Groupe de travail Réseau
Demande for Comments : 3315
Catégorie : En cours de normalisation
juillet 2003

Traduction Claude Brière de L'Isle

R. Droms, éditeur, Cisco
J. Bound, Hewlett Packard
B. Volz, Ericsson
T. Lemon, Nominum
C. Perkins, Nokia Research Center
M. Carney, Sun Microsystems

Protocole de configuration dynamique des hôtes pour IPv6 (DHCPv6)

Résumé
Le protocole de configuration dynamique d'hôte pour IPv6 (DHCP) permet aux serveurs DHCP de passer les paramètres de configuration tels que les adresses réseau IPv6 aux nœuds IPv6. Il offre la capacité d'allocation automatique des adresses réseau réutilisables et une souplesse de configuration supplémentaire. Ce protocole est la contrepartie à états pleins du protocole d'autoconfiguration d'adresse IPv6 sans état de la RFC 2462, et il peut être utilisé séparément ou en concurrence avec ce dernier pour obtenir les paramètres de configuration.

Table des matières

1. Introduction et généralités

Le présent document décrit le DHCP pour IPv6 (DHCPv6) un protocole de client/serveur qui fournit la gestion de la configuration des appareils.

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

DHCP est le "protocole d'autoconfiguration d'adresse à états pleins" et le "protocole d'autoconfiguration à états pleins" auquel se réfère "l'autoconfiguration d'adresse IPv6 sans état" [17].

Les modèles de fonctionnement et les informations de configuration pertinentes pour DHCPv4 [18], [19] et DHCPv6 sont suffisamment différents pour que l'intégration entre les deux services ne soit pas incluse dans le présent document. Si l'intérêt et la demande en étaient suffisants, l'intégration pourrait être spécifiée dans un document qui étendrait DHCPv6 pour porter les adresses IPv4 et les informations de configuration.

Le reste de cette introduction fait un résumé de DHCP, expliquant les mécanismes d'échange de message et les exemples de flux de message. Les flux de message des paragraphes 1.2 et 1.3 sont destinés à l'illustrations du fonctionnement de DHCP plutôt qu'à une description exhaustive de toutes les possibles interactions client-serveur. Les Sections 17, 18, et 19 expliquent en détail le fonctionnement du client et du serveur.

1.1 Protocoles et adressage

Clients et serveurs échangent des messages DHCP en utilisant UDP [15]. Le client utilise une adresse de liaison locale ou des adresses déterminées par d'autres mécanismes pour transmettre et recevoir des messages DHCP.

Les serveurs DHCP reçoivent des messages des clients en utilisant une adresse réservée de diffusion groupée à portée de liaison. Un client DHCP transmet la plupart des messages à cette adresse réservée de diffusion groupée, de sorte que le client n'a pas besoin d'être configuré avec la ou les adresses de serveurs DHCP.

Pour permettre au client DHCP d'envoyer un message à un serveur DHCP qui n'est pas rattaché à la même liaison, un agent relais DHCP sur la liaison du client va relayer les messages entre le client et le serveur. Le fonctionnement de l'agent relais est transparent pour le client et l'exposé sur l'échange de messages dans le reste de cette section omettra la description du relais de messages par les agents relais.

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

1.2 Échange client-serveur impliquant deux messages

Lorsque un client DHCP n'a pas besoin qu'un serveur DHCP lui alloue des adresses IP, il peut obtenir des informations de configuration telles qu'une liste des serveurs DNS [20] ou des serveurs NTP [21] disponibles grâce à un seul message et sa réponse, échangés avec un serveur DHCP. Pour obtenir les 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 Réponse qui contient les informations de configuration pour le client.

Cet échange de messages suppose que le client ne demande que les informations de configuration et n'exige pas l'allocation d'une adresse IPv6.

Lorsque un serveur a des adresses IPv6 et d'autres informations de configuration relatives à un client, le client et le serveur peuvent être capables de compléter l'échange en utilisant seulement deux messages, au lieu de quatre messages comme décrit au paragraphe suivant. Dans ce cas, le client envoie un message Sollicitation à l'adresse Tous_Agents_de_Relais_et_Serveurs_DHCP pour demander l'allocation des adresses et les autres informations de configuration. Ce message comporte une indication que le client accepte un message Réponse immédiat de la part du serveur. Le serveur qui accepte d'engager l'allocation des adresses au client répond immédiatement par un message Réponse. Les informations de configuration et les adresses dans le message Réponse sont alors immédiatement disponibles pour que le client les utilise.

Chaque adresse allouée au client a des durées de vie associée et préférée qui sont spécifiées par le serveur. Pour demander une extension de la durée de vie allouée à une adresse, le client envoie un message Renouveler 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 sans interruption.

1.3 Échange client-serveur impliquant quatre messages

Pour demander l'allocation d'une ou plusieurs adresses IPv6, un client commence par localiser un serveur DHCP puis il demande alors l'allocation des adresses et les autres informations de configuration au serveur. Le client envoie un message Sollicitation à l'adresse Tous_Agents_de_Relais_et_Serveurs_DHCP pour trouver des serveurs DHCP disponibles. Tout serveur qui peut satisfaire les exigences du client répond par un message Annonce. Le client choisit alors un des serveurs et envoie un message Demande au serveur demandant une allocation confirmée des adresses et autres informations de configuration. Le serveur répond par un message Réponse qui contient les adresses et la configuration confirmées.

Comme décrit au paragraphe précédent, le client envoie un message Renouveler au serveur pour étendre les durées de vie associées à ses adresses, permettant au client de continuer d'utiliser ces adresses sans interruption.

2. Exigences

Les mots-clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" lorsque ils apparaissent dans le présent document sont à interpréter comme décrit dans [1].

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

3. Fondements

La spécification IPv6 donne l'architecture et la conception de base d'IPv6. Les travaux connexes sur IPv6 qui serviraient le mieux les études pour la mise en œuvre d'IPv6 incluent la spécification IPv6 [3], l'architecture d'adressage IPv6 [5], l'autoconfiguration d'adresse IPv6 sans état [17], le traitement de la découverte de voisin IPv6 [13], et la mise à jour dynamique du DNS [22]. Ces spécifications permettent à DHCP de construire sur la base du travail sur IPv6 pour fournir une autoconfiguration sans état et un auto enregistrement des noms d'hôtes du DNS robustes.

La spécification de l'architecture d'adressage IPv6 [5] définit la portée d'une adresse qui peut être utilisée dans une mise en œuvre de IPv6, et les diverses lignes directrices de l'architecture de configuration pour les concepteurs de réseaux de l'espace d'adresse 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 locales 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 des serveurs DHCP ou des agents relais sur sa liaison et communiquer avec eux.

L'autoconfiguration d'adresse IPv6 sans état [17] spécifie les procédures par lesquelles un nœud peut autoconfigurer des adresses sur la base des annonces de routeur [13], et l'utilisation d'une durée de vie valide pour prendre en charge la dénumérotation des adresses sur l'Internet. De plus, l'interaction de protocole par laquelle un nœud commence une

autoconfiguration sans état ou à états pleins est spécifiée. DHCP est un véhicule pour effectuer l'autoconfiguration à états pleins. La compatibilité avec l'autoconfiguration d'adresse sans état est une exigence de conception de DHCP.

La découverte de voisin IPv6 [13] est le protocole de découverte de nœuds dans IPv6 qui remplace et améliore les fonctions de ARP [14]. Pour comprendre IPv6 et l'autoconfiguration d'adresse sans état, il est vivement recommandé que les développeurs comprennent la découverte de voisin IPv6.

Les mises à jour dynamiques du DNS [22] sont une spécification qui prend en charge la mise à jour dynamique des enregistrements du DNS à la fois pour IPv4 et IPv6. DHCP peut utiliser les mises à jour dynamiques du DNS pour intégrer l'espace d'adresses et de noms non seulement pour prendre en charge l'autoconfiguration, mais aussi l'auto enregistrement dans IPv6.

4. Terminologie

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

4.1 Terminologie IPv6

La terminologie IPv6 pertinente pour la présente spécification, tirée du protocole IPv6 [3], de l'architecture d'adressage IPv6 [5], et de l'autoconfiguration d'adresse IPv6 sans état [17], est incluse ci-dessous.

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

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 ils sont nécessaires pour éviter une ambiguïté.

interface : rattachement d'un nœud à une liaison.
liaison : facilité ou support de communication sur lequel les nœuds peuvent communiquer à la couche liaison, c'est-à-dire, la couche immédiatement en dessous de IP. Des exemples en sont Ethernet (simple ou ponté), un anneau à jetons, des liaisons PPP, X.25, en relais de trame ou des réseaux ATM, et des tunnels de couche Internet (ou supérieure) tels que les tunnels sur IPv4 ou IPv6 lui-même.

identifiant de couche liaison : identifiant de couche liaison pour une interface. Les exemples incluent les adresses IEEE 802 pour les interfaces de réseau Ethernet ou d'anneau à jetons, et les adresses E.164 pour les liaisons RNIS.

adresse de liaison locale : adresse IPv6 qui a une portée limitée à la liaison, ce qui est indiqué par le préfixe (FE80::/10) et qui peut être utilisée pour atteindre les nœuds du voisinage rattachés à la même liaison. Chaque interface 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 qui ne lui sont pas explicitement adressés.

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

4.2 Terminologie DHCP

On trouvera ci-dessous la terminologie spécifique de DHCP.

approprié à la liaison : une adresse est "appropriée à la liaison" lorsque elle est cohérente avec la connaissance qu'a le serveur DHCP de la topologie du réseau, de l'allocation des préfixes et des politiques d'allocation d'adresse.

Groupe d'affectation *(binding)* : un groupe d'affectation (ou groupe d'affectation de clients) est un groupe d'enregistrements de données de serveur qui contient les informations qu'a le serveur sur les adresses dans une association d'identités (IA) ou dans des informations de configuration explicitement allouées au client. Les informations de configuration qui ont été retournées à un client au moyen d'une politique - par exemple, les informations retournées à tous les clients sur la même liaison - ne requièrent pas un groupe d'affectation. Un groupe d'affectation qui contient des informations sur une IA est indexé par le tuplet <DUID, IA-type, IAID> (où IA-type est le type d'adresse dans la IA ; par exemple, temporaire). Un groupe d'affectation qui contient des informations de configuration pour un client est indexé par <DUID>.

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

DHCP : Protocole de configuration dynamique d'hôte pour IPv6. Les termes DHCPv4 et DHCPv6 ne sont utilisés que dans les contextes où ils sont nécessaires pour éviter les ambiguïtés.

client DHCP (ou client) : Nœud qui initie les demandes sur une liaison pour obtenir les paramètres de configuration de la part d'un ou plusieurs serveurs DHCP.

domaine DHCP : Ensemble de liaisons gérées par DHCP et que fait fonctionner une seule entité administrative.

royaume DHCP : Nom utilisé pour identifier le domaine administratif DHCP à partir duquel une clé d'authentification DHCP a été choisie.

agent relais (DHCP) : Nœud qui agit comme intermédiaire pour délivrer les messages DHCP entre clients et serveurs, et est sur la même liaison que le client.

serveur (DHCP) : Nœud qui répond aux demandes des clients, et peut ou non être sur la même liaison que le ou les clients.

DUID : Identifiant DHCP univoque pour un participant DHCP ; chaque client et serveur DHCP a exactement un DUID. Voir à la section 9 les détails sur les façons dont un DUID peut être construit.

association d'identité (IA) : Collection d'adresses allouées à un client. Chaque IA a un IAID associé. Un client peut avoir plus d'une IA allouée ; par exemple, une pour chacune de ses interfaces. Chaque IA détient un type d'adresse ; par exemple, une association d'identité pour adresses temporaires (IA_TA) détient des adresses temporaires (voir "association d'identité pour adresses temporaires"). Tout au long du présent document, "IA" est utilisé pour se référer à une association d'identité sans identifier le type d'adresses dans l'IA.

Identifiant d'association d'identité (IAID) : Identifiant pour une IA, choisi par le client. Chaque IA a un IAID, qui est choisi pour être unique parmi tous les IAID pour les IA qui appartiennent à ce client.

Association d'identité pour adresses non temporaires (IA_NA) : IA qui porte des adresses allouées qui ne sont pas des adresses temporaires (voir à "association d'identité pour adresses temporaires").

Association d'identité pour adresses temporaires (IA_TA) : IA qui porte des adresses temporaires (voir RFC3041 [12]).

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

clé Reconfigurer : clé fournie à un client par un serveur et utilisée pour fournir la sécurité pour les messages Reconfigurer.

relayer : Un agent relais DHCP relaie les messages DHCP entre les participants DHCP.

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

5. Constantes DHCP

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

5.1 Adresses de diffusion groupée

DHCP fait usage des adresses de diffusion groupée suivantes :

Tous_Agents_de_Relais_et_Serveurs_DHCP (FF02::1:2)
C'est une adresse de diffusion groupée dont la portée est la 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)
C'est une adresse de diffusion groupée dont la portée est le site, qui est 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 que il ne connaît pas les adresses d'envoi individuel des serveurs. Noter que pour qu'un agent de relais utilise cette adresse, il doit avoir une adresse d'une portée suffisante pour être accessible par les serveurs. Tous les serveurs au sein du site sont membres de ce groupe de diffusion groupée.

5.2. Accès UDP

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

5.3 Types de message DHCP

DHCP définit les types de message suivants. Des détails supplémentaires sur ces types de message se trouvent dans les sections 6 et 7. Les types de message qui ne sont pas énumérés ici sont réservés pour une utilisation future. Le codage numérique de chaque type de message est indiqué entre parenthèses.

Sollicite (1) Un client envoie un message Sollicite pour localiser les serveurs.

Annoncer (2) Un serveur envoie un message Annoncer pour indiquer qu'il est disponible pour le service DHCP, en réponse à un message Sollicite reçu d'un client.

Demande (3) Un client envoie un message Demande pour demander des paramètres de configuration, y compris des adresses IP, à un serveur spécifique.

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

Renouvelle (5) Un client envoie un message Renouvelle au serveur qui a à l'origine fourni les adresses et les paramètres de configuration du client pour rallonger les durées de vie des adresses allouées au client et pour mettre à jour d'autres paramètres de configuration.

Relier (6) Un client envoie un message Relier à tout serveur disponible pour rallonger les durées de vie des adresses allouées au client et pour mettre à jour d'autres paramètres de configuration ; ce message est envoyé après qu'un client n'a reçu aucune réponse à un message Renouvelle.

Répondre (7) Un serveur envoie un message Répondre contenant les adresses allouées et les paramètres de configuration en réponse à un message Sollicite, Demande, Renouvelle, Relier, reçu d'un client. Un serveur envoie un message Répondre qui contient les paramètres de configuration en réponse à un message Demande-d'informations. Un serveur envoie un message Répondre en réponse à un message Confirme qui confirme ou nie que les adresses allouées au client sont appropriées à la liaison à laquelle est connecté le client. Un serveur envoie un message Répondre pour accuser réception d'un message Libérer ou Refuser.

Libérer (8) Un client envoie un message Libérer au serveur qui a alloué les adresses au client pour indiquer que celui-ci ne va plus utiliser une ou plusieurs des adresses allouées.

Refuser (9) Un client envoie un message Refuser à un serveur pour indiquer que le client a déterminé que une ou plusieurs 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 va devoir réinitialiser une transaction Renouvelle/Répondre ou Demande-d'informations/Répondre avec le serveur afin de recevoir les informations à jour.

Demande-d'informations (11) Un client envoie un message Demande-d'informations à un serveur pour demander les paramètres de configuration sans affectation d'aucune adresse IP au client.

Transmission-relais (12) Un agent de relais envoie un message Relais-de-transmission pour relayer les messages aux serveurs, soit directement, soit à travers un autre agent de relais. Le message reçu, qui est un message de client ou un message Relais-de-transmission provenant d'un autre agent de relais, est encapsulé dans une option dans le message Relais-de-transmission.

Réponse-de-relais (13) Un serveur envoie un message Réponse-de-relais à un agent de relais qui contient un message que l'agent de relais livre à un client. Le message Réponse-de-relais peut être relayé par d'autres agents de relais pour la livraison à l'agent de relais de destination. Le serveur encapsule le message client comme une option dans le message Réponse-de-relais, que l'agent de relais extrait et relaye au client.

5.4 Codes d'état

DHCPv6 utilise des codes d'état pour communiquer le succès ou l'échec des opérations demandées dans les messages provenant des clients et des serveurs, et pour fournir des informations supplémentaires sur la cause spécifique de l'échec d'un message. Les codes d'état particuliers sont définis au paragraphe 24.4.

5.5 Paramètres de transmission et de retransmission

Ce paragraphe présente un tableau des valeurs utilisées pour décrire le comportement de transmission de message des clients et des serveurs.

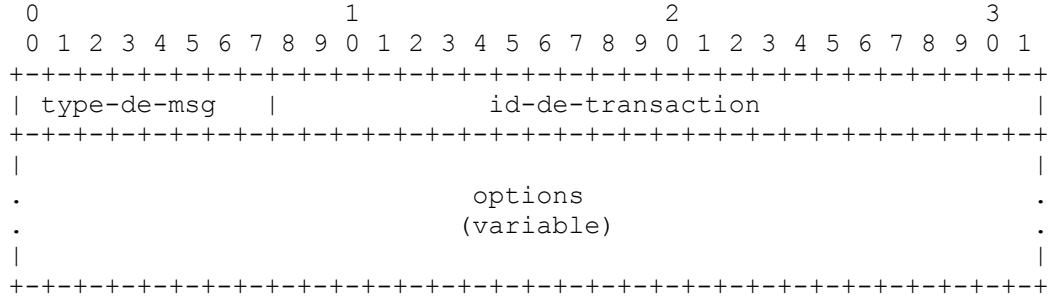
Paramètre	Par défaut	Description
SOL_MAX_DELAY	1 s	Délai maximum du premier Sollicite
SOL_TIMEOUT	1 s	Temporisation du Sollicite initial
SOL_MAX_RT	120 s	Valeur maximale de temporisation de Sollicite
REQ_TIMEOUT	1 s	Temporisation de la demande initiale
REQ_MAX_RT	30 s	Valeur maximale de temporisation de demande
REQ_MAX_RC	10	Nombre maximal de tentatives de demande
CNF_MAX_DELAY	1 s	Délai maximum du premier Confirme
CNF_TIMEOUT	1 s	Temporisation du Confirme initial
CNF_MAX_RT	4 s	Temporisation maximale de Confirme
CNF_MAX_RD	10 s	Durée maximale de Confirme
REN_TIMEOUT	10 s	Temporisation du Renouvelle initial
REN_MAX_RT	600 s	Valeur maximale de temporisation de Renouvelle
REB_TIMEOUT	10 s	Temporisation du Relier initial
REB_MAX_RT	600 s	Valeur maximale de temporisation de Relier
INF_MAX_DELAY	1 s	Délai maximum de la première Demande-d'informations
INF_TIMEOUT	1 s	Temporisation de Demande-d'informations initiale
INF_MAX_RT	120 s	Valeur maximale de temporisation de Demande-d'informations
REL_TIMEOUT	1 s	Temporisation de Libérer initiale
REL_MAX_RC	5	Nombre maximal de tentatives de Libérer
DEC_TIMEOUT	1 s	Temporisation de Refuser initial
DEC_MAX_RC	5	Nombre maximal de tentatives de Refuser
REC_TIMEOUT	2 s	Temporisation de Reconfigurer initial
REC_MAX_RC	8	Nombre maximal de tentatives de Reconfigurer
HOP_COUNT_LIMIT	32	Compte de bonds maximum dans un message Relais-de-transmission

5.6 Représentation des valeurs temporelles et "infini" comme valeur de temps

Toutes les valeurs de temps pour les durées de vie, T1 et T2 sont des entiers non signés. La valeur 0xffffffff est prise pour signifier "infini" lorsque elle est utilisée comme durée de vie (comme dans la RFC2461 [17]) ou une valeur pour T1 ou T2.

6. Formats de message client/serveur

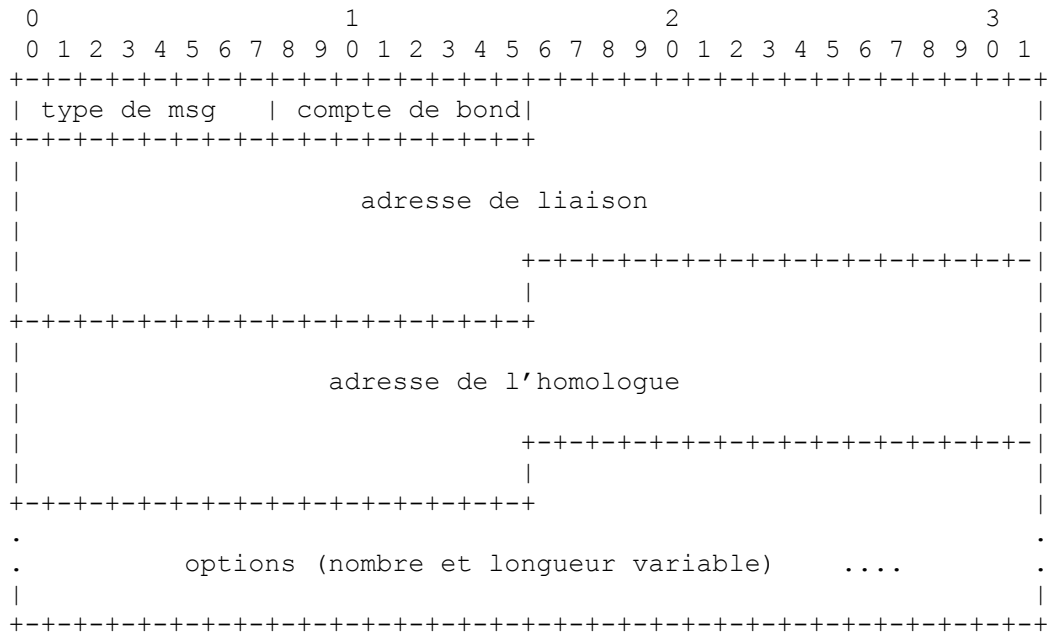
Tous les messages DHCP envoyés entre clients et serveurs partagent un en-tête identique de format fixe et une zone de format variable pour les options.
Toutes les valeurs dans l'en-tête de message et dans les options sont dans l'ordre des octets du réseau.
Les options sont mémorisées à la suite les unes des autres dans le champ des options, sans bourrage entre les options. Les options sont verrouillées sur l'octet mais ne sont pas alignées d'une autre façon sur des limites de 2 ou 4 octets.
Le diagramme suivant illustre le format des messages DHCP envoyés entre clients et serveurs :



type-de-msg : Identifie le type de message DHCP ; la liste des types de message disponibles figure au paragraphe 5.3.
id-de-transaction : Identifiant de transaction pour cet échange de messages.
options : Ce sont les options portées dans ce message ; les options sont décrites à la section 22.

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

Les agents de relais échangent des messages avec les serveurs pour relayer les messages entre clients et serveurs qui ne sont pas connectés sur 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 à la suite dans le champ Options, sans bourrage entre les options. Les options sont alignées sur les octets mais ne sont pas alignées d'autre façon telle que sur des limites de 2 ou 4 octets.
Il y a deux messages d'agent de relais, qui partagent le format suivant :



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

7.1 Message Relais-de-transmission

Le tableau suivant définit l'utilisation des champs de message dans un message Relais-de-transmission.

type de msg	Relais-de-transmission
compte de bond	nombre d'agents de relais qui ont relayé ce message.
adresse de liaison	Adresse mondiale ou de site local qui sera utilisée par le serveur pour identifier la liaison sur laquelle est situé le client.
adresse de l'homologue	Adresse du client ou agent de relais duquel le message à relayer a été reçu.
options	DOIT comporter une "option Message relais" (voir § 22.10) ; peut inclure d'autres options ajoutées par l'agent de relais.

7.2 Message Réponse-de-relais

Le tableau suivant définit l'utilisation des champs de message dans un message Réponse-de-relais.

type de msg	Réponse-de-relais
compte de bond	Copié du message Relais-de-transmission
adresse de liaison	Copiée du message Relais-de-transmission
adresse de l'homologue	Copiée du message Relais-de-transmission
options	DOIT comporter une "option Message relais" (voir § 22.10) ; peut inclure d'autres options.

8. Représentation et usage des noms de domaines

Pour que les noms de domaines puissent être codés de façon uniforme, 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 [10]. Dans DHCP, un nom de domaine, ou liste de noms de domaines, NE DOIT PAS être mémorisé en forme compressée, comme décrit au paragraphe 4.1.4 de la RFC1035.

9. Identifiant DHCP univoque (DUID)

Chaque client et serveur DHCP a un DUID. Les serveurs DHCP utilisent les 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 lorsque un serveur a besoin d'être identifié. Voir aux paragraphes 22.2 et 22.3 la représentation d'un DUID dans un message DHCP.

Clients et serveurs DOIVENT traiter les DUID comme des valeurs opaques et DOIVENT seulement comparer les DUID pour égalité. Les clients et serveurs NE DOIVENT PAS interprêter d'autre façon les DUID. Les clients et serveurs NE DOIVENT PAS restreindre les DUID aux types définis dans le présent document, car des types supplémentaires de DUID seront définis à l'avenir.

Le DUID est porté dans une option parce qu'il peut être de longueur variable et parce qu'il n'est pas obligatoire dans tous les messages DHCP. Le DUID est conçu comme unique parmi tous les clients et 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.

La raison pour avoir plus d'un type de DUID est que le DUID doit être unique au monde et doit aussi être facile à générer. La sorte d'identifiant unique au monde qui est facile à générer pour tous les appareils peut différer assez largement. Aussi, certains appareils peuvent ne pas contenir de moyens de mémorisation permanents. 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.

9.1 Contenu du DUID

Un DUID consiste en un code de type de deux octets représenté dans l'ordre des octets du réseau, suivi par un nombre variable d'octets qui constituent l'identifiant réel. Un DUID ne doit pas faire plus de 128 octets de long (non inclus le code de type). Les types suivants sont actuellement définis :

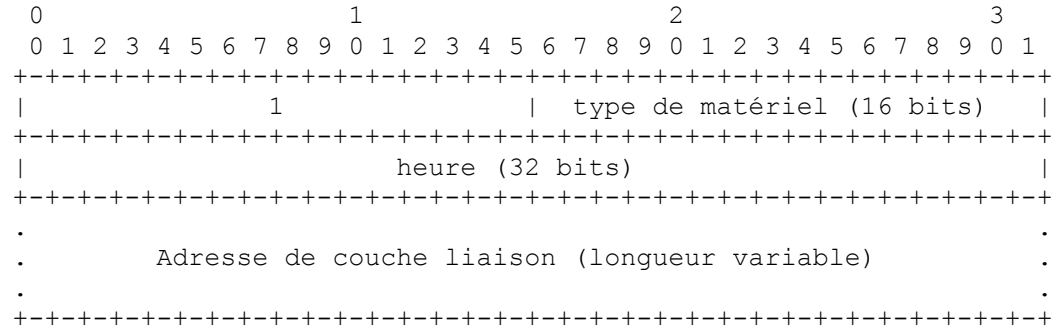
1 Adresse de couche liaison plus heure.
2 Identifiant unique alloué par le fabricant fondé sur le numéro d'entreprise.
3 Adresse de couche liaison.

Les formats du champ variable du DUID pour chacun des types ci-dessus sont donnés dans les paragraphes qui suivent.

9.2 DUID fondé sur l'adresse de couche liaison plus l'heure [DUID-LLT]

Ce type de DUID consiste en un champ de type de deux octets contenant la valeur 1, un code de type de matériel de deux octets, quatre octets contenant une valeur horaire, suivis par l'adresse de couche liaison d'une interface réseau qui est connectée à l'appareil DHCP au moment où le DUID est généré. La valeur horaire est l'heure à laquelle le DUID est généré, représentée en secondes depuis le premier janvier 2000 à minuit (UTC), modulo 2^32. Le type de matériel DOIT être un type de matériel valide alloué par l'IANA, comme décrit dans la RFC826 [14]. L'heure et le type de matériel sont tous deux mémorisés dans l'ordre des octets du réseau. L'adresse de couche liaison est mémorisée en forme canonique, comme décrit dans la RFC2464 [2].

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



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

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

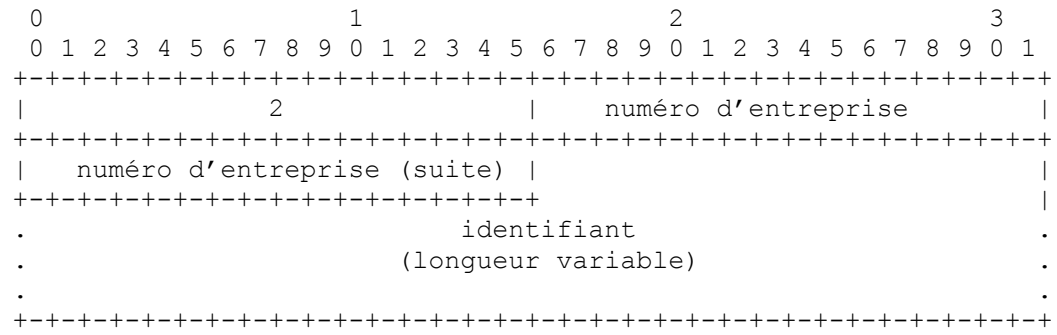
Les clients et serveurs qui utilisent ce DUID DEVRAIENT tenter de configurer l'heure avant de générer le DUID, si c'est possible, et DOIVENT utiliser une source horaire (par exemple, une horloge en temps réel) pour générer le DUID, même si la source horaire n'a pas pu être configurée avant la génération du DUID. L'utilisation d'une source horaire rend peu vraisemblable 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 peu vraisemblable 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 de calcul général comme les ordinateurs portables et individuels, et aussi pour les appareils du type imprimante, routeur, et ainsi de suite qui contiennent une forme de mémorisation inscriptible non volatile.

En dépit de nos efforts, il est possible que cet algorithme de génération de DUID puisse résulter en une collision d'identifiant de client. Un DHCP client 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.

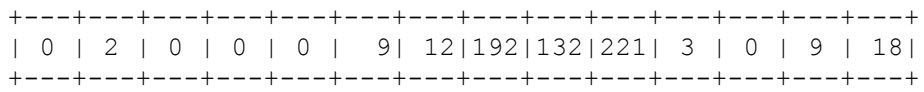
9.3 DUID alloué par le fabricant à partir du numéro d'entreprise [DUID-EN]

Cette forme de DUID est allouée par le fabricant de l'appareil. Il comporte le numéro d'entreprise privée du fabricant tel que conservé par l'IANA [6] suivi par un identifiant unique alloué par le fabricant. Le diagramme suivant résume la structure d'un DUID-EN:



La source de l'identifiant est à la discrétion du fabricant qui la définit, mais chaque identifiant qui fait partie de chaque DUID-EN DOIT être unique pour l'appareil qui l'utilise, et DOIT être alloué à l'appareil au moment de sa fabrication et mémorisé dans une forme de support non volatile. Le DUID généré DEVRAIT être enregistré sur un support non effaçable. Le numéro d'entreprise est le numéro d'entreprise privée enregistré pour le fabricant auprès de l'IANA [6]. Il est mémorisé comme un nombre non signé de 32 bits.

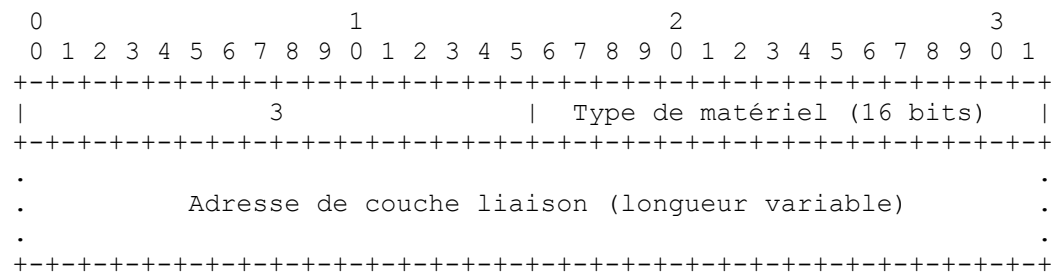
Un exemple de DUID de ce type pourrait ressembler à ceci :



Cet exemple comporte le type 2 de deux octets, le numéro d'entreprise (9), suivi par huit octets de données d'identifiant (0x0CC084D303000912).

9.4 DUID fondés sur l'adresse de couche liaison [DUID-LL]

Ce type de DUID comporte deux octets qui contiennent le type de DUID 3, un code de type de matériel réseau de deux octets, suivi par l'adresse de couche liaison de toute interface réseau connectée en permanence à l'appareil client ou serveur. Par exemple, un hôte qui a une interface réseau mise en œuvre dans une puce dont il est peu vraisemblable qu'elle soit retirée et utilisée quelque part ailleurs pourrait utiliser un DUID-LL. Le type de matériel DOIT être un type de matériel valide alloué par l'IANA, comme décrit dans la RFC826 [14]. Le type de matériel est mémorisé dans l'ordre des octets du réseau. L'adresse de couche liaison est mémorisée en forme canonique, comme décrit dans la RFC2464 [2]. Le diagramme suivant illustre le format d'un DUID-LL :



Le choix de l'interface réseau peut être complètement arbitraire, pour autant que cette interface fournisse une adresse de liaison unique et qu'elle 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 quelle adresse de couche liaison de l'interface a été utilisée pour générer le DUID.

Le DUID-LL est recommandé pour les appareils qui ont une interface réseau connectée en permanence avec une adresse de couche liaison, et qui n'a pas de support de mémorisation stable inscriptible et non volatile. Le DUID-LL NE DOIT PAS être utilisé par les clients ou 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.

10. 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 IPv6 qui sont en relation. Chaque IA consiste en un IAID et des informations de configuration associées.

Un client doit associer au moins une IA distincte à chacune de ses interfaces réseau pour laquelle 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 de la part d'un serveur pour cette interface. Chaque IA doit être associée à exactement une interface.

L'IAID identifie de façon univoque la IA et doit être choisi de façon à être unique parmi les IAID sur le client. Le IAID est choisi par le client. Pour toute utilisation d'une IA par le client, l'IAID pour cette IA DOIT être cohérent à travers les redémarrages du client DHCP. Le client peut conserver la cohérence soit en mémorisant le IAID sur un support non volatile, soit en utilisant un algorithme qui va toujours produire le même IAID tant que la configuration du client n'aura pas changé. Il peut n'y avoir aucun moyen pour qu'un client conserve la cohérence des IAID si il ne dispose pas de mémoire non volatile et si la configuration matérielle du client change.

Les informations de configuration dans une IA consistent en une ou plusieurs adresses IPv6 ainsi que les temps T1 et T2 pour la IA. Voir au paragraphe 22.4 la représentation d'une IA dans un message DHCP.

Chaque adresse dans une IA a une durée de vie préférée et une durée de validité, commeé défini dans la RFC2462 [17]. Les durées de vie sont transmises du serveur DHCP au client dans l'option IA. Les durées de vie s'appliquent à l'utilisation des adresses IPv6, comme décrit au paragraphe 5.5.4 de la RFC2462.

11. Choix des adresses à allouer à une IA

Un serveur choisit des adresses à allouer à une IA conformément aux politiques d'allocation d'adresse déterminées par l'administrateur du serveur et aux informations spécifiques que le serveur détermine sur le client à partir d'une combinaison des sources suivantes :

- La liaison à laquelle est rattaché le client. 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 de 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 sur laquelle est rattachée l'interface identifiée par le champ Adresse de liaison provenant de l'agent de relais.
  * 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 survenir que si le serveur a activé l'utilisation de la livraison de message en envoi individuel par le client et si 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.
- D'autres informations dans les options fournies par l'agent de relais.

Toute adresse allouée par un serveur qui se fonde sur un identifiant EUI-64 DOIT inclure un identifiant d'interface avec les bits "u" (universel/local) et "g" (individuel/groupe) de l'identifiant d'interface réglé de la façon appropriée, comme indiqué au paragraphe 2.5.1 de la RFC2373 [5].

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 des adresses réservées d'envoi à la cantonade, comme défini par la RFC2526, à partir d'aucun sous-réseau.

12. Gestion des adresses temporaires

Un client peut demander l'allocation d'adresses temporaires (voir dans la RFC3041 [12] la définition des adresses temporaires). Le traitement de l'allocation d'adresse par DHCPv6 n'est pas différent pour les adresses temporaires. DHCPv6 ne dit rien sur les détails des adresses temporaires comme la durée de vie, comment les clients utilisent les adresses temporaires, les règles pour générer les adresses temporaires successives, etc.

Les clients demandent les adresses temporaires et les serveurs les allouent. Les adresses temporaires sont portées dans l'option Association d'identité pour adresses temporaires (IA_TA) (voir au paragraphe 22.5). Chaque option IA_TA contient au plus une adresse temporaire pour chaque préfixe sur la liaison à laquelle le client est rattaché.

L'espace de nombre d'IAID pour l'option IA_TA est distinct de l'espace de nombre d'IAID pour l'option IA_NA.

Le serveur PEUT mettre à jour le DNS pour une adresse temporaire, comme décrit à la section 4 de la RFC3041.

13. Transmission des messages par un client

Sauf spécification contraire dans le présent document, ou dans un document qui décrit comment IPv6 est porté sur un type spécifique de liaison (pour les types de liaison qui n'acceptent pas la diffusion groupée) un client envoie les messages DHCP à l'adresse Tous_agents_de_relais_et_serveurs_DHCP.

Un client utilise la diffusion groupée pour atteindre tous les serveurs ou un serveur individuel. Un serveur individuel est indiqué en spécifiant le DUID de ce serveur dans une option Identifiant de serveur (voir au paragraphe 22.3) dans le message du client (tous les serveurs vont recevoir ce message mais seul le serveur indiqué va répondre). Tous les serveurs reçoivent l'indication mais tous ne fournissent pas cette option.

Un client peut envoyer des messages directement à un serveur en utilisant l'envoi individuel, comme décrit au paragraphe 22.12.

14. Fiabilité des échanges de messages initiés par un client

Les clients DHCP sont responsables de la livraison fiable des messages dans les échanges de messages initiés par le client décrits aux sections 17 et 18. Si un client DHCP échoue à recevoir une réponse attendue d'un serveur, le client doit retransmettre son message. Le présente section décrit la stratégie de retransmission à utiliser par les clients dans les échanges de messages à l'initiative du client.

Noter que la procédure décrite dans cette section est légèrement modifiée lorsque elle est utilisée avec le message Sollicite La procédure modifiée est décrite au paragraphe 17.1.2.

Le client commence l'échange de messages en transmettant un message au serveur. L'échange de messages se termine lorsque soit le client reçoit bien la ou les réponses appropriées d'un ou des serveurs, soit lorsque l'échange de messages est considéré comme ayant échoué selon le mécanisme de retransmission décrit ci-dessous.

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

RT	Fin de temporisation de retransmission
IRT	Heure initiale de retransmission
MRC	Compte maximum de retransmission
MRT	Heure maximale de retransmission
MRD	Durée maximum de retransmission
RAND	Facteur d'aléation

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

Chacun des calculs d'un nouveau RT comporte 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 pour choisir un nombre aléatoire n'a pas besoin d'être fondé sur la cryptographie. L'algorithme DEVRAIT produire une séquence différente de nombres aléatoires à partir de chaque invocation par le client DHCP.

Pour la première transmission de message, RT se fonde sur IRT :

RT = IRT + RAND*IRT

Pour chaque transmission de message suivant, RT se fonde sur la valeur précédente de RT :

RT = 2*RTprev + RAND*RTprev

MRT spécifie une limite supérieure de la valeur de RT (sans considération de l'aléation ajoutée 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 que le client a transmis le message pour la première fois.

Si MRC et MRD sont tous deux différents de zéro, l'échange de messages échoue chaque fois que l'une ou l'autre des conditions spécifiées dans les deux paragraphes précédents sont réunies.

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

15. Validation du message

Les clients et serveurs DEVRAIENT éliminer tout message qui contient des options qui ne sont pas permises dans le message reçu. Par exemple, une option IA n'est pas permise dans un message Demande d'informations. Les clients et serveurs PEUVENT choisir d'extraire les informations de tels messages si les informations sont utiles au receveur.

Un serveur DOIT éliminer tous les messages Sollicite, Confirme, Relier ou Demande d'informations qu'il reçoit avec une adresse de destination en envoi individuel.

La validation de message sur la base de l'authentification DHCP est exposée au paragraphe 21.4.2.

Si un serveur reçoit un message qui contient des options qu'il ne devrait pas contenir (comme un message Demande d'informations avec une option IA) si il manque des options qu'il devrait contenir, ou si il est par ailleurs invalide, il PEUT envoyer une Réponse (ou une Annonce si c'est approprié) avec une option Identifiant de serveur, une option Identifiant de client si il en était une d'incluse dans le message, et une option Code d'état avec l'état UnSpecFail.

15.1 Utilisation des identifiants de transaction

Le champ "transaction-id" contient une valeur qui est 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 être aisément deviné ou prédit pour l'utiliser comme l'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 sortes d'attaques de la part d'intrus hors du chemin. Un client DOIT laisser l'identifiant de transaction inchangé dans la retransmissions d'un message.

15.2 Message Sollicite

Les clients DOIVENT éliminer tout message Sollicite reçu.
Les serveurs DOIVENT éliminer tout message Sollicite qui ne comporte pas une option Identifiant de client ou qui comporte une option Identifiant de serveur.

15.3. Message Annoncer

Les clients DOIVENT éliminer tout message Annoncer reçu qui satisfait à une des conditions suivantes :
- le message ne comporte pas une option Identifiant de serveur,
- le message ne comporte pas une option Identifiant de client,
- le contenu de l'option Identifiant de client ne correspond pas au DUID du client,
- la valeur du champ "transaction-id" ne correspond pas à la valeur que le client a utilisée dans son message Sollicite

Les serveurs et agents de relais DOIVENT éliminer tous les messages Annoncer reçus.

15.4 Message Demande

Les clients DOIVENT éliminer tout message Demande reçu.

Les serveurs DOIVENT éliminer tout message Demande reçu qui satisfait une des conditions suivantes :
- le message ne comporte pas une option Identifiant de serveur,
- le contenu de l'option identifiant de serveur ne correspond pas au DUID du serveur,
- le message ne comporte pas d'option Identifiant de client.

15.5 Message Confirme

Les clients DOIVENT éliminer tout message Confirme reçu.

Les serveurs DOIVENT éliminer tout message Confirme reçu qui ne comporte pas une option Identifiant de client ou qui comporte une option Identifiant de serveur.

15.6 Message Renouvelle

Les clients DOIVENT éliminer tout message Renouvelle reçu.

Les serveurs DOIVENT éliminer tout message Renouvelle qui satisfait à une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur,
- 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.

15.7 Message Relier

Les clients DOIVENT éliminer tout message Relier reçu.

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

15.8 Message Refuser

Les clients DOIVENT éliminer tout message Refuser reçu.

Les serveurs DOIVENT éliminer tout message Refuser reçu qui satisfait une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur,
- 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.

15.9 Message Libérer

Les clients DOIVENT éliminer tout message Libérer reçu.

Les serveurs DOIVENT éliminer tout message Libérer qui satisfait une des conditions suivantes :
- le message ne comporte pas d'option Identifiant de serveur,
- 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.

15.10 Message Répondre

Les clients DOIVENT éliminer tout message Répondre reçu qui satisfait une des conditions suivantes :
- le message ne comporte pas une option Identifiant de serveur,
- le champ "transaction-id" dans le message ne correspond pas à la valeur utilisée dans le message d'origine.

Si le client a inclus une option Identifiant de client dans le message d'origine, le message Répondre DOIT inclure une option Identifiant de client et le contenu de celle-ci DOIT correspondre au DUID du client; OU, si le client n'avait pas inclus d'option Identifiant de client dans le message d'origine, le message Répondre NE DOIT PAS inclure d'option Identifiant de client.

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

15.11 Message Reconfigure

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

Les clients DOIVENT éliminer tout message Reconfigure qui satisfait une des conditions suivantes :
- le message n'était pas en envoi individuel au client,
- le message ne comporte pas d'option Identifiant de serveur,
- le message ne comporte pas d'option Identifiant de client qui contienne le DUID du client,
- le message ne contient pas d'option Reconfiguration de message et le type de message doit être une valeur valide,
- le message comporte des options IA et le type de msg dans l'option Reconfiguration de message est Demande d'information,
- le message ne comporte pas d'authentification DHCP :
  * le message ne contient pas d'option d'authentification,
  * le message n'a pas réussi la validation d'authentification effectuée par le client.

15.12 Message Demande d'information

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

Les serveurs DOIVENT éliminer tout message Demande d'information reçu qui satisfait à une des conditions suivantes :
- le message comporte une option Identifiant de serveur et le DUID dans l'option ne correspond pas au DUID du serveur,
- le message comporte une option IA.

15.13 Message Relais-de-transmission

Les clients DOIVENT éliminer tout message Relais-de-transmission reçu.

15.14 Message Réponse-de-relais

Clients et serveurs DOIVENT éliminer tout message Réponse-de-relais reçu.

16. Adresse de source du client et choix de l'interface

Lorsque un client envoie un message DHCP à l'adresse Tous_Agents_de_Relais_et_Serveurs_DHCP, il DEVRAIT envoyer le message à travers l'interface pour laquelle il demande les informations de configuration. Cependant, le client PEUT envoyer le message à travers une autre interface rattachée à la même liaison, si et seulement si le client est certain que les deux interfaces sont rattachées à la même liaison. Le client DOIT utiliser l'adresse de liaison locale allouée à l'interface pour laquelle il demande des informations de configuration comme adresse de source dans l'en-tête du datagramme IP.

Lorsque un client envoie un message DHCP directement à un serveur en utilisant l'envoi individuel (après avoir reçu l'option Envoi individuel au serveur de ce serveur) l'adresse de source dans l'en-tête du datagramme IP DOIT être une adresse allouée à l'interface pour laquelle le client souhaite obtenir la configuration et qui convient pour que le serveur l'utilise en réponse au client.

17. Sollicitation du serveur DHCP

La présente section décrit comment un client localise les serveurs qui vont allouer des adresses aux IA qui appartiennent au client.

Le client est chargé de la création des IA et de demander qu'un serveur alloue des adresses IPv6 à l'IA. Le client crée d'abord une IA et lui alloue une IAID. Le client transmet ensuite un message Sollicite qui contient une option IA qui décrit l'IA. Les serveurs qui peuvent allouer des adresses à l'IA répondent au client avec un message Annoncer. Le client initie alors un échange de configuration comme décrit à la section 18.

Si le client va accepter un message Répondre avec engagement d'allocations d'adresse et d'autres ressources en réponse au message Sollicite, le client inclut une option Engagement rapide (*Rapid Commit*, voir au paragraphe 22.14) dans le message Sollicite

17.1 Comportement du client

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

17.1.1 Création des messages Sollicite

Le client règle le champ "type-de-msg" à SOLLICITE. Le client génère un Identifiant de transaction et insère cette valeur dans le champ "id-de-transaction".

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client inclut des options IA pour toute IA à laquelle il veut que le serveur alloue une adresse. Le client PEUT inclure des adresses dans les IA comme conseil au serveur sur les adresses pour lesquelles le client a une préférence. Le client NE DOIT PAS inclure d'autre option dans les messages Sollicite, sauf spécifiquement permis dans la définition de l'option individuelle.

Le client utilise les options IA_NA pour demander l'allocation d'adresses non temporaires et utilise les options IA_TA pour demander l'allocation d'adresses temporaires. Les options IA_NA ou IA_TA, ou une combinaison des deux, peuvent être incluses dans les messages DHCP.

Le client DEVRAIT inclure une option Demande d'option (voir au paragraphe 22.7) pour indiquer les options par lequelles il est intéressé. De plus, le client PEUT inclure des instances de ces options qui sont identifiées dans l'option Demande d'option, avec des valeurs de données comme indications au serveur sur les valeurs de paramètre que le client voudrait qu'il lui retourne.

Le client inclut une option Reconfigure Accepte (voir au paragraphe 22.20) si il veut accepter les messages Reconfigure provenant du serveur.

17.1.2 Transmission des messages Sollicite

Le premier message Sollicite provenant du client sur l'interface DOIT être retardé d'une durée aléatoire comprise entre 0 et SOL_MAX_DELAY. Dans le cas d'un message Sollicite transmis à l'initialisation de DHCP par la découverte de voisin IPv6, le délai donne la durée d'attente après que la découverte de voisin IPv6 a causé l'invocation par le client du protocole d'autoconfiguration d'adresse à états pleins (voir au paragraphe 5.5.3 de la RFC2462). Ce retard aléatoire désynchronise les clients qui démarrent au même moment (par exemple, après une panne de courant).

Le client transmet le message conformément aux dispositions de la section 14, en utilisant les paramètres suivants :

IRT	SOL_TIMEOUT
MRT	SOL_MAX_RT
MRC	0
MRD	0

Si le client a inclus une option Engagement rapide dans son message Sollicite, il termine le processus d'attente aussitôt qu'est reçu un message Répondre avec une option Engagement rapide.

Si le client attend un message Annoncer, le mécanisme de la section 14 est modifié comme suit pour être utilisé à la transmission du message Sollicite L'échange de messages n'est pas terminé par la réception d'un Annoncer avant l'écoulement du premier RT. Le client collecte plutôt les messages Annoncer jusqu'à ce que le premier RT soit écoulé. Le premier RT DOIT aussi être choisi strictement supérieur à l'IRT en choisissant RAND strictement supérieur à 0.

Un client DOIT collecter les messages Annoncer pendant les RT premières secondes, sauf si il reçoit un message Annoncer avec une valeur de préférence de 255. La valeur de préférence est portée dans l'option Préférence (paragraphe 22.8). Tout Annoncer qui ne comporte pas une option Préférence est considéré comme ayant une valeur de préférence de 0. Si le client reçoit un message Annoncer qui comporte une option Préférence avec une valeur de préférence de 255, le client commence immédiatement un échange de messages à l'initiative du client (comme décrit à la section 18) en envoyant un message Demande au serveur d'où a été reçu ce message Annoncer. Si le client reçoit un message Annoncer qui ne comporte pas d'option Préférence avec une valeur de préférence de 255, le client continue d'attendre jusqu'à ce que le premier RT soit écoulé. Si le premier RT s'écoule et si le client a reçu un message Annoncer, le client DEVRAIT continuer avec un échange de messages à l'initiative du client en envoyant un message Demande.

Si le client n'a pas reçu de message Annoncer avant que le premier RT soit écoulé, il commence le mécanisme de

retransmission décrit à la section 14. Le client termine le processus de retransmission aussitôt qu'il reçoit un message Annoncer, et le client agit sur le message Annoncer reçu sans attendre d'autre message Annoncer supplémentaire.

Un client DHCP DEVRAIT choisir MRC et MRD comme étant à 0. Si le client DHCP est configuré avec MRC ou MRD réglés à une valeur autre que 0, il DOIT arrêter d'essayer de configurer l'interface si l'échange de messages échoue. Après l'arrêt par le client DHCP des essais de configuration de l'interface, il DEVRAIT redémarrer le processus de reconfiguration après quelque événement externe, tel qu'une entrée d'utilisateur, un redémarrage système, ou lorsque le client se rattache à une nouvelle liaison.

17.1.3 Réception des messages Annoncer

Le client DOIT ignorer tout message Annoncer qui comporte une option Code d'état contenant la valeur NoAddrsAvail, sauf si le client PEUT afficher le message d'état associé à l'usager.

À réception d'un ou plusieurs messages Annoncer valides, le client choisit un ou plusieurs messages Annoncer sur la base des critères suivants :
- Les messages Annoncer avec la plus forte valeur de préférence de serveur sont préférés à tous les autres messages Annoncer.
- Au sein d'un groupe de messages Annoncer de la même valeur de préférence de serveur, un client PEUT choisir les serveurs dont les messages Annoncer annoncent des informations qui intéressent le client. Par exemple, le client peut choisir un serveur qui a retourné une annonce avec des options de configuration qui intéressent le client.
- Le client PEUT choisir un serveur de moindre préférence si ce serveur a un meilleur ensemble de paramètres annoncés, tels que les adresses disponibles annoncées dans les IA.

Une fois qu'un client a choisi un ou des messages Annoncer, il va normalement mémoriser les informations sur chaque serveur, telles que la valeur de préférence de serveur, les adresses annoncées, quand l'annonce a été reçue, et ainsi de suite.

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

17.1.4 Réception des messages Répondre

Si le client inclut une option Engagement rapide dans le message Sollicite, il va s'attendre à un message Répondre qui comporte une option Engagement rapide en réponse. Le client élimine tout message Répondre qu'il reçoit et ne comporte pas l'option Engagement rapide. Si le client reçoit un message Répondre valide qui inclut une option Engagement rapide, il traite le message comme décrit au paragraphe 18.1.8. Si il ne reçoit pas un tel message Répondre et reçoit un message Annoncer valide, le client traite le message Annoncer comme décrit au paragraphe 17.1.3.

Si le client reçoit ensuite un message Répondre valide qui comporte une option Engagement rapide, soit :
- il traite le message Répondre comme décrit au paragraphe 18.1.8, et
- il élimine tout message Répondre recu en réponse au message Demande, soit
- il traite tout message Répondre reçu en réponse au message Demande et élimine le message Répondre qui comporte l'option Engagement rapide.

17.2 Comportement du serveur

Un serveur envoie un message Annoncer en réponse aux messages Sollicite valides qu'il reçoit pour annoncer la disponibilité du serveur au client.

17.2.1 Réception des messages Sollicite

Le serveur détermine les informations sur le client et sa localisation comme décrit à la section 11 et vérifie sa politique administrative sur le fait de répondre au client. Si il n'est pas permis au serveur de répondre au client, le serveur élimine le message Sollicite. Par exemple, si la politique administrative pour le serveur est qu'il ne peut répondre qu'à un client qui va accepter un message Reconfigure, si le client indique par une option Reconfigure Accepte dans le message Sollicite qu'il ne va pas accepter un message Reconfigure, les serveurs éliminent le message Sollicite

Si le client a inclus une option Engagement rapide dans le messags Sollicite et si le serveur a été configuré pour répondre par des engagements d'allocations d'adresse et autres ressources, le serveur répond au Sollicite par un message Répondre comme décrit au paragraphe 17.2.3. Autrement, le serveur ignore l'option Engagement rapide et traite le reste du message comme si aucune option Engagement rapide n'était présente.

17.2.2 Création et transmission des messages Annoncer

Le serveur régle le champ "type-de-message" à ANONCER et copie le contenu du champ ID-de-transaction du message Sollicite reçu du client dans le message Annoncer. Le serveur inclut son identifiant de serveur dans une option Identifiant de serveur et copie l'identifiant de client du message Sollicite dans le message Annoncer.

Le serveur PEUT ajouter une option Preference pour porter la valeur de préférence pour le message Annoncer. La mise en œuvre de serveur DEVRAIT permettre le réglage par l'administrateur d'une valeur de préférence de serveur. La valeur de préférence de serveur DOIT par défaut être zéro sauf configurée autrement par l'administrateur du serveur.

Le serveur inclut une option Reconfigure Accepte si le serveur veut exiger que le client accepte les messages Reconfigure.

Le serveur inclut des options qu'il va retourner au client dans un message Répondre ultérieur. Les informations dans ces options peuvent être utilisées par le client dans le choix d'un serveur si le client reçoit plus d'un message Annoncer. Si le client a inclus une option Demande d'option dans le message Sollicite, le serveur inclut les options dans le message Annoncer qui contient 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 pour le faire. Le serveur doit être averti des recommandations sur les tailles de paquet et l'utilisation de la fragmentation de la section 5 de la RFC2460.

Si le message Sollicite qui provient du client comporte une ou plusieurs options IA, le serveur DOIT inclure dans le message Annoncer des options IA qui contiennent toutes les adresses qui auraient été allouées aux IA contenues dans le messags Sollicite provenant du client. Si le client a inclus des adresses dans les IA dans le message Sollicite, le serveur utilise ces adresses comme indications sur les adresses que le client aimerait recevoir.

Si le serveur ne va allouer aucune adresse à aucune IA dans une Demande ultérieure provenant du client, le serveur DOIT envoyer un message Annoncer au client qui ne comporte qu'une option Code d'état avec le code NoAddrsAvail et un message d'état pour l'usager, une option Identifiant de serveur avec le DUID du serveur, et une option Identifiant de client avec le DUID du client.

Si le messags Sollicite a été reçu directement par le serveur, le serveur envoie en individuel le message Annoncer directement au client en utilisant l'adresse qui se trouve dans le champ Adresse de source provenant du datagramme IP dans lequel a été reçu le message Sollicite. Le message Annoncer DOIT être en envoi individuel sur la liaison de laquelle a été reçu le message Sollicite.

Si le messags Sollicite a été reçu dans un message Relais-de-transmission, le serveur construit un message Réponse-de-relais avec le message Annoncer dans la charge utile d'une option "Message de relais". Si le message Relais-de-transmission comportait une option Interface-id, le serveur copie cette option dans le message Réponse-de-relais. Le serveur envoie le message Réponse-de-relais en individuel directement à l'agent de relais en utilisant l'adresse dans le champ Adresse de source provenant du datagramme IP dans lequel a été reçu le message Relais-de-transmission.

17.2.3 Création et transmission des messages Répondre

Le serveur DOIT engager l'allocation de toutes les adresses ou autres messages d'informations de configuration avant d'envoyer un message Répondre à un client en réponse à un message Sollicite.

DISCUSSION :

Lorsque on utilise l'échange de messages Sollicite-Répondre, le serveur engage l'allocation de toutes les adresses avant d'envoyer le message Répondre. Le client peut supposer que les adresses lui ont été allouées dans le message Répondre et n'a pas besoin d'envoyer un message Demande pour ces adresses.

Normalement, les serveurs qui sont configurés pour utiliser l'échange de messages Sollicite-Répondre seront déployés de telle sorte qu'un seul serveur va répondre à un messags Sollicite. Si plus d'un serveur répond, le client va seulement utiliser les adresses d'un des serveurs, tandis que les adresses des autres serveurs seront engagées au client mais non utilisées par lui.

Le serveur inclut une option Engagement rapide dans le message Répondre pour indiquer que le Répondre est en réponse à un messags Sollicite.

Le serveur inclut une option Reconfigure Accepte si il veut exiger que le client accepte les messages Reconfigure.

Le serveur produit le message Répondre bien qu'il ait reçu un message Demande, comme décrit au paragraphe 18.2.1. Le serveur transmet le message Répondre comme décrit au paragraphe 18.2.8.

18 Échange DHCP de configuration à l'initiative du client

Un client initie un échange de messages avec un ou des serveurs pour acquérir ou mettre à jour des informations de configuration qui l'intéressent. Le client peut initier l'échange de configuration au titre du processus de configuration du système d'exploitation, lorsque il lui est demandé de le faire par la couche application, lorsque c'est exigé par l'autoconfiguration d'adresse sans état ou lorsque c'est exigé pour étendre la durée de vie d'une adresse (messages Renouvelle et Relier).

18.1 Comportement du client

Un client utilise les messages Demande, Renouvelle, Relier, Libérer et Refuser durant le cycle de vie normal des adresses. Il utilise Confirme pour valider les adresses lorsque il peut avoir été déplacé sur une nouvelle liaison. Il utilise les messages Demande d'informations lorsque il a besoin d'informations de configuration mais pas d'adresses.

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 une option Serveur en envoi individuel (paragraphe 22.12) de la part du serveur, le client DEVRAIT envoyer au serveur tous les messages Demande, Renouvelle, Libérer et Refuser en envoi individuel.

DISCUSSION :

L'utilisation de l'envoi individuel peut éviter des retards dus au relais des messages par les agents de relais, aussi bien que d'éviter des redondances et des réponses dupliquées par les serveurs à cause de la livraison des messages de client à plusieurs serveurs. Exiger du client qu'il relaie 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 n'activer l'utilisation de l'envoi individuel que lorsque les options d'agent de relais ne seront pas utilisées.

18.1.1 Création et transmission des messages Demande

Le client utilise un message Demande pour remplir les IA d'adresses et obtenir d'autres informations de configuration. Le client inclut une ou plusieurs options IA dans le message Demande. Le serveur retourne alors les adresses et autres informations sur les IA au client dans les options IA dans un message Répondre.

Le client génère un identifiant de transaction et insère cette valeur dans le champ ID-de-transaction.

Le client place l'identifiant du serveur de destination dans une option Identifiant de serveur.

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client ajoute toutes autres options appropriérs, y compris une ou plusieurs options IA (si le client demande que le serveur lui alloue des adresses réseau).

Le client DOIT inclure une option Demande d'option (voir au paragraphe 22.7) pour indiquer les options que le client est intéressé à recevoir. Le client PEUT inclure des options des valeurs de données comme indications au serveur sur les valeurs de paramètres que le client aimerait qu'il lui retourne.

Le client inclut une option Reconfigure Accepte (voir au paragraphe 22.20) qui indique si le client veut ou non accepter des messages Reconfigurer de la part du serveur.

Le client transmet le message conformément à la section 14, 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 peut prendre le client sont :

- de choisir un autre serveur sur une liste de serveurs connus du client ; par exemple, les serveurs qui ont répondu par un message Annoncer,

- d'initier le processus de découverte de serveur décrit à la section 17,
- de le processus de configuration et faire rapport de l'échec.

18.1.2 Création et transmission des messages Confirme

Chaque fois qu'un client peut avoir été déplacé sur une nouvelle liaison, les préfixes provenant des adresses allouées aux interfaces sur cette liaison peuvent n'être plus appropriés pour la liaison à laquelle est rattaché le client. Des exemples de cas où un client peut avoir été déplacé sur une nouvelle liaison sont :

o Le client se réamorce.
o Le client est physiquement connecté à une connexion filaire.
o Le client revient d'un mode dormant.
o Le client qui utilise une technologie sans fil change de point d'accès.

Dans toute situation où un client peut avoir été déplacé sur une nouvelle liaison, le client DOIT initier un échange de messages Confirme/Répondre. Le client inclut toutes les IA allouées à l'interface qui peut avoir été déplacée sur une nouvelle liaison, ainsi que les adresses associées à ces IA, dans son message Confirme. Tous les serveurs qui répondent vont indiquer si ces adresses sont appropriées pour la liaison à laquelle le client est rattaché avec son statut dans le message Répondre qu'il retourne au client.

Le client règle le champ "type-de-msg" à CONFIRME. Le client génère un identifiant de transaction et insère cette valeur dans le champ "id-de-transaction".

Le client DOIT inclure une option Identifiant de client pour s'identifer auprès du serveur. Le client inclut des options IA pour toutes les IA allouées à l'interface pour laquelle le message Confirme est envoyé. Les options IA incluent toutes les adresses que le client a actuellement associé à ces IA. Le client DEVRAIT régler les champs T1 et T2 dans toutes les options IA_NA, et les champs Durée de vie préférée et Durée de validité dans les options d'adresse IA à 0, car le serveur va ignorer ces champs.

Le premier message Confirme 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 14, 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 que se termine le processus de transmission du message, comme décrit à la section 14, le client DEVRAIT continuer d'utiliser toutes les adresses IP, en utilisant les dernières durées de vie connues pour ces adresses, et DEVRAIT continuer d'utiliser tous les autres paramètres de configuration précédemment obtenus.

18.1.3 Création et transmission des messages Renouvelle

Pour étendre les durées de vie valide et préférée pour les adresses associées à une IA, le client envoie un message Renouvelle au serveur duquel le client a obtenu les adresses dans l'IA qui contient une option IA pour l'IA. Le client inclut les options Adresse d'IA dans l'option IA pour les adresses associées à l'IA. Le serveur détermine de nouvelles durées de vie pour les adresses dans l'IA conformément à la configuration administrative du serveur. Le serveur peut aussi ajouter de nouvelles adresses à l'IA. Le serveur peut retirer des adresses de l'IA en réglant à zéro les durées de vie préférée et de validité de ces adresses.

Le serveur contrôle par les paramètres T1 et T2 l'heure à laquelle le client contacte le serveur pour étendre les durées de vie sur les adresses allouées à une IA.

Au moment T1 pour une IA, le client initie un échange de messages Renouvelle/Répondre pour étendre les durées de vie sur toutes les adresses dans l'IA. Le client inclut une option IA avec toutes les adresses actuellement allouées à l'IA dans son message Renouvelle.

Si T1 ou T2 est réglé à 0 par le serveur (pour une IA_NA) ou si il n'y a pas de temps T1 ou T2 (pour une IA_TA) le client peut envoyer un message, respectivement, Renouvelle ou Relier, à la discretion du client.

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

Le client place l'identifiant du serveur de destination dans une option Identifiant de serveur.

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client ajoute toutes les options approprées, y compris une ou plusieurs options IA. Le client DOIT inclure la liste des adresses que le client a actuellement associé aux IA dans le message Renouvelle.

Le client DOIT inclure une option Demande d'option (voir au paragraphe 22.7) pour indiquer les 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 qu'il aimerait se voir retourner.

Le client transmet le message conformément à la section 14, en utilisant les paramètres suivants :

IRT	REN_TIMEOUT
MRT	REN_MAX_RT
MRC	0
MRD	temps restant jusqu'à T2

L'échange de messages se termine quand le temps T2 est atteint (voir au paragraphe 18.1.4) qui est le moment où le client commence un échange de messages Relier.

18.1.4 Création et transmission des messages Relier

À l'instant T2 pour une IA (qui ne sera atteint que si le serveur auquel le message Renouvelle a été envoyé à l'instant T1 n'a pas reçu de réponse) le client initie un échange de messages Relier/Répondre avec tout serveur disponible. Le client inclut une option IA avec toutes les adresses actuellement allouées à l'IA dans son message Relier.

Le client règle le champ "type-de-msg" à RELIER. Le client génère un identifiant de transaction et insère cette valeur dans le champ "id-de-transaction".

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client ajoute toutes les options appropriées, y compris une ou plusieurs options IA. Le client DOIT inclure la liste des adresses que le client a actuellement associées aux IA dans le message Relier.

Le client DOIT inclure une option Demande d'option (voir au paragraphe 22.7) pour indiquer les options qu'il est intéressé à recevoir. Le client PEUT inclure des options avec des valeurs de données comme indications au serveur sur les valeurs de paramètre qu'il aimerait se voir retourner.

Le client transmet le message conformément à la section 14, en utilisant les paramètres suivants :

IRT	REB_TIMEOUT
MRT	REB_MAX_RT
MRC	0
MRD	Temps restant jusqu'à l'expiration de la durée de validité de toutes les adresses.

L'échange de messages se termine lorsque les durées de validité de toutes les adresses allouées à l'IA sont arrivées à expiration (voir à la section 10) moment auquel le client a à choisir entre plusieurs actions ; par exemple :

- Le client peut choisir d'utiliser un messags Sollicite pour localiser un nouveau serveur DHCP et envoyer un Demande pour l'IA arrivée à expiration au nouveau serveur.
- Le client peut avoir d'autres adresses dans d'autres IA, de sorte qu'il peut choisir d'éliminer l'IA arrivée à expiration et utiliser les adresses des autres IA.

18.1.5 Création et transmission des messages Demande-d'informations

Le client utilise un message Demande-d'informations pour obtenir des informations de configuration sans avoir d'adresse qui lui soit allouée.

Le client règle le champ "type-de-msg" à SEMANDE-D'INFORMATIONS. Le client génère un identifiant de transaction et insère cette valeur dans le champ "id-de-transaction".

Le client DEVRAIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Si le client n'inclut pas une option Identifiant de client, le serveur ne sera pas capable de retourner d'option spécifique du client au client, ou le serveur peut choisir de ne pas répondre du tout au message. Le client DOIT inclure une option Identifiant de client si le message Demande d'informations doit être authentifié.

Le client DOIT inclure une option Demande d'option (voir au paragraphe 22.7) pour indiquer les options qu'il est intéressé à recevoir. Le client PEUT inclure des options avec des valeurs de données comme indications au serveur sur les valeurs de paramètre qu'il aimerait se voit retourner.

Le premier message Demande d'informations 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 14, en utilisant les paramètres suivants :

IRT	INF_TIMEOUT
MRT	INF_MAX_RT
MRC	0
MRD	0

18.1.6 Création et transmission des messages Libérer

Pour libérer une ou plusieurs adresses, un client envoie un message Libérer au serveur.

Le client règle le champ "type-de-msg" à LIBÉRER. Le client génère un identifiant de transaction et place cette valeur dans le champ "id-de-transaction".

Le client place l'identifiant du serveur qui a alloué la ou les adresses dans une option Identifiant de serveur.

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client inclut des options qui contiennent les IA pour les adresses qu'il libère dans le champ "options". Les adresses à libérer DOIVENT être incluses dans les IA. Toutes adresses pour les IA que le client souhaite continuer d'utiliser NE DOIVENT PAS être ajoutées aux IA.

Le client NE DOIT PAS utiliser une des adresses qu'il libère comme adresse de source dans le message Libérer ou dans un message transmis ultérieurement.

Parce que les messages Libérer peuvent être perdus, le client devrait retransmettre Libérer si aucun Répondre n'est reçu. Cependant, il y a des scénarios où le client peut ne pas souhaiter attendre pendant la temporisation normale de retransmission avant d'abandonner (par exemple, sur une coupure de courant). Les mises en œuvre DEVRAIENT retransmettre une ou plusieurs fois, mais PEUVENT choisir de terminer plus tôt la procédure de retransmission.

Le client transmet le message conformément à la section 14, en utilisant les paramètres suivants :

IRT	REL_TIMEOUT
MRT	0
MRC	REL_MAX_RC
MRD	0

Le client DOIT arrêter d'utiliser toutes les adresses qui sont libérées aussitôt qu'il commence le processus d'échange de messages Libérer. Si les adresses sont libérées mais si le Répondre du serveur DHCP est perdu, le client va retransmettre le message Libérer, et le serveur peut répondre par un Répondre qui indique un état de NoBinding. Donc, le client ne traite pas un message Répondre avec un état de NoBinding dans un échange de messages Libérer comme si il indiquait une erreur.

Noter que si le client échoue à libérer les adresses, chaque adresse allouée à l'IA sera réclamée par le serveur lorsque la durée de validité de cette adresse va arriver à expiration.

18.1.7 Création et transmission des messages Refuser

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

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

Le client place l'identifiant du serveur qui a alloué la ou les adresses dans une option Identifiant de serveur.

Le client DOIT inclure une option Identifiant de client pour s'identifier auprès du serveur. Le client inclut des options qui contiennent les IA pour les adresses qu'il décline dans le champ "options". Les adresses à décliner DOIVENT être incluses dans les IA. Aucune des adresses pour les IA que le client souhaite continuer à utiliser ne devrait être ajoutée dans les IA.

Le client NE DOIT PAS utiliser une des adresses qu'il décline comme adresse de source dans le message Refuser ou dans tout autre message transmis ultérieurement.

Le client transmet le message conformément à la section 14, en utilisant les paramètres suivants :

IRT	DEC_TIMEOUT
MRT	0
MRC	DEC_MAX_RC
MRD	0

Si des adresses sont déclinées mais le Répondre du serveur DHCP est perdu, le client va retransmettre le message Refuser, et le serveur peut répondre par un Répondre indiquant un état de NoBinding. Donc, le client ne traite pas un message Répondre avec un état de NoBinding dans un échange de messages Refuser comme si il indiquait une erreur.

18.1.8 Réception des messages Répondre

À réception d'un message Répondre valide en réponse à un message Sollicite (avec une option Engagement rapide) Demande, Confirme, Renouvelle, Relier ou Demande-d'informations, le client extrait les informations de configuration contenues dans le Répondre. Le client PEUT choisir de faire rapport de tout code d'état ou message provenant de l'option code d'état dans le message Répondre.

Le client DEVRAIT effectuer une détection d'adresse dupliquée [17] sur chacune des adresses dans toute IA qu'il reçoit dans le message Répondre avant d'utiliser cette adresse pour du trafic. Si une des adresses se trouve être en usage sur la liaison, le client envoie un message Refuser au serveur comme décrit au paragraphe 18.1.7.

Si le Répondre a été reçu en réponse à un message Sollicite (avec une option Engagement rapide) Demande, Renouvelle ou Relier, le client met à jour les informations qu'il a enregistrées sur les IA à partir des options IA contenues dans le message Répondre :

- l'enregistrement des temps T1 et T2,
- l'ajout de toutes les nouvelles adresses de l'option IA à l'IA comme enregistré par le client,
- la mise à jour des durées de vie pour toute adresse dans l'option IA que le client a déjà enregistré dans l'IA,
- l'élimination de toute adresse de l'IA, telle qu'enregistrée par le client, qui a une durée de validité de 0 dans l'option Adresse d'IA,
- laisser inchangée toute information sur les adresses que le client a enregistrées dans l'IA mais n'étaient pas incluses dans l'IA provenant du serveur.

La gestion des informations de configuration spécifique est détaillée dans la définition de chaque option à la section 22.

Si le client reçoit un message Répondre avec un code d'état contenant UnspecFail, le serveur indique qu'il n'a pas été capable de traiter le message à cause d'une condition d'échec non spécifiée. Si le client retransmet le message d'origine 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.

Lorsque le client reçoit un message Répondre avec une option Code d'état avec la valeur UseMulticast, le client enregistre la réception du message et envoie les messages ultérieurs au serveur à travers l'interface sur laquelle le message a été reçu en utilisant la diffusion groupée. Le client envoie à nouveau le message d'origine en utilisant la diffusion groupée.

Lorsque le client reçoit un état NotOnLink de la part du serveur en réponse à un message Confirme, le client effectue une sollicitation de serveur DHCP, comme décrit à la section 17, et la configuration à l'initiative du client, comme décrit à la section 18. Si le client reçoit des messages Répondre qui n'indiquent pas un état NotOnLink, le client peut utiliser les adresses dans l'IA et ignorer tout message qui indique un état NotOnLink.

Lorsque le client reçoit un état NotOnLink de la part du serveur en réponse à un Demande, le client peut émettre à nouveau le Demande sans spécifier d'adresse ou redémarrer le processus de découverte de serveur DHCP (voir la section 17).

Le client examine le code d'état dans chaque IA individuelle. Si le code d'état est NoAddrsAvail, le client n'a reçu aucune adresse utilisable dans l'IA et peut choisir d'essayer d'obtenir des adresses pour l'IA à partir d'un autre serveur. Le client utilise les adresses et autres informations provenant de toute IA qui ne contient pas une option Code d'état avec le code NoAddrsAvail. Si le client ne reçoit d'adresses dans aucune des IA, il peut essayer un autre serveur (peut-être en redémarrant le processus de découverte de serveur DHCP) ou utiliser le message Demande-d'informations pour obtenir seulement d'autres informations de configuration.

Lorsque le client reçoit un message Répondre en réponse à un message Renouvelle ou Relier, le client examine indépendamment chaque IA. Pour chaque IA dans le message Renouvelle ou Relier original, le client :

- envoie un message Demande si l'IA contenait une option Code d'état avec l'état NoBinding (et n'envoie aucun message Renouvelle/Relier supplémentaire)
- envoie un Renouvelle/Relier si l'IA n'est pas dans le message Répondre
- accepte par ailleurs les informations contenues dans l'IA.

Lorsque le client reçoit un message Répondre valide en réponse à un message Libérer, le client considère que l'événement de libération est terminé, sans considération de la ou des options Code d'état retournées par le serveur.

Lorsque le client reçoit un message Répondre valide en réponse à un message Refuser, le client considère que l'événement Refuser est achevé, sans considération des options Code d'état retournées par le serveur.

18.2 Comportement du serveur

Pour cet exposé, le serveur est supposé avoit été configuré d'une façon spécifique d'une mise en œuvre avec la configuration qui intéresse les clients.

Dans la plupart des cas, le serveur va envoyer un Répondre en réponse au message du client. Ce message Répondre DOIT toujours contenir l'option Identifiant de serveur qui contient le DUID du serveur et l'option Identifiant de client provenant du message du client si l'un était présent.

Dans la plupart des messages Répondre, le serveur inclut des options qui contiennent 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 exprimées à la section 5 de la RFC2460. Si le client comportait une option Demande d'option dans son message, le serveur inclut dans le message Répondre des options qui contiennent des paramètres de configuration pour toutes les options identifiées dans l'option Demande d'option que le serveur a été configuré pour retourner au client. Le serveur PEUT retourner des options supplémentaires au client si il a été configuré pour ce faire.

18.2.1 Réception des messages Demande

Lorsque le serveur reçoit un message Demande par envoi individuel de la part d'un client auquel le serveur n'a pas envoyé une option Envoi individuel, le serveur élimine le message Demande et répond par un message Répondre contenant une option Code d'état avec la valeur UseMulticast *(utiliser la diffusion groupée)*, une option Identifiant de serveur contenant le DUID du serveur, l'option Identifiant de client provenant du message du client, et pas d'autre option.

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

Le serveur construit un message Répondre en réglant le champ "type-de-msg" à RÉPONDRE, et en copiant dans le champ id-de-transaction l'identifiant de transaction provenant du message Demande.

Le serveur DOIT inclure dans le message Répondre une option Identifiant de serveur contenant le DUID du serveur et l'option Identifiant de client provenant du message Demande.

Si le serveur trouve que, sur une ou plusieurs adresses IP dans une IA du message provenant du client, le préfixe 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 avec la valeur NotOnLink.

Si le serveur ne peut pas allouer d'adresse à une IA dans le message provenant du client, le serveur DOIT inclure l'IA dans le message Répondre avec aucune adresse dans l'IA et une option Code d'état dans l'IA contenant le code d'état NoAddrsAvail.

Pour toutes les IA auxquelles le serveur peut allouer des adresses, le serveur inclut l'IA avec les adresses et autres paramètres de configuration, et enregistre l'IA comme nouveau lien de client.

Le serveur inclut une option Reconfigure Accepte si le serveur veut demander que le client accepte les messages Reconfigure.

Le serveur inclut d'autres options contenant des informations de configuration à retourner au client comme décrit au paragraphe 18.2.

Si le serveur trouve que le client a inclus une IA dans le message Demande pour lequel le serveur a déjà un lien qui associe l'IA au client, le client a envoyé à nouveau un message Demande pour lequel il n'avait pas reçu de message Répondre. Le serveur envoie à nouveau un message Répondre mis précédement en antémémoire, ou bien envoie un nouveau message Répondre.

18.2.2 Réception des messages Confirme

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

Le serveur ignore les champs T1 et T2 dans les options IA et et les champs durée de vie préférée et de validité dans les options Adresse d'IA.

Le serveur construit un message Répondre en réglant le champ "type-de-msg" à RÉPONDRE, et en copiant l'identifiant de transaction du message Confirme dans le champ ID-de-transaction.

Le serveur DOIT inclure une option Identifiant de serveur contenant le DUID du serveur et l'option Identifiant de client du message Confirme dans le message Répondre. Le serveur inclut une option Code d'état qui indique l'état du message Confirme.

18.2.3 Réception des messages Renouvelle

Lorsque le serveur reçoit un message Renouvelle en envoi individuel d'un client auquel le serveur n'a pas envoyé l'option d'envoi individuel, le serveur élimine le message Renouvelle et répond par un message Répondre contenant une option Code d'état avec la valeur UseMulticast, une option Identifiant de serveur contenant le DUID du serveur, l'option Identifiant de client du message du client, et aucune autre option.

Lorsque le serveur reçoit un message Renouvelle qui contient une option IA d'un client, il localise le lien du client et vérifie que les informations dans l'IA venant du client correspondent aux informationx mémorisées pour ce client.

Si le serveur ne peut pas trouver une entrée de client pour la IA, le serveur retourne l'IA ne contenant pas d'adresse avec une option Code d'état réglée à NoBinding dans le message Répondre.

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

Si le serveur trouve dans l'IA les adresses pour le client, il renvoie l'IA au client avec de nouvelles durées de vie et les temps T1/T2. Le serveur peut choisir de changer la liste des adresses et les durées de vie des adresses dans les IA qui sont retournées au client.

Le serveur construit un message Répondre en réglant le champ "type-de-msg" à RÉPONDRE, et en copiant l'identifiant de transaction du message Renouvelle dans le champ ID-de-transaction.

Le serveur DOIT inclure une option Identifiant de serveur contenant le DUID du serveur et l'option Identifiant de client du message Renouvelle dans le message Répondre.

Le serveur inclut d'autres options contenant des informations de configuration à retourner au client comme décrit au paragraphe 18.2.

18.2.4 Réception des messages Relier

Lorsque le serveur reçoit d'un client un message Relier qui contient une option IA, il 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 ne peut pas trouver une entrée de client pour l'IA et si le serveur détermine que les adresses dans l'IA ne sont pas appropriées pour la liaison à laquelle est rattachée l'interface du client, conformément aux informations de configuration explicites du serveur, il PEUT envoyer un message Répondre au client contenant l'IA du client, avec les

durées de vie pour les adresses dans l'IA réglées à zéro. Ce Répondre constitue une notification explicite au client que les adresses dans l'IA ne sont plus valides. Dans cette situation, si le serveur n'envoie pas un message Répondre, il élimine en silence le message Relier.

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

Si le serveur trouve les adresses dans l'IA pour le client, il DEVRAIT alors renvoyer l'IA au client avec de nouvelles durées de vie et les temps T1/T2.

Le serveur construit un message Répondre en réglant le champ "type-de-msg" à RÉPONDRE, et en copiant l'identifiant de transaction du message Relier dans le champ ID-de-transaction.

Le serveur DOIT inclure une option Identifiant de serveur contenant le DUID du serveur et l'option Identifiant de client du message Relier dans le message Répondre.

Le serveur inclut les autres options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.2.

18.2.5 Réception des messages Demande-d'informations

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

Le serveur construit un message Répondre en réglant le champ "type-de-msg" à RÉPONDRE, et en copiant l'identifiant de transaction du message Demande-d'informations dans le champ ID-de-transaction.

Le serveur DOIT inclure une option Identifiant de serveur contenant le DUID du serveur dans le message Répondre. Si le client a inclus une option Identification de client dans le message Demande-d'informations, le serveur copie cette option dans le message Répondre.

Le serveur inclut des options contenant les informations de configuration à retourner au client comme décrit au paragraphe 18.2.

Si le message Demande-d'informations reçu du client ne comportait pas d'option Identifiant de client, le serveur DEVRAIT répondre par un message Répondre 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'informations.

18.2.6 Réception des messages Libérer

Lorsque un serveur reçoit un message Libérer en envoi individuel d'un client auquel le serveur n'a pas envoyé une option d'envoi individuel, le serveur élimine le message Libérer et répond par un message Répondre qui contient une option Code d'état avec la valeur UseMulticast, une option Identifiant de serveur contenant le DUID du serveur, l'option Identifiant de client provenant du message du client, et aucune autre option.

À réception d'un message Libérer valide, le serveur examine les IA et la validité des adresses dans les IA. Si les IA dans le message sont dans des liens pour le client, et si les adresses dans les IA ont été allouées par le serveur à ces IA, le serveur supprime les adresses des IA et rend les adresses disponibles pour être allouées à d'autres clients. Le serveur ignore les adresses non allouées à l'IA, bien qu'il puisse choisir d'enregistrer une erreur.

Lorsque toutes les adresses ont été traitées, le serveur génère un message Répondre et inclut une option Code d'état avec la valeur Succès, une option Identifiant de serveur avec le DUID du serveur, et une option Identifiant de client avec le DUID du client. Pour chaque IA dans le message Libérer pour lequel le serveur n'a pas d'informations de lien, le serveur ajoute une option IA en utilisant l'IAID provenant du message Libérer, et inclut une option Code d'état avec la valeur NoBinding dans l'option IA. Aucune autre option n'est incluse dans l'option IA.

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

18.2.7 Réception des messages Refuser

Lorsque le serveur reçoit un message Refuser en envoi individuel d'un client auquel il n'a pas envoyé une option d'envoi individuel, le serveur élimine le message Refuser et répond par un message Répondre qui contient une option Code d'état avec la valeur UseMulticast, une option Identifiant de serveur contenant le DUID du serveur, l'option Identifiant de client provenant du message du client, et aucune autre option.

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

Le client a trouvé que des adresses dans les messages Refuser sont déjà utilisées sur sa liaison. Donc, le serveur DEVRAIT marquer les adresses déclinées par le client afin que ces adresses ne soient pas allouées à d'autres clients, et PEUT choisir de faire une notification que des adresses ont été déclinées. La politique locale du serveur détermine quand les adresses identifiées dans un message Refuser peuvent être rendues disponibles pour allocation.

Après que toutes les adresses ont été traitées, le serveur génère un message Répondre et inclut une option Code d'état avec la valeur Succès, une option Identifiant de serveur avec le DUID du serveur, et une option Identifiant de client avec le DUID du client. Pour chaque IA dans le message Refuser pour laquelle le serveur n'a pas d'information de lien, le serveur ajoute une option IA en utilisant l'IAID provenant du message Libérer et inclut une option Code d'état avec la valeur NoBinding dans l'option IA. Aucune autre option n'est incluse dans l'option IA.

18.2.8 Transmission des messages Répondre

Si le message d'origine a été reçu directement par le serveur, celui-ci envoie en individuel le message Répondre directement au client en utilisant l'adresse qui est dans le champ d'adresse de source dans le datagramme IP dans lequel le message d'origine a été reçu. Le message Répondre DOIT être en envoi individuel à travers l'interface sur laquelle le message d'origine a été reçu.

Si le message d'origine a été reçu dans un message Relais-de-transmission, le serveur construit un message Réponse-de-relais avec le message Répondre dans la charge utile d'une option Message relais (voir au paragraphe 22.10). Si les messages Relais-de-transmission comportaient une option Interface-id, le serveur copie cette option dans le message Réponse-de-relais. Le serveur envoie en individuel le message Réponse-de-relais directement à l'agent de relais en utilisant l'adresse qui figure dans le champ adresse de source du datagramme IP dans lequel a été reçu le message Relais-de-transmission.

19. Échange DHCP de configuration à l'initiative du serveur

Un serveur initie un échange de configuration pour que les clients DHCP obtiennent de nouvelles adresses et autres informations de configuration. Par exemple, un administrateur peut utiliser un échange de configuration initié par le serveur lorsque les liaisons doivent être dénumérotées dans le domaine DHCP. Parmi d'autres, les exemples du changement de localisation des serveurs d'annuaire, de l'ajout de nouveaux services comme l'impression, et la disponibilité de nouveaux logiciels.

19.1 Comportement du serveur

Un serveur envoie un message Reconfigure pour amener un client à initier immédiatement un échange de messages Renouvelle/Répondre ou Demande-d'informations/Répondre avec le serveur.

19.1.1 Création et transmission des messages Reconfigure

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

Le serveur PEUT inclure une option Demande d'option pour informer le client des informations qui ont changé ou des nouvelles informations qui ont été ajoutées. En particulier, le serveur spécifie l'option IA dans l'option Demande d'option si le serveur veut que le client obtienne de nouvelles informations d'adresse. Si le serveur identifie l'option IA dans l'option Demande d'option, le serveur DOIT inclure une option IA qui ne contient aucune autre sous-option pour identifier chaque

IA qui est à reconfigurer chez le client.

À cause du risque d'attaque de déni de service contre les clients DHCP, l'utilisation d'un mécanisme de sécurité est rendue obligatoire dans les messages Reconfigure. Le serveur DOIT utiliser l'authentification DHCP dans le message Reconfigure.

Le serveur DOIT inclure une option Reconfigurer Message (définie au paragraphe 22.19) pour choisir si le client répond par un message Renouvelle ou par un message Demande d'informations.

Le serveur NE DOIT PAS inclure d'autre option dans Reconfigure sauf lorsque spécifiquement permis dans la définition de l'option en question.

Un serveur envoie chaque message Reconfigure à un seul client DHCP, en utilisant une adresse IPv6 d'envoi individuel de portée suffisante, qui appartient au client DHCP. Si le serveur n'a pas une adresse à laquelle il puisse envoyer le message Reconfigure directement au client, il utilise un message Réponse-de-relais (comme décrit au paragraphe 20.3) 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, ou par quelque 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 en même temps, par exemple, un serveur peut envoyer un message Reconfigure à d'autres clients alors que des échanges de messages de reconfiguration précédents sont encore en cours.

Le message Reconfigure fait que le client initie un échange de messages Renouvelle/Répondre ou Demande-d'informations/Répondre avec le serveur. Le serveur interprète la réception d'un message Renouvelle ou Demande-d'informations (quel que soit celui qui était spécifié dans le message Reconfigure original) provenant du client comme satisfaisant à la demande du message Reconfigure.

19.1.2 Fin de temporisation et retransmission des messages Reconfigure

Si le serveur ne reçoit pas de message Renouvelle ou Demande-d'informations de la part du client dans les REC_TIMEOUT millisecondes, le serveur retransmet le message Reconfigure, double la valeur de REC_TIMEOUT et attend à nouveau. Le serveur continue ce processus jusqu'à ce que REC_MAX_RC tentatives infructueuses aient été faites ; lorsque cela arrive, 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 données au paragraphe 5.5.

19.2 Réception des messages Renouvelle

Le serveur génère et envoie le message Répondre au client comme décrit aux paragraphes 18.2.3 et 18.2.8, y compris les options de paramètres de configuration.

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

19.3 Réception des messages Demande-d'informations

Le serveur génère et envoie un message Répondre au client comme décrit aux paragraphes 18.2.5 et 18.2.8, y compris les options de paramètres de configuration.

Le serveur PEUT inclure des options contenant les nouvelles valeurs pour les autres paramètres de configuration dans le message Répondre, même si ces paramètres n'étaient pas demandés dans le message Demande-d'informations du client.

19.4 Comportement du client

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

19.4.1 Réception des messages Reconfigure

À réception d'un message Reconfigure valide, le client répond par un message Renouvelle ou par un message Demande-d'informations comme indiqué par l'option Reconfigurer-message (définie au paragraphe 22.19). Le client ignore le champ id-de-transaction dans le message Reconfigure reçu. Lorsque la transaction est en cours, le client élimine en silence tout message Reconfigure qu'il reçoit.

Discussion :

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 un échange de messages (en retransmettant le message Renouvelle ou Demande-d'informations si nécessaire) ; le client ignore tout message Reconfigure supplémentaire jusqu'à ce que l'échange soit terminé. Les messages Reconfigure suivants font que le client prend l'initiative d'un nouvel échange.

Comment ce mécanisme fonctionne t-il en présence de messages Reconfigure dupliqués ou retransmis ? Les messages dupliqués seront ignorés parce que le client va commencer l'échange après la réception du premier Reconfigure. Les messages retransmis vont déclencher l'échange (si le premier Reconfigure n'a pas été reçu par le client) ou vont être ignorés. Le serveur peut interrompre la retransmission de messages Reconfigure au client une fois que le serveur reçoit du client le message Renouvelle ou Demande-d'informations.

Il serait possible qu'un Reconfigure dupliqué ou retransmis soit suffisamment en retard (et livré décalé) pour arriver chez le client après que l'échange (initié par le premier Reconfigure) s'est achevé. Dans ce cas, le client va initier un échange redondant. La probabilité de livraison retardée et décalée est assez faible pour être ignorée. La conséquence d'un échange redondant est l'inefficacité plutôt qu'un fonctionnement incorrect.

19.4.2 Création et transmission des messages Renouvelle

Lorsque il répond à un Reconfigure, le client crée et envoie le message Renouvelle exactement de la même manière que décrit au paragraphe 18.1.3, sauf que le client copie l'option Demande d'option et toutes les options IA du message Reconfigure dans le message Renouvelle.

19.4.3 Création et transmission des messages Demande-d'informations

Lorsque il répond à un Reconfigure, le client crée et envoie le message Demande-d'informations exactement de la même façon que décrit au paragraphe 18.1.5, sauf que le client inclut une option Identifiant de serveur avec l'identifiant provenant du message Reconfigure auquel répond le client.

19.4.4 Fin de temporisation et retransmission des messages Renouvelle ou Demande-d'informations

Le client utilise les mêmes variables et algorithme de retransmission qu'avec les messages Renouvelle ou Demande-d'informations générés au titre d'un échange de configuration à l'initiative du client. Voir les détails aux paragraphes 18.1.3 et 18.1.5. Si le client ne reçoit pas de réponse du serveur avant la fin du processus de retransmission, le client ignore et élimine le message Reconfigure.

19.4.5 Réception des messages Répondre

À réception d'un message Répondre valide, le client traite les options et règle (ou rétablit) les paramètres de configuration de façon appropriée. Le client enregistre et met à jour les durées de vie de toute adresse spécifiée dans les IA du message Répondre.

20. Comportement de l'agent de relais

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

Si l'agent de relais relaye les messages à l'adresse de diffusion groupée Tous_Serveurs_DHCP ou à d'autres adresses de diffusion groupée, il établit le champ Limite de bonds à 32.

20.1 Relais d'un message de client ou d'un message Relais-de-transmission

Un agent de relais relaye les messages des clients et les messages Relais-de-transmission provenant des autres agents de relais. Lorsque un agent de relais reçoit un message valide à relayer, il construit un nouveau message Relais-de-transmission. 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 d'homologue du message Relais-de-transmission. L'agent de relais copie le message DHCP reçu (à l'exclusion de tout en-tête IP ou UDP) dans une option Relais de message dans le nouveau message. L'agent de relais ajoute le message Relais-de-transmission dans toute option qu'il est configuré à inclure.

20.1.1 Relais d'un message provenant d'un client

Si l'agent de relais a reçu le message à relayer d'un client, l'agent de relais place une adresse de portée mondiale ou limitée au site avec un préfixe alloué à la liaison sur laquelle le client devrait avoir une adresse allouée dans le champ Adresse-de-liaison. Cette adresse sera utilisée par le serveur pour déterminer la liaison à partir de laquelle le client devrait avoir allouées une adresse et d'autres informations de configuration. Le compte de bonds dans le message Relais-de-transmission est réglé à 0.

Si l'agent de relais ne peut pas utiliser l'adresse qui est dans le champ Adresse de liaison pour identifier l'interface par laquelle sera relayée la réponse au client, l'agent de relais DOIT inclure une option Identifiant d'interface (voir au paragraphe 22.18) dans le message Relais-de-transmission. Le serveur va inclure l'option Identifiant d'interface dans son message Réponse-de-relais. L'agent de relais remplit le champ Adresse de liaison comme décrit au paragraphe précédent sans considération de savoir si l'agent de relais a inclus une option Identifiant d'interface dans le message Relais-de-transmission.

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

Si le message reçu par l'agent de relais est un message Relais-de-transmission et si le compte de bonds dans le message est supérieur ou égal à HOP_COUNT_LIMIT, l'agent de relais élimine le message reçu.

L'agent de relais copie l'adresse de source du datagramme IP dans lequel a été reçu le message du client dans le champ Adresse d'homologue dans le message Relais-de-transmission et règle le champ Compte de bonds à la valeur du champ Compte de bonds du message reçu augmenté de 1.

Si l'adresse de source provenant de l'en-tête du datagramme IP du message reçu est une adresse mondiale ou de site local (et si l'appareil sur lequel fonctionne l'agent de relais n'appartient qu'à un seul site) 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 mondiale ou de site local allouée à l'interface sur laquelle le message a été reçu, ou inclut une option Identifiant d'interface pour identifier l'interface sur laquelle le message a été reçu.

20.2 Relais d'un message Réponse-de-relais

L'agent de relais traite toutes les options incluses dans le message Réponse-de-relais en plus de l'option Relais de message, et élimine ensuite ces options.

L'agent de relais extrait le message de l'option Relais de message et la relaye à l'adresse contenue dans le champ Adresse d'homologue du message Réponse-de-relais.

Si le message Réponse-de-relais comporte une option Identifiant d'interface, l'agent de relais relaye le message du serveur au client sur la liaison identifiée par l'option Id-d'interface. Autrement, si le champ Adresse de liaison n'est pas réglé à zéro, l'agent de relais relaye le message sur la liaison identifiée par le champ Adresse de liaison.

20.3 Construction des messages Réponse-de-relais

Un serveur utilise un message Réponse-de-relais pour retourner une réponse à un client si le message d'origine du client a été relayé au serveur dans un message Relais-de-transmission ou pour 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 client original. Le serveur fait arriver cela en créant un message Réponse-de-relais qui inclut une option Relais de ùessage contenant le message pour le prochain agent de relais sur le chemin de retour vers le client. Le message Réponse-de-relais inclus contient une autre

option Relais de message à envoyer au prochain agent de relais, et ainsi de suite. Le serveur doit enregistrer le contenu des champs Adresse d'homologue du message reçu afin de pouvoir construire le message Réponse-de-relais approprié pour porter la réponse du serveur.

Par exemple, si le client C envoie 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 Réponse-de-relais suivant à l'agent de relais B :

type-de-msg : RÉPONSE-DE-RELAIS
compte-de-bonds : 1
adresse-de-liaison : 0
adresse-de-l'homologue : A
option Relais de message, contenant :
type-de-msg : RÉPONSE-DE-RELAIS
compte-de-bonds : 0
adresse-de-liaison : adresse de la liaison à laquelle C est rattaché
adresse-de-l'homologue : C
option Relay Message : <réponse du serveur>

Lors de l'envoi d'un message Reconfigure à un client par un agent de relais, le serveur crée un message Réponse-de-relais qui comporte une option Relais de message contenant le message Reconfigure pour le prochain agent de relais sur le chemin de retour vers le client. Le serveur règle le champ Adresse-de-l'homologue dans l'en-tête de message Réponse-de-relais 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 au moyen d'une interaction antérieure avec le client ou par quelque mécanisme externe.

21. Authentification des messages DHCP

Certains administrateurs de réseau peuvent souhaiter fournir l'authentication de la source et du contenu des messages DHCP. Par exemple, les clients peuvent être soumis à des attaques de déni de service au moyen de serveurs DHCP falsifiés, ou peuvent être simplement mal configurés par suite d'une mauvaise mise en œuvre accidentelle des serveurs DHCP. Les administrateurs de réseau peuvent souhaiter restreindre l'allocation des adresses aux hôtes autorisés pour éviter les attaques de déni de service dans des environnements "hostiles" où le support réseau n'est pas sécurisé physiquement, tels que les réseaux sans fils ou les halls de résidence universitaires.

Le mécanisme de l'authentification DHCP se fonde sur le concept de l'authentication pour DHCPv4 [4].

21.1 Sécurité des messages envoyés entre serveurs et agents de relais

Les agents de relais et serveurs qui échangent des messages en toute sécurité utilisent le mécanisme IPsec pour IPv6 [7]. Si un message de client est relayé par plusieurs agents de relais, chacun des agents de relais doit avoir établi des relations de confiance indépendantes, deux à deux. C'est-à-dire que si les messages provenant du client C sont relayés par l'agent de relais A à l'agent de relais B et ensuite au serveur, les agents de relais A et B doivent être configurés pour utiliser IPSec pour les messages qu'ils échangent, et que l'agent de relais B et le serveur doivent être configurés pour utiliser IPSec pour les messages qu'ils échangent.

Les agents de relais et serveurs qui prennent en charge la communication sécurisée d'agent de relais à serveur ou d'agent de relais à agent de relais utilisent IPsec dans les conditions suivantes :

Selecteurs : Les agents de relais sont configurés manuellement avec les adresses de l'agent de relais ou du serveur auquel les messages DHCP sont à transmettre. Chaque agent de relais et serveur qui va utiliser IPsec pour sécuriser les messages DHCP doit aussi être configuré avec une liste des agents de relais auxquels les messages seront retournés. Les sélecteurs pour les agents de relais et serveurs seront les paires d'adresses qui définissent les agents de relais et serveurs qui échangent les messages DHCP sur les accès UDP DHCPv6 546 et 547.

Mode : Les agents de relais et serveurs utilisent le mode transport et ESP. Les informations dans les messages DHCP ne sont généralement pas considérées comme confidentielles, de sorte que le chiffrement n'a pas besoin d'être utilisé (c'est-à-dire, le chiffrement NULL peut être utilisé).

Gestion de clé : Comme les agents de relais et serveurs sont utilisés au sein d'une organisation, les schémas de clé publique ne sont pas nécessaires. Comme les agents de relais et serveurs doivent être configurés à la

main, une configuration de gestion de clé manuelle peut suffire, mais ne fournit pas de défense contre la répétition de messages. En conséquence, IKE avec des secrets prépartagés DEVRAIT être pris en charge. IKE avec clés publiques PEUT être pris en charge.

Politique de sécurité : Les messages DHCP entre agents de relais et serveurs ne devraient être acceptés des homologues DHCP que lorsque ils sont identifiés dans la configuration locale.

Authentification : Les clés partagées, indexées sur l'adresse IP de source du message DHCP reçu, sont adéquates dans cette application.

Disponibilité : Des mises en œuvre IPsec appropriéss seront vraisemblablement disponibles pour les serveurs et les agents de relais dans les appareils plus élaborés qui sont utilisés dans les entreprises et les réseaux des FAI. IPsec sera probablement moins disponible pour les agents de relais dans les appareils d'extrémité utilisés sur le marché des particuliers et des entreprises individuelles.

21.2 Résumé de l'authentification DHCP

L'authentification des messages DHCP est réalisée par l'utilisation de l'option Authentification (voir au paragraphe 22.11). 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 fournit un cadre pour plusieurs protocoles d'authentification. Deux de ces protocoles sont définis ici. 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) dans l'option Authentification. Le champ Méthode de détection de répétition (RDM, *replay detection method*) spécifie le type de détection de répétition utilisée dans le champ Détection de répétition.

21.3 Détection des répétitions

Le champ RDM 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 compteur à accroissement monotone. Utiliser la valeur d'un compteur, comme l'heure en cours (par exemple, un horodatage au format NTP [9]) peut réduire le danger des attaques en répétition. Cette méthode DOIT être prise en charge par tous les protocoles.

21.4 Protocole d'authentification retardée

Si le champ Protocole est à 2, le message utilise le mécanisme "authentification retardée". Dans l'authentification retardée, le client demande l'authentification dans son messags Sollicite, et le serveur répond par un message Annoncer qui comporte des informations d'authentification. Ces informations d'authentification contiennent une valeur de nom occasionnel générée par la source comme code d'authentification de message (MAC) pour assurer l'authentification du message et l'authentification de l'entité.

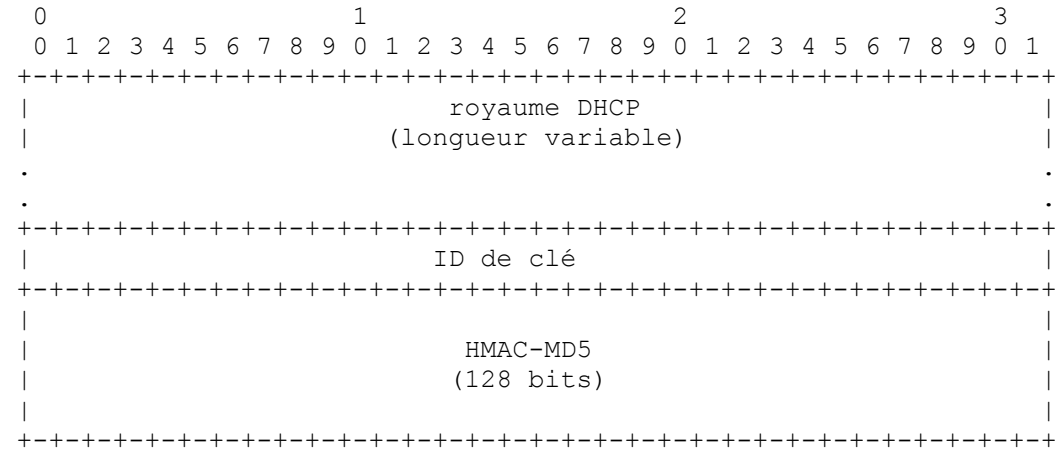
L'utilisation d'une technique particulière fondée sur le protocole HMAC [8] en utilisant le hachage MD5 [16] est définie ici.

21.4.1 Utilisation de l'option Authentification dans le protocole d'authentification retardée

Dans un message Sollicite, le client remplit les champs Protocole, Algorithme et RDM dans l'option Authentification avec les préférences du client. Le client règle le champ Détection de répétition à zéro et omet le champ Informations d'authentification. Le client règle le champ Longueur d'option à 11.

Dans tous les autres messages, les champs Protocole et Algorithme identifient la méthode utilisée pour construire le contenu du champ Informations d'authentification. Le champ RDM identifie la méthode utilisée pour construire le contenu du champ Détection de répétition.

Le format des informations d'authentification est :



royaume DHCP : C'est le royaume DHCP qui identifie la clé utilisée pour générer la valeur HMAC-MD5.

ID de clé : C'est l'identifiant de clé qui identifie la clé utilisée pour générer la valeur HMAC-MD5.

HMAC-MD5 : Code d'authentification de message généré en appliquant MD5 au message DHCP en utilisant la clé identifiée par le royaume DHCP, le DUID du client, et l'identitifant de clé.

L'envoyeur calcule le MAC en utilisant l'algorithme de génération HMAC [8] et la fonction de hachage MD5 [16]. Le message DHCP entier (réglage du champ MAC de l'option Authentification à zéro) y compris l'en-tête de message DHCP et le champ Options, est utilisé comme entrée pour la fonction de calcul HMAC-MD5.

Discussion :

L'algorithme 1 spécifie l'utilisation de HMAC-MD5. L'utilisation d'une technique différente, telle que HMAC-SHA, sera spécifiée dans un autre protocole.

Le royaume DHCP utilisé pour identifier les clés d'authentification est choisi comme étant unique parmi les domaines administratifs. L'utilisation du royaume DHCP permet aux administrateurs DHCP d'éviter d'entrer en conflit lors de l'utilisation des identifiants de clés, et permet à un hôte qui utilise DHCP d'avoir du DHCP authentifié lors d'une itinérance parmi des domaines administratifs DHCP.

21.4.2 Validation du message

Tout message DHCP qui inclut plus d'une option d'authentification DOIT être éliminé.

Pour valider un message entrant, le receveur vérifie d'abord que la valeur dans le champ Détection de répétition est acceptable conformément à la méthode de détection de répétition spécifiée par le champ RDM. Ensuite, le receveur calcule le MAC comme décrit dans [8]. Le message DHCP entier (en réglant le champ MAC de l'option d'authentification à 0) est utilisé comme entrée à la fonction de calcul de HMAC-MD5. Si le MAC calculé par le receveur ne correspond pas au MAC contenu dans l'option d'authentification, le receveur DOIT éliminer le message DHCP.

21.4.3 Utilisation des clés

Chaque client DHCP a un ensemble de clés. Chaque clé est identifiée par <royaume DHCP, DUID de client, identifiant de clé>. Chaque clé a aussi une durée de vie. La clé ne peut plus être utilisée après la fin de sa durée de vie. Les clés du client sont initialement distribuées au client par un mécanisme hors bande. La durée de vie pour chaque clé est distribuée avec la clé. La spécification des mécanismes de distribution des clés et des durées de vie sortent du domaine d'application du présent document.

Le client et le serveur utilisent une des clés du client pour authentifier les messages DHCP durant une session (jusqu'au prochain message Sollicite envoyé par le client).

21.4.4 Questions de client dans le protocole d'authentification retardée

Le client annonce son intention d'utiliser l'authentification DHCP en incluant une option Authentification dans son message Sollicite Le serveur choisit une clé pour le client sur la base du DUID du client. Le client et le serveur utilisent cette clé pour authentifier tous les messages DHCP échangés durant la session.

21.4.4.1 Envoi des messages Sollicite

Lorsque le client envoie un messags Sollicite et souhaite utiliser l'authentification, il inclut une option Authentification avec le protocole, l'algorithme et la RDM désirés comme décrit au paragraphe 21.4. Le client n'inclut aucune détection de répétition ou information d'authentification dans l'option Authentification.

21.4.4.2 Réception des messages Annoncer

Le client valide tout message Annoncer contenant une option Authentification qui spécifie le protocole d'authentification retardée en utilisant l'essai de validation décrit au paragraphe 21.4.2.

Le comportement du client, si aucun message Annoncer ne comporte d'information d'authentification ou ne réussit l'essai de validation, est contrôlé par la politique locale chez le client. Conformément à la politique du client, celui-ci PEUT choisir de répondre à un message Annoncer qui n'a pas été authentifié.

La décision de régler la politique locale à accepter les messages non authentifiés devrait être prise avec précaution. Accepter un message Annoncer non authentifié peut rendre le client vulnérable à des attaques par usurpation ou autres. Si les utilisateurs locaux ne sont pas explicitement informés que le client a accepté un message Annoncer non authentifié, les utilisateurs peuvent supposer à tort que le client a reçu une adresse authentifiée et est à l'abri des attaques de DHCP par des messages non authentifiés.

Un client DOIT être configurable à éliminer les messages non authentifiés, et DEVRAIT être configuré par défaut à éliminer les messages non authentifiés si le client a été configuré avec une clé d'authentification ou d'autres informations d'authentification. Un client PEUT choisir de faire la différence entre les messages Annoncer sans informations d'authentification et les messages Annoncer qui ne réussissent pas l'essai de validation ; par exemple, un client pourrait accepter le premier et éliminer le dernier. Si un client accepte un message non authentifié, il DEVRAIT informer tous les utilisateurs locaux et DEVRAIT enregistrer l'événement.

21.4.4.3 Envoi des messages Demande, Confirme, Renouvelle, Relier, Refuser ou Libérer

Si le client a authentifié le message Annoncer par lequel le client a choisi le serveur, le client DOIT générer les informations d'authentification pour les messages Demande, Confirme, Renouvelle, Relier ou Libérer suivants envoyés au serveur, comme décrit au paragraphe 21.4. Lorsque le client envoie ensuite un message, il DOIT utiliser la même clé qu'utilisée par le serveur pour générer les informations d'authentification.

21.4.4.4 Envoi des messages Demande-d'informations

Si le serveur a choisi une clé pour le client dans un échange de messages précédent (voir au paragraphe 21.4.5.1) le client DOIT utiliser la même clé pour générer les informations d'authentification tout au long de la session.

21.4.4.5 Réception des messages Répondre

Si le client a authentifié le Annoncer qu'il a accepté, il DOIT valider le message Répondre associé provenant du serveur. Le client DOIT éliminer le message Répondre si il échoue à l'essai de validation et PEUT enregistrer l'échec de validation dans le journal. Si le Répondre échoue à l'essai de validation, le client DOIT redémarrer le processus de configuration DHCP en envoyant un message Sollicite

Si le client a accepté un message Annoncer qui ne comportait pas d'informations d'authentification ou qui a échoué à l'essai de validation, le client PEUT accepter un message Répondre non authantifié de la part du serveur.

21.4.4.6 Réception des messages Reconfigure

Le client DOIT éliminer le message Reconfigure si il échoue à l'essai de validation test et PEUT enregistrer l'échec de validation dans son journal.

21.4.5 Questions de serveur concernant le protocole d'authentification retardée

Après avoir reçu un messags Sollicite qui contient une option Authentification, le serveur choisit une clé pour le client, sur la base du DUID du client et des politiques de sélection de clé avec lesquelles le serveur a été configuré. Le serveur identifie la clé choisie dans le message Annoncer et utilise la clé pour valider les messages suivants entre le client et le serveur.

21.4.5.1 Réception des messages Sollicite et envoi des messages Annoncer

Le serveur choisit une clé pour le client et inclut les informations d'authentification dans le message Annoncer retourné au client comme spécifié au paragraphe 21.4. Le serveur DOIT enregistrer l'identifiant de la clé choisie pour le client et utiliser cette même clé pour valider les messages ultérieurs avec le client.

21.4.5.2 Réception des messages Demande, Confirme, Renouvelle, Relier ou Libérer et envoi des messages Répondre

Le serveur utilise la clé identifiée dans le message et valide le message comme spécifié au paragraphe 21.4.2. Si le message échoue à l'essai de validation ou si le serveur ne connaît pas la clé identifiée par le champ "ID-de-clé", le serveur DOIT éliminer le message et PEUT choisir d'enregistrer l'échec de validation dans son journal.

Si le message réussit l'essai de validation, le serveur répond au message spécifique comme décrit au paragraphe 18.2. Le serveur DOIT inclure les informations d'authentification générées en utilisant la clé identifiée dans le message reçu, comme spécifié au paragraphe 21.4.

21.5 Protocole d'authentification de reconfiguration de clés

Le protocole d'authentification de reconfiguration de clé apporte 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 un Reconfigurer la clé au client dans l'échange initial des messages DHCP. Le client enregistrr le Reconfigurer la clé pour l'utiliser à authentifier les messages Reconfigure suivants en provenance de ce serveur. Le serveur les inclut dans un HMAC calculé à partir du Reconfigurer la clé dans les messages Reconfigure suivants.

Le Reconfigurer la clé envoyé du serveur au client et le HMAC dans les messages Reconfigure suivants sont tous deux portés comme informations d'authentification dans une option Authentification. Le format des informations d'authentification est défini dans les paragraphes qui suivent.

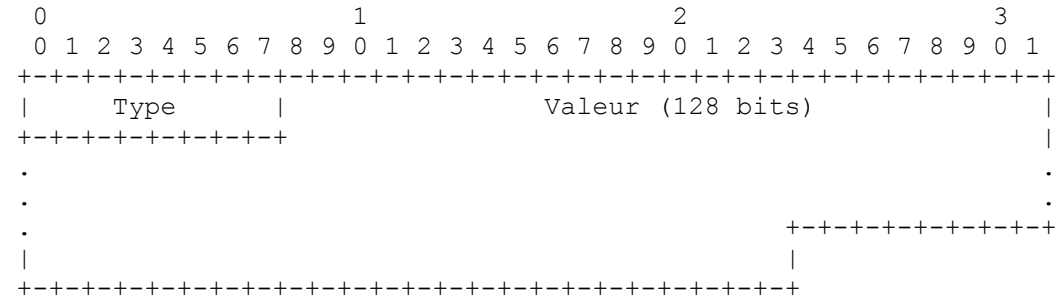
Le protocole de reconfiguration de clé n'est utilisé (initié par le serveur) que si le client et le serveur n'utilisent aucun autre protocole d'authentification et si le client et le serveur ont négocié l'utilisation des messages Reconfigure.

21.5.1 Utilisation de l'option Authentification dans le protocole d'authentification de reconfiguration de clés

Les champs suivants sont établis dans une option Authentification pour le protocole d'authentification de reconfiguration de clé :

protocole	3
algorithme	1
RDM	0

Le format des informations d'authentification pour le protocole d'authentification de reconfiguration de clé est :



Type C'est le type de données dans le champ Valeur porté dans cette option :

1 Valeur de Reconfigurer la clé (utilisé dans le message Répondre).

2 Résumé HMAC-MD5 du message (utilisé dans le message Reconfigure).

Valeur Données telles que définies par le champ.

21.5.2 Questions de serveur dans le protocole de reconfiguration de clés

Le serveur choisit une reconfiguration de clé pour un client durant l'échange de messages Demande/Répondre, Sollicite/Répondre ou Demande-d'informations/Répondre. Le serveur enregistre le Reconfigurer la clé et transmet cette clé au client dans une option Authentification dans le message Répondre.

Le Reconfigurer la clé est long de 128 bits, et DOIT être un nombre aléatoire ou pseudo aléatoire cryptographiquement fort qu'on ne peut pas prévoir facilement.

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 le Reconfigurer la clé pour le client. Le serveur calcule le HMAC-MD5 sur le message DHCP Reconfigure entier, y compris l'option Authentification ; le champ HMAC-MD5 dans l'option Authentification est réglé à zéro 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.

21.5.3 Questions de client dans le protocole de reconfiguration de clés

Le client va recevoir un Reconfigurer la clé du serveur dans le message Répondre initial du serveur. Le client enregistre le Reconfigurer la clé pour l'utiliser à authentifier les messages Reconfigure ultérieurs.

Pour authentifier un message Reconfigure, le client calcule un HMAC-MD5 sur le message DHCP , en utilisant le Reconfigurer la clé reçu du serveur. Si ce HMAC-MD5 calculé correspond à la valeur dans l'option Authentification, le client accepte le message Reconfigure.

22 Options DHCP

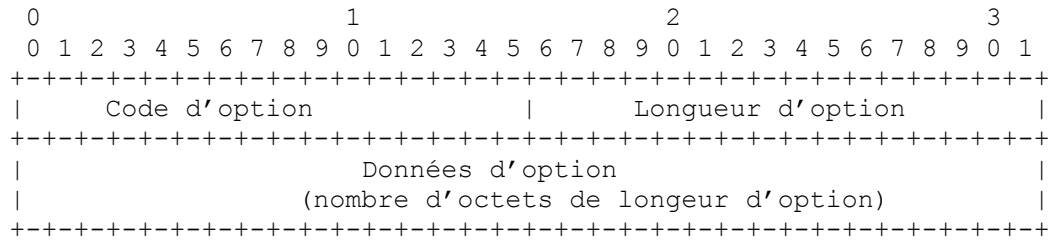
Les options sont utilisées pour porter des informations et paramètres supplémentaires dans les messages DHCP. Chaque option partage un format de base commun, comme décrit au paragraphe 22.1. Toutes les valeurs dans les options sont représentées dans l'ordre des octets du réseau.

Le présent document décrit les options DHCP définies au titre de la spécification DHCP de base. D'autres options peuvent être définies à l'avenir dans d'autres documents.

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

22.1 Format des options DHCP

Le format des options DHCP est :

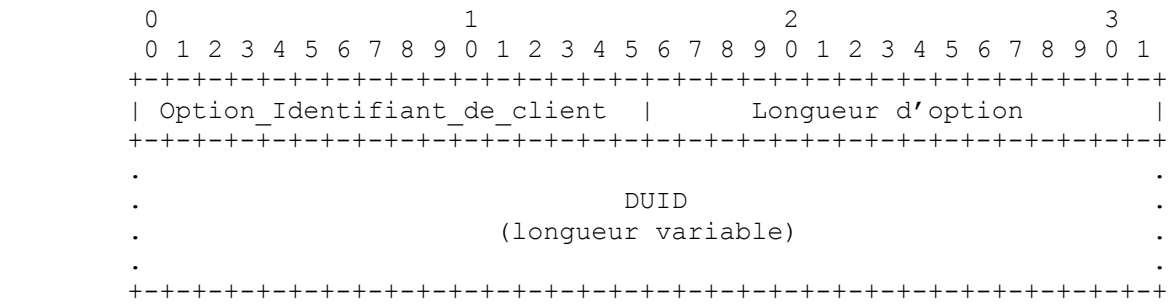


Code d'option C'est un entier non signé qui identifie le type d'option spécifique porté dans cette option.
Longueur d'option Un entier non signé qui donne la longueur du champ Données d'option de cette option en octets.
Données d'option Les données pour l'option ; le format de ces données dépend de la définition de l'option.

Les options DHCPv6 sont étendues en utilisant l'encapsulation. Certaines options s'appliquent de façon générale au client, certaines sont spécifiques d'une IA, et certaines sont spécifiques des adresses au sein d'une IA. Ces deux derniers cas sont exposés aux paragraphes 22.4 et 22.6.

22.2 Option d'identifiant de client

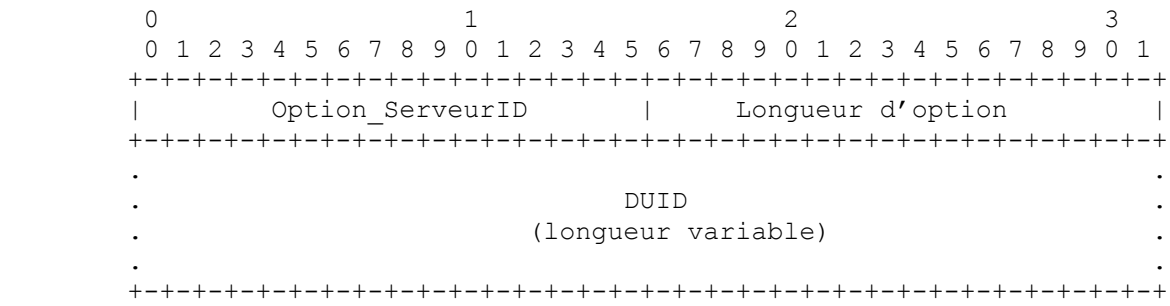
L'option Identifiant de client est utilisée pour porter un DUID (voir la section 9) qui identifie un client entre un client et un serveur. Le format de l'option Identifiant de client est :



Code d'option Option_Identifiant_de_client (1).
Longueur d'option Longueur du DUID en octets.
DUID Le DUID pour le client.

22.3 Option d'identifiant de serveur

L'option Identifiant de serveur est utilisée pour porter un DUID (voir la section 9) qui identifie un serveur entre un client et un serveur. Le format de l'option Identifiant de serveur est :



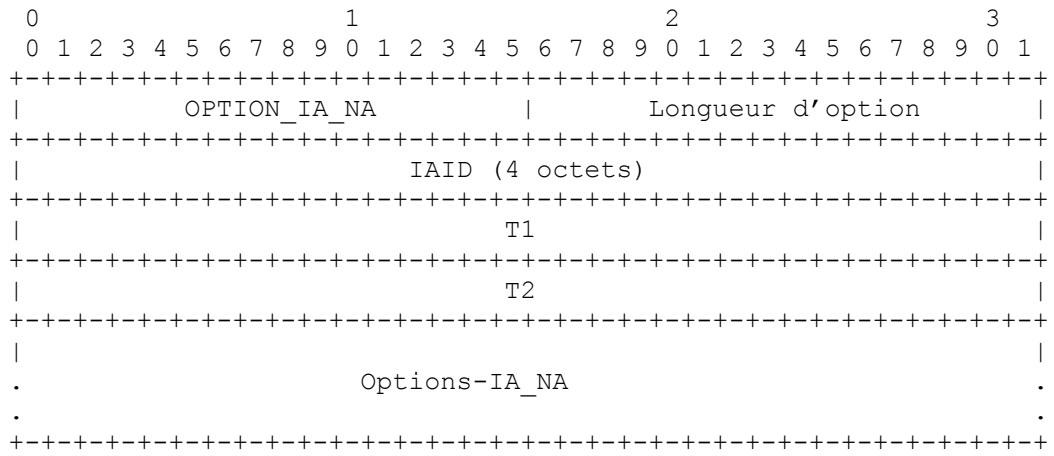
Code d'option Option_ServeurID (2).
Longueur d'option Longueur du DUID en octets.
DUID Le DUID pour le serveur.

22.4 Option Association d'identité pour adresses non temporaires

L'option Association d'identité pour adresses non temporaires (option IA_NA) est utilisée pour porter une IA_NA, les paramètres associés à l'IA_NA, et les adresses non temporaires associées à l'IA_NA.

Les adresses qui apparaissent dans une option IA_NA ne sont pas des adresses temporaires (voir au paragraphe 22.5).

Le format de l'option IA_NA est :



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 toutes les IA_NA de ce client. L'espace de nombres pour les IAID d'IA_NA est distinct de celui des IAID pour les IA_TA.

T1 : Heure à laquelle le client contacte le serveur d'où ont été obtenues les adresses dans l'IA_NA pour étendre la durée de vie des adresses allouées à l'IA_NA ; T1 est une durée par rapport à l'heure actuelle exprimée en unités de secondes.

T2 : Heure à laquelle le client contacte tout serveur disponible pour étendre la durée de vie des adresses allouées à l'IA_NA ; T2 est une durée par rapport à l'heure actuelle exprimée en secondes.

Options-IA_NA : Options associées à cette IA_NA. Le champ Options IA_NA encapsule les options qui sont spécifiques de cette IA_NA. Par exemple, toutes les options d'adresse d'IA qui portent les adresses associées à cette IA_NA sont dans le champ Options-IA_NA.

Une option IA_NA ne peut apparaître que dans la zone options d'un message DHCP. Un message DHCP peut contenir plusieurs options IA_NA.

L'état de toutes les opérations qui impliquent cette IA_NA est indiqué dans une option Code d'état dans le champ Options-IA_NA.

Noter qu'une IA_NA n'a pas de "durée de vie" explicite ou de "longueur d'application" propre. Lorsque les durées de vies valides de toutes les adresses dans une IA_NA sont arrivées à expiration, l'IA_NA peut être considérée comme étant arrivée à expiration. T1 et T2 sont inclus pour donner aux serveurs un contrôle explicite sur le moment où un client recontacte le serveur au sujet d'une IA_NA spécifique.

Dans un message envoyé par un client à un serveur, les valeurs dans les champs T1 et T2 indiquent la préférence du client pour ces paramètres. Le client règle T1 et T2 à 0 si il n'a pas de préférence pour ces valeurs.

Dans un message envoyé par un serveur à un client, le client DOIT utiliser les valeurs des champs T1 et T2 pour les paramètres T1 et T2, sauf si ces valeurs dans 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 les temps T1 et T2 de façon à permettre au client d'étendre la durée de vie de toute adresse du IA_NA avant que cette durée de vie arrive à expiration, même si le serveur est indisponible pour ine brève période. 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 ("l'infini") les valeurs recommandées de T1 et T2 sont aussi 0xffffffff. Si l'heure à laquelle les adresses dans une IA_NA sont à renouveler doit être laissée à la discrétion du client, le serveur règle T1 et T2 à 0.

Si un serveur reçoit une IA_NA avec T1 supérieur à T2, et si T1 et T2 sont tous deux supérieurs à 0, le serveur ignore les valeurs invalides de T1 et T2 et traite l'IA_NA bien que le client ait réglé T1 et T2 à 0.

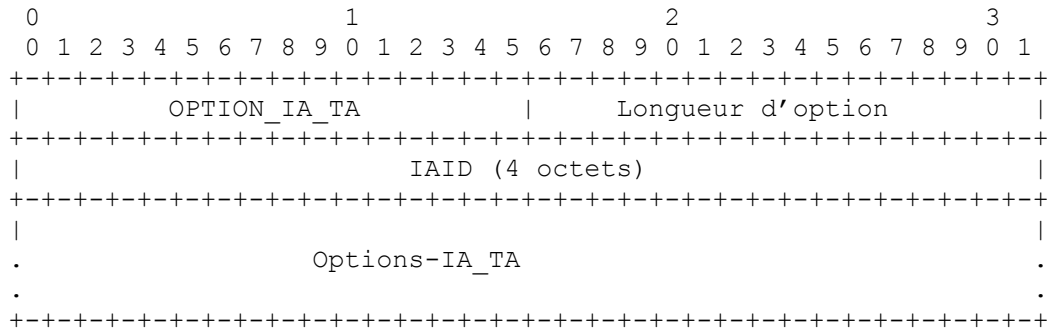
Si un client reçoit une IA_NA avec T1 supérieur à T2, et si T1 et T2 sont tous deux supérieurs à 0, le client élimine l'option IA_NA et traite le reste du message bien que le serveur n'ait pas inclus l'option IA_NA invalide.

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

localiser un serveur différent pour étendre la durée de vie d'aucune adresse dans une IA avec T2 réglé à 0xffffffff.

22.5 Option Association d'identité pour adresses temporaires

L'option Association d'identité pour adresses temporaires (IA_TA) est utilisée pour porter une IA_TA, les paramètres associés à l'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 RFC3041 [12].
Le format de l'option IA_TA est :



Code d'option OPTION_IA_TA (4).
Longueur d'option 4 + longueur du champ Option-IA_TA.
IAID : Identifiant univoque pour cette IA_TA ; le IAID doit être unique parmi les identifiants pour toutes les IA_TA de ce client. L'espace de nombres pour les IAID d'IA_TA est distinct de celui des IAID pour les IA_NA.
Options-IA_TA Options associées à cette IA_TA.

Le champ Options-IA_TA encapsule les options qui sont spécifiques de cette IA_TA. Par exemple, toutes les options Adresse d'IA qui portent les adresses associées à cette IA_TA sont dans le champ Options-IA_TA.

Chaque IA_TA porte un "ensemble" d'adresses temporaires ; c'est-à-dire, au plus une adresse provenant de chaque préfixe alloué à la liaison à laquelle le client est rattaché.

Une option IA_TA ne peut apparaître que dans la zone d'options d'un message DHCP. Un message DHCP peut contenir plusieurs options IA_TA.

L'état de toute opération qui implique cette IA_TA est indiqué dans une option Code d'état dans le champ Options-IA_TA.

Noter qu'une IA n'a pas de "durée de vie" explicite ou "de longueur d'application" propre. Lorsque la durée de validité de toutes les adresses dans une IA_TA est arrivée à expiration, la IA peut être considérée comme étant arrivée à expiration.

Une option IA_TA ne comporte pas de valeurs pour T1 et T2. Un client PEUT demander que les durées de vie des adresses temporaires soient étendues en incluant les adresses dans une option IA_TA envoyée dans un message Renouvelle ou Relier à un serveur. Par exemple, un client demanderait une extension de la durée de vie d'une adresse temporaire pour permettre à une application de continuer d'utiliser une connexion TCP établie.

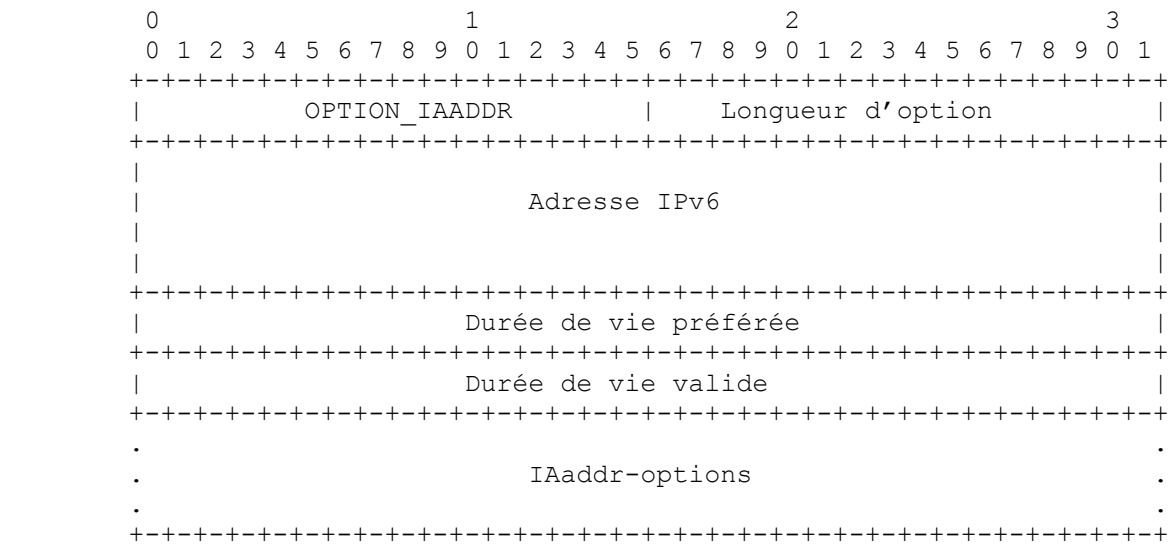
Le client obtient de nouvelles adresses temporaires en envoyant une option IA_TA avec un nouvel IAID à un serveur. Demander de nouvelles adresses temporaires au serveur est équivalent à générer de nouvelles adresses temporaires comme décrit dans la RFC3041. Le serveur va générer de nouvelles adresses temporaires et les retourner au client. Le client devrait demander de nouvelles adresses temporaires avant l'arrivée à expiration de la durée de vie des adresses précédemment allouées.

Un serveur DOIT retourner le même ensemble d'adresses temporaires pour la même IA_TA (telle qu'identifiée par le IAID) aussi longtemps que ces adresses sont valides. Après l'arrivée à expiration de la durée de vie des adresses dans une IA_TA, le IAID peut être réutilisé pour identifier une nouvelle IA_TA avec de nouvelles adresses temporaires.

Cette option PEUT apparaître dans un message Confirme si la durée de vie des adresses temporaires dans l'IA associée n'est pas arrivée à expiration.

22.6 Option Adresse d'IA

L'option Adresse d'IA est utilisée pour spécifier des adresses IPv6 associées à une IA_NA ou une IA_TA. L'option Adresse d'IA doit être encapsulée dans le champ Options d'une option IA_NA ou IA_TA. Le champ Options encapsule les options qui sont spécifiques de cette adresse.
Le format de l'option Adresse d'IA est :



Code d'option : OPTION_IAADDR (5).
Longueur d'option : 24 + la longueur du champ IAaddr-options.
Adresse IPv6 : une adresse IPv6.
Durée de vie préférée : la durée de vie préférée pour l'adresse IPv6 dans l'option, exprimée en unités de secondes.
Durée de vie valide : la durée de vie valide pour l'adresse IPv6 dans l'option, exprimée en unités de secondes.
IAaddr-options : les options associées à cette adresse.

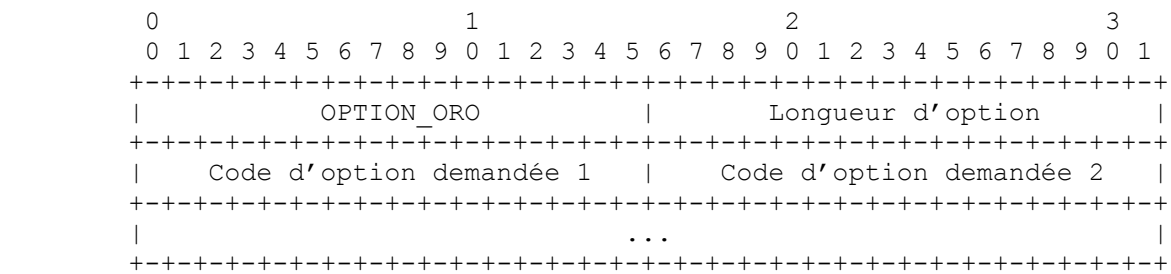
Dans un message envoyé par un client à un serveur, les valeurs dans les champs Durée de vie préferée et valide indiquent la préférence du client pour ces paramètres. Le client peut envoyer 0 si il n'a pas de préference pour les durées de vie préférée et valide. Dans un message envoyé d'un serveur à un client, le client DOIT utiliser les valeurs dans les champs Durée de vie préférée et valide pour les durées de vie préférée et valide. Les valeurs dans les durées de vie préférée et valide sont le nombre de secondes restant dans chaque durée de vie.

Un client élimine toute addresse pour laquelle la durée de vie préférée est supérieure à la durée de vie valide. Un serveur ignore la durée de vie réglée par le client si la durée de vie préférée est supérieure à la durée de vie valide et ignore les valeurs pour T1 et T2 réglées par le client si ces valeurs sont supérieures à la durée de vie préférée.
Il faut y réflechir à deux fois avant de régler la durée de vie valide d'une adresse à 0xffffffff ("infini") ce qui revient à une affectation permanente d'une adresse à un client. Une option d'adresse IA ne peut apparaître que dans une option IA_NA ou une option IA_TA. Plus d'une option d'adresse IA peut apparaître dans une option IA_NA ou une option IA_TA.

L'état de toute opération impliquant cette adresse IA est indiqué dans une option Code d'état dans le champ IAaddr-options.

22.7 Option Demande d'option

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



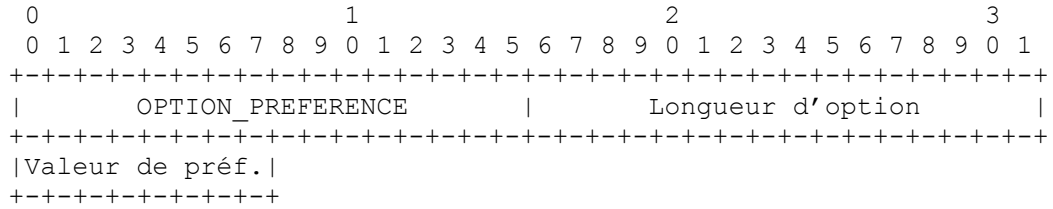
Code d'option ;: OPTION_ORO (6).
Longueur d'option : 2 * nombre d'options demandées.
Code d'option demandée n : code d'option pour une option demandée par le client.

Un client PEUT inclure une option Demande d'option dans un message Sollicite, Demande, Renouvelle, Relier, Confirme ou Demande-d'informations pour informer le serveur des options que le client veut que le serveur envoie au client. Un serveur PEUT inclure une option Demande d'option dans une option Reconfigure pour indiquer quelles options le client devrait demander au serveur.

22.8 Option Préférence

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

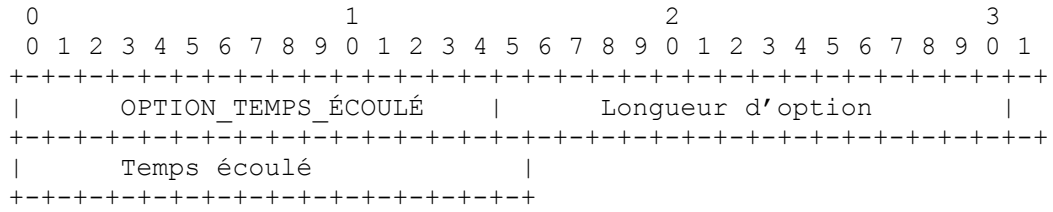
Le format de l'option Préférence est :



Code d'option : OPTION_PREFERENCE (7).
Longueur d'option : 1.
Valeur de préf. : la valeur de la préférence pour le serveur dans ce message.

Un serveur PEUT inclure une option Préférence dans un message Annoncer pour contrôler le choix d'un serveur par le client. Voir au paragraphe 17.1.3 l'utilisation de l'option Préférence par le client et l'interprétation de la valeur des données de l'option Préférence.

22.9 Option Temps écoulé



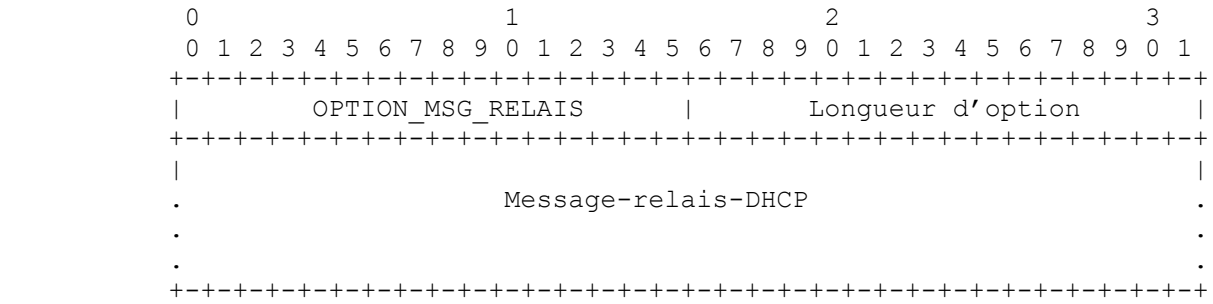
Code d'option : OPTION_TEMPS_ÉCOULÉ (8).
Longueur d'option : 2.
Temps écoulé : Temps écoulé depuis que le client a commencé la transaction DHCP en cours. Ce temps est exprimé en centièmes de seconde (10^{-2} s).

Un client DOIT inclure une option Temps écoulé dans les messages pour indiquer pendant combien de temps le client a essayé de mener à bien un échange de messages DHCP. Le temps écoulé est mesuré depuis le moment 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 des données dans cette option comme entrée du contrôle de régulation de la façon dont 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 lorsque un serveur primaire n'a pas répondu dans un délai raisonnable. La valeur du temps écoulé est un entier non signé de 16 bits. Le client utilise la valeut 0xffff pour représenter toutes valeurs de temps écoulé supérieure à la plus grande valeur de temps qui peut être représentée dans l'option Temps écoulé.

22.10 Option Message relais

L'option Message relais porte un message DHCP dans un message Transmission-relais ou Réponse-relais.

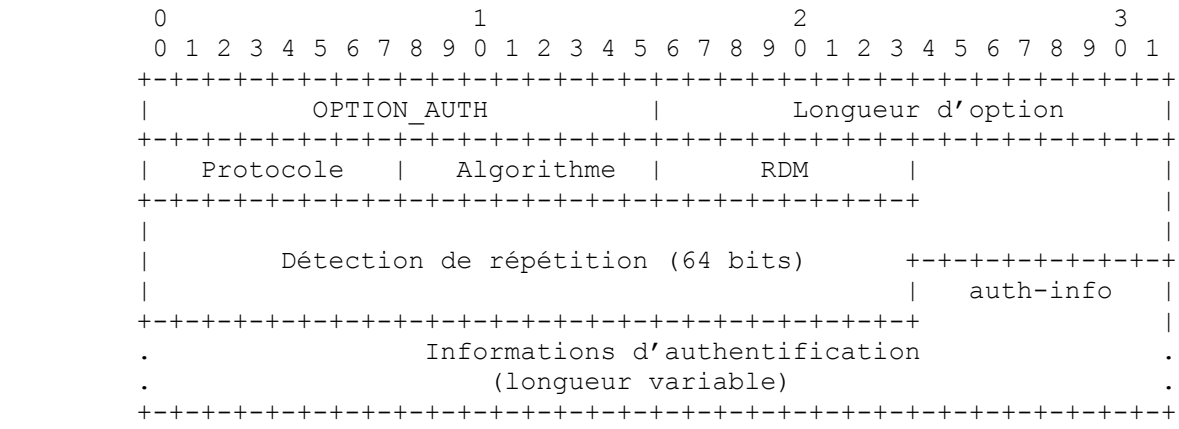
Le format de l'option Message relais est :



Code d'option : OPTION_MSG_RELAIS (9)
Longueur d'option : longueur du Message-relais-DHCP.
Message-relais-DHCP : Dans un message Transmission-relais, le message reçu, relayé textuellement au prochain agent de relais ou serveur; dans un message Réponse-relais, le message à copier et relayer à l'agent de relais ou au client dont l'adresse est dans le champ Adresse d'homologue du message Réponse-relais

22.11 Option Authentification

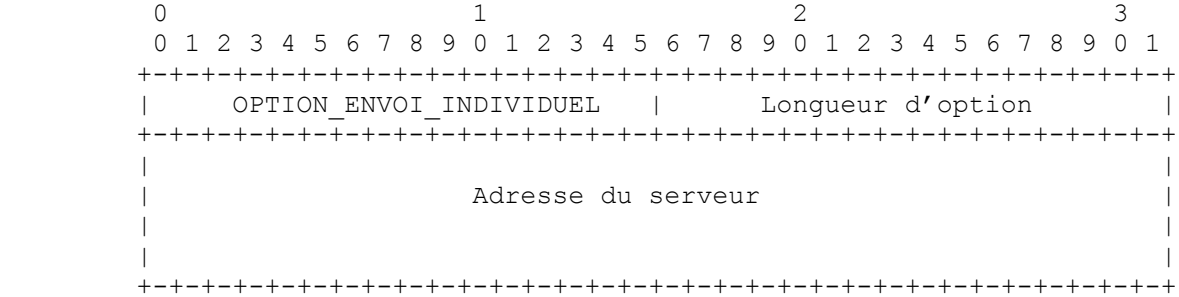
L'option Authentification porte des informations d'authentification pour authentifier l'identité et le contenu des messages DHCP. L'utilisation de l'option Authentification est décrite à la section 21. Le format de l'option Authentification est :



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.
Algorithme : Algorithme utilisé dans le protocole d'authentification.
RDM : Méthode de détection de répétition utilisée dans cette option Authentification.
Détection de répétition : Informations de détection de répétition pour la RDM.
Informations d'authentification : Les informations d'authentification, comme spécifiées par le protocole et l'algorithme utilisés dans cette option Authentification.

22.12 Option Envoi individuel au serveur

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



Code d'option : OPTION_ENVOI_INDIVIDUEL (12).
Longueur d'option : 16.
Adresse du serveur : Adresse IP à laquelle le client devrait envoyer les messages délivrés en utilisant l'envoi individuel.

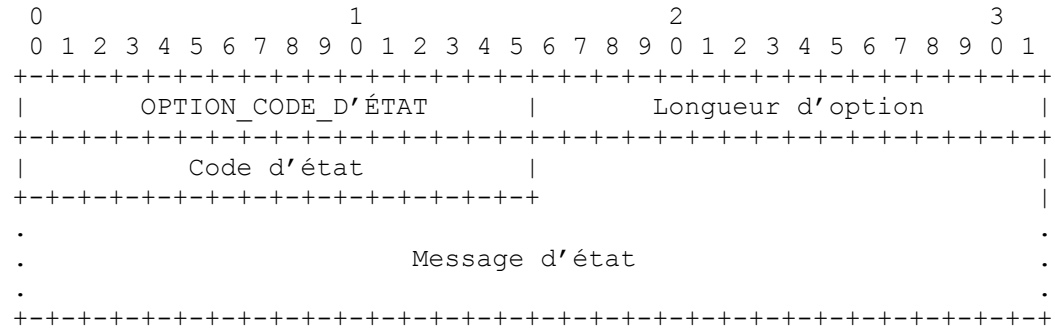
Le serveur spécifie l'adresse IPv6 à laquelle le client va envoyer les messages en individuel dans le champ Adresse du serveur. Lorsque un client reçoit cette option, si c'est permis et approprié, le client envoie les messages directement au serveur en utilisant l'adresse IPv6 spécifiée dans le champ Adresse du serveur de l'option.

Lorsque le serveur envoie une option Envoi individuel au client, certains messages du client ne seront pas relayés par des agents de relais, et n'incluront pas les options d'agent de relais provenant des agents de relais. Donc, un serveur ne devrait envoyer une option Envoi individuel à un client que quand les agents de relais n'envoient pas les options Agent de relais. Un serveur DHCP rejette tous les messages envoyés de façon inappropriée qui utilisent l'envoi individuel pour assurer que les messages sont relayés par les agents de relais quand les options Agent de relais sont utilisées.

Les détails sur le moment où le client peut envoyer des messages au serveur en se servant de l'envoi individuel sont à la section 18.

22.13 Option Code d'état

Cette option retourne une indication d'état qui se rapporte au message ou option DHCP dans lequel il apparaît. Le format de l'option Code d'état est :

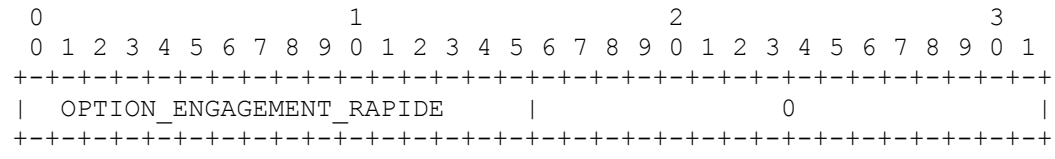


Code d'option : OPTION_CODE_D'ÉTAT (13).
Longueur d'option : 2 + longueur du message d'état.
Code d'état : Code numérique pour l'état codé dans cette option. Les codes d'état sont définis au paragaphe 24.4.
Message d'état : Chaîne de texte codée en UTF-8 convenable pour l'affichage à un utilisateur final, qui NE DOIT PAS être terminée par NUL.

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.

22.14 Option Engagement rapide

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



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

Un client PEUT inclure cette option dans un message Sollicite si le client est prêt à effectuer l'échange de messages Sollicite-Réponse décrit au paragraphe 17.1.1.

Un serveur DOIT inclure cette option dans un message Réponse envoyé en réponse à un message Sollicite lors de

l'achèvement de l'échange de messages Sollicite-Réponse.

DISCUSSION :

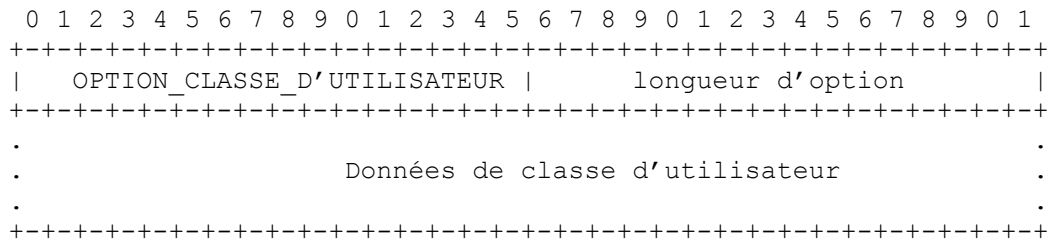
Chaque serveur qui répond avec un message Réponse à un message Sollicite qui inclut une option Engagement rapide va engager les adresses allouées dans le message Réponse au client, et ne va recevoir aucune confirmation que le client a reçu le message Réponse. Donc, si plus d'un serveur répond à un message Sollicite qui inclut une option Engagement rapide, certains serveurs vont engager des adresses qui ne seront pas réellement utilisées par le client.

Le problème des adresses non utilisées peut être minimisé, par exemple, en concevant le service DHCP de telle sorte qu'un seul serveur réponde au message Sollicite, ou en utilisant des durées de vie relativement brèves pour les adresses allouées.

22.15 Option Classe d'utilisateur

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

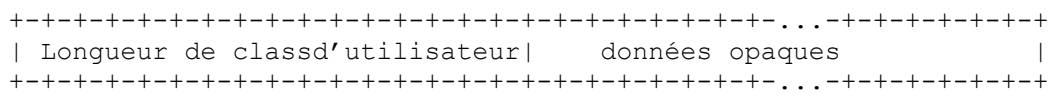
Le format de l'option Classe d'utilisateur est :



Code d'option : OPTION_CLASSE_D'UTILISATEUR (15).
Longueur d'option : Longueur du champ Données de classe d'utilisateur.
Données de classe d'utilisateur : Les classes d'utilisateur portées par le client.

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 d'utilisateur 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 personnels du département de comptabilité qui ont une imprimante différentes des clients des gens 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 de données de classe d'utilisateur. Chaque instance des données de classe d'utilisateur est formatée comme suit :



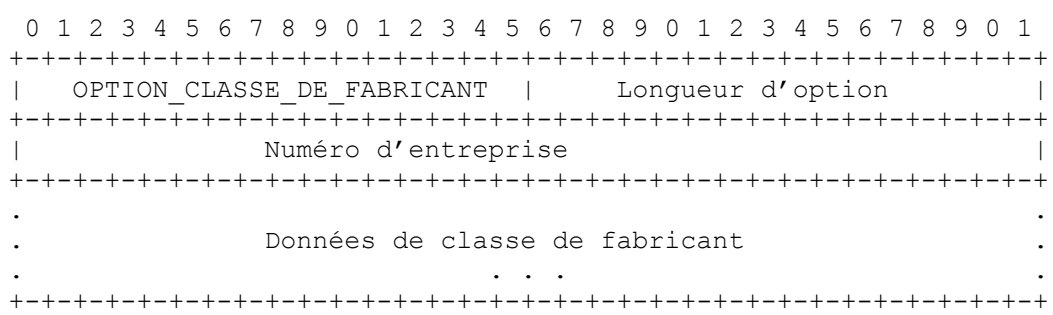
La Longueur de classe d'utilisateur fait deux octets et spécifie la longueur des données opaques de classe d'utilisateur dans l'ordre des octets du réseau.

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 utiliser seulement les classes d'utilisateur qu'il est configuré à interpréter en choisissant les informations de configuration pour un client et ignorer toutes les autres classes d'utilisateur. En réponse à un message contenant une option Classe d'utilisateur, un serveur inclut une option Classe d'utilisateur contenant ces classes qui ont bien été interprétées par le serveur, de sorte que le client peut être informé des classes interprétées par le serveur.

22.16 Option Classe de fabricant

Cette option est utilisée par un client pour identifier le fabricant qui a manufacturé le matériel sur lequel le client fonctionne. 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 du matériel.

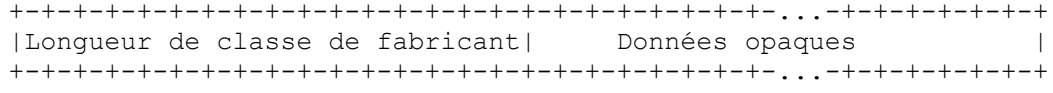
Le format de l'option Classe de fabricant est :



Code d'option : OPTION_CLASSE_DE_FABRICANT (16).
Longueur d'option : 4 + longueur du champ Données de classe de fabricant.
Numéro d'entreprise : Le numéro d'entreprise enregistré du fabricant tel qu'enregistré auprès de l'IANA [6].
Données de classe de fabricant : Configuration matérielle de l'hôte sur lequel fonctionne le client.

Les données de classe de fabricant sont composées d'une série d'éléments distincts, dont chacun décrit des caractéristiques de la configuration matérielle du client. Des exemples d'instances de données de classe de fabricant pourraient inclure la version du système d'exploitation sur lequel fonctionne le client ou la quantité de mémoire installée sur le client.

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

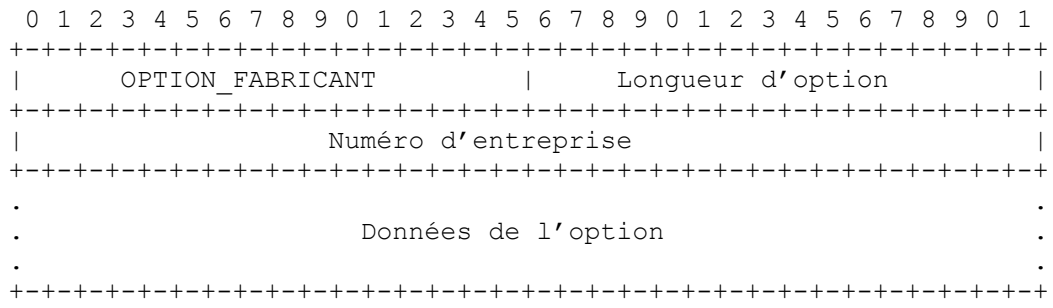


La longueur de classe de fabricant est de deux octets et spécifie la longueur des données opaques de classe de fabricant dans l'ordre des octets du réseau.

22.17 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 :

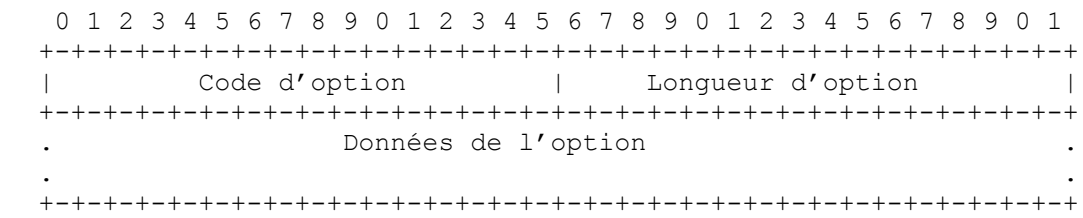


Code d'option : OPTION_FABRICANT (17)
Longueur d'option : 4 + longueur du champ Données de l'option.
Numéro d'entreprise : Numéro d'entreprise enregistré du fabricant tel qu'enregistré auprès de l'IANA [6].
Données de l'option : Objet opaque de Longueur d'option octets, interprété par le code spécifique de fabricant chez les clients et serveurs

La définition des informations portées dans cette option est spécifique du fabricant. Le fabricant est indiqué dans le champ Numéro d'entreprise. L'utilisation d'informations spécifiques du fabricant permet une amélioration du fonctionnement, en utilisant des caractéristiques supplémentaires dans la mise en œuvre de DHCP par le fabricant. Un client DHCP qui ne reçoit pas les informations spécifiques du fabricant demandées va quand même configurer la pile IPv6 de l'appareil hôte de façon à fonctionner.

Le champ d'options encapsulées spécifiques du fabricant DOIT être codé comme une séquence de champs code/longueur/valeur de format identique au champ d'options DHCP. Les codes d'option sont définis par le fabricant identifié dans le champ Numéro d'entreprise, et ne sont pas gérés par l'IANA. Chacune des options encapsulées est

formatée comme suit :

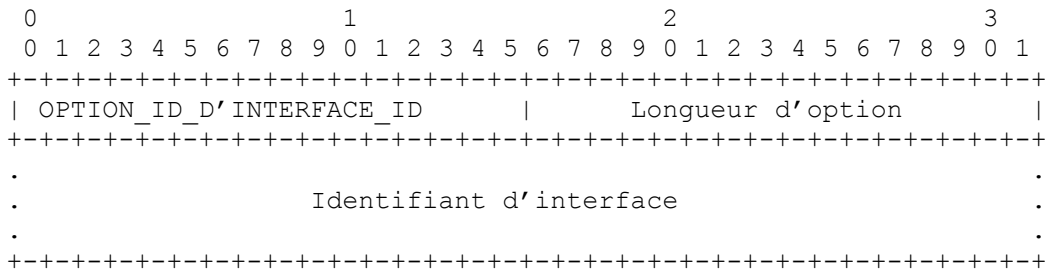


Code d'option : C'est le code pour l'option encapsulée.
Longueur d'option : Entier non signé qui donne en octets la longueur du champ Données d'option dans cette option encapsulée.
Données d'option : C'est la zone de données pour l'option encapsulée.

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.

22.18 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 Réponse-relais avec une option Identifiant d'interface, l'agent de relais relaie le message au client à travers l'interface identifiée par l'option. Le format de l'option Identifiant d'interface est :



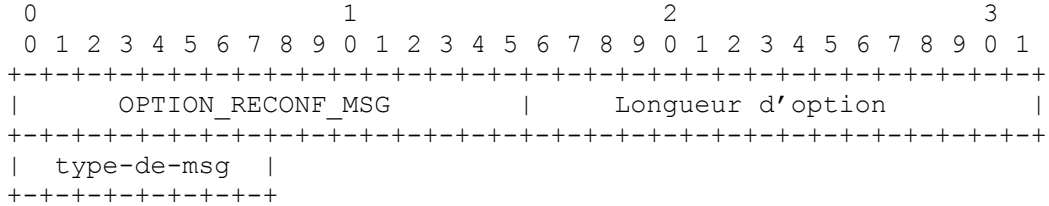
Code d'option : OPTION_ID_D'INTERFACE (18).
Longueur d'option : Longueur du champ Identifiant d'interface.
Identifiant d'interface : Valeur opaque de longueur arbitraire générée par l'agent de relais pour identifier une des interfaces de l'agent de relais.

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

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

22.19 Option Reconfigurer message

Un serveur inclut une option Reconfigurer message dans un message Reconfigure pour indiquer au client si le client répond par un message Renouvelle ou un message Demande d'information. Le format de cette option est :

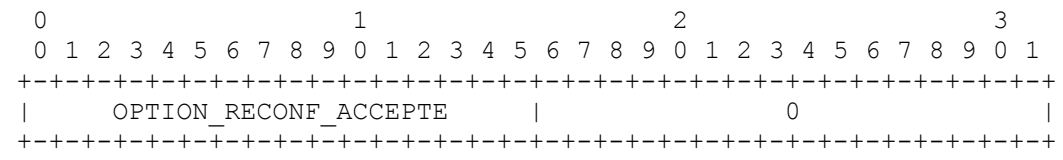


Code d'option : OPTION_RECONF_MSG (19).
Longueur d'option : 1.
type-de-msg : 5 pour le message Renouvelle, 11 pour le message Demande d'informations.

L'option Reconfigurer message ne peut apparaître que dans un message Reconfigure.

22.20 Option Reconfigure-Accepte

Un client utilise l'option Reconfigure-Accepte pour annoncer au serveur si le client veut accepter les messages Reconfigure, et un serveur utilise cette option pour dire au client si il doit ou non accepter les messages Reconfigure. Le comportement par défaut, en l'absence de cette option, signifie le refus d'accepter les messages Reconfigure, ou l'instruction de ne pas accepter les messages Reconfigure, pour les messages, respectivement, de client et de serveur. La figure suivante donne le format de l'option Reconfigure-Accepte :



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

23 Considérations sur la sécurité

Pour DHCP, la menace est par nature une menace de l'intérieur (en supposant un réseau correctement configuré où les accès DHCPv6 sont bloqués sur les passerelles périphériques de l'entreprise). Cependant, sans considération de la configuration des passerelles, le potentiel d'attaques par l'intérieur et par l'extérieur est le même.

L'utilisation de clés pré-partagées configurées manuellement pour IPsec entre les agents de relais et les serveurs ne défend pas contre la répétition des messages DHCP. Les messages répétés peuvent représenter une attaque de déni de service par l'épuisement des ressources de traitement, mais pas par une mauvaise configuration ou l'épuisement d'autres ressources telles que les adresses affectables.

Une attaque spécifique d'un client DHCP est l'établissement d'un serveur malvaillant avec l'intention de fournir des informations de configuration incorrectes au client. La motivation d'une telle action peut être le montage d'une attaque "par interposition" qui cause la communication du client avec un serveur malveillant au lieu d'un serveur valide pour des services comme le DNS ou NTP. Le serveur malveillant peut aussi monter une attaque de déni de service grâce à la mauvaise configuration du client qui cause l'échec de toutes les communications réseau provenant du client.

Il y a une autre menace pour les clients DHCP qui provient des serveurs DHCP mal configurés par erreur ou accident qui répondent aux demandes de clients DHCP avec des paramètres de configuration involontairement incorrects.

Un client DHCP peut aussi être l'objet d'une attaque au moyen de la réception d'un message Reconfigure provenant d'un serveur malveillant qui amène le client à obtenir des informations de configuration incorrectes de la part de ce serveur. Noter que bien qu'un client envoie sa réponse (message Renouvelle ou Demande d'information) à travers un agent de relais, et donc que cette réponse ne soit reçue que par les serveurs auxquels les messages DHCP sont relayés, un serveur malveillant pourrait envoyer un message Reconfigurer à un client, suivi (après un délai approprié) par un message Réponse qui serait accepté par le client. Donc, un serveur malveillant qui n'est pas sur le chemin 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 transactions qui soient bien chiffrés et ne puissent pas être facilement devinés va aussi réduire la probabilité qu'une telle attaque réussisse.

La menace spécifique du serveur DHCP est celle d'un client invalide qui se déguise en client valide. La motivation de cette action peut être le vol de service, ou de circonvenir l'analyse pour n'importe quel objet abominable.

La menace commune au client et au serveur est l'attaque en "déni de service" (DoS) de ressource. Ces attaques impliquent normalement l'épuisement des adresses disponibles, ou l'épuisement de la CPU ou de la bande passante du réseau, et sont présentes chaque fois qu'il y a une ressource partagée.

Dans le cas où des agents de relais ajoutent des options supplémentaires aux messages Relais de transmission, les messages

échangés entre les agents de relais et les serveurs peuvent être utilisés pour monter une attaque "par interposition" ou de déni de service.

Ce modèle de menace ne considère pas comme importante la confidentialité du contenu des messages DHCP. DHCP n'est pas utilisé pour échanger des authentifications ou des informations de configuration qui doivent être gardées secrètes pour les autres nœuds du réseau.

L'authentification DHCP fournit l'authentification de l'identité des clients et serveurs DHCP, et la protection de l'intégrité des messages livrés entre clients et serveurs DHCP. L'authentification DHCP ne protège pas la confidentialité du contenu des messages DHCP.

Le protocole d'authentification retardée décrit au paragraphe 21.4 utilise une clé secrète qui est partagée par un client et un serveur. L'utilisation d'un "royaume DHCP" dans la clé partagée permet l'identification des domaines administratifs afin qu'un client puisse choisir la ou les clés appropriées lors de l'itinérance entre domaines administratifs. Cependant, le protocole d'authentification ne définit aucun mécanisme pour partager les clés, de sorte qu'un client peut demander des clés distinctes pour chaque domaine administratif qu'il rencontre. L'utilisation de clés partagées peut ne pas bien s'adapter à toutes les situations et n'assure pas la répudiation des clés compromises. Ce protocole se concentre sur la résolution de problèmes intradomaine où l'échange hors bande d'une clé partagée est faisable.

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 réussit pas au processus de validation pour le protocole d'authentification.

Le protocole de reconfiguration de clé décrit au paragraphe 21.5 fournit une protection contre l'usage d'un message Reconfigure par un serveur DHCP malveillant pour monter une attaque de déni de service ou une attaque par interposition contre un client. Ce protocole peut être compromis par un attaquant qui peut intercepter le message initial dans lequel le serveur DHCP envoie la clé au client.

La communication entre un serveur et un agent de relais, et la communication entre les agents de relais, peut être sécurisée par l'utilisation de IPSec, comme décrit au paragraphe 21.1. L'utilisation de la configuration manuelle et l'installation de clés statiques sont acceptables dans cette instance parce que les agents de relais et le serveur vont appartenir au même domaine administratif et que les agents de relais vont exiger une autre configuration spécifique (par exemple, la configuration de l'adresse du serveur DHCP) en plus de la configuration IPsec.

24. Considérations pour l'IANA

Le présent document définit plusieurs nouveaux espaces de noms associés à DHCPv6 et aux options DHCPv6 :

- Types de message
- Codes d'état
- DUID
- Codes d'option

L'IANA a établi un registre des valeurs pour chacun de ces espaces de noms, qui sont décrit dans le reste de cette section. Ces espaces de nom seront gérés par l'IANA et tous seront gérés séparément des espaces de noms définis pour DHCPv4.

Les adresses de diffusion groupée, types de message, codes d'état, et types de DUID nouveaux sont alloués par action de normalisation [11].

Les nouveaux codes d'option DHCP seront alloués à l'essai après la révision par experts de la spécification de l'option associée, publiée comme projet Internet, par l'expert désigné [11]. L'allocation finale des codes d'option DHCP se fait par action de normalisation, comme défini dans la RFC2434 [11].

Le présent document fait aussi référence à la section 21 à trois espaces de noms qui sont associés à l'option Authentification (paragraphe 22.11). Ces espaces de noms sont définis par le mécanisme d'authentification pour DHCPv4 dans la RFC3118 [4].

Les espaces de noms d'authentification actuellement enregistrés par l'IANA s'appliqueront à DHCPv6 et DHCPv4. À l'avenir, les spécifications qui définissent de nouveaux mécanismes de Protocole, Algorithme et RDM définiront explicitement si les nouveaux mécanismes sont utilisés par DHCPv4, DHCPv6 ou les deux.

24.1 Adresses de diffusion groupée

Le paragraphe 5.1 définit les adresses de diffusion groupée suivantes, qui ont été allouées par l'IANA pour l'usage de DHCPv6 :

Tous_Agents_de_Relais_et_Serveurs_DHCP : FF02::1:2

Tous_Serveurs_DHCP : FF05::1:3

24.2 Types de message DHCP

L'IANA a enregistré les types de message suivants (définis au paragraphe 5.3). L'IANA tiendra le registre des types de message DHCP.

SOLLICITE	1
ANNONCE	2
DEMANDE	3
CONFIRME	4
RENOUVELLE	5
RELIE	6
RÉPONDRE	7
LIBÉRER	8
REFUSER	9
RECONFIGURE	10
DEMANDE-D'INFORMATION	11
TRANSMISSION-RELAIS	12
RÉPONSE-DE-RELAIS	13

24.3 Options DHCP

L'IANA a enregistré les codes d'option suivants (comme définis à la section 22). L'IANA tiendra le registre des codes d'option DHCP.

OPTION_CLIENTID	1
OPTION_SERVERID	2
OPTION_IA_NA	3
OPTION_IA_TA	4
OPTION_IAADDR	5
OPTION_ORO	6
OPTION_PREFERENCE	7
OPTION_ELAPSED_TIME	8
OPTION_RELAY_MSG	9
OPTION_AUTH	11
OPTION_UNICAST	12
OPTION_STATUS_CODE	13
OPTION_RAPID_COMMIT	14
OPTION_USER_CLASS	15
OPTION_VENDOR_CLASS	16
OPTION_VENDOR_OPTS	17
OPTION_INTERFACE_ID	18
OPTION_RECONF_MSG	19
OPTION_RECONF_ACCEPT	20

24.4 Codes d'état

L'IANA a enregistré les codes d'état définis dans le tableau suivant. L'IANA gèrera à l'avenir la définition des codes d'état supplémentaires.

Nom	**Description du code**
Success	0 Succès.
UnspecFail	1 Échec, pour une raison non spécifiée ; ce code d'état est envoyé par un client ou un serveur pour indique un échec non explicitement spécifié dans le présent document.

NoAddrsAvail	2	Le serveur n'a pas d'adresse disponible pour en allouer aux IA.
NoBinding	3	L'enregistrement du client (son lien) n'est pas 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 celui-ci à envoyer des messages au serveur en utilisant l'adresse Tous_Agents_de_Relais_et_Serveurs_DHCP.

24.5 DUID

L'IANA a enregistré les types de DUID suivants (définis au paragraphe 9.1). L'IANA gèrera à l'avenir la définition des types de DUID supplémentaires.

DUID	LLT	1
DUID	EN	2
DUID	LL	3

25 Remerciements

Nous remercions le groupe de travail DHC et les membres de l'IETF pour le temps qu'ils ont passé sur cette spécification et pour leurs apports. En particulier, nos remerciement pour les apports, les idées et la révision de (par ordre alphabétique) Bernard Aboba, Bill Arbaugh, Thirumalesh Bhat, Steve Bellovin, A. K. Vijayabhaskar, Brian Carpenter, Matt Crawford, Francis Dupont, Richard Hussong, Kim Kinnear, Fredrik Lindholm, Tony Lindstrom, Josh Littlefield, Gerald Maguire, Jack McCann, Shin Miyakawa, Thomas Narten, Erik Nordmark, Jarno Rajahalme, Yakov Rekhter, Mark Stapp, Matt Thomas, Sue Thomson, Tatuya Jinmei et Phil Wells.

Merci à Steve Deering et Bob Hinden, qui ont donné beaucoupe de leur temps pour discuter avec nous des parties les plus complexes des spécifications d'IPv6.

Et aussi, merci à Steve Deering pour avoir fait valoir à la réunion IETF 51 de Londres que la spécification de DHCPv6 avait le plus fort numéro de révision jamais atteint par un projet Internet.

26 Références

26.1 Références normatives

[1] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", RFC2119, BCP 14, mars 1997.

[2] M. Crawford, "Transmission de paquets IPv6 sur réseaux Ethernet", RFC2464, décembre 1998. *(P.S.)*

[3] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", RFC2460, décembre 1998. *(MàJ par 5095, D.S)*

[4] R. Droms et W. Arbaugh, "Authentification des messages DHCP", RFC3118, juin 2001.

[5] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", RFC2373, juillet 1998. (*Obsolète, voir* RFC3513) *(P.S.)*

[6] IANA, "Private Enterprise Numbers." à http://www.iana.org/assignments/enterprise-numbers.html.

[7] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC2401, novembre 1998. (*Obsolète, voir* RFC4301)

[8] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", RFC2104, février 1997.

[9] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", RFC1305, STD 12, mars 1992. *(Remplacée par RFC5905)*

[10] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", RFC1035, STD 13, novembre 1987.

[11] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", RFC2434, BCP 26, octobre, 1998. *(Rendue obsolète par la RFC 5226)*

[12] T. Narten, R. Draves, "Extensions de confidentialité pour l'auto-configuration d'adresse sans état dans IPv6", RFC3041, janvier 2001. (*Obsolète, voir* RFC4941) *(P.S.)*

[13] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", RFC2461, décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[14] 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", RFC0826, STD 37, novembre 1982.

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

[16] R. Rivest, "Algorithme de résumé de message MD5", RFC1321, avril 1992. *(Information)*

[17] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", RFC2462, décembre 1998. (*Obsolète, voir* RFC4862) *(D.S.)*

26.2 Références pour information

[18] S. Alexander et R. Droms, "Options DHCP et Extensions de fabricant BOOTP", RFC2132, mars 1997.

[19] R. Droms, "Protocole de configuration dynamique d'hôte", RFC2131, mars 1997. *(MàJ par RFC3396 et 4361)*

[20] R. Droms, éd., "Options de configuration du DNS pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", RFC3646, décembre 2003. *(P.S.)*

[21] A. K. Vijayabhaskar, "Options de configuration de l'heure pour DHCPv6", mai 2002. Non publiée.

[22] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", RFC2136, avril 1997.

Annexe A Apparition des options dans les types de message

Le tableau suivant indique avec une "*" les options admises dans chaque type de message DHCP :

	ID de client	ID de serveur	IA_NA/IA_TA	Demande d'option	Pref.	Heure	Msg Relais	Auth.	Envoi indiv. serveur
Sollicite	*		*	*		*		*	
Annonce	*	*	*		*			*	
Demande	*	*	*	*		*		*	
Confirme	*		*	*		*		*	
Renouvelle	*	*	*	*		*		*	
Relier	*		*	*		*		*	
Refuser	*	*	*	*		*		*	
Libérer	*	*	*	*		*		*	
Répondre	*	*	*		*			*	*
Reconf.	*	*		*				*	
Inform.	*	(note)		*		*		*	
R-trans.							*	*	
Rép-rel.							*	*	

Note : Ne sont inclus que dans les messages Information-Demande qui sont envoyés en réponse à Reconfigurer (voir au paragraphe 19.4.3).

	Code d'état	Rap. Comm.	Classe d'usager	Classe de fabricant	Spec de fabricant	Id Inter.	Msg Recon.	Accept. Recon.
Sollicite		*	*	*	*			*
Annonce	*		*	*	2*			*
Demande			*	*	*			*
Confirme			*	*	*			
Renouvelle			*	*	*			*
Relier			*	*	*			*
Refuser			*	*	*			
Libérer			*	*	*			
Répondre	*	*	*	*	*			*
Reconf.							*	
Inform.			*	*	*			*
R-trans.		*	*	*	*	*		
Rép-rel.			*	*	*	*		

Annexe B Apparition des options dans le champ Options des options DHCP

Le tableau suivant indique avec une "*" lorsque les options peuvent apparaître dans le champ Options d'autres options :

	Champ Options	IA_NA/IA_TA	IAADDR	Relais trans.	Réponse-relais
Client ID	*				
Server ID	*				
IA_NA/IA_TA	*				
IAADDR		*			
ORO	*				
Préférence	*				
Temps écoulé	*				
Relay Message				*	*
Authentif.	*				
Envoi indiv au serv.	*				
Code d'état	*	*	*		
Engag. rapide	*				
Classe d'usag.	*				
Classe de fabr.	*				
Info. de fabr.	*				
ID d'interface				*	*
MSG Reconf.	*				
Reconf. Accept	*				

Note : Les options "Relais trans"/"Réponse-relais" apparaissent dans le champ Options du message mais ne peuvent apparaître que dans ces messages.

Adresse du président du groupe de travail

Le groupe de travail peut être contacté via l'actuel président :

Ralph Droms
Cisco Systems
1414 Massachusetts Avenue
Boxborough, MA 01719
téléphone : (978) 936-1674
mél : rdroms@cisco.com

Adresse des auteurs

Jim Bound
Hewlett Packard Corporation
ZK3-3/W20
110 Spit Brook Road
Nashua, NH 03062-2698
USA
téléphone : +1 603 884 0062
mél : Jim.Bound@hp.com

Bernie Volz
116 Hawkins Pond Road
Center Harbor, NH 03226-3103
USA
téléphone : +1-508-259-3734
mél : volz@metrocast.net

Ted Lemon
Nominum, Inc.
950 Charter Street
Redwood City, CA 94043
USA
mél : Ted.Lemon@nominum.com

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
téléphone : +1-650 625-2986
mél : charles.perkins@nokia.com

Mike Carney
Sun Microsystems, Inc
17 Network Circle
Menlo Park, CA 94025
USA
téléphone : +1-650-786-4171
mél : michael.carney@sun.com

Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.