (paragraphe 21.13) avec la valeur Succès, une option Identifiant de serveur (paragraphe 21.3) avec le DUID du serveur, et une option Identifiant de client (paragraphe 21.2) avec le DUID du client. Pour chaque IA dans le message Release pour laquelle le serveur n'a pas d'information de lien, le serveur ajoute une option d'IA en utilisant l'IAID provenant du message Release et il inclut une option Code d'état avec la valeur NoBinding dans l'option d'IA. Aucune autre option n'est incluse dans l'option d'IA.

Un serveur peut choisir de conserver un enregistrement des prêts alloués et des IA après l'expiration des durées de vie de ces prêts pour permettre au serveur de réallouer à un client les prêts précédemment alloués.

18.3.8 Réception des messages Decline

Voir au paragraphe 18.4 les détails du traitement des messages Decline reçus via l'envoi individuel.

À réception d'un message Decline valide, le serveur examine la validité des IA et des prêts dans les IA. Si les IA dans le message sont dans un lien pour le client et si les prêts dans les IA ont été alloués par le serveur à ces IA, le serveur supprime les adresses des IA. Le serveur ignore les adresses non allouées aux IA (bien qu'il puisse choisir d'enregistrer une erreur si il trouve une telle adresse).

Le client a trouvé dans le message Decline qu'une des adresses est déjà utilisée sur sa liaison. Donc, le serveur DEVRAIT marquer l'adresse refusée par le client afin qu'elle ne soit pas allouée à un autre client et il PEUT choisir de faire une notification que cette adresse a été refusée. La politique locale au serveur détermine quand les adresses identifiées dans un message Decline peuvent être rendues disponibles à l'allocation.

Après que toutes les adresses ont été traitées, le serveur génère un message Reply en réglant le champ "type de message" à REPLY et en copiant l'identifiant de transaction provenant du message Decline dans le champ "transaction-id". Le client inclut une option Code d'état (paragraphe 21.13) avec la valeur de Succès, une option Identifiant de serveur (paragraphe 21.3) avec le DUID du serveur, et une option Identifiant de client (paragraphe 21.2) avec le DUID du client. Pour chaque IA dans le message Decline pour laquelle le serveur n'a pas d'information de lien, le serveur ajoute une option d'IA en utilisant l'IAID provenant du message Decline et il inclut une option Code d'état avec la valeur NoBinding dans l'option d'IA. Aucune autre option n'est incluse dans l'option d'IA.

18.3.9 Création des messages Advertise

Le serveur règle le champ "type de message" à ADVERTISE et copie le contenu du champ "transaction-id" provenant du message Solicit reçu du client dans le message Advertise. Le serveur inclut son identifiant de serveur dans une option Identifiant de serveur (paragraphe 21.3) et copie l'option Identifiant de client (paragraphe 21.2) provenant du message Solicit dans le message Advertise.

Le serveur PEUT ajouter une option Préférence (paragraphe 21.8) pour porter la valeur de préférence pour le message Advertise. La mise en œuvre de serveur DEVRAIT permettre le réglage d'une valeur de préférence de serveur par l'administrateur. La valeur de préférence de serveur DOIT avoir 0 par défaut sauf autrement configuré pat l'administrateur du serveur.

Le serveur inclut une option Accepte Reconfigure (paragraphe 21.20) si le serveur veut indiquer qu'il prend en charge le mécanisme Reconfigure. Cette information peut être utilisée par le client durant le processus de choix du serveur.

Le serveur inclut les options qu'il va retourner au client dans un message Reply ultérieur. Les informations de ces options peuvent être utilisées par le client dans le choix d'un serveur si le client reçoit plus d'un message Advertise. Le serveur DOIT inclure dans le message Advertise des options contenant les paramètres de configuration pour toutes les options identifiées dans l'option Demande d'option (paragraphe 21.7) dans le message Solicit que le serveur a été configuré à retourner au client. Si l'option Demande d'option comporte une option conteneur, le serveur DOIT inclure toutes les options qui sont éligibles à être encapsulées dans le conteneur. L'option Demande d'option PEUT être utilisée pour signaler la prise en charge d'une caractéristique même quand cette option est encapsulée, comme dans le cas de l'option Exclusion de préfixe [RFC6603]. Dans ce cas, un traitement spécial est exigé par le serveur. Le serveur PEUT retourner des options supplémentaires au client si il a été configuré à le faire.

Le serveur DOIT inclure dans le message Advertise des options d'IA contenant toutes adresses et/ou préfixes délégués qui pourraient être alloués aux IA contenues dans le message Solicit provenant du client. Si le client a inclus des adresses dans les options Adresse d'IA (21.6) dans le message Solicit, le serveur PEUT utiliser ces adresses comme indications sur les adresses qui le client aimerait recevoir. Si le client a inclus des options Préfixe d'IA (paragraphe 21.22) le serveur PEUT utiliser le préfixe contenu dans le champ "Préfixe IPv6" et/ou la longueur de préfixe contenue dans le champ "Longueur de préfixe" comme indications sur les préfixes que le client aimerait recevoir. Si le serveur ne va pas allouer d'adresse ou préfixe délégué reçu comme indication dans le message Solicit, le serveur NE DOIT PAS inclure cette adresse ou préfixe délégué dans le message Advertise.

Si le serveur ne va pas allouer d'adresses à une IA_NA ou IA_TA dans les messages Request suivants du client, il DOIT inclure l'option d'IA dans le message Advertise avec aucune adresse dans cette IA et une option Code d'état (paragraphe 21.13) encapsulée dans l'option d'IA contenant le code d'état NoAddrsAvail.

Si le serveur ne va pas allouer de préfixes à une IA_PD dans les messages Request suivants du client, il DOIT inclure

l'option IA_PD (paragraphe 21.21) dans le message Advertise sans préfixe dans l'option IA_PD et une option Code d'état encapsulée dans l'IA_PD contenant le code d'état NoPrefixAvail.

La transmission des messages Advertise est décrite au paragraphe suivant.

18.3.10 Transmission des messages Advertise et Reply

Si le message original a été reçu directement par le serveur, il envoie le message Advertise ou Reply en envoi individuel directement au client en utilisant l'adresse du champ Adresse de source provenant du datagramme IP dans lequel le message original a été reçu. Le message Advertise ou Reply DOIT être en envoi individuel à travers l'interface sur laquelle le message original a été reçu.

Si le message original a été reçu dans un message Relay-forward, le serveur construit un message Relay-reply avec le message Reply dans la charge utile d'une option Relais de message (21.10). Si les messages Relay-forward incluaient une option Identifiant d'interface (paragraphe 21.18) le serveur copie cette option dans le message Relay-reply. Le serveur envoie en individuel le message Relay-reply directement à l'agent de relais en utilisant l'adresse qui est dans le champ Adresse de source du datagramme IP dans lequel le message Relay-forward a été reçu. Voir au paragraphe 19.3 les détails de la construction des messages Relay-reply.

18.3.11 Création et transmission des messages Reconfigure

Le serveur règle le champ "type de message" à RECONFIGURE et règle le champ "transaction-id" à 0. Le serveur inclut une option Identifiant de serveur (paragraphe 21.3) contenant son DUID et une option Identifiant de client (paragraphe 21.2) contenant le DUID du client dans le message Reconfigure.

À cause du risque d'attaques de déni de service (DoS) contre les clients DHCP, l'utilisation de mécanismes de sécurité est rendue obligatoire dans les messages Reconfigure. Le serveur DOIT utiliser l'authentification DHCP dans le message Reconfigure (voir au paragraphe 20.4).

Le serveur DOIT inclure une option Reconfiguration de message (paragraphe 21.19) pour choisir si le client répond avec un message Renew, un message Rebind, ou un message Demande d'information.

Le serveur NE DOIT PAS inclure d'autres options dans le message Reconfigure, sauf comme spécifiquement permis dans la définition des options individuelles.

Un serveur envoie chaque message Reconfigure à un seul client DHCP, en utilisant une adresse d'envoi individuel IPv6 de portée suffisante appartenant au client DHCP. Si le serveur n'a pas d'adresse à laquelle il puisse envoyer le message Reconfigure directement au client, le serveur utilise un message Relay-reply (comme décrit au paragraphe 19.3) pour envoyer le message Reconfigure à un agent de relais qui va relayer le message au client. Le serveur peut obtenir l'adresse du client (et de l'agent de relais approprié, si nécessaire) par les informations que le serveur a sur les clients qui ont été en contact avec le serveur (18.3) ou par un agent externe.

Pour reconfigurer plus d'un client, le serveur envoie en individuel un message séparé à chaque client. Le serveur peut initier la reconfiguration de plusieurs clients concurremment ; par exemple, un serveur peut envoyer un message Reconfigure à des clients supplémentaires alors que des échanges de messages de reconfiguration précédents sont encore en cours.

Le message Reconfigure cause l'initiation par le client d'un échange de messages Renew/Reply, Rebind/Reply, ou Demande d'information/Reply avec le serveur. Le serveur interprète la réception d'un message Renew, Rebind, ou Demande d'information (selon celui qui était spécifié dans le message original Reconfigure) de la part du client comme satisfaisant à la demande du message Reconfigure.

Quand il transmet le message Reconfigure, le serveur règle le temps de retransmission (RT, *retransmission time*) à REC_TIMEOUT. Si le serveur ne reçoit pas de message Renew, Rebind, ou Demande d'information du client avant que RT s'écoule, le serveur retransmet le message Reconfigure, double la valeur de RT, et attend à nouveau. Le serveur continue ce processus jusqu'à ce que REC_MAX_RC tentatives infructueuses aient été faites, point auquel le serveur DEVRAIT interrompre le processus de reconfiguration pour ce client.

Les valeurs initiales et par défaut pour REC_TIMEOUT et REC_MAX_RC sont documentées au paragraphe 7.6.

18.4 Réception des messages en envoi individuel

Sauf mention contraire dans les sous paragraphes du paragraphe 18.3 qui discutent de la réception des messages spécifiques, le serveur n'est pas supposé accepter de trafic en envoi individuel quand il n'est pas explicitement configuré à le faire. Par exemple, la transmission en envoi individuel n'est pas permise pour les messages Solicit, Confirm, et Rebind (respectivement aux paragraphes 18.3.1, 18.3.3, et 18.3.5) même si l'option Serveur en envoi individuel (paragraphe 21.12) est configurée. Pour les messages Request, Renew, Information-request, Release, et Decline, il n'est permis que si l'option Serveur en envoi individuel est configurée.

Quand le serveur reçoit un message via l'envoi individuel d'un client auquel le serveur n'a pas envoyé une option Serveur en envoi individuel (ou n'est pas actuellement configuré pour le faire) le serveur élimine ce message et répond avec un Advertise (quand il répond à un message Solicit) ou un message Reply (quand il répond à tout autre message) contenant une option Code d'état (paragraphe 21.13) avec la valeur UseMulticast, une option Identifiant de serveur (paragraphe 21.3) contenant le DUID du serveur, l'option Identifiant de client (paragraphe 21.2) provenant du message du client (si il en est) et aucune autre option.

19. Comportement de l'agent de relais

L'agent de relais DEVRAIT être configuré à utiliser une liste d'adresses de destination qui inclut les adresses d'envoi individuel. La liste des adresses de destination PEUT inclure l'adresse de diffusion groupée Tous_Serveurs_DHCP ou d'autres adresses choisies par l'administrateur de réseau. Si l'agent de relais n'a pas été explicitement configuré, il DOIT utiliser l'adresse de diffusion groupée Tous_Serveurs_DHCP par défaut.

Si l'agent de relais relaye des messages à l'adresse de diffusion groupée Tous_Serveurs_DHCP ou autres adresses de diffusion groupée, il règle le champ Limite de bonds à 8.

Si l'agent de relais reçoit un message autre que Relay-forward et Relay-reply et si l'agent de relais ne reconnaît pas son type de message, il DOIT transmettre le message comme décrit au paragraphe 19.1.1.

19.1 Relais d'un message de client ou d'un message de relais transmission

Un agent de relais relaye les messages provenant des clients et les messages Relay-forward provenant des autres agents de relais. Quand un agent de relais reçoit un message Relay-forward, un type de message reconnu pour lequel il n'est pas la cible prévue, ou un type de message non reconnu [RFC7283], il construit un nouveau message Relay-forward. L'agent de relais copie l'adresse de source de l'en-tête du datagramme IP dans lequel le message a été reçu dans le champ Adresse de l'homologue du message Relay-forward. L'agent de relais copie le message DHCP reçu (en excluant tous les en-têtes IP ou UDP) dans une option Message de relais (paragraphe 21.10) dans le nouveau message. L'agent de relais ajoute au message Relay-forward toutes les autres options qu'il est configuré à inclure.

La [RFC6221] définit un agent de relais DHCPv6 léger (LDRA, *Lightweight DHCPv6 Relay Agent*) qui permet que les informations d'agent de relais soient insérées par un nœud d'accès qui effectue une fonction de pontage de couche de liaison (c'est-à-dire, non d'acheminement).

19.1.1 Relais d'un message d'un client

Si l'agent de relais a reçu le message à relayer d'un client, l'agent de relais place dans le champ Adresse de liaison une adresse d'envoi individuel de portée mondiale (c'est-à-dire, GUA ou ULA) à partir d'un préfixe alloué à la liaison sur laquelle le client devrait voir des prêts alloués. Si une telle adresse n'est pas disponible, l'agent de relais peut régler le champ Adresse de liaison à une adresse de liaison locale à partir de l'interface sur laquelle le message original a été reçu. Ceci n'est pas recommandé, car cela peut exiger que des informations supplémentaires soient fournies dans la configuration du serveur. Voir au paragraphe 3.2 de la [RFC7969] une discussion détaillée.

Cette adresse va être utilisée par le serveur pour déterminer la liaison à partir de laquelle le client devrait avoir des prêts alloués et les autres informations de configuration.

La valeur du compte de bonds dans le message Relay-forward est réglée à 0.

Si l'agent de relais ne peut pas utiliser l'adresse du champ Adresse de liaison pour identifier l'interface à travers laquelle la

réponse au client va être relayée, l'agent de relais DOIT inclure une option Identifiant d'interface (paragraphe 21.18) dans le message Relay-forward. Le serveur va inclure l'option Identifiant d'interface dans son message Relay-reply. L'agent de relais règle le champ Adresse de liaison comme décrit plus haut dans ce paragraphe, sans considération de si l'agent de relais inclut une option Identifiant d'interface dans le message Relay-forward.

19.1.2 Relais d'un message provenant d'un agent de relais

Si le message reçu par l'agent de relais est un message Relay-forward et si la valeur du compte de bonds dans le message est supérieure ou égale à HOP_COUNT_LIMIT, l'agent de relais élimine le message reçu.

L'agent de relais copie l'adresse de source provenant du datagramme IP dans lequel le message a été reçu dans le champ Adresse de l'homologue dans le message Relay-forward et règle le champ compte de bonds à la valeur du champ Compte de bonds dans le message reçu, incrémenté de 1.

Si l'adresse de source dans l'en-tête du datagramme IP du message reçu est une adresse d'envoi individuel de portée mondiale (c'est-à-dire, GUA ou ULA) l'agent de relais règle le champ Adresse de liaison à 0 ; autrement, l'agent de relais règle le champ Adresse de liaison à une adresse d'envoi individuel de portée mondiale (c'est-à-dire, GUA ou ULA) allouée à l'interface sur laquelle le message a été reçu ou inclut une option Identifiant d'interface (21.18) pour identifier l'interface sur laquelle le message a été reçu.

19.1.3 Comportement d'agent de relais avec délégation de préfixe

Un agent de relais transmet les messages contenant des options de délégation de préfixe de la même façon qu'il relaye les adresses (c'est-à-dire, selon les paragraphes 19.1.1 et 19.1.2).

Si un serveur communique avec un client à travers un agent de relais sur des préfixes délégués, le serveur peut avoir besoin d'un protocole ou autre communication hors bande pour configurer les informations d'acheminement pour les préfixes délégués sur tout routeur à travers lequel le client peut transmettre du trafic.

19.2 Relais d'un message Relay-reply

L'agent de relais traite toutes les options incluses dans le message Relay-reply en plus de l'option Message de relais (paragraphe 21.10).

L'agent de relais extrait le message de l'option Message de relais et le relaye à l'adresse contenue dans le champ Adresse de l'homologue du message Relay-reply. Les agents de relais NE DOIVENT PAS modifier le message.

Si le message Relay-reply comporte une option Identifiant d'interface (paragraphe 21.18) il relaye le message du serveur au client sur la liaison identifiée par l'option Identifiant d'interface. Autrement, si le champ Adresse de liaison n'est pas réglé à 0, l'agent de relais relaye le message sur la liaison identifiée par le champ Adresse de liaison.

Si l'agent de relais reçoit un message Relay-reply, il DOIT traiter le message comme défini ci-dessus, sans considération du type de message encapsulé dans l'option Message de relais.

19.3 Construction des messages Relay-reply

Un serveur utilise un message Relay-reply pour (1) retourner une réponse à un client si le message original provenant du client a été relayé au serveur dans un message Relay-forward ou (2) envoyer un message Reconfigure à un client si le serveur n'a pas d'adresse qu'il puisse utiliser pour envoyer le message directement au client.

Une réponse au client DOIT être relayée par les mêmes agents de relais que le message original du client. Le serveur fait arriver cela en créant un message Relay-reply qui inclut une option Message de relais (paragraphe 21.10) contenant le message pour le prochain agent de relais sur le chemin de retour au client. Le message Relay-reply contient une autre option Message de relais à envoyer au prochain agent de relais, et ainsi de suite. Le serveur doit enregistrer le contenu des champs Adresse de l'homologue dans le message reçu afin qu'il puisse construire le message Relay-reply approprié portant la réponse du serveur.

Par exemple, si le client C a envoyé un message qui a été relayé par l'agent de relais A à l'agent de relais B et ensuite au

serveur, le serveur va envoyer le message Relay-reply suivant à l'agent de relais B :

type de message : RELAY-REPL
compte de bonds : 1
adresse de liaison : 0
adresse de l'homologue : A

option Message de relais contenant ce qui suit :
type de message : RELAY-REPL
compte de bonds : 0
adresse de liaison : adresse provenant de la liaison à laquelle C est rattaché
adresse de l'homologue : C
option Message de relais : <réponse du serveur>

Figure 10 : Exemple de Relay-reply

Quand il envoie un message Reconfigure à un client à travers un agent de relais, le serveur crée un message Relay-reply qui inclut une option Message de relais contenant le message Reconfigure pour le prochain agent de relais sur le chemin de retour au client. Le serveur règle le champ Adresse de l'homologue dans l'en-tête de message Relay-reply à l'adresse du client et règle le champ Adresse de liaison comme exigé par l'agent de relais pour relayer le message Reconfigure au client. Le serveur obtient les adresses du client et de l'agent de relais par une interaction antérieure avec le client ou par un mécanisme externe.

19.4 Interaction entre agents de relais et serveurs

Chaque fois qu'un paquet est relayé par un agent de relais vers un serveur, un nouveau niveau d'encapsulation est ajouté autour du paquet. Chaque relais est autorisé à insérer des options supplémentaires sur le niveau d'encapsulation qu'il ajoute mais NE DOIT PAS changer quelque chose dans le paquet encapsulé. Si il y a plusieurs relais entre un client et un serveur, plusieurs encapsulations sont utilisées. Bien que cela rende le traitement de paquet un peu plus complexe, cela donne l'avantage majeur d'avoir une claire indication sur quel relais a inséré quelle option. Le paquet de réponse est supposé voyager à travers les mêmes relais, mais en ordre inverse. Chaque fois qu'un paquet de réponse est relayé en retour vers le client, un niveau d'encapsulation est retiré.

Dans certains cas, les relais peuvent ajouter une ou plusieurs options. Ces options peuvent être ajoutées pour plusieurs raisons :

- En premier lieu, les relais peuvent fournir des informations supplémentaires sur le client. Cette source d'informations est généralement plus digne de confiance pour un administrateur de serveur, car elle vient de l'infrastructure du réseau plutôt que du client et ne peut pas être facilement contrefaite. Ces options peuvent être utilisées par le serveur pour déterminer sa politique d'allocations.

- En second lieu, un relais peut avoir besoin de certaines informations pour renvoyer une réponse au client. Les agents de relais sont supposés être sans état (ils ne conservent aucun état après qu'un paquet a été traité). Un agent de relais peut inclure l'option Identifiant d'interface (paragraphe 21.18) qui va avoir son écho dans la réponse. Il peut inclure d'autres options et demander au serveur de faire écho à une ou plusieurs des options dans la réponse. Ces options peuvent alors être utilisées par l'agent de relais pour renvoyer la réponse au client, ou pour d'autres besoins. Le client ne va jamais voir ces options. Voir les détails dans la [RFC4994].

- Troisièmement, parfois un relais est le meilleur appareil pour fournir des valeurs pour certaines options. Un relais peut insérer une option dans le paquet transmis au serveur et demander au serveur de repasser cette option au client. Le client va recevoir cette option. On devrait noter que le serveur est l'autorité ultime ici, et – selon sa configuration -- il peut ou non renvoyer l'option au client. Voir les détails dans la [RFC6422].

Pour diverses raisons, les serveurs peuvent avoir besoin de conserver les informations de relais après l'achèvement du traitement du paquet. Une d'elles est le mécanisme brut de leasequery qui peut demander toutes les adresses et/ou préfixes qui ont été alloués via un relais spécifique. Une seconde est pour le mécanisme de reconfiguration. Le serveur peut choisir de ne pas envoyer le message Reconfigure directement au client mais plutôt de l'envoyer via des relais. Ce comportement particulier est considéré comme un détail de mise en œuvre et sort du domaine d'application du présent document.

20. Authentification des messages DHCP

Le présent document introduit deux mécanismes de sécurité pour l'authentification des messages DHCP : (1) l'authentification (et le chiffrement) des messages envoyés entre les serveurs et agents de relais en utilisant IPsec et (2) la protection contre la mauvaise configuration d'un client causée par un message Reconfigure envoyé par un serveur DHCP malveillant.

Le protocole d'authentification retardée, défini dans la [RFC3315], a été rendu obsolète par le présent document (voir la Section 25).

20.1 Sécurité des messages envoyés entre serveurs et agents de relais

Les agents de relais et les serveurs qui échangent des messages peuvent utiliser IPsec comme précisé dans la [RFC8213].

20.2 Résumé de l'authentification DHCP

L'authentification des messages DHCP est réalisée par l'utilisation de l'option Authentification (paragraphe 21.11). Les informations d'authentification portées dans l'option Authentification peuvent être utilisées pour identifier de façon fiable la source d'un message DHCP et pour confirmer que le contenu du message DHCP n'a pas été altéré.

L'option Authentification donne un cadre pour plusieurs protocoles d'authentification. Un de ces protocoles, RKAP, est défini au paragraphe 20.4. D'autres protocoles qui seront définis à l'avenir seront spécifiés dans des documents distincts.

Aucun message DHCP NE DOIT inclure plus d'une option Authentification.

Le champ Protocole dans l'option Authentification identifie le protocole spécifique utilisé pour générer les informations d'authentification portées dans l'option. Le champ Algorithme identifie un algorithme spécifique au sein du protocole d'authentification ; par exemple, le champ Algorithme spécifie l'algorithme de hachage utilisé pour générer le code d'authentification de message (MAC, *Message Authentication Code*) dans l'option Authentification. Le champ RDM spécifie le type de détection de répétition utilisé dans le champ Détection de répétition.

20.3 Détection de répétition

Le champ RDM de l'option Authentification (paragraphe 21.11) détermine le type de détection de répétition utilisé dans le champ Détection de répétition.

Si le champ RDM contient 0x00, le champ Détection de répétition DOIT être réglé à la valeur d'un entier non signé de 64 bits à croissance strictement monotone (modulo 2^64). Utiliser cette technique peut réduire le danger des attaques en répétition. Cette méthode DOIT être prise en charge par tous les protocoles de l'option Authentification. Un choix pourrait être d'utiliser le format d'horodatage de 64 bits de NTP [RFC5905]).

Un client qui reçoit un message avec le champ RDM réglé à 0x00 DOIT comparer son champ Détection de répétition avec la valeur précédente envoyée par le même serveur (sur la base de l'option Identifiant de serveur ; voir au paragraphe 21.3) et n'accepter le message que si la valeur reçue est supérieure et enregistrer celle-ci comme la nouvelle valeur. Si c'est la première fois qu'un client traite une option Authentification envoyée par un serveur, le client DOIT enregistrer la valeur de détection de répétition et sauter la vérification de détection de répétition.

Les serveurs qui prennent en charge le mécanisme de reconfiguration DOIVENT s'assurer que la valeur de détection de répétition est conservée entre les redémarrages. Manquer à le faire peut causer le refus des clients de messages Reconfigure envoyés par le serveur, rendant effectivement inutile le mécanisme de reconfiguration.

20.4 Protocole d'authentification de clé de reconfiguration

Le protocole d'authentification de clé de reconfiguration (RKAP, *Reconfiguration Key Authentication Protocol*) assure la protection contre la mauvaise configuration d'un client causée par un message Reconfigure envoyé par un serveur DHCP malveillant. Dans ce protocole, un serveur DHCP envoie une clé de reconfiguration au client dans l'échange initial de messages DHCP. Le client enregistre la clé de reconfiguration à utiliser pour authentifier les messages Reconfigure suivants en provenance de ce serveur. Le serveur inclut alors un code d'authentification de message haché (HMAC, *Hashed*

Message Authentication Code) calculé à partir de la clé de reconfiguration dans les messages Reconfigure suivants.

La clé de reconfiguration envoyée du serveur au client et le HMAC dans les messages Reconfigure suivants sont tous deux portés comme informations d'authentification dans une option Authentification (paragraphe 21.11). Le format des informations d'authentification est défini au paragraphe suivant.

RKAP n'est utilisé (initié par le serveur) que si client et serveur ont négocié l'utilisation des messages Reconfigure.

20.4.1 Utilisation de l'option d'authentification dans RKAP

Les champs suivants sont établis dans l'option Authentification (paragraphe 21.11) pour RKAP :
Protocole : 3
Algorithme : 1
RDM : 0

Le format des informations d'authentification pour RKAP est :

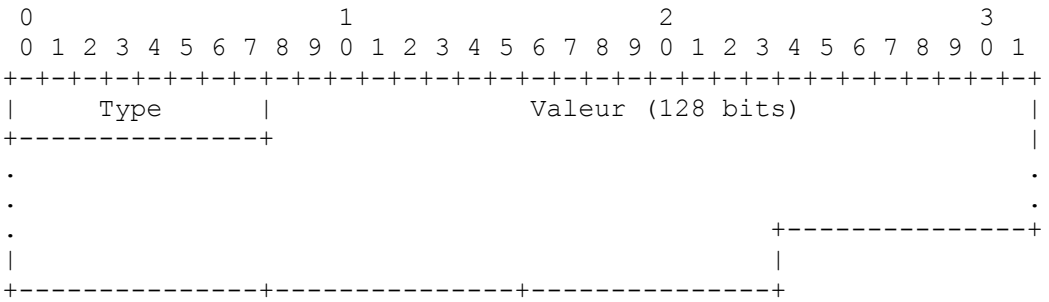


Figure 11 : Informations d'authentification RKAP

Type : Champ d'un octet. Type des données dans le champ Valeur porté dans cette option :
1 : valeur de la clé Reconfigure (utilisée dans le message Reply).
2 : résumé HMAC-MD5 du message (utilisé dans le message Reconfigure).

Valeur : données comme défini dans le champ Type. Champ de 16 octets.

20.4.2 Considérations de serveur pour RKAP

Le serveur choisit une clé de reconfiguration pour un client durant l'échange de messages Request/Reply, Solicit/Reply, ou Information-request/Reply. Le serveur enregistre la clé de reconfiguration et transmet cette clé au client dans une option Authentification (paragraphe 21.11) dans le message Reply.

La clé de reconfiguration fait 128 bits et DOIT être un nombre aléatoire ou pseudo aléatoire cryptographiquement fort qui ne puisse pas être facilement prédit.

Pour assurer l'authentification d'un message Reconfigure, le serveur choisit une valeur de détection de répétition conformément à la RDM choisie par le serveur et calcule un HMAC-MD5 du message Reconfigure en utilisant la clé de reconfiguration pour le client. Le serveur calcule le HMAC-MD5 sur le message DHCP Reconfigure entier, incluant l'option Authentification ; le champ HMAC-MD5 dans l'option Authentification est réglé à 0 pour le calcul du HMAC-MD5. Le serveur inclut le HMAC-MD5 dans le champ Informations d'authentification dans une option Authentification incluse dans le message Reconfigure envoyé au client.

20.4.3 Considérations de client pour RKAP

Le client va recevoir une clé de reconfiguration du serveur dans une option Authentification (paragraphe 21.11) dans le message Reply initial du serveur. Le client enregistre la clé de reconfiguration pour l'utiliser à l'authentification des messages Reconfigure suivants.

Pour authentifier un message Reconfigure, le client calcule un HMAC-MD5 sur le message Reconfigure, avec des zéros

substitués au champ HMAC-MD5, en utilisant la clé de reconfiguration reçue du serveur. Si ce HMAC-MD5 calculé correspond à la valeur dans l'option Authentification, le client accepte le message Reconfigure.

21. Options DHCP

Les options sont utilisées pour porter des informations et paramètres supplémentaires dans les messages DHCP. Toutes les options partagent un format de base commun, comme décrit au paragraphe 21.1. Toutes les valeurs dans les options sont représentées dans l'ordre des octets du réseau.

Le présent document décrit les options DHCP définies au titre de la spécification DHCP de base. D'autres options pourront être définies à l'avenir dans des documents distincts. Voir dans la [RFC7227] des lignes directrices sur la définition de nouvelles options. Voir à la Section 24 des informations supplémentaires sur le registre des codes d'option DHCPv6 tenu par l'IANA.

Sauf mention contraire, chaque option peut apparaître seulement dans la zone d'options d'un message DHCP et ne peut apparaître qu'une seule fois. Si une option apparaît plusieurs fois, chaque instance est considérée séparément et les zones de données des options NE DOIVENT PAS être enchaînées ou autrement combinées.

Les options qui ne sont autorisées à apparaître qu'une seule fois sont appelées "options singletons". Les seules options non singletons définies dans le présent document sont les options IA_NA (paragraphe 21.4) IA_TA (paragraphe 21.5) Classe de fabricant (paragraphe 21.16) Informations spécifiques de fabricant (21.17) et IA_PD (paragraphe 21.21). Aussi, Adresse d'IA (paragraphe 21.6) et Préfixe d'IA (paragraphe 21.22) peuvent apparaître plus d'une fois dans leurs options respectives.

21.1 Format des options DHCP

Le format des options DHCP est :

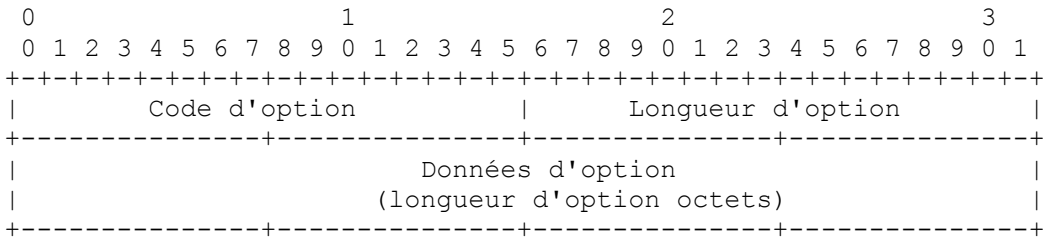


Figure 12 : Format d'option

Code d'option : entier non signé qui identifie le type d'option spécifique porté dans cette option. Champ de 2 octets.

Longueur d'option : entier non signé donnant la longueur du champ Données d'option dans cette option en octets. Champ de 2 octets.

Données d'option : données pour l'option ; le format de ces données dépend de la définition de l'option. Un champ de longueur variable (la longueur, en octets, est spécifiée par Longueur d'option).

Les options DHCP ont leur portée définie en utilisant l'encapsulation. Certaines options s'appliquent généralement au client, certaines sont spécifiques d'une IA, et certaines sont spécifiques des adresses au sein d'une IA. Ces deux derniers cas sont discutés aux paragraphes 21.4, 21.5, et 21.6.

21.2 Option Identifiant de client

L'option Identifiant de client est utilisée pour porter un DUID (voir la Section 11) qui identifie le client. Le format de l'option Identifiant de client est :

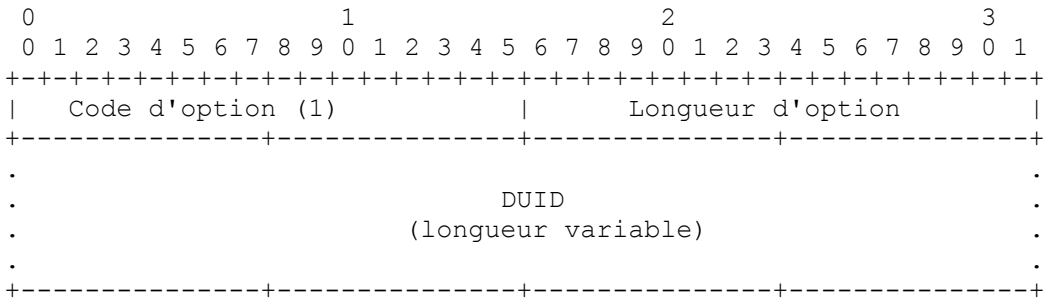


Figure 13 : Format d'option Identifiant de client

Code d'option : OPTION_CLIENTID (1).
Longueur d'option : longueur du DUID en octets.
DUID : le DUID pour le client.

21.3 Option Identifiant de serveur

L'option Identifiant de serveur est utilisée pour porter un DUID (voir la Section 11) qui identifie le serveur. Le format de l'option Identifiant de serveur est :

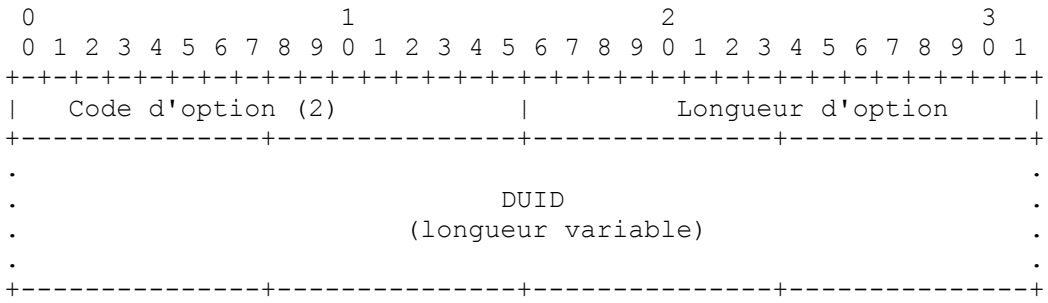


Figure 14 : Format d'option Identifiant de serveur

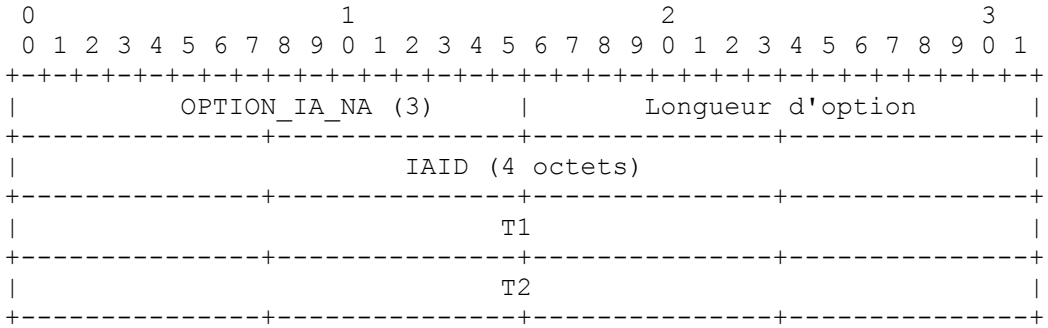
Code d'option : OPTION_SERVERID (2).
Longueur d'option : longueur du DUID en octets.
DUID : le DUID pour le serveur.

21.4 Option Association d'identité pour adresses non temporaires

L'option Association d'identité pour adresses non temporaires (IA_NA, *Identity Association for Non-temporary Addresses*) est utilisée pour porter une IA_NA, les paramètres associés à la IA_NA, et les adresses non temporaires associées à la IA_NA.

Les adresses qui apparaissent dans une option IA_NA sont des adresses non temporaires (voir au paragraphe 21.5).

Le format de l'option IA_NA est :



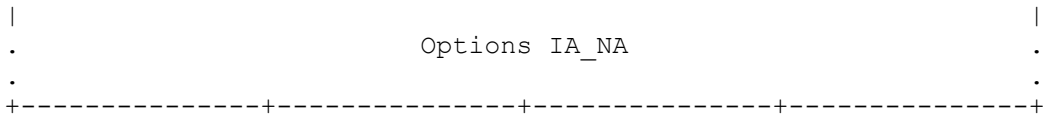


Figure 15 : Format de l'option Association d'identité pour adresses non temporaires

Code d'option : OPTION_IA_NA (3).
Longueur d'option : 12 + longueur du champ Options IA_NA.
IAID : identifiant univoque pour cette IA_NA ; l'IAID doit être unique parmi les identifiants pour tous les IAID de ce client. L'espace de nombres pour les IAID de IA_NA est séparé de l'espace de nombres pour les autres types d'option d'IA (c'est-à-dire, IA_TA et IA_PD). Champ de 4 octets contenant un entier non signé.

T1 : intervalle de temps après lequel le client devrait contacter le serveur de qui les adresses dans la IA_NA ont été obtenues pour étendre les durées de vie des adresses allouées à la IA_NA ; T1 est une durée relative à l'heure actuelle exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.

T2 : intervalle de temps après lequel le client devrait contacter tout serveur disponible pour étendre les durées de vie des adresses allouées à la IA_NA ; T2 est une durée relative à l'heure actuelle exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.

Options IA_NA : options associées à cette IA_NA. Champ de longueur variable (12 octets de moins que la valeur dans le champ Longueur d'option).

Le champ Options IA_NA encapsule les options qui sont spécifiques de cette IA_NA. Par exemple, toutes les options Adresse d'IA (paragraphe 21.6) portant les adresses associées à cette IA_NA sont dans le champ Options IA_NA.

Chaque IA_NA porte un "ensemble" d'adresses non temporaires ; il relève de la politique du serveur de déterminer combien d'adresses sont allouées, mais normalement au plus une adresse est allouée à partir de chaque préfixe alloué à la liaison à laquelle le client est rattaché.

Une option IA_NA peut seulement apparaître dans la zone d'options d'un message DHCP. Un message DHCP peut contenir plusieurs options IA_NA (bien que chacune doive avoir un IAID unique).

Le statut de toute opération impliquant cette IA_NA est indiqué dans une option Code d'état (paragraphe 21.13) dans le champ Options IA_NA.

Noter qu'une IA_NA n'a pas de "durée de vie" ou de "longueur de prêt" explicite par elle-même. Quand les durées de vie valides de toutes les adresses dans une IA_NA ont expiré, la IA_NA elle-même peut être considérée comme ayant expiré. T1 et T2 sont inclus pour donner aux serveurs un contrôle explicite sur quand un client recontacte le serveur sur une IA_NA spécifique.

Dans un message envoyé par un client à un serveur, les champs T1 et T2 DEVRAIT être réglés à 0. Le serveur DOIT ignorer toute valeur dans ces champs dans les messages reçus d'un client.

Dans un message envoyé par un serveur à un client, le client DOIT utiliser les valeurs dans les champs T1 et T2 pour les temps T1 et T2, sauf si les valeurs dans ces champs sont 0. Les valeurs dans les champs T1 et T2 sont le nombre de secondes depuis T1 et T2 et sont calculées depuis la réception du message.

Conformément au paragraphe 7.7, la valeur 0xffffffff est prise pour signifier "infini" et devrait être utilisée avec prudence.

Le serveur choisit les valeurs T1 et T2 pour permettre au client d'étendre les durées de vie de toute adresse dans la IA_NA avant que les durées de vie expirent, même si le serveur est indisponible pour un court instant. Les valeurs recommandées pour T1 et T2 sont, respectivement, 0,5 et 0,8 fois la plus courte durée de vie préférée des adresses dans l'IA que le serveur veut étendre. Si la "plus courte" durée de vie préférée est 0xffffffff ("infini") les valeurs recommandées de T1 et T2 sont aussi 0xffffffff. Si le moment auquel les adresses dans une IA_NA sont à renouveler est à laisser à la discrétion du client, le serveur règle les valeurs de T1 et T2 à 0. Le client DOIT suivre les règles définies au paragraphe 14.2.

Si un client reçoit une IA_NA avec T1 supérieur à T2 et si T1 et T2 sont tous deux supérieurs à 0, le client élimine l'option IA_NA et traite le reste du message comme si le serveur n'avait pas inclus l'option IA_NA invalide.

21.5 Option Association d'identité pour adresses temporaires

L'option Association d'identité pour adresses temporaires (IA_TA, *Identity Association for Temporary Addresses*) est utilisée pour porter une IA_TA, les paramètres associés à la IA_TA, et les adresses associées à la IA_TA. Toutes les adresses dans cette option sont utilisées par le client comme des adresses temporaires, comme défini dans la [RFC4941]. Le format de l'option IA_TA est :

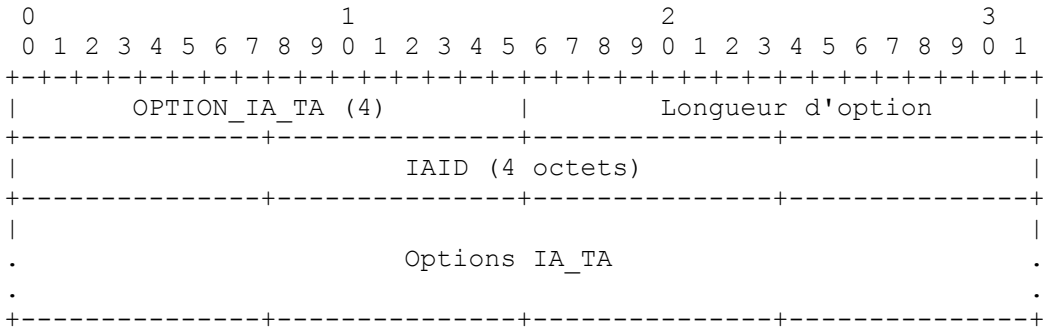


Figure 16 : Format d'option Association d'identité pour adresses temporaires

Code d'option : OPTION_IA_TA (4).
Longueur d'option : 4 + longueur du champ Options IA_TA.
IAID : identifiant univoque pour cette IA_TA ; l'IAID doit être unique parmi les identifiants pour toutes IA_TA de ce client. L'espace de nombres pour les IAID de IA_TA est séparé de l'espace de nombres pour les autres types d'option d'IA (c'est-à-dire, IA_NA et IA_PD). Champ de 4 octets contenant un entier non signé.
Options IA_TA : options associées à cette IA_TA. Champ de longueur variable (4 octets de moins que la valeur dans le champ Longueur d'option).

Le champ Options IA_TA encapsule les options qui sont spécifiques de cette IA_TA. Par exemple, toutes les options Adresse d'IA (voir au paragraphe 21.6) portant les adresses associés à cette IA_TA sont dans le champ Options IA_TA.

Chaque IA_TA porte un "ensemble" d'adresses temporaires. Il appartient à la politique du serveur de déterminer combien d'adresses sont allouées.

Une option IA_TA peut seulement apparaître dans la zone d'options d'un message DHCP. Un message DHCP peut contenir plusieurs options IA_TA (bien que chacune doive avoir un IAID unique).

Le statut de toute opération impliquant cette IA_TA est indiqué dans une option Code d'état (voir au paragraphe 21.13) dans le champ Options IA_TA.

Noter qu'une IA n'a pas de "durée de vie" ou "longueur de prêt" explicite par elle-même. Quand les durées de vie valides de toutes les adresses dans une IA_TA ont expiré, l'IA peut être considérée comme ayant expiré.

Une option IA_TA n'inclut pas de valeurs pour T1 et T2. Un client PEUT demander que la durée de vie valide sur les adresses temporaires soit étendue en incluant les adresses dans une option IA_TA envoyée dans un message Renew ou Rebind à un serveur. Par exemple, un client demanderait une extension sur la durée de vie valide d'une adresse temporaire pour permettre à une application de continuer d'utiliser une connexion TCP établie. Étendre seulement la durée de vie valide, mais pas la préférée signifie que l'adresse va finir éventuellement dans un état déconseillé. Les connexions existantes pourraient continuer, mais aucune nouvelle ne serait créée en utilisant cette adresse.

Le client obtient de nouvelles adresses temporaires en envoyant une option IA_TA avec un nouvel IAID à un serveur. Demander de nouvelles adresses temporaires au serveur est équivalent à générer de nouvelles adresses temporaires comme décrit à la [RFC4941]. Le serveur va générer de nouvelles adresses temporaires et les retourner au client. Le client devrait demander de nouvelles adresses temporaires avant qu'expirent les durées de vie sur les adresses allouées précédemment.

Un serveur DOIT retourner le même ensemble d'adresses temporaires pour la même IA_TA (identifiée par son IAID) pour autant que ces adresses soient encore valides. Après l'expiration des durées de vie des adresses dans une IA_TA, l'IAID peut être réutilisé pour identifier une nouvelle IA_TA avec de nouvelles adresses temporaires.

21.6 Option Adresse d'IA

L'option Adresse d'IA est utilisée pour spécifier une adresse associée à une IA_NA ou IA_TA. L'option Adresse d'IA doit être encapsulée dans le champ Options IA_NA d'une option IA_NA (paragraphe 21.4) ou dans le champ Options IA_TA d'une option IA_TA (paragraphe 21.5). Le champ Options d'adresse d'IA encapsule les options spécifiques de cette adresse.

Le format de l'option Adresse d'IA est :

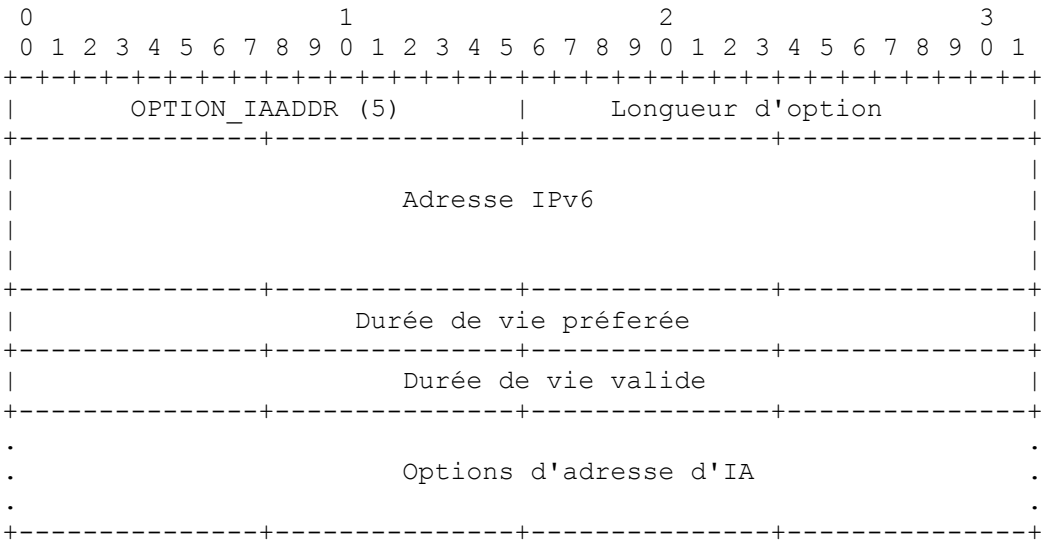


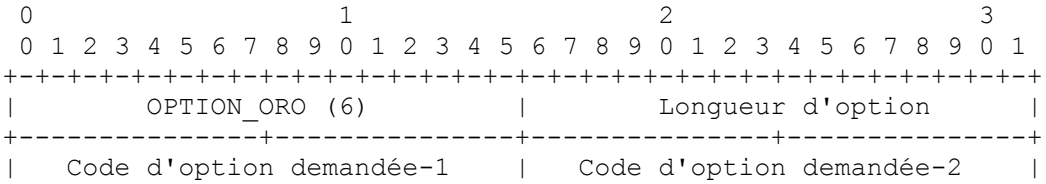
Figure 17 : Format d'option Adresse d'IA

Code d'option : OPTION_IAADDR (5).
Longueur d'option : 24 + longueur du champ Options d'adresse d'IA.
Adresse IPv6 : adresse IPv6. Un client NE DOIT PAS former un préfixe implicite avec une longueur autre que 128 pour cette adresse. Champ de seize octets.
Durée de vie préférée : durée de vie préférée pour l'adresse dans l'option, exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.
Durée de vie valide : durée de vie valide pour l'adresse dans l'option, exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.
Options d'adresse d'IA : options associées à cette adresse. Champ de longueur variable (24 octets de moins que la valeur dans le champ Longueur d'option).

Dans un message envoyé par un client à un serveur, les champs Durée de vie préférée et Durée de vie valide DEVRAIENT être réglés à 0. Le serveur DOIT ignorer toute valeur reçue. Le client NE DEVRAIT PAS envoyer l'option Adresse d'IA avec une adresse non spécifiée (::). Dans un message envoyé par un serveur à un client, le client DOIT utiliser les valeurs dans les champs Durée de vie préférée et Durée de vie valide pour les durées de vie préférée et valide. Les valeurs dans ces champs sont le nombre de secondes restantes dans chaque durée de vie. Le client DOIT éliminer toute adresse pour laquelle la durée de vie préférée est supérieure à la durée de vie valide. Conformément au paragraphe 7.7, si la durée de vie valide d'une adresse est 0xffffffff, elle est prise comme signifiant "infini" et devrait être utilisée avec prudence. Plus d'une option d'adresse d'IA peut apparaître dans une option IA_NA ou IA_TA. Le statut de toute opération impliquant cette adresse d'IA est indiqué dans une option Code d'état dans le champ Options d'adresse d'IA, comme spécifié au paragraphe 21.13.

21.7. Option Demande d'option

L'option Demande d'option est utilisée pour identifier une liste des options dans un message entre un client et un serveur. Le format de l'option Demande d'option est :



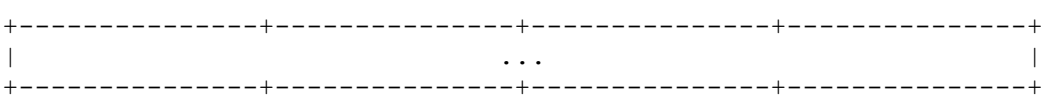


Figure 18 : Format d'option Demande d'option

Code d'option : OPTION_ORO (6).
Longueur d'option : 2 fois le nombre d'options demandé.
Code d'option demandée-n : code d'option pour une option demandée par le client. Chaque code d'option est un champ de deux octets contenant un entier non signé.

Un client DOIT inclure une option Demande d'option dans un message Solicit, Request, Renew, Rebind, ou Demande d'information pour informer le serveur des options que le client veut que le serveur lui envoie. Pour certains types de messages, certains codes d'option DOIVENT être inclus dans l'option Demande d'option ; voir les détails au Tableau 4 à la Section 24.

L'option Demande d'option NE DOIT PAS inclure les options suivantes :
- Identifiant de client (paragraphe 21.2)
- Identifiant de serveur (paragraphe 21.3)
- IA_NA (paragraphe 21.4)
- IA_TA (paragraphe 21.5)
- IA_PD (paragraphe 21.21)
- Adresse d'IA (paragraphe 21.6)
- Préfixe d'IA (paragraphe 21.22)
- Demande d'option (ce paragraphe)
- Temps écoulé (paragraphe 21.9)
- Préférence (paragraphe 21.8)
- Message de relais (paragraphe 21.10)
- Authentification (paragraphe 21.11)
- Serveur en envoi individuel (paragraphe 21.12)
- Code d'état (paragraphe 21.13)
- Engagement rapide (paragraphe 21.14)
- Classe d'utilisateur (paragraphe 21.15)
- Classe de fabricant (paragraphe 21.16)
- Identifiant d'interface (paragraphe 21.18)
- Message Reconfigure (paragraphe 21.19)
- Accepte Reconfigure (paragraphe 21.20)

Les autres options de niveau supérieur DOIVENT apparaître dans l'option Demande d'option sinon elles ne seront pas envoyées par le serveur. Seules les options de niveau supérieur PEUVENT apparaître dans l'option Demande d'option. Les options encapsulées dans une option conteneur NE DEVRAIENT PAS apparaître dans une option Demande d'option ; voir dans la [RFC7598] un exemple d'options conteneur. Cependant, des options PEUVENT être définies qui spécifient des exceptions à cette restriction sur l'inclusion d'options encapsulées dans une option Demande d'option. Par exemple, l'option Demande d'option PEUT être utilisée pour signaler la prise en charge d'une caractéristique même quand cette option est encapsulée, comme dans le cas de l'option Exclusion de préfixe [RFC6603]. Voir le Tableau 4.

21.8 Option Préférence

L'option Préférence est envoyée par un serveur à un client pour contrôler le choix d'un serveur par le client.

Le format de l'option Préférence est :

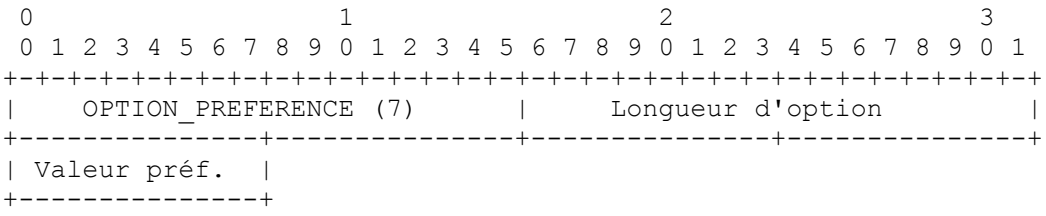


Figure 19 : Format d'option Preference

Code d'option : OPTION_PREFERENCE (7).
Longueur d'option : 1.
Valeur préf : valeur de préférence pour le serveur dans ce message. Entier d'un octet non signé.

Un serveur PEUT inclure une option Préférence dans un message Advertise pour contrôler le choix d'un serveur par le client. Voir au paragraphe 18.2.9 les informations concernant l'utilisation de l'option Préférence par le client et l'interprétation de la valeur de données de l'option Préférence.

21.9 Option Temps écoulé

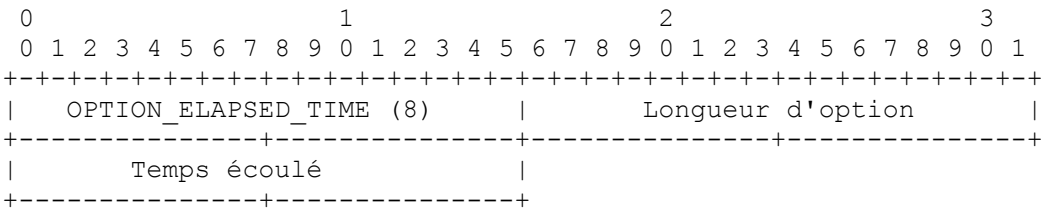


Figure 20 : Format d'option Temps écoulé

Code d'option : OPTION_ELAPSED_TIME (8).
Longueur d'option : 2.
Temps écoulé : quantité de temps depuis que le client a commencé sa transaction DHCP en cours. Ce temps est exprimé en centièmes de seconde (10^-2 seconde). Champ de 2 octets contenant un entier non signé.

Un client DOIT inclure une option Temps écoulé dans les messages pour indiquer pendant combien de temps le client a essayé d'achever un échange de messages DHCP. Le temps écoulé est mesuré depuis l'instant où le client a envoyé le premier message de l'échange de messages, et le champ Temps écoulé est réglé à 0 dans le premier message de l'échange de messages. Les serveurs et agents de relais utilisent la valeur en données dans cette option comme entrée de politique qui contrôle comment un serveur répond au message d'un client. Par exemple, l'option Temps écoulé permet à un serveur DHCP secondaire de répondre à une demande quand un serveur principal n'a pas répondu dans un délai raisonnable. La valeur du temps écoulé est un entier non signé de 16 bits (deux octets). Le client utilise la valeur 0xffff pour représenter toute valeur de temps écoulé supérieure à la plus grande valeur de temps qui peut être représentée dans l'option Temps écoulé.

21.10 Option Message de relais

L'option Message de relais porte un message DHCP dans un message Relay-forward ou Relay-reply. Le format de l'option Message de relais est :

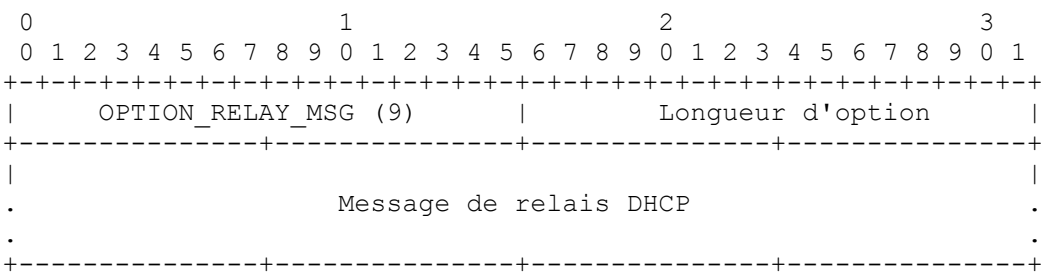


Figure 21 : Format d'option Message de relais

Code d'option : OPTION_RELAY_MSG (9).
Longueur d'option : longueur du champ Mesage de relais DHCP.
Message de relais DHCP : dans un message Relay-forward, le message reçu, relayé verbatim au prochain agent de relais ou serveur ; dans un message Relay-reply, le message à copier et relayer à l'agent de relais ou client dont l'adresse est dans le champ Adresse de l'homologue du message Relay-reply. La longueur, en octets, est spécifiée par Longueur d'option.

21.11 Option Authentification

L'option Authentification porte les informations d'authentification pour authentifier l'identité et le contenu des messages DHCP. L'utilisation de l'option Authentification est décrite à la Section 20. Le protocole d'authentification retardée, défini dans la [RFC3315], a été rendu obsolète par le présent document, à cause du manque d'usage (voir la Section 25). Le format de l'option Authentification est :

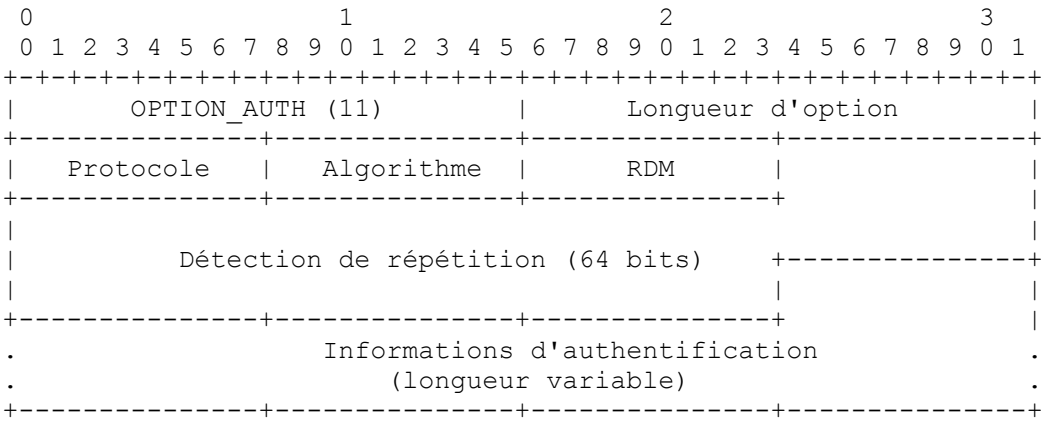


Figure 22 : Format d'option Authentification

Code d'option : OPTION_AUTH (11).
Longueur d'option : 11 + longueur du champ Informations d'authentification.
Protocole : protocole d'authentification utilisé dans cette option Authentification. Entier non signé d'un octet.
Algorithme : algorithme utilisé dans le protocole d'authentification. Entier non signé d'un octet.
RDM : méthode de détection de répétition utilisée dans cette option Authentification. Entier non signé d'un octet.
Détection de répétition : informations de détection de répétition pour la RDM. Champ de 64 bits (8 octets).
Informations d'authentification : informations d'authentification, comme spécifié par le protocole et l'algorithme utilisés dans cette option Authentification. Champ de longueur variable (11 octets de moins que la valeur dans le champ Longueur d'option).

L'IANA tient un registre des valeurs de protocole, algorithme, et RDM à < https://www.iana.org/assignments/auth-namespaces >.

21.12 Option Serveur en envoi individuel

Le serveur envoie cette option à un client pour lui indiquer qu'il lui est permis d'envoyer des messages en envoi individuel au serveur. Le format de l'option Serveur en envoi individuel est :

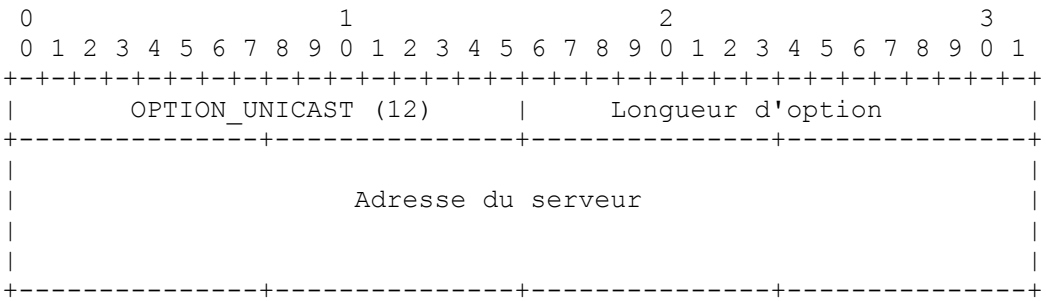


Figure 23 : Format d'option Serveur en envoi individuel

Code d'option : OPTION_UNICAST (12).
Longueur d'option : 16.
Adresse du serveur : adresse de 128 bits à laquelle le client devrait envoyer des messages livrés en envoi individuel.

Le serveur spécifie dans le champ Adresse du serveur l'adresse à laquelle le client va envoyer des messages en envoi individuel. Quand un client reçoit cette option, lorsque elle est permise et appropriée, il envoie ses messages directement au serveur en utilisant l'adresse spécifiée dans le champ Adresse du serveur de l'option.
Quand le serveur envoie l'option Serveur en envoi individuel au client, certains messages du client ne seront pas relayés par des agents de relais et n'incluront pas d'options Agent de relais des agents de relais. Donc, un serveur devrait n'envoyer une option Serveur en envoi individuel à un client que quand les agents de relais n'envoient pas d'options Agent de relais. Un serveur DHCP rejette tout message envoyé de façon inapproprié en utilisant l'envoi individuel pour s'assurer que les messages sont relayés par des agents de relais quand des options Agent de relais sont utilisées.
Les détails sur quand le client peut envoyer des messages au serveur en utilisant l'envoi individuel sont fournis à la Section 18.

21.13 Option Code d'état

Cette option retourne une indication d'état relative au message DHCP ou à l'option dans laquelle elle apparaît. Le format de l'option Code d'état est :

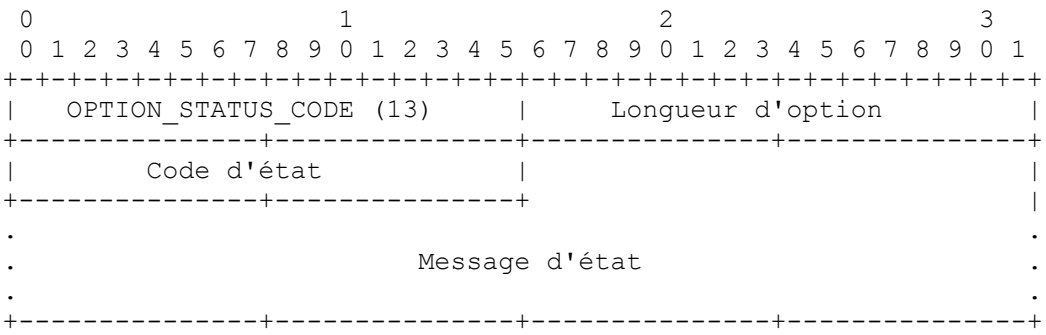


Figure 24 : Format d'option Code d'état

Code d'option : OPTION_STATUS_CODE (13).
Longueur d'option : 2 + longueur du champ Message d'état.
Code d'état : code numérique pour l'état codé dans cette option. Champ de 2 octets contenant un entier non signé.
Message d'état : chaîne de texte codée en UTF-8 [RFC3629] convenable pour l'affichage à l'utilisateur d'extrémité. NE DOIT PAS être terminée par un nul. Champ de longueur variable (2 octets de moins que la valeur dans le champ Longueur d'option).

Une option Code d'état peut apparaître dans le champ "options" d'un message DHCP et/ou dans le champ "options" d'une autre option. Si l'option Code d'état n'apparaît pas dans un message dans lequel l'option pourrait apparaître, l'état du message est supposé être Succès.

Les valeurs de code d'état définies précédemment par les [RFC3315] et [RFC3633] sont :

Nom	Code	Description
Succès	0	Succès.
UnspecFail	1	Échec de raison non spécifiée ; ce code d'état est envoyé par un client ou un serveur pour indiquer un échec non explicitement spécifié dans le présent document.
NoAddrsAvail	2	Le serveur n'a pas d'adresse disponible à allouer à la ou aux IA.
NoBinding	3	Enregistrement de client (lien) non disponible.
NotOnLink	4	Le préfixe pour l'adresse n'est pas approprié pour la liaison à laquelle le client est rattaché.
UseMulticast	5	Envoyé par un serveur à un client pour forcer le client à envoyer les messages au serveur en utilisant l'adresse de diffusion groupée Tous_Agents_de_Relais_et_Serveurs_DHCP.
NoPrefixAvail	6	Le serveur n'a pas de préfixes disponibles à allouer aux IA_PD.

Tableau 3 : Définitions des codes d'état

Voir dans le registre "Status Codes" à < https://www.iana.org/assignments/dhcpv6-parameters > la liste actuelle des codes d'état.

21.14 Option Engagement rapide

L'option Engagement rapide est utilisée pour signaler l'utilisation de l'échange de deux messages pour l'allocation d'adresse. Le format de l'option Engagement rapide est :

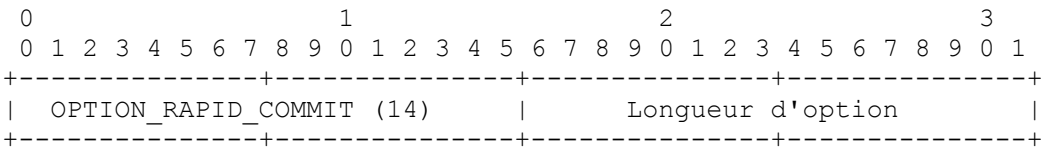


Figure 25 : Format d'option Engagement rapide

Code d'option : OPTION_RAPID_COMMIT (14).
Longueur d'option : 0.

Un client PEUT inclure cette option dans un message Solicit si le client est prêt à effectuer l'échange de messages Solicit/Reply décrit au paragraphe 18.2.1.

Un serveur DOIT inclure cette option dans un message Reply envoyé en réponse à un message Solicit quand il achève l'échange de messages Solicit/Reply.

Discussion : Chaque serveur qui répond par un Reply à un Solicit qui inclut une option Engagement rapide va engager le prêt dans le message Reply au client mais ne va recevoir aucune confirmation que le client a reçu le message Reply. Donc, si plus d'un serveur répond à un Solicit qui inclut une option Engagement rapide, tous sauf un vont engager des prêts qui ne seront en fait pas utilisés par le client ; il pourrait en résulter des informations d'adresse incorrectes dans le DNS si les mises à jour de serveurs DHCP dans le DNS [RFC4704], et des réponses à des demandes leasequery [RFC5007] peuvent inclure des informations sur des prêts non utilisés par le client.

Le problème des prêts non utilisés peut être minimisé en concevant le service DHCP de telle sorte que seul un serveur réponde au Solicit ou en utilisant des durées de vie relativement courtes pour les nouvelles allocations de prêts.

21.15 Option Classe d'utilisateur

L'option Classe d'utilisateur est utilisée par un client pour identifier le type ou la catégorie des utilisateurs ou applications qu'elle représente.

Le format de l'option Classe d'utilisateur est :

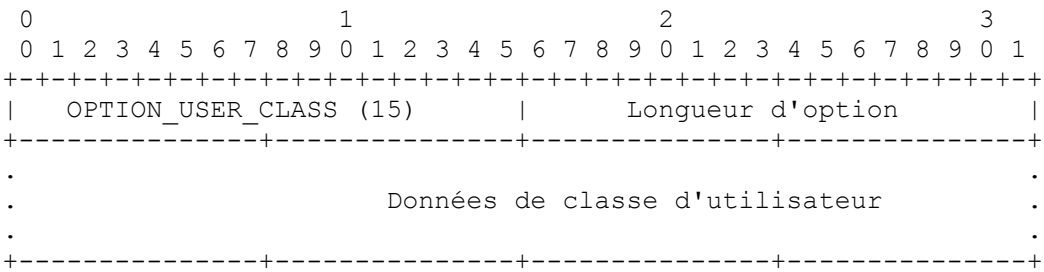


Figure 26 : Format d'option Classe d'utilisateur

Code d'option : OPTION_USER_CLASS (15).
Longueur d'option : longueur du champ Données de classe d'utilisateur.
Données de classe d'utilisateur : classes d'utilisateur portées par le client. La longueur, en octets, est spécifiée par le champ Longueur d'option.

Les informations contenues dans la zone de données de cette option sont contenues dans un ou plusieurs champs opaques qui représentent la ou les classes dont le client est membre. Un serveur choisit les informations de configuration pour le client sur la base des classes identifiées dans cette option. Par exemple, l'option Classe d'utilisateur peut être utilisée pour configurer tous les clients des personnes du département de comptabilité avec une imprimante différente des clients des personnes du département commercial. Les informations de classe d'utilisateur portées dans cette option DOIVENT être configurables sur le client.

La zone de données de l'option Classe d'utilisateur DOIT contenir une ou plusieurs instances d'informations de données de classe d'utilisateur. Chaque instance de données de classe d'utilisateur est formatée comme suit :

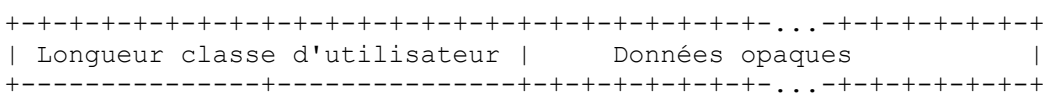


Figure 27 : Format du champ Données de classe d'utilisateur

Le champ données de classe d'utilisateur fait 2 octets et spécifie la longueur des données de classe d'utilisateur opaques dans l'ordre des octets du réseau.

Un serveur interprète les classes identifiées dans cette option conformément à sa configuration pour choisir les informations de configuration appropriées pour le client. Un serveur peut seulement utiliser les classes d'utilisateur qu'il est configuré à interpréter pour le choix des informations de configuration pour un client et ignorer toute autre classe d'utilisateur. En réponse à un message contenant une option Classe d'utilisateur, un serveur peut inclure une option Classe d'utilisateur contenant les classes qui ont été interprétées avec succès par le serveur afin que le client puisse être informé des classes interprétées par le serveur.

21.16 Option Classe de fabricant

Cette option est utilisée par un client pour identifier le fabricant qui a manufacturé le matériel sur lequel le client est installé. Les informations contenues dans la zone de données de cette option sont contenues dans un ou plusieurs champs opaques qui identifient les détails de la configuration de matériel. Le format de l'option Classe de fabricant est :

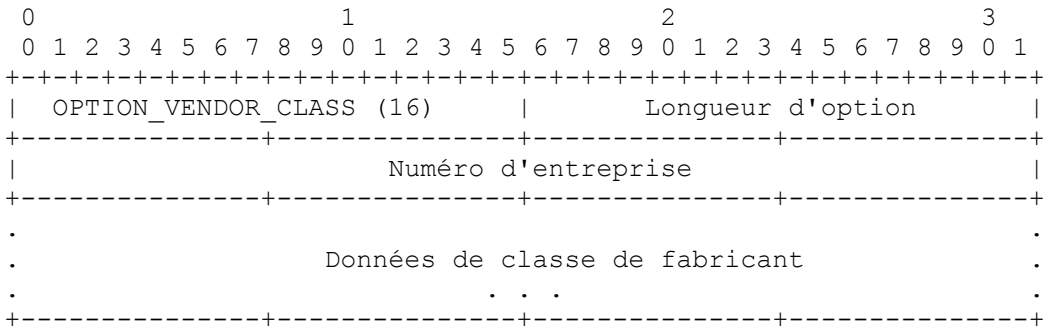


Figure 28 : Format d'option Classe de fabricant

Code d'option : OPTION_VENDOR_CLASS (16).
Longueur d'option : 4 + longueur du champ Données de classe de fabricant.
Numéro d'entreprise : numéro d'entreprise du fabricant comme enregistré par l'IANA [IANA-PEN]. Champ de 4 octets contenant un entier non signé.
Données de classe de fabricant : configuration matérielle du nœud sur lequel fonctionne le client. Champ de longueur variable (4 octets de moins que la valeur dans le champ Longueur d'option).

Le champ Données de classe de fabricant est composé d'une série d'éléments séparés, dont chacun décrit une caractéristique de la configuration matérielle du client. Des exemples d'instances de données de classe de fabricant pourraient inclure la version du système d'exploitation du client ou la quantité de mémoire installée sur le client.

Chaque instance de données de classe de fabricant est formatée comme suit :

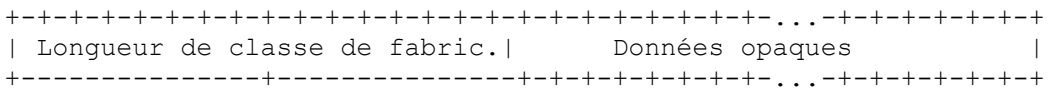


Figure 29 : Format du champ Données de classe de fabricant

Le champ Longueur de -classe de fabricant fait 2 octets et spécifie la longueur des données opaques de classe de fabricant dans l'ordre des octets du réseau.

Les serveurs et clients NE DOIVENT PAS inclure plus d'une instance de l'option Classe de fabricant avec le même numéro d'entreprise. Chaque instance de l'option Classe de fabricant peut porter plusieurs instances de données de classe de fabricant.

21.17 Option Informations spécifiques du fabricant

Cette option est utilisée par les clients et les serveurs pour échanger des informations spécifiques du fabricant.

Le format de l'option Informations spécifiques du fabricant est :

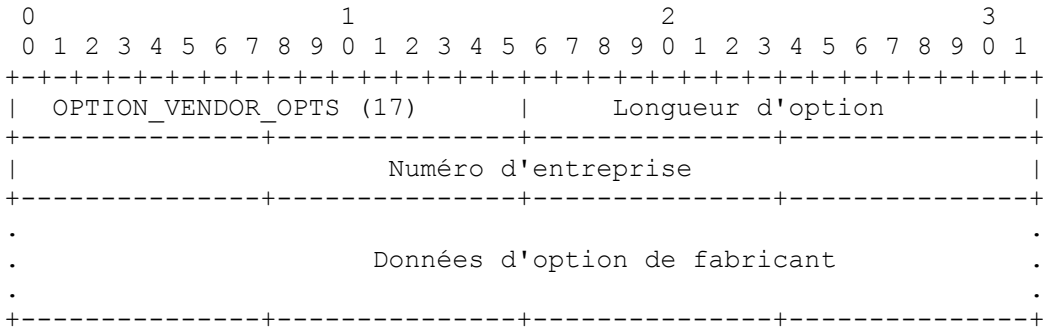


Figure 30 : Format d'option Informations spécifiques du fabricant

Code d'option : OPTION_VENDOR_OPTS (17).
Longueur d'option : 4 + longueur du champ Données d'option de fabricant.
Numéro d'entreprise : numéro d'entreprise enregistré du fabricant comme tenu par l'IANA [IANA-PEN]. Champ de 4 octets contenant un entier non signé.
Données d'option de fabricant : options du fabricant, interprétées par un code spécifique du fabricant sur les clients et les serveurs. Champ de longueur variable (4 octets de moins que la valeur dans le champ Longueur d'option).

La définition des informations portées dans cette option est spécifique du fabricant. Le fabricant est indiqué par le champ Numéro d'entreprise. L'utilisation d'informations spécifiques du fabricant permet d'améliorer le fonctionnement, en utilisant des caractéristiques supplémentaires dans la mise en œuvre de DHCP du fabricant. Un client DHCP qui ne reçoit pas les informations spécifiques du fabricant demandées va quand même configurer la pile IPv6 du nœud pour être fonctionnelle.

Le champ Données d'option de fabricant DOIT être codé comme une séquence de champs code/longueur/valeur de format identique aux options DHCP (voir au paragraphe 21.1). Les codes de sous options sont définies par le fabricant identifié dans le champ Numéro d'entreprise et ne sont pas gérés par l'IANA. Chaque sous option est formatée comme suit :

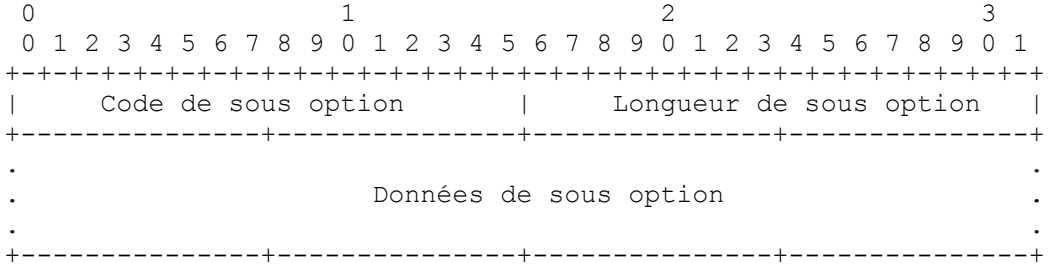


Figure 31 : Format de sous option spécifique de fabricant

Code de sous option : code de la sous option. Champ de 2 octets.
Longueur de sous option : entier non signé donnant la longueur du champ Données de sous option dans cette sous option en octets. Champ de 2 octets.
Données de sous option : zone de données de la sous option. La longueur, en octets, est spécifiée par Longueur de sous option.

Plusieurs instances de l'option Informations spécifiques du fabricant peuvent apparaître dans un message DHCP. Chaque instance de l'option est interprétée conformément aux codes d'option définis par le fabricant identifié par le numéro d'entreprise dans cette option. Les serveurs et clients NE DOIVENT PAS envoyer plus d'une instance de l'option Informations spécifiques du fabricant avec le même numéro d'entreprise. Chaque instance de l'option Informations spécifiques du fabricant PEUT contenir plusieurs sous options.

Un client qui est intéressé à recevoir une l'option Informations spécifiques du fabricant :
- DOIT spécifier l'option Informations spécifiques du fabricant dans une option Demande d'option.
- PEUT spécifier une option Classe de fabricant associée (paragraphe 21.16).
- PEUT spécifier l'option Informations spécifiques du fabricant avec les données appropriées.

Les serveurs ne retournent les options Informations spécifiques du fabricant que si elles sont spécifiées dans les options Demande d'option des clients et :
- PEUVENT utiliser les numéros d'entreprise dans les options Classe de fabricant associées pour restreindre l'ensemble des numéros d'entreprise dans les options Informations spécifiques du fabricant retournées.
- PEUVENT retourner toutes les options Informations spécifiques du fabricant configurées.
- PEUVENT utiliser d'autres informations dans le paquet ou dans sa configuration pour déterminer quel ensemble de numéros d'entreprise retourner dans les options Informations spécifiques du fabricant.

21.18 Option Identifiant d'interface

L'agent de relais PEUT envoyer l'option Identifiant d'interface pour identifier l'interface sur laquelle le message du client a été reçu. Si un agent de relais reçoit un message Relay-reply avec une option Identifiant d'interface, l'agent de relais relaye le message au client à travers l'interface identifiée par l'option. Le format de l'option Identifiant d'interface est :

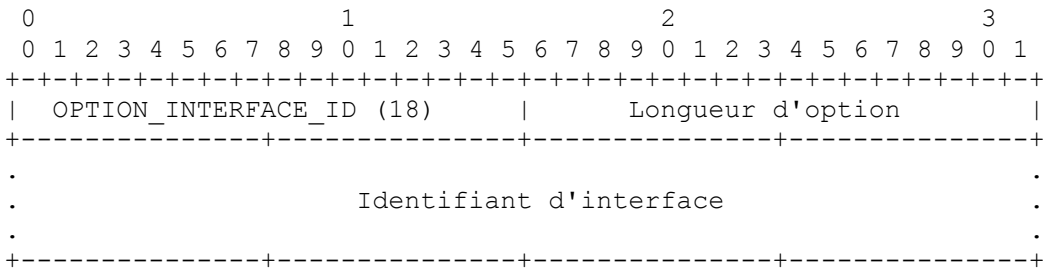


Figure 32 : Format d'option Identifiant d'interface

Code d'option : OPTION_INTERFACE_ID (18).
Longueur d'option : longueur du champ Identifiant d'interface.
Identifiant d'interface : valeur opaque de longueur arbitraire générée par l'agent de relais pour identifier une des interfaces de l'agent de relais. La longueur, en octets, est spécifiée par Longueur d'option.

Le serveur DOIT copier l'option Identifiant d'interface du message Relay-forward dans le message Relay-reply que le serveur envoie à l'agent de relais en réponse au message Relay-forward. Cette option NE DOIT PAS apparaître dans un message sauf Relay-forward ou Relay-reply.

Les serveurs PEUVENT utiliser le champ Identifiant d'interface pour leur politique d'allocation de paramètres. La valeur d'identifiant d'interface DEVRAIT être considérée comme valeur opaque, avec des politiques fondées seulement sur une correspondance exacte ; c'est-à-dire que le champ Identifiant d'interface NE DEVRAIT PAS être analysé en interne par le serveur. La valeur d'identifiant d'interface pour une interface DEVRAIT être stable et rester inchangée -- par exemple, après le redémarrage de l'agent de relais; si la valeur d'identifiant d'interface change, un serveur ne sera pas capable de l'utiliser de façon fiable dans les politiques d'allocation de paramètres.

21.19 Option Reconfiguration de message

Un serveur inclut une option Reconfiguration de message dans un message Reconfigure pour indiquer au client si il répond par un message Renew, Rebind, ou Demande d'information. Le format de l'option Reconfiguration de message est :

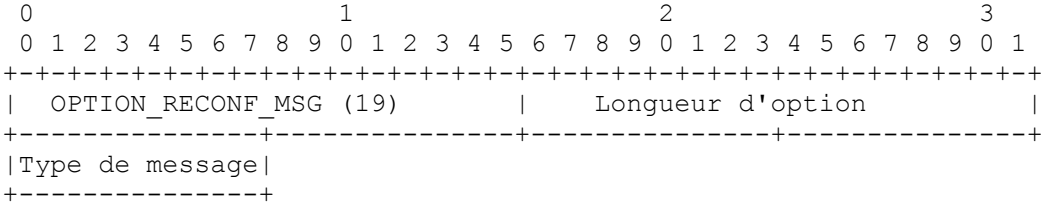


Figure 33 : Format d'option Reconfiguration de message

Code d'option : OPTION_RECONF_MSG (19).
Longueur d'option : 1.
Type de message : 5 pour un message Renew, 6 pour un message Rebind, 11 pour un message Demande d'information. Entier d'un octet non signé.
L'option Reconfiguration de message peut seulement apparaître dans un message Reconfigure.

21.20 Option Accepte Reconfigure

Un client utilise l'option Accepte Reconfigure pour annoncer au serveur si il veut accepter les messages Reconfigure, et un serveur utilise cette option pour dire au client si accepter ou non les messages Reconfigure. En l'absence de cette option, le comportement par défaut est que le client ne veut pas accepter les messages Reconfigure. Le format de l'option Accepte Reconfigure option est :

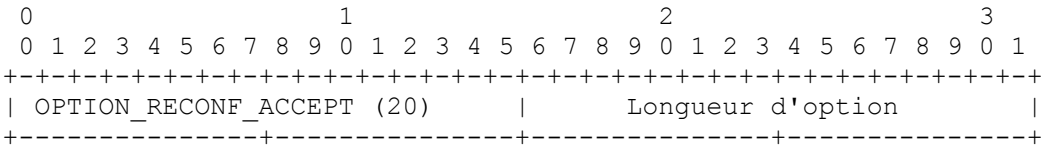


Figure 34 : Format d'option Accepte Reconfigure

Code d'option : OPTION_RECONF_ACCEPT (20).
Longueur d'option : 0.

21.21 Option Délégation de préfixe pour association d'identité

L'option IA_PD est utilisée pour porter une délégation de préfixe d'association d'identité, les paramètres associés à la IA_PD, et les préfixes qui lui sont associés. Le format de l'option IA_PD est :

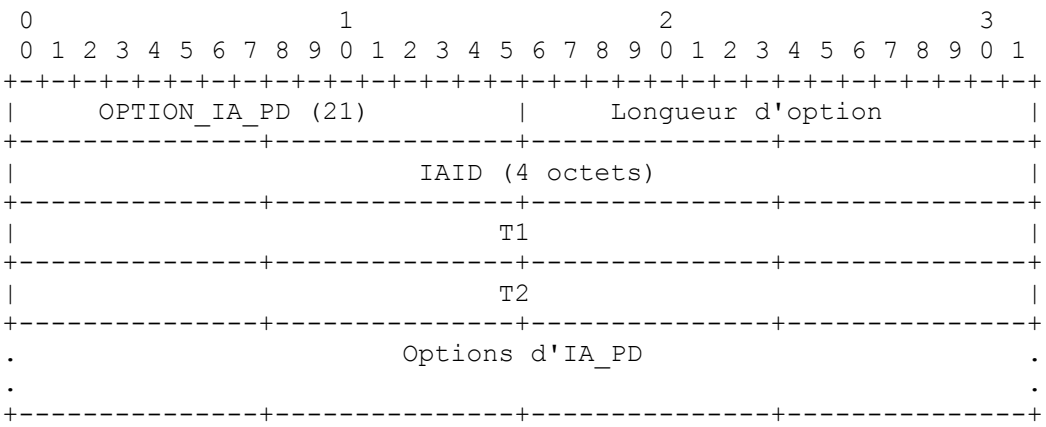


Figure 35 : Format d'option Délégation de préfixe pour l'association d'identité

Code d'option : OPTION_IA_PD (25).
Longueur d'option : 12 + longueur du champ Options d'IA_PD.
IAID : identifiant univoque pour cette IA_PD ; l'IAID doit être unique parmi les identifiants pour toutes les IA_PD de ce client. L'espace de nombres pour les IA_PD IAID est distinct de l'espace de nombres pour les autres types d'option d'IA (c'est-à-dire, IA_NA et IA_TA). Champ de 4 octets contenant un entier non signé.
T1 : intervalle de temps après lequel le client devrait contacter le serveur d'où ont été obtenus les préfixes dans la IA_PD pour étendre les durées de vie des préfixes délégués à l'IA_PD ; T1 est une durée relative à l'heure de réception d'un message, exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.
T2 : intervalle de temps après lequel le client devrait contacter tout serveur disponible pour étendre les durées de vie des préfixes allouée à l'IA_PD ; T2 est une durée relative à l'heure de réception d'un message, exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.
Options d'IA_PD : options associés à cette IA_PD. Champ de longueur variable (12 octets de moins que la valeur dans le champ Longueur d'option).

Le champ Options d'IA_PD encapsule les options spécifiques de cette IA_PD. Par exemple, toutes les options Préfixe d'IA (paragraphe 21.22) portant les préfixes associés à cette IA_PD sont dans le champ Options d'IA_PD.

Une option d'IA_PD ne peut apparaître que dans la zone d'options d'un message DHCP. Un message DHCP peut contenir plusieurs options d'IA_PD (bien que chacune doive avoir un IAID univoque).

L'état de toute opération impliquant cette IA_PD est indiqué dans une option Code d'état (paragraphe 21.13) dans le champ Options d'IA_PD.

Noter qu'une IA_PD n'a pas de "durée de vie" ou de "longueur de prêt" explicite par elle-même. Quand les durées de vie valide de tous les préfixes dans une IA_PD ont expiré, la IA_PD peut être considérée comme ayant expiré. Les champs T1 et T2 sont inclus pour donner au serveur le contrôle explicite sur quand un client devrait le contacter sur une IA_PD spécifique.

Dans un message envoyé par un client à un serveur, les champs T1 et T2 DEVRAIENT être réglés à 0. Le serveur DOIT ignorer toutes valeurs dans ces champs des messages reçus d'un client.

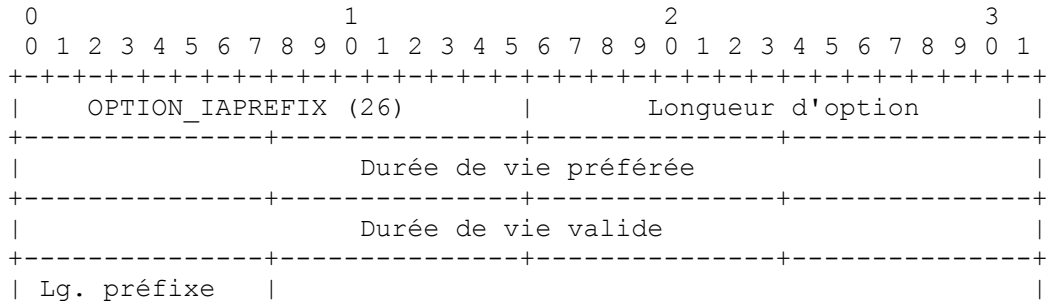
Dans un message envoyé d'un serveur à un client, le client DOIT utiliser les valeurs des champs T1 et T2 pour les temporisateurs T1 et T2, sauf si les valeurs de ces champs sont 0. Les valeurs dans les champs T1 et T2 sont le nombre de secondes jusqu'à T1 et T2.

Le serveur choisit le temps T1 et T2 pour permettre au client d'étendre les durées de vie de tout préfixe dans l'IA_PD avant que les durées de vie expirent, même si le serveur est indisponible pour une courte période. Les valeurs recommandées pour T1 et T2 sont respectivement 0,5 et 0,8 fois la plus courte durée de vie préférée des préfixes dans l'IA_PD que le serveur est d'accord pour étendre. Si l'heure à laquelle les préfixes d'une IA_PD sont à renouveler doit être laissée à la discrétion du client, le serveur règle T1 et T2 à 0. Le client DOIT suivre les règles définies au paragraphe 14.2.

Si un client reçoit une IA_PD avec T1 supérieur à T2 et que T1 et T2 sont tous deux supérieurs à 0, le client élimine l'option d'IA_PD et traite le reste du message comme si le serveur n'avait pas inclus l'option d'IA_PD.

21.22 Option Préfixe d'IA

L'option Préfixe d'IA est utilisée pour spécifier un préfixe associé à une IA_PD. L'option Préfixe d'IA doit être encapsulée dans le champ Options d'IA_PD d'une option d'IA_PD (voir au paragraphe 21.21).



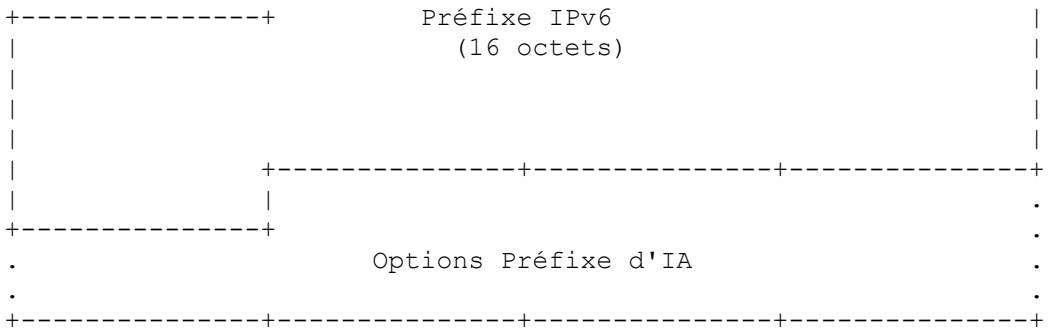


Figure 36 : Format d'option Préfixe d'IA

Code d'option : OPTION_IAPREFIX (26).
Longueur d'option : 25 + longueur du champ Options préfixe d'IA.
Durée de vie préférée : durée de vie préférée pour le préfixe dans l'option, exprimée en unités de secondes. Une valeur de 0xffffffff représente "infini" (voir au paragraphe 7.7). Champ de 4 octets contenant un entier non signé.
Durée de vie valide : durée de vie valide pour le préfixe dans l'option, exprimée en unités de secondes. La valeur de 0xffffffff représente "infini". Champ de 4 octets contenant un entier non signé.
Longueur de préfixe : longueur de ce préfixe en bits. Entier d'un octet non signé.
Préfixe IPv6 : préfixe IPv6. Champ de seize octets.
Options Préfixe d'IA : options associées à ce préfixe. Champ de longueur variable (25 octets de moins que la valeur dans le champ Longueur d'option).

Dans un message envoyé par un client à un serveur, les champs Durée de vie préférée et Durée de vie valide DEVRAIENT être réglés à 0. Le serveur DOIT ignorer toute valeur reçue dans ces champs de durée de vie.

Le client NE DEVRAIT PAS envoyer une option Préfixe d'IA avec 0 dans le champ "Longueur de préfixe" (et une valeur non spécifiée (::) dans le champ "Préfixe IPv6"). Un client PEUT envoyer une valeur non zéro dans le champ "Longueur de préfixe" et la valeur non spécifiée (::) dans le champ "Préfixe IPv6" pour indiquer une préférence pour la taille du préfixe à déléguer. Voir dans la [RFC8168] des détails sur les indications de longueur de préfixes.

Le client DOIT éliminer tout préfixe pour lequel la durée de vie préférée est supérieure à la durée de vie valide.

Les valeurs dans les champs Durée de vie préférée et Durée de vie valide sont le nombre de secondes restant dans chaque durée de vie. Voir au paragraphe 18.2.10.1 des détails sur la façon dont des valeurs sont utilisées pour les préfixes délégués.

Conformément au paragraphe 7.7, la valeur de 0xffffffff pour la durée de vie préférée ou la durée de vie valide est prise pour signifier "infini" et devrait être utilisé avec prudence.

Une option Préfixe d'IA peut apparaître seulement dans une option IA_PD. Plus d'une option Préfixe d'IA peut apparaître dans une seule option d'IA_PD.

L'état de toute opération impliquant cette option Préfixe d'IA est indiqué dans une option Code d'état (paragraphe 21.13) dans le champ Options de préfixe d'IA.

21.23 Option Heure de rafraîchissement d'informations

Cette option est demandée par les clients et retournée par les serveurs pour spécifier une limite supérieure au temps que devrait attendre un client avant de rafraîchir les informations restituées d'un serveur DHCP. Elle n'est utilisée que dans les messages Reply en réponse aux messages Demande d'information. Dans les autres messages, il va généralement y avoir d'autres informations qui indiquent quand le client devrait contacter le serveur, par exemple, les temps T1/T2 et les durées de vie. Cette option est utile quand les paramètres de configuration changent ou durant un événement de dénumérotation, car les clients qui fonctionnent en mode sans état vont être capables de mettre à jour leur configuration.

Le format de l'option Heure de rafraîchissement d'informations est :

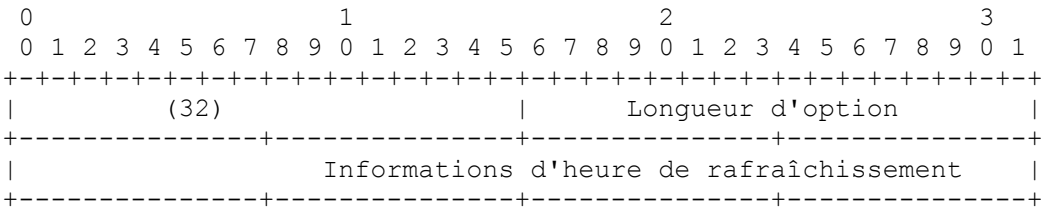


Figure 37 : Format d'option Informations d'heure de rafraîchissement

Code d'option : OPTION_INFORMATION_REFRESH_TIME (32).
Longueur d'option : 4.
Informations d'heure de rafraîchissement : durée relative à l'heure actuelle, exprimée en unités de secondes. Champ de 4 octets contenant un entier non signé.

Un client DHCP DOIT demander cette option dans l'option Demande d'option (paragraphe 21.7) quand il envoie des messages Demande d'information. Un client NE DOIT demander cette option dans l'option Demande d'option dans aucun autre message.

Un serveur qui envoie un Reply à un message Demande d'information DEVRAIT inclure cette option si elle est demandée dans l'option Demande d'option de la demande d'information. La valeur d'option NE DOIT PAS être inférieure à IRT_MINIMUM. Cette option DOIT apparaître seulement dans la zone options de niveau supérieur des messages Reply.

Si le Reply à un message Demande d'information ne contient pas cette option, le client DOIT se comporter comme si l'option avait été fournie avec la valeur IRT_DEFAULT.

Un client DOIT utiliser le temps de rafraîchissement IRT_MINIMUM si il reçoit l'option avec une valeur inférieure à IRT_MINIMUM.

Conformément au paragraphe 7.7, la valeur 0xffffffff est prise comme signifiant "infini" et implique que le client ne devrait pas rafraîchir ses données de configuration sans un autre déclencheur (comme de détecter le passage à une nouvelle liaison).

Si un client contacte le serveur pour obtenir de nouvelles données ou rafraîchir des données existantes avant l'expiration de l'heure de rafraîchissement, il DEVRAIT alors aussi rafraîchir toutes les données couvertes par cette option.

Quand le client détecte que l'heure de rafraîchissement a expiré, il DEVRAIT essayer de mettre à jour ses données de configuration en envoyant une demande d'informations comme spécifié au paragraphe 18.2.6, sauf que le client DOIT retarder l'envoi de la première demande d'informations d'un délai aléatoire entre 0 et INF_MAX_DELAY.

Un client PEUT avoir une valeur maximum pour le temps de rafraîchissement, où cette valeur est utilisée chaque fois que le client reçoit cette option avec une valeur supérieure au maximum. Cela signifie aussi que la valeur maximum est utilisée quand la valeur reçue est "infini". Une valeur maximum pourrait rendre le client moins vulnérable aux attaques fondées sur des messages DHCP falsifiés. Sans une valeur maximum, un client peut être conduit à utiliser de fausses informations pendant une durée éventuellement infinie. Il peut cependant y avoir des raisons d'avoir une très longue période de rafraîchissement, et donc il peut être utile que cette valeur maximum soit configurable.

21.24 Option SOL_MAX_RT

Un serveur DHCP envoie l'option SOL_MAX_RT à un client pour outrepasser la valeur par défaut de SOL_MAX_RT. La valeur de SOL_MAX_RT dans l'option remplace la valeur par défaut définie au paragraphe 7.6. Une utilisation de l'option SOL_MAX_RT est de régler SOL_MAX_RT à une valeur supérieure ; cela réduit le trafic de Solicit provenant d'un client qui n'a pas reçu de réponse à ses messages Solicit.

Le format de l'option SOL_MAX_RT est :

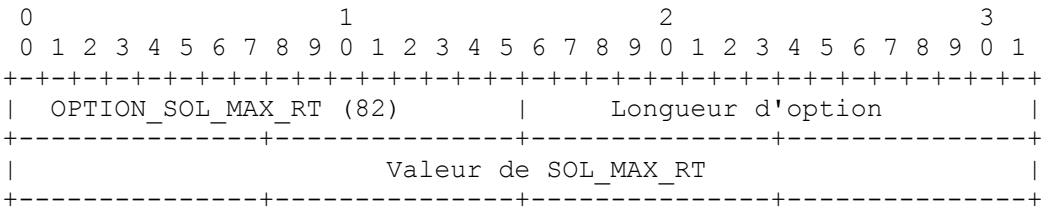


Figure 38 : Format d'option SOL_MAX_RT

Code d'option : OPTION_SOL_MAX_RT (82).
Longueur d'option : 4.
Valeur de SOL_MAX_RT : valeur de remplacement pour SOL_MAX_RT en secondes ; DOIT être dans la gamme 60 ≤ "valeur" ≤ 86400 (1 jour). Champ de 4 octets contenant un entier non signé.

Un client DHCP DOIT inclure le code d'option SOL_MAX_RT dans toute option Demande d'option (paragraphe 21.7) qu'il envoie dans un message Solicit.

Le serveur DHCP PEUT inclure l'option SOL_MAX_RT dans toute réponse qu'il envoie à un client qui a inclus le code d'option SOL_MAX_RT dans une option Demande d'option. L'option SOL_MAX_RT est envoyée comme option de niveau supérieur dans le message au client.

Un client DHCP DOIT ignorer toutes valeurs d'option SOL_MAX_RT inférieures à 60 ou supérieure à 86 400.

Si un client DHCP reçoit un message contenant une option SOL_MAX_RT qui a une valeur valide pour SOL_MAX_RT, le client DOIT régler son paramètre SOL_MAX_RT interne à la valeur contenue dans l'option SOL_MAX_RT. Cette valeur de SOL_MAX_RT est alors utilisée par le mécanisme de retransmission défini à la Section 15 et au paragraphe 18.2.1.

L'objet de ce mécanisme est de donner aux administrateurs de réseau un moyen d'éviter un trafic DHCP excessif si tous les serveurs DHCP deviennent indisponibles. Donc, cette valeur est supposée être conservée aussi longtemps que pratiquement possible.

Une valeur mise à jour de SOL_MAX_RT ne s'applique qu'à l'interface réseau sur laquelle le client a reçu l'option SOL_MAX_RT.

21.25 Option INF_MAX_RT

Un serveur DHCP envoie l'option INF_MAX_RT à un client pour outrepasser la valeur par défaut de INF_MAX_RT. La valeur de INF_MAX_RT dans l'option remplace la valeur par défaut définie au paragraphe 7.6. Une utilisation de l'option INF_MAX_RT est d'établir une valeur plus élevée pour INF_MAX_RT ; cela réduit le trafic de demandes d'informations provenant d'un client qui n'a pas reçu de réponse à ses messages Demande d'information. Le format de l'option INF_MAX_RT est :

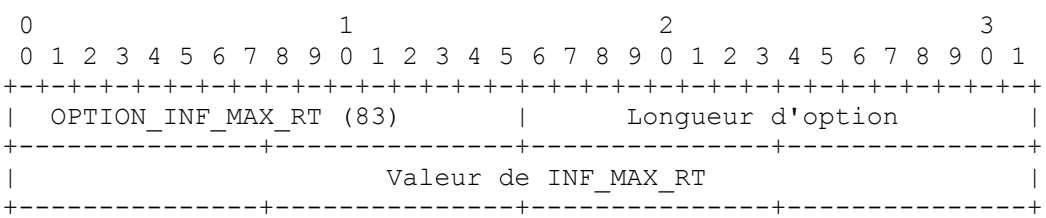


Figure 39 : Format d'option INF_MAX_RT

Code d'option : OPTION_INF_MAX_RT (83).
Longueur d'option : 4.
Valeur de INF_MAX_RT : valeur d'outrepassement de INF_MAX_RT en secondes ; DOIT être dans la gamme 60 ≤ "valeur" ≤ 86 400 (1 jour). Champ de 4 octets contenant un entier non signé.

Un client DHCP DOIT inclure le code d'option INF_MAX_RT dans toute option Demande d'option (paragraphe 21.7) qu'il

envoie dans un message Demande d'information.

Le serveur DHCP PEUT inclure l'option INF_MAX_RT dans toute réponse qu'il envoie à un client qui a inclus le code d'option INF_MAX_RT dans une option Demande d'option. L'option INF_MAX_RT est une option de niveau supérieur dans le message au client.

Un client DHCP DOIT ignorer toutes les valeurs d'option INF_MAX_RT inférieures à 60 ou supérieures à 86 400.

Si un client DHCP reçoit un message contenant une option INF_MAX_RT qui a une valeur valide pour INF_MAX_RT, il DOIT régler son paramètre INF_MAX_RT interne à la valeur contenue dans l'option INF_MAX_RT. Cette valeur de INF_MAX_RT est alors utilisée par le mécanisme de retransmission défini à la Section 15 et au paragraphe 18.2.6.

Une valeur de INF_MAX_RT mise à jour ne s'applique qu'à l'interface réseau sur laquelle le client a reçu l'option INF_MAX_RT.

22. Considérations de sécurité

Cette section discute des considérations de sécurité qui ne relèvent pas de la confidentialité. Voir à la Section 23 une discussion dédiée à la confidentialité.

La menace sur DHCP est par nature une menace de l'intérieur (en supposant un réseau configuré de façon appropriée où les accès DHCP sont bloqués sur les passerelles périphériques de l'entreprise). Sans considération de la configuration des passerelles, les attaques potentielles par l'intérieur et l'extérieur sont cependant les mêmes.

DHCP n'a pas de chiffrement de bout en bout entre clients et serveurs ; donc, les attaques de capture, d'altération, et d'espionnage sont par suite toutes possibles. Certains environnements de réseau (discutés ci-dessous) peuvent être sécurisés par divers moyens pour minimiser ces attaques.

Une attaque spécifique d'un client DHCP est l'établissement d'un serveur malveillant dans l'intention de fournir des informations de configuration incorrectes au client. Le motif de tels actes peut être de monter une attaque "par interposition" qui cause la communication du client avec un serveur malveillant au lieu d'un serveur valide pour un certain service (comme DNS ou NTP). Le serveur malveillant peut aussi monter une attaque de déni de service par une mauvaise configuration du client ; cette attaque causerait l'échec de toutes les communications réseau provenant du client.

Un serveur DHCP malveillant pourrait causer le réglage par un client de ses paramètres SOL_MAX_RT et INF_MAX_RT à des valeurs déraisonnablement élevées avec les options SOL_MAX_RT (paragraphe 21.24) et INF_MAX_RT (paragraphe 21.25) ; cela peut causer un retard non motivé de l'achèvement des transactions de protocole DHCP du client dans le cas où aucune autre réponse valide n'est reçue. En supposant que le client reçoive aussi une réponse d'un serveur DHCP valide, les grandes valeurs de SOL_MAX_RT et INF_MAX_RT n'auront aucun effet.

Un serveur malveillant peut aussi envoyer une option Serveur en envoi individuel (paragraphe 21.12) à un client dans un message Advertise, causant donc potentiellement l'outrepassement par le client des relais et la communication seulement avec le serveur malveillant pour les messages Request et Renew suivants.

Une autre menace sur les clients DHCP à son origine dans des serveurs DHCP mal configurés par malveillance ou accidentellement qui répondent aux demandes de client DHCP avec des paramètres de configuration involontairement incorrects.

Un client DHCP peut aussi être soumis à une attaque par la réception d'un message Reconfigure provenant d'un serveur malveillant qui cause l'obtention par le client d'informations de configuration incorrectes de ce serveur. Noter que bien que un client envoie sa réponse (message Renew, Rebind, ou Demande d'information) à travers un agent de relais et, donc, que la réponse ne sera reçue que par les serveurs auxquels les messages DHCP sont relayés, un serveur malveillant pourrait envoyer un message Reconfigure à un client, suivi (après un délai approprie) par un message Reply qui serait accepté par le client. Donc, un serveur malveillant qui n'est pas sur le chemin de réseau entre le client et le serveur peut quand même être capable de monter une attaque de reconfiguration contre un client. L'utilisation d'identifiants de transaction qui sont cryptographiquement fondés et ne peuvent pas être facilement prédits va aussi réduire la probabilité qu'une telle attaque réussisse.

À cause de l'opportunité d'attaque par le message Reconfigure, un client DHCP DOIT éliminer tout message Reconfigure

qui ne comporte pas d'authentification ou qui ne satisfait pas au processus de validation du protocole d'authentification.

RKAP, décrit au paragraphe 20.4, fournit une protection contre l'utilisation d'un message Reconfigure par un serveur DHCP malveillant pour monter une attaque de DoS ou par interposition contre un client. Ce protocole peut être compromis par un attaquant qui pourrait intercepter le message initial dans lequel le serveur DHCP envoie la clé "en clair" au client.

Beaucoup de ces attaques par des serveurs félons peuvent être atténuées en utilisant les mécanismes décrits dans les [RFC7610] et [RFC7513].

La menace spécifique pour un serveur DHCP est celle d'un client invalide qui se fait passer pour un client valide. Le motif peut en être le vol de service, ou de circonvenir l'examen pour toutes sortes d'objets néfastes.

La menace commune au client et au serveur est l'attaque de DoS par "épuisement de ressources". Ces attaques impliquent normalement l'épuisement des adresses disponibles ou des préfixes délégables à allouer, ou l'épuisement de la CPU ou de la bande passante du réseau, et sont présentes chaque fois qu'il y a des ressources partagées. Certaines formes de ces attaques par épuisement peuvent être partiellement atténuées par une politique de serveur appropriée, par exemple, en limitant le nombre maximum de prêts que tout client peut obtenir.

Les messages échangés entre agents de relais et serveurs peuvent être utilisés pour monter une attaque par interposition ou de DoS. La communication entre un serveur et un agent de relais, et la communication entre agents de relais, peut être authentifiée et chiffrée par l'utilisation de IPsec, comme décrit à la [RFC8213].

Cependant, l'utilisation de clés pré partagées configurée manuellement pour IPsec entre agents de relais et serveurs ne défend pas contre les messages DHCP répétés. Les messages répétés peuvent représenter une attaque de DoS par épuisement des ressources de traitement mais pas par la mauvaise configuration ou l'épuisement d'autres ressources comme les adresses et préfixes délégables à allouer.

Divers environnements de réseau offrent aussi des niveaux de sécurité si ils sont déployé comme décrit ci-dessous.

- Dans les réseaux d'entreprise et d'usines, l'utilisation de l'authentification selon [IEEE-802.1x] peut empêcher des clients inconnus ou non fiables de se connecter au réseau. Cependant, ceci n'assure pas nécessairement que le client connecté va être un bon acteur DHCP ou réseau.

- Pour les réseaux filaires où les clients sont normalement connecté à un accès commuté, l'espionnage du trafic DHCP en diffusion groupée (ou en envoi individuel) devient difficile, car les commutateurs limitent le trafic livré à un accès. Les paquets DHCP en diffusion groupée du client (avec l'adresse de destination fe02::1:2) ne sont transmis qu'à l'accès commuté du serveur DHCP (ou du relais) – et non à tous les accès. Aussi, les réponses en envoi individuel du serveur (ou du relais) ne sont livrées qu'à l'accès du client ciblé – et non à tous les accès.

- Dans les réseaux publics (comme un réseau Wi-Fi dans un café Internet ou un aéroport) il est possible à ceux qui sont à portée de radio d'espionner le trafic DHCP et autre. Mais dans ces environnements, il n'y a rien ou pas grand chose à apprendre du trafic DHCP lui-même (du client au serveur ou du serveur au client) si les considérations de confidentialité fournies à la Section 23 sont suivies. Même pour les appareils qui ne suivent pas les considérations sur la confidentialité, il n'y a pas grand chose à apprendre qui ne soit de toutes façons disponibles par les communications suivantes (comme l'adresse de contrôle d'accès au support de l'appareil). Aussi, parce que tous les clients vont normalement recevoir des détails de configuration similaires, un mauvais acteur qui initie une demande DHCP peut lui-même apprendre beaucoup de ces informations. Comme mentionné plus haut, une menace est que que la clé RKAP pour un client puisse être apprise (si l'échange initial Solicit/Advertise/Request/Reply est surveillé) et déclenche une reconfiguration prématurée, mais ceci est relativement facile à empêcher en interdisant la communication directe de client à client sur ces réseaux ou en utilisant les [RFC7610] et [RFC7513].

23. Considérations de confidentialité

Voir dans la [RFC7824] une discussion étendue sur considérations de confidentitalité pour le client :
- En particulier, sa Section 3 discute des divers identifiants qui pourraient être mal utilisés à traquer le client.
- Sa Section 4 discute des mécanismes existants qui peuvent avoir un impact sur la confidentialité d'un client.
- Finalement, sa Section 5 discute des vecteurs potentiels d'attaque.

Pour des recommandations sur la façon de traiter ou atténuer ces problèmes, voir la [RFC7844].

La présente spécification ne définie aucune stratégie d'allocation pour les serveurs. Les mises en œuvre sont supposées développer leur propre algorithme pour que le serveur choisisse une ressource à partir d'un réservoir de disponibilités. Plusieurs stratégies d'allocation possibles sont mentionnées au paragraphe 4.3 de la [RFC7824]. On notera que la liste de la [RFC7824] n'est pas exhaustive ; il y a certainement d'autres stratégies possibles. Les lecteurs sont aussi invités à lire la [RFC7707] -- en particulier, son paragraphe 4.1.2, qui discute des problèmes de certaines stratégies d'allocation.

24. Considérations relatives à l'IANA

Le présent document ne définit aucun nouvel espace de noms ni définition DHCP.

La publication du présent document ne change pas les règles d'allocation pour les nouvelles valeurs de types de message, codes d'option, types de DUID, ou codes d'état.

La liste de valeurs allouées utilisée dans DHCPv6 est disponible à <https://www.iana.org/assignments/dhcpv6-parameters>

L'IANA a mis à jour <https://www.iana.org/assignments/dhcpv6-parameters> pour y ajouter une référence au présent document pour les définitions précédemment créées par les [RFC3315], [RFC3633], [RFC4242], et [RFC7083].

L'IANA a ajouté deux colonnes au registre des codes d'option DHCPv6 à <https://www.iana.org/assignments/dhcpv6-parameters> pour indiquer quelles options peuvent apparaître dans une option Demande d'option d'un client (paragraphe 21.7) et quelles options sont des options singletons (dont l'apparition n'est permise qu'une seule fois comme option de niveau supérieur ou encapsulée ; voir la Section 16 de la [RFC7227]). Le Tableau 4 fournit les données pour les options allouées par l'IANA au moment de la rédaction du présent document.

Option	Nom d'option (sans le préfixe "OPTION")	Client ORO (1)	Option singleton
1	CLIENTID	Non	Oui
2	SERVERID	Non	Oui
3	IA_NA	Non	Non
4	IA_TA	Non	Non
5	IAADDR	Non	Non
6	ORO	Non	Oui
7	PREFERENCE	Non	Oui
8	ELAPSED_TIME	Non	Oui
9	RELAY_MSG	Non	Oui
11	AUTH	Non	Ou
12	UNICAST	Non	Oui
13	STATUS_CODE	Non	Oui
14	RAPID_COMMIT	Non	Oui
15	USER_CLASS	Non	Oui
16	VENDOR_CLASS	Non	Non (2)
17	VENDOR_OPTS	Facultative	Non (2)
18	INTERFACE_ID	Non	Oui
19	RECONF_MSG	Non	Oui
20	RECONF_ACCEPT	Non	Oui
21	SIP_SERVER_D	Oui	Oui
22	SIP_SERVER_A	Oui	Oui
23	DNS_SERVERS	Oui	Oui
24	DOMAIN_LIST	Oui	Oui
25	IA_PD	Non	Non
26	IAPREFIX	Non	Non
27	NIS_SERVERS	Oui	Oui
28	NISP_SERVERS	Oui	Oui
29	NIS_DOMAIN_NAME	Oui	Oui
30	NISP_DOMAIN_NAME	Oui	Oui
31	SNTP_SERVERS	Oui	Oui
32	INFORMATION_REFRESH_TIME	exigée pour Info.-request	Oui
33	BCMCS_SERVER_D	Oui	Oui
34	BCMCS_SERVER_A	Oui	Oui

36	GEOCONF_CIVIC	Oui	Oui
37	REMOTE_ID	Non	Oui
38	SUBSCRIBER_ID	Non	Oui
39	CLIENT_FQDN	Oui	Oui
40	PANA_AGENT	Oui	Oui
41	NEW_POSIX_TIMEZONE	Oui	Oui
42	NEW_TZDB_TIMEZONE	Oui	Oui
43	ERO	Non	Oui
44	LQ_QUERY	Non	Oui
45	CLIENT_DATA	Non	Oui
46	CLT_TIME	Non	Oui
47	LQ_RELAY_DATA	Non	Oui
48	LQ_CLIENT_LINK	Non	Oui
49	MIP6_HNIDF	Oui	Oui
50	MIP6_VDINF	Oui	Oui
51	V6_LOST	Oui	Oui
52	CAPWAP_AC_V6	Oui	Oui
53	RELAY_ID	Non	Oui
54	Ipv6_Address-MoS	Oui	Oui
55	Ipv6_FQDN-MoS	Oui	Oui
56	NTP_SERVER	Oui	Oui
57	V6_ACCESS_DOMAIN	Oui	Oui
58	SIP_UA_CS_LIST	Oui	Oui
59	OPT_BOOTFILE_URL	Oui	Oui
60	OPT_BOOTFILE_PARAM	Oui	Oui
61	CLIENT_ARCH_TYPE	Non	Oui|
62	NII	Oui	Oui
63	GEOLOCATION	Oui	Oui
64	AFTR_NAME	Oui	Oui
65	ERP_LOCAL_DOMAIN_NAME	Oui	Oui
66	RSOO	Non	Oui
67	PD_EXCLUDE	Oui	Oui
68	VSS	Non	Oui
69	MIP6_IDINF	Oui	Oui
70	MIP6_UDINF	Oui	Oui
71	MIP6_HNP	Oui	Oui
72	MIP6_HAA	Oui	Oui
73	MIP6_HAF	Oui	Oui
74	RDNSS_SELECTION	Oui	Non
75	KRB_PRINCIPAL_NAME	Oui	Oui
76	KRB_REALM_NAME	Oui	Oui
77	KRB_DEFAULT_REALM_NAME	Oui	Oui
78	KRB_KDC	Oui	Oui
79	CLIENT_LINKLAYER_ADDR	Non	Oui
80	LINK_ADDRESS	Non	Oui
81	RADIUS	Non	Oui
82	SOL_MAX_RT	exigée pour Solicit	Oui
83	INF_MAX_RT	exigée pour Info.-request	Oui
84	ADDRSEL	Oui	Oui
85	ADDRSEL_TABLE	Oui	Oui
86	V6_PCP_SERVER	Oui	Non
87	DHCPV4_MSG	Non	Oui
88	DHCP4_O_DHCP6_SERVER	Oui	Oui
89	S46_RULE	Non	Non (3)
90	S46_BR	Non	Non
91	S46_DMR	Non	Oui
92	S46_V4V6BIND	Non	Oui
93	S46_PORTPARAMS	Non	Oui
94	S46_CONT_MAPE	Oui	Non|
95	S46_CONT_MAPT	Oui	Oui
96	S46_CONT_LW	Oui	Oui

97	4RD	Oui	Oui
98	4RD_MAP_RULE	Oui	Oui
99	4RD_NON_MAP_RULE	Oui	Oui
100	LQ_BASE_TIME	Non	Oui
101	LQ_START_TIME	Non	Oui
102	LQ_END_TIME	Non	Oui
103	DHCP Captive-Portal	Oui	Oui
104	MPL_PARAMETERS	Oui	Non
105	ANI_ATT	Non	Oui
106	ANI_NETWORK_NAME	Non	Oui
107	ANI_AP_NAME	Non	Oui
108	ANI_AP_BSSID	Non	Oui
109	ANI_OPERATOR_ID	Non	Oui
110	ANI_OPERATOR_REALM	Non	Oui
111	S46_PRIORITY	Oui	Oui
112	MUD_URL_V6	Non	Oui
113	V6_PREFIX64	Oui	Non
114	F_BINDING_STATUS	Non	Oui
115	F_CONNECT_FLAGS	Non	Oui
116	F_DNS_REMOVAL_INFO	Non	Oui
117	F_DNS_HOST_NAME	Non	Oui
118	F_DNS_ZONE_NAME	Non	Oui
119	F_DNS_FLAGS	Non	Oui
120	F_EXPIRATION_TIME	Non	Oui
121	F_MAX_UNACKED_BNDUPD	Non	Oui
122	F_MCLT	Non	Oui
123	F_PARTNER_LIFETIME	Non	Oui
124	F_PARTNER_LIFETIME_SENT	Non	Oui
125	F_PARTNER_DOWN_TIME	Non	Oui
126	F_PARTNER_RAW_CLT_TIME	Non	Oui
127	F_PROTOCOL_VERSION	Non	Oui
128	F_KEEPALIVE_TIME	Non	Oui
129	F_RECONFIGURE_DATA	Non	Oui
130	F_RELATIONSHIP_NAME	Non	Oui
131	F_SERVER_FLAGS	Non	Oui
132	F_SERVER_STATE	Non	Oui
133	F_START_TIME_OF_STATE	Non	Oui
134	F_STATE_EXPIRATION_TIME	Non	Oui
135	RELAY_PORT	Non	Oui
143	Ipv6_Address-ANDSF	Oui	Oui

Tableau 4 : Options mise à jour

Notes du Tableau 4 :

(1) Dans la colonne "Client ORO, un "Oui" pour une option signifie que le client inclut ce code d'option dans l'option Demande d'option (voir au paragraphe 21.7) si il désire ces informations de configuration, et un "Non" signifie que l'option NE DOIT PAS être incluse (et les serveurs DEVRAIENT ignorer en silence ce code d'option si il apparaît dans une option Demande d'option d'un client).

(2) Pour chaque numéro d'entreprise, il DOIT y avoir une seule instance.

(3) Voir les détails dans la [RFC7598].

L'IANA a corrigé la gamme des codes d'état possibles dans le tableau des "Codes d'état" à <https://www.iana.org/assignments/dhcpv6-parameters> en remplaçant 23-255 (comme Non alloués) par 23-65535 (les codes sont des entiers de16 bits non signés).

L'IANA a mis à jour les entrées de tableau All_DHCP_Relay_Agents_and_Servers (ff02::1:2) et All_DHCP_Servers (ff05::1:3) dans "IPv6 Multicast Address Space Registry" à <https://www.iana.org/assignments/ipv6-multicast-adresses> pour faire référence au présent document au lieu de la [RFC3315].

L'IANA a ajouté une annotation "Obsolete" dans l'entrée "DHCPv6 Delayed Authentication" dans le registre "Authentication Suboption (valeur 8) - Protocol identifier values" à <https://www.iana.org/assignments/bootp-dhcp-parameters> et a ajouté une annotation "Obsolete" dans l'entrée "Delayed Authentication" dans le registre "Protocol Name Space Values" à <https://www.iana.org/assignments/auth-namespaces>. L'IANA a aussi mis à jour ces pages pour faire référence au présent document au lieu de la [RFC3315].

L'IANA a ajouté une référence au présent document pour la valeur de RDM de 0 au registre "RDM Name Space Values" à <https://www.iana.org/assignments/auth-namespaces>.

L'IANA a mis à jour le "Service Name and Transport Protocol Port Number Registry" à <https://www.iana.org/assignments/ service-names-port-numbers> comme suit :

546/udp Le présent document
547/udp Le présent document
547/tcp [RFC5460]
647/tcp [RFC8156]

25. Mécanismes obsolètes

La présente spécification est principalement une version corrigée et nettoyée de la spécification originale -- [RFC3315] – avec de nombreux ajouts des RFC ultérieures. Cependant, un petit nombre de mécanismes n'étaient pas largement déployés, étaient sous spécifiés, ou avait d'autres problèmes de fonctionnement. Ces mécanismes sont maintenant considérés comme déconseillés. Les mises en œuvre traditionnelles PEUVENT les prendre en charge, mais les mises en œuvre conformes au présent document NE DOIVENT PAS s'appuyer sur eux.

Les mécanismes suivants sont maintenant obsolètes :

Authentification retardée : ce mécanisme était sous spécifié et représentait une charge opérationnelle significative. Par suite, après 10 années on voit que son adoption est restée au mieux extrêmement limitée.

Conseils de durée de vie envoyés par un client : il était permis aux clients d'envoyer des valeurs de durée de vie à titre d'indication. Ce mécanisme n'a pas été largement mis en œuvre, et certaines mauvaises mises en œuvre connues envoyaient les durées de vie restantes plutôt que les durées de vie totales désirées. Ceci était parfois mal interprété par les serveurs comme une demande de diminution de la durée de vie des prêts, ce qui causait des problèmes quand les valeurs commençaient à approcher de zéro. Les clients DEVRAIENT maintenant établir les durées de vie à 0 dans les options Adresse d'IA et Préfixe d'IA, et les serveurs DOIVENT ignorer toute valeur de durée de vie demandée.

Indications de T1/T2 envoyées par un client : il y a eu des problèmes similaires à ceux des indications de durée de vie. Les clients DEVRAIENT maintenant régler les valeurs de T1/T2 à 0 dans les options IA_NA et IA_PD, et les serveurs DOIVENT ignorer toute valeur de T1/T2 fournie par un client.

26. Références

26.1 Références normatives

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980, DOI 10.17487/RFC0768.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987, DOI 10.17487/RFC1035. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997, DOI 10.17487/RFC2119. *(MàJ par* RFC8174)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006, DOI 10.17487/RFC4291. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007, DOI 10.17487/RFC4861. (*Remplace* RFC2461) *(D.S. ; MàJ par* RFC8028, RFC8319, RFC8425)

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007, DOI 10.17487/RFC4862. (*Remplace* RFC2462) *(D.S.)*

[RFC6221] D. Miles et autres, "Agent léger de relais DHCPv6", DOI 10.17487/RFC6221, mai 2011. *(MàJ la* RFC3315) *(P.S.)*

[RFC6355] T. Narten, J. Johnson, "Définition de l'identifiant univoque DHCPv6 fondé sur l'UUID (DUID-UUID)", DOI 10.17487/RFC6355, août 2011. *(P.S.)*

[RFC7227] D. Hankins et autres, "Lignes directrices pour créer de nouvelles options DHCPv6", BCP0187, DOI 10.17487/RFC7227, mai 2014. (*MàJ* RFC3315)

[RFC7283] Y. Cui, Q. Sun, T. Lemon, "Traitement des messages DHCPv6 inconnus", DOI 10.17487/RFC7283, juillet 2014. *(P.S. ; rendue obsolète par* RFC8415)

[RFC8085] L. Eggert, et autres, "Lignes directrices pour l'utilisation de UDP", mars 2017. BCP 145, DOI 10.17487/RFC8085. *(MàJ* 5405 *; MàJ par* RFC8899)

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", DOI 10.17487/RFC8174, mai 2017. BCP14. *(MàJ* 2119)

[RFC8200] S. Deering, R. Hinden, "Spécification du protocole Internet version 6 (IPv6)", DOI 10.17487/RFC8200, juillet 2017. STD 86. *(Remplace* 2460)

[RFC8213] B. Volz, Y. Pal, "Sécurité des messages échangés entre serveurs et agents de relais dans DHCP", DOI 10.17487/RFC8213, août 2017. *(P.S.)*

26.2 Références pour information

[IANA-HARDWARE-TYPES] IANA, "Hardware Types", <https://www.iana.org/assignments/arp-parameters >.

[IANA-PEN] IANA, "Private Enterprise Numbers", <https://www.iana.org/assignments/enterprise-numbers >.

[IANA-RESERVED-IID] IANA, "Reserved IPv6 Interface Identifiers", <https://www.iana.org/assignments/ipv6-interface-ids >.

[IEEE-802.1x] IEEE, "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control", IEEE 802.1X-2010, DOI 10.1109/IEEESTD.2010.5409813, <https://ieeexplore.ieee.org/servlet/opac?punumber=5409757 >.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982, DOI 10.17487/RFC0826.

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997, DOI 10.17487/RFC2131. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2132] S. Alexander et R. Droms, "Options DHCP et Extensions de fabricant BOOTP", mars 1997, DOI 10.17487/RFC2132.

[RFC2464] M. Crawford, "Transmission de paquets IPv6 sur réseaux Ethernet", décembre 1998, DOI 10.17487/RFC2464. *(P.S. ; MàJ par* RFC8064)

[RFC3162] B. Aboba, G. Zorn, D. Mitton, "RADIUS et IPv6", août 2001, DOI 10.17487/RFC3162. *(P.S. ; MàJ par* RFC8044)

[RFC3290] Y. Bernet et autres, "Modèle informel de gestion pour routeurs Diffserv", mai 2002, DOI 10.17487/RFC3290. *(Information)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003, DOI 10.17487/RFC3315. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003, DOI 10.17487/RFC3629.

[RFC3633] O. Troan, R. Droms, "Options de préfixes IPv6 pour le protocole de configuration dynamique d'hôte (DHCP) version 6", décembre 2003, DOI 10.17487/RFC3633. (*MàJ par la* RFC6603) *(P.S. ; Obsolète voir* RFC8415)

[RFC3646] R. Droms, éd., "Options de configuration du DNS pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", décembre 2003, DOI 10.17487/RFC3646. *(P.S.)*

[RFC3736] R. Droms, "Service sans état du protocole de configuration dynamique d'hôte (DHCP) pour IPv6", avril 2004, DOI 10.17487/RFC3736. *(P.S. ; rendue obsolète par* RFC8415)

[RFC3769] S. Miyakawa, R. Droms, "Exigences pour la délégation de préfixe IPv6", juin 2004, DOI 10.17487/RFC3769. *(Information)*

[RFC4193] R. Hinden, B. Haberman, "Adresses IPv6 en envoi individuel uniques localement", octobre 2005, DOI 10.17487/RFC4193. *(P.S.)*

[RFC4242] S. Venaas et autres, "Option de délai de rafraîchissement d'informations pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", novembre 2005, DOI 10.17487/RFC4242. *(P.S. ; rendue obsolète par* RFC8415)

[RFC4477] T. Chown et autres, "Protocole de configuration dynamique d'hôte (DHCP) : problèmes de la double pile IPv4 et IPv6", mai 2006, DOI 10.17487/RFC4477. *(Information)*

[RFC4704] B. Volz, "Option de nom de domaine pleinement qualifié (FQDN) de client du protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", octobre 2006, DOI 10.17487/RFC4704. *(P.S.)*

[RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007, DOI 10.17487/RFC4941. (*Remplace* RFC3041) *(D.S.)*

[RFC4943] S. Roy et autres, "L'hypothèse "en liaison" dans la découverte de voisin IPv6 est considérée comme dommageable", septembre 2007, DOI 10.17487/RFC4943. *(Information)*

[RFC4994] S. Zeng et autres, "Option DHCPv6 de demande d'écho d'agent de relais", septembre 2007, DOI 10.17487/RFC4994. *(P.S.)*

[RFC5007] J. Brzozowski et autres, "Leasequery dans DHCPv6", DOI 10.17487/RFC5007, septembre 2007. *(P.S.)*

[RFC5453] S. Krishnan, "Identifiants d'interface IPv6 réservés", DOI 10.17487/RFC5453, février 2009. *(P.S.)*

[RFC5460] M. Stapp, "Extensions au protocole Leasequery sur l'identification des liaisons dans DHCPv6", DOI 10.17487/RFC5460, février 2009. *(P.S.)*

[RFC5905] D. Mills, J. Martin, J. Burbank, W. Kasch, "Protocole de l'heure du réseau version 4 (NTPv4) : Spécification du protocole et des algorithmes ", DOI 10.17487/RFC5905, juin 2010. (*Remplace* RFC1305, RFC4330) *(P. S ; MàJ par* RFC7822, RFC8573)

[RFC5908] R. Gayraud, B. Lourdelet, "Option Serveur du protocole de l'heure du réseau (NTP) pour DHCPv6", DOI 10.17487/RFC5908, juin 2010. *(P. S.)*

[RFC6422] T. Lemon, Q. Wu, "Options DHCP fournies par relais", DOI 10.17487/RFC6422, décembre 2011. (*MàJ la* RFC3315) *(P.S.)*

[RFC6603] J. Korhonen, T. Savolainen, S. Krishnan, O. Troan, "Option 'Prefix Exclude' pour délégation de préfixe fondée sur DHCPv6", DOI 10.17487/RFC6603, mai 2012. ((*MàJ la* RFC3633) *(P.S.)*

[RFC6724] D. Thaler, R. Draves, A. Matsumoto, T. Chown, "Choix de l'adresse par défaut pour IPv6", DOI 10.17487/RFC6724, septembre 2012. (*Remplace la* RFC3484) *(P.S.)*

[RFC6879] S. Jiang, B. Liu, B. Carpenter, "Scénarios de dénumérotage de réseau d'entreprise IPv6, considérations et méthodes", DOI 10.17487/RFC6879, février 2013. *(Information)*

[RFC6939] G. Halwasia, S. Bhandari, W. Dec, "Option Adresse de couche liaison de client dans DHCPv6", DOI 10.17487/RFC6939, mai 2013. *(P.S.)*

[RFC7083] R. Droms, "Modification aux valeurs par défaut de SOL_MAX_RT et INF_MAX_RT", DOI 10.17487/RFC7083, novembre 2013. (*MàJ* RFC3315) *(P.S. ; rendue obsolète par* RFC8415)

[RFC7084] H. Singh et autres, "Exigences de base pour les routeurs bordures de consommateur IPv6", DOI 10.17487/RFC7084, novembre 2013 (*Remplace* RFC6204) *(Information)*

[RFC7136] B. Carpenter, S. Jiang, "Signification des identifiants d'interface IPv6", DOI 10.17487/RFC7136, février 2014. (*MàJ* RFC4291) *(P.S.)*

[RFC7341] Q. Sun, et autres,"Transport DHCPv4 sur DHCPv6", DOI 10.17487/RFC7341, août 2014. *(P.S.)*

[RFC7368] T. Chown, et autres, "Principes d'architecture de réseautage résidentiel IPv6", DOI 10.17487/RFC7368, octobre 2014. *(Information)*

[RFC7513] J. Bi, J. Wu, G. Yao, F. Baker, "Solutions d'amélioration de la validation de l'adresse de source (SAVI) pour DHCP", DOI 10.17487/RFC7513, mai 2015. *(P.S.)*

[RFC7550] O. Troan, B. Volz, M. Siodelski, "Problèmes et recommandations pour les options DHCPv6 multiples à états pleins", DOI 10.17487/RFC7550, mai 2015. *(P.S. ; rendue obsolète par* RFC8415)

[RFC7598] T. Mrugalaki, et autres, "Options DHCPv6 pour la configuration de clients dont l'adresse et l'accès sont transposés de IPv4 à IPv6", DOI 10.17487/RFC7598, juillet 2015. *(P.S. ; MàJ par* RFC8539*)*

[RFC7610] F. Gont, et autres, "Bouclier DHCPv6 : protection contre les serveurs DHCPv6 félons", DOI 10.17487/RFC7610, août 2015. BCP 198.

[RFC7707] F. Gont, T. Chown, "Reconnaissance de réseau dans les réseaux IPv6", DOI 10.17487/RFC7707, mars 2016. *(Information)*

[RFC7721] A. Cooper, F. Gent, D. Thaler, "Considérations de sécurité et de confidentialité pour les mécanismes de génération d'adresse IPv6", DOI 10.17487/RFC7721, mars 2016. *(Information)*

[RFC7824] S. Krishnan, et autres, "Considérations de confidentialité pour DHCPv6", DOI 10.17487/RFC7824, mai 2016. *(Information)*

[RFC7844] C. Huitema, et autres, "Profils d'anonymat pour clients DHCP", DOI 10.17487/RFC7844, mai 2016. *(P.S.)*

[RFC7969] T. Lemon, T. Mrugalski, "Personnalisation de la configuration de DHCP sur la base de la topologie du réseau", DOI 10.17487/RFC7969, octobre 2016. *(Information)*

[RFC8156] T. Mrugalski, K. Kinnear, "Protocole de reprise sur défaillance de DHCPv6", DOI 10.17487/RFC8156, juin 2017. *(P.S.)*

[RFC8168] T. LI, C. Liu, Y. Cui, "Problèmes de l'indication de longueur de préfixe DHCPv6", DOI 10.17487/RFC8168, mai 2017. *(P.S.)*

[TR-187] Broadband Forum, "TR-187 - IPv6 for PPP Broadband Access", février 2013, <https://www.broadband-forum.org/technical/download/TR-187_Issue-2.pdf >

Appendice A. Résumé des changements

Cet appendice donne un résumé des changements significatifs faits par cette mise à jour de la spécification DHCPv6.

1. L'introduction (Section 1) a été réorganisée et mise à jour. En particulier, les échanges de messages client/serveur ont été déplacés dans une section nouvelle (et étendue) autonome (Section 5).

2. De nouvelles sections ont été ajoutées pour discuter des relations avec les précédents documents DHCPv6 et aussi avec DHCPv4.

3. Les Sections 2 ("Exigences") et 3 ("Fondements") ont de très petites corrections rédactionnelles.

4. La Section 4 ("Terminologie") a des corrections mineures.

5. Le paragraphe 4.2 ("Terminologie DHCP") a été développé pour incorporer les définitions de la RFC 3633, ajouter les définitions de T1/T2, ajouter des définitions utiles pour décrire l'allocation combinée d'opérations d'adresse et de délégation de préfixe, et améliorer des définitions existantes.

6. La Section 5 ("Échanges client/serveur") a été ajoutée à partir de matériaux précédemment dans la Section 1 de la RFC 3315 ("Introduction et vue d'ensemble") et a été développée.

7. La Section 6 ("Modèles de fonctionnement") est nouvelle. Elle fournit des informations sur les sortes de clients DHCP et comment ils opèrent.

8. La Section 7 ("Constantes DHCP") a été principalement mise à jour pour ajouter des constantes provenant des RFC 4242 et RFC 7083. Noter que la valeur par défaut HOP_COUNT_LIMIT a été réduite de 32 à 8.

9. Les Sections 8 ("Formats de message de client/serveur") 9 ("Formats de message d'agent de relais/serveur") et 10 ("Représentation et utilisation des noms de domaines") ont seulement des changements très mineurs.

10. La Section 11 ("Identifiant unique DHCP (DUID)") déconseille maintenant, plutôt que d'interdire, qu'un serveur analyse le DUID ; elle inclut maintenant des informations sur le DUID-UUID (RFC 6355) et a d'autres corrections mineures.

11. La Section 12 ("Association d'identité") a été développée pour mieux expliquer le concept et aussi inclure la délégation de préfixe.

12. La Section 13 ("Allocation à une IA") incorpore des matériaux provenant de deux sections (11 et 12) de la RFC 3315 et aussi inclut une section sur la délégation de préfixe.

13. La Section 14 ("Transmission de messages par un client") a été développée pour inclure la limitation de taux par les clients et comment les clients devraient traiter la valeur de 0 de T1 ou T2.

14. La Section 15 ("Fiabilité des échanges de messages initiés par le client") a été développée pour préciser que l'option Temps écoulé doit être mise à jour dans les messages retransmis et qu'un client n'est pas obligé d'écouter le trafic DHCP pendant toute la période de retransmission.

15. La Section 16 ("Validation de message") a des corrections mineures.

16. La Section 17 ("Choix de l'adresse de source et de l'interface par le client") a été développée pour inclure la délégation de préfixe.

17. La Section 18 ("Échanges de configuration DHCP") consolide ce qui était dans les sections suivantes de la RFC 3315 : "Sollicitation de serveur DHCP" (Section 17), " Échanges de configuration DHCP initié par le client" (Section 18), et "Échanges de configuration DHCP initiés par le serveur" (Section 19). Ce matériel a été réorganisé et amélioré, et il incorpore la délégation de préfixe provenant de la RFC 3633 et d'autres changements des RFC 4242, 7083, et 7550. Quelques changements à noter :

    A. L'option Demande d'option n'est plus facultative pour certains messages (Solicit et Demande d'information), car la RFC 7083 exige des clients qu'ils demandent les options SOL_MAX_RT ou INF_MAX_RT.

B. Le message Reconfigure ne devrait plus contenir IA_NA/IA_PD, ORO, ou autres options pour indiquer au client ce qui est reconfiguré. Le client devrait demander tout ce dont il a besoin dans la réponse au Reconfigure.

C. Les conseils de durée de vie et de T1/T2 ne devrait pas être envoyés par un client (il devrait envoyer des valeurs de 0 dans ces champs) et toute valeur non zéro devrait être ignorée par le serveur.

D. Il est précisé qu'un serveur peut retourner dans le Reply des adresses différentes de celles demandées par un client dans le message Request. Précisé aussi qu'un serveur ne doit pas inclure d'adresses qu'il ne va pas allouer.

Aussi, le paragraphe 18.2.12 ("Rafraîchissement des informations de configuration ") a été ajouté pour indiquer des cas où un client devrait essayer de rafraîchir les informations de réseau.

18. La Section 19 ("Comportement de l'agent de relais") incorpore la RFC 7283 et quelques corrections mineures. Un nouveau paragraphe, "Interaction entre agents de relais et serveurs" (19.4) a été ajouté.

19. La Section 20 ("Authentification des messages DHCP") comporte des changements significatifs : les matériaux IPsec ont été retirés et remplacés par une référence à la RFC 8213, et le protocole d'authentification retardée a été rendu obsolète (voir la Section 25). Noter que RKAP est toujours considéré comme actuel.

20. La Section 21 ("Options DHCP") a été développée pour incorporer OPTION_IA_PD et OPTION_IAPREFIX de la RFC 3633, l'option Heure de rafraîchissement des informations (OPTION_INFORMATION_REFRESH_TIME) de la RFC 4242, et les options SOL_MAX_RT et INF_MAX_RT de la RFC 7083. Quelques corrections rédactionnelles ont été faites pour préciser le traitement des options, comme quelles options ne devraient pas être dans une option Demande d'option.

21. Les considérations sur la sécurité (Section 22) ont été mises à jour pour développer la discussion des menaces sur la sécurité et inclure du matériel provenant des documents incorporés, principalement la RFC 3633.

22. De nouvelles considérations de confidentialité ont été ajoutées (Section 23) pour tenir compte des questions de confidentialité.

23. La Section 24 ("Considérations relatives à l'IANA") a été réécrite pour refléter les changements demandés par le présent document, car d'autres documents ont déjà fait les allocations de message, option, DUID, et code d'état et le présent document n'ajoute aucune nouvelle allocation.

24. La Section 25 ("Mécanismes obsolètes") est une nouvelle section qui documente les mécanismes rendus obsolètes par cette spécification.

25. Les Appendices B ("Apparition des options dans les types de messages") et C ("Apparition des options dans les champs "options" des options DHCP") ont été mis à jour pour refléter les options incorporées des RFC 3633, 4242, et 7083.

26. Lorsque approprié, des références pour information ont été ajoutées pour donner le cadre et des indications tout au long du document (comme on peut le noter d'après l'augmentation des références).

27. Des changements ont été faits pour incorporer les errata de la RFC 3315 : errata 294, 295, 1373, 1815, 2471, 2472, 2509, 2928, 3577, 5450 ; de la RFC 3633 : errata 248, 2468, 2469, 2470, 3736 ; et de la RFC 3736 : errata 3796. Noter que l'errata 1880 pour la RFC 3633 ne s'applique plus, car les serveurs (routeurs délégants) ignorent les indications de T1/T2 reçues (voir le (C) dans le point 17 ci-dessus).

28. Des changements généraux aux autres spécifications IPv6, comme de retirer l'utilisation des adresses d'envoi individuel de site local et l'ajout des adresses locales uniques, ont été faits au document.

29. On devrait noter que le présent document ne se réfère pas à toutes les fonctionnalités et spécifications DHCPv6. Les lecteurs de cette spécification devrait visiter < https://www.iana.org/assignments/dhcpv6-parameters > et <https://datatracker.ietf.org/wg/dhc/ > pour avoir la liste des RFC qui définissent les messages, options, codes d'état DHCPv6, et plus encore.

Appendice B. Apparition des options dans les types de messages

Les tableaux qui suivent indiquent par "*" les options permises dans chaque type de message DHCP.

Ces tableaux sont pour information. Si ils sont en conflit avec le texte du présent document, le texte devrait être considéré comme d'autorité.

	ID client	ID serveur	IA_NA/IA_TA	IA_PD	ORO	Pref	Temps écoulé	Relais msg	Auth.	Serveur indiv.
Solicit	*		*	*	*		*			
Advert.	*	*	*	*		*				
Request	*	*	*	*	*		*			
Confirm	*		*				*			
Renew	*	*	*	*	*		*			
Rebind	*		*	*	*		*			
Decline	*	*	*	*			*			
Release	*	*	*	*			*			
Reply	*	*	*	*					*	*
Reconf.	*	*							*	
Inform.	* (voir note)				*		*			
R-forw.								*		
R-repl.								*		

Note : L'option Identifiant de serveur (paragraphe 21.3) est seulement incluse dans les messages Demande d'information qui sont envoyés en réponse à Reconfigure (paragraphe 18.2.6).

	Code d'état	Eng. rapide	Classe util.	Classe fabr.	Spec. fabr.	ID inter.	Msg. recon.	Accepte recon.	Info rafr.
Solicit		*	*	*	*			*	
Advert.	*		*	*	*			*	
Request			*	*	*			*	
Confirm			*	*	*				
Renew			*	*	*			*	
Rebind			*	*	*			*	
Decline			*	*	*				
Release			*	*	*				
Reply	*	*	*	*	*			*	*
Reconf.							*		
Inform.			*	*	*			*	
R-forw.					*	*			
R-repl.					*	*			

	SOL_MAX_RT	INF_MAX_RT
Solicit		
Advertise	*	
Request		
Confirm		
Renew		
Rebind		
Decline		
Release		
Reply	*	*
Reconf.		
Inform.		
R-forw.		
R-repl.		

Appendice C. Apparition des options dans le champ "options"des options DHCP

Le tableau qui suit indique par "*" où les options définies dans le présent document peuvent apparaître comme options de

niveau supérieur ou peuvent être encapsulées dans d'autres options définies dans le présent document. D'autres RFC pourront définir des situations supplémentaires où les options définies dans le présent document sont encapsulées dans d'autres options.

Ce tableau est pour information. Si il entre en conflit avec le texte du présent document, c'est le texte qui devrait être considéré comme d'autorité.

	Niveau sup.	IA_NA/IA_TA	IAADDR	IA_PD	IAPREFIX	RELAY-FORW	RELAY-REPL
Client ID	*						
Server ID	*						
IA_NA/IA_TA	*						
IAADDR		*					
IA_PD	*						
IAPREFIX				*			
ORO	*						
Preference	*						
Elapsed Time	*						
Relay Message						*	*
Authentic.	*						
Server Uni.	*						
Status Code	*	*		*			
Rapid Comm.	*						
User Class	*						
Vendor Class	*						
Vendor Info.	*					*	*
Interf. ID						*	*
Reconf. MSG.	*						
Reconf. Accept	*						
Info Refresh Time	*						
SOL_MAX_RT	*						
INF_MAX_RT	*						

Note : Les options marquées d'un astérisque dans la colonne "Niveau supérieur" apparaissent dans le champ "options" des messages du client (voir la Section 8). Les options marquées d'un astérisque dans les colonnes "RELAY-FORW" et "RELAY-REPL" apparaissent dans le champ "options" des messages Relay-forward et Relay-reply (voir la Section 9).

Remerciements

Le présent document est simplement une reprise de travaux antérieurs des auteurs des documents suivants et n'aurait pas été possible sans ces travaux originaux :
- RFC 3315 (Ralph Droms, Jim Bound, Bernie Volz, Ted Lemon, Charles Perkins, et Mike Carney)
- RFC 3633 (Ole Troan et Ralph Droms)
- RFC 3736 (Ralph Droms)
- RFC 4242 (Stig Venaas, Tim Chown, et Bernie Volz)
- RFC 7083 (Ralph Droms)
- RFC 7283 (Yong Cui, Qi Sun, et Ted Lemon)
- RFC 7550 (Ole Troan, Bernie Volz, et Marcin Siodelski)

Un certain nombre de personnes supplémentaires ont contribué à identifier les problèmes posés par les RFC 3315 et 3633 et proposé des solutions à ces problèmes comme reflété dans le présent document (cités ici sans ordre particulier) : Ole Troan, Robert Marks, Leaf Yeh, Michelle Cotton, Pablo Armando, John Brzozowski, Suresh Krishnan, Hideshi Enokihara, Alexandru Petrescu, Yukiyo Akisada, Tatuya Jinmei, Fred Templin, et Christian Huitema.

Nous remerciaons aussi les personnes suivantes de leurs relecture et leurs commentaires : Jeremy Reed, Francis Dupont, Lorenzo Colitti, Tianxiang Li, Ian Farrer, Yogendra Pal, Kim Kinnear, Shawn Routhier, Michayla Newcombe, Alissa Cooper, Allison Mankin, Adam Roach, Kyle Rose, Elwyn Davies, Eric Rescorla, Ben Campbell, Warren Kumari, et Kathleen Moriarty.

Des remerciements particuliers à Ralph Droms qui a répondu à de nombreuses questions relatives aux RFC 3315 et 3633

d'origine et pour avoir guidé le présent document à travers les processus de l'IETF.

Adresse des auteurs

Tomek Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
United States of America
mél : tomasz.mrugalski@gmail.com

Marcin Siodelski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
United States of America
mél : msiodelski@gmail.com

Bernie Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
United States of America
mél : volz@cisco.com

Andrew Yourtchenko
Cisco Systems, Inc.
De kleetlaan 6a
Diegem BRABANT 1831
Belgium
mél : ayourtch@cisco.com

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
Canada
mél : mcr+ietf@sandelman.ca

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus,
156 Beiqing Road
Hai-Dian District, Beijing 100095
China
mél : jiangsheng@huawei.com

Ted Lemon
Nibbhaya Consulting
P.O. Box 958
Brattleboro, VT 05301-0958
United States of America
mél : mellon@fugue.com

Timothy Winters
University of New Hampshire,
Interoperability Lab (UNH-IOL)
Durham, NH
United States of America
mél : twinters@iol.unh.edu