Groupe de travail Réseau
Request for Comments : 5007
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

J. Brzozowski, Comcast Cable
K. Kinnear, Cisco Systems Inc.
B. Volz, Cisco Systems, Inc.
S. Zeng, Cisco Systems, Inc.
septembre 2007

Leasequery pour DHCPv6

Résumé
Le présent document spécifie un échange leasequery pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) qui peut être utilisé pour obtenir des informations de prêts sur les clients DHCPv6 de la part d'un serveur DHCPv6. Le présent document spécifie la portée des données qui peuvent être restituées ainsi que le comportement du demandeur et du serveur leasequery DHCPv6. Le présent document étend DHCPv6.

Table des Matières

1. Introduction

Le protocole DHCPv6 [RFC3315] spécifie un mécanisme pour l'allocation d'adresse IPv6 et les informations de configuration aux nœuds IPv6. "Options de préfixe IPv6 pour DHCPv6" [RFC3633] spécifie un mécanisme pour la délégation automatique des préfixes IPv6 et des options qui s'y rapportent. Comme pour DHCPv4 [RFC2131], les serveurs DHCPv6 tiennent les informations d'autorité relatives à leurs opérations incluant, mais sans s'y limiter, les informations de prêt pour les adresses IPv6 et les préfixes délégués.

Il existe dans les divers types de déploiements IPv6, en particulier ceux d'une variété de large bande, l'exigence de donner l'avantage à DHCPv6 [RFC3315] pour restituer programmatiquement les données relatives au fonctionnement des serveurs DHCPv6. En particulier, il est souhaitable d'être capable d'extraire les informations de prêt des adresses IPv6 et des préfixes délégués alloués en utilisant DHCPv6 [RFC3315], [RFC3633]. Des exemples spécifiques où ces informations ont une valeur prouvée sont dans les réseaux à large bande pour faciliter le contrôle d'accès par les appareils de bordure. Cette capacité d'extraire programmatiquement les données de prêt d'un serveur DHCPv6 est appelé "leasequery" *(interrogation de prêt)*.

La capacité leasequery décrite dans le présent document est parallèle à la capacité leasequery de DHCPv4 documentée dans la [RFC4388]. À ce titre, elle partage les motivations de base, les fondements, les buts de conception et les contraintes décrites dans la [RFC4388]. Les différences sont dues aux différences entre IPv4 et IPv6 et par extension, DHCPv4 et DHCPv6. Par exemple, la découverte de voisin [RFC2461] est utilisée dans IPv6 à la place du protocole de résolution d'adresse (ARP) [RFC0826] (paragraphe 4.1 de la [RFC4388]) et DOCSIS 3.0 [MULPI] définit la prise en charge par IPv6 des environnements de modem câble.

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

La terminologie DHCPv6 est définie dans la [RFC3315]. La terminologie spécifique de leasequery DHCPv6 se trouve ci-dessous :

concentrateur d'accès : un concentrateur d'accès est un routeur ou commutateur à la bordure d'un fournisseur d'accès large bande d'un réseau d'accès public large bande. Le présent document suppose que le concentrateur d'accès inclut la fonction d'agent de relais DHCPv6.

client(s) : nœuds qui ont un ou plusieurs liens avec un serveur DHCPv6. Cela ne se réfère pas au nœud qui produit le LEASEQUERY sauf si il a lui-même un ou plusieurs liens avec un serveur DHCPv6.

glanage : le glanage est l'extraction des informations de localisation des messages DHCPv6, lorsque les messages sont transmis par la fonction d'agent de relais DHCP.

informations de localisation : ce sont les informations nécessaires au concentrateur d'accès pour transmettre le trafic à un hôte accessible en haut débit. Ces informations incluent la connaissance de l'adresse de matériel de l'hôte, l'accès ou le circuit virtuel qui conduit à l'hôte, et/ou l'adresse de matériel du modem d'abonné intermédiaire.

demandeur : nœud qui envoie des messages LEASEQUERY à un ou plusieurs serveurs pour restituer les informations sur les liens pour un client.

3. Vue d'ensemble du protocole

Le présent document se concentre sur l'extention du protocole DHCPv6 pour permettre aux processus et appareils qui souhaitent accéder aux informations provenant d'un serveur DHCPv6 de le faire d'une manière légère et pratique. Il est particulièrement approprié pour les processus et appareils qui interprètent déjà les messages DHCPv6.

Le message LEASEQUERY est seulement un message d'interrogation et n'affecte pas l'état de l'adresse ou préfixe IPv6, ou les informations de lien qui lui sont associées.

Un important exemple de motivation est que le message LEASEQUERY permet aux concentrateurs d'accès d'interroger les serveurs DHCP pour obtenir les informations de localisation des appareils de réseau d'accès large bande. Ceci est décrit à la Section 1 de la [RFC4388] pour IPv4.

3.1 Interrogation à la demande

La capacité leasequery à la demande permet de demander juste les informations nécessaires pour satisfaire un besoin immédiat. Si le demandeur est un concentrateur d'accès, alors le besoin immédiat va normalement être qu'il a reçu un paquet IPv6 et qu'il a besoin de rafraîchir ses informations concernant le client DHCPv6 auquel cette adresse IPv6 est actuellement prêtée. Dans ce cas, la demande va être par adresse. Cela tient clairement dans le cycle d'une seule demande/réponse commun aux autres échanges de messages DHCPv6.

Cependant, cette approche a des limitations quand elle est utilisée avec la délégation de préfixe [RFC3633] car aucun trafic ne peut arriver parce que le concentrateur d'accès n'est pas capable d'injecter les informations d'acheminement appropriées dans l'infrastructure d'acheminement, comme après un réamorçage. Cette approche fonctionne si le concentrateur d'accès est configuré à injecter les informations d'acheminement pour un préfixe qui agrège les préfixes potentiellement délégués. Ou, cela fonctionne aussi si le concentrateur d'accès et le routeur demandeur utilisent un protocole d'acheminement ; car alors le routeur demandeur peut déclencher au concentrateur d'accès la demande d'informations auprès d'un serveur DHCPv6 et injecter les informations d'acheminement appropriées dans l'infrastructure d'acheminement.

3.2 Interrogation anticipée

Une seconde approche pour demander les informations à un serveur DHCPv6 serait d'utiliser une capacité du genre leasequery pour reconstruire un magasin de données interne contenant les informations disponibles d'un serveur DHCPv6. La reconstruction d'un magasin de données dans cette approche peut avoir lieu aussitôt que possible après la découverte du besoin de le reconstruire (comme à l'amorçage) et n'attend pas la réception de paquets spécifiques pour déclencher une mise à jour morceau par morceau d'une base de données (comme c'est le cas pour leasequery à la demande). Cette approche supprimerait aussi la limitation discutée plus haut pour la délégation de préfixe.

Cette interrogation anticipée n'est pas spécifiée dans le présent document et est un sujet d'étude futur.

3.3 Types d'interrogation

Leasequery fournit les interrogations suivantes :

Interrogation par adresse IPv6 : cette interrogation permet à un demandeur de demander à un serveur les liens pour un client qui soit est lié à l'adresse, soit a eu délégation du préfixe qui contient l'adresse.

Interrogation par identifiant de client (DUID) : cette interrogation permet à un demandeur de demander à un serveur les liens pour un client spécifique sur une liaison spécifique ou une liste des liaisons sur lesquelles le client a un ou plusieurs liens.

4. Détails du protocole

4.1 Définitions de message et d'option

4.1.1 Messages

Les messages LEASEQUERY et LEASEQUERY-REPLY utilisent les formats de message client/serveur décrits dans la [RFC3315], Section 6. Deux nouveaux codes de message sont définis :

LEASEQUERY (14) - un demandeur envoie un message LEASEQUERY à tout serveur disponible pour obtenir les informations sur les prêts d'un client. Les options dans une OPTION_LQ_QUERY déterminent l'interrogation.

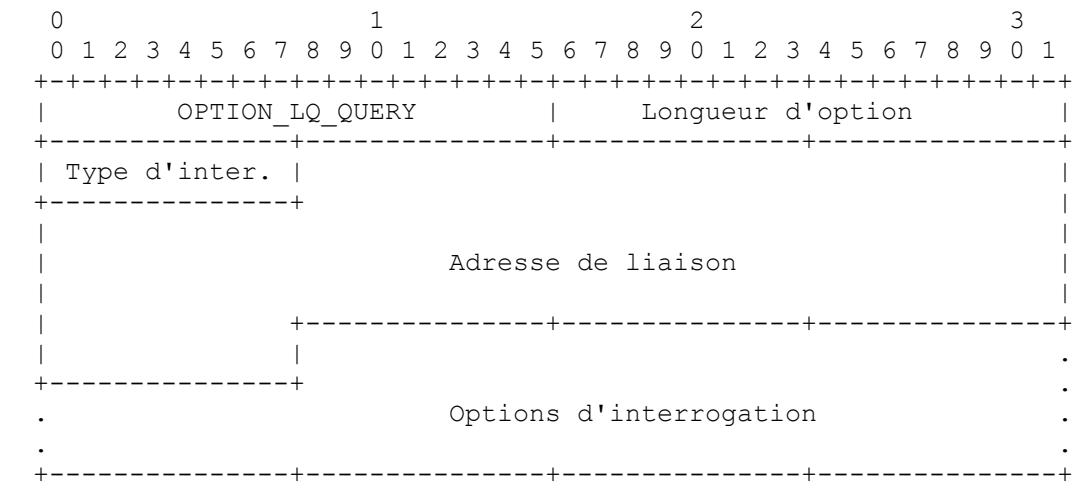
LEASEQUERY-REPLY (15) - un serveur envoie un message LEASEQUERY-REPLY contenant les données du client en réponse à un message LEASEQUERY.

4.1.2 Options

4.1.2.1 Option Query

L'option Query n'est utilisée que dans un message LEASEQUERY et identifie l'interrogation effectuée. L'option inclut le type d'interrogation, l'adresse de liaison (ou 0::0), et la ou les options pour fournir les données nécessaires à l'interrogation.

Le format de l'option Query est :



Code d'option : OPTION_LQ_QUERY (44)

Longueur d'option : 17 + longueur du champ Options d'interrogation.

Adresse de liaison : adresse mondiale qui va être utilisée par le serveur pour identifier la liaison à laquelle l'interrogation s'applique, ou 0::0 si elle n'est pas spécifiée.

Type d'interrogation : l'interrogation demandée (voir ci-dessous).

Options d'interrogation : les options relatives à l'interrogation.

Le type d'interrogation et les options d'interrogation exigées sont :

QUERY_BY_ADDRESS (1) *(interrogation par adresse)* - les options d'interrogation DOIVENT contenir une option OPTION_IAADDR [RFC3315]. Le champ Adresse de liaison, si il n'est pas 0::0, spécifie une adresse pour la liaison sur laquelle le client est situé si l'adresse dans l'option OPTION_IAADDR est d'une portée insuffisante. Seules les informations pour le client qui a un prêt pour l'adresse spécifiée ou à qui un préfixe a été délégué qui contient l'adresse spécifiée sont retournées (si elles sont disponibles).

QUERY_BY_CLIENTID (2) *(interrogation par identifiant de client)* - les options d'interrogation DOIVENT contenir une option OPTION_CLIENTID [RFC3315]. Le champ Adresse de liaison, si il n'est pas 0::0, spécifie une adresse pour la liaison sur laquelle le client est situé. Si le champ Adresse de liaison est 0::0, le serveur DEVRAIT rechercher toutes ses liaisons pour le client.

Les options d'interrogation PEUVENT aussi inclure une option OPTION_ORO [RFC3315] pour indiquer les options pour chaque client que le demandeur aimerait que le serveur retourne. Noter que cette OPTION_ORO est distincte et séparée d'une OPTION_ORO qui peut être dans le message LEASEQUERY du demandeur.

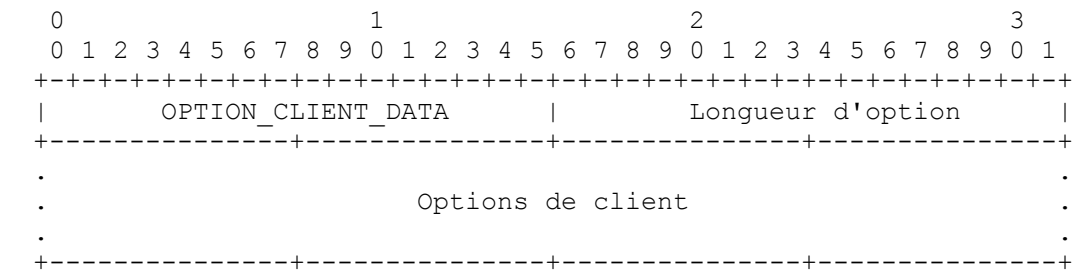
Si un serveur reçoit une OPTION_LQ_QUERY avec un type d'interrogation qu'il ne prend pas en charge, le serveur DEVRAIT retourner un code d'état UnknownQueryType *(type d'interrogation inconnu)*. Si un serveur reçoit un type d'interrogation pris en charge, mais qu'il manque une option exigée dans les options d'interrogation, le serveur DEVRAIT

retourner un code d'état MalformedQuery *(interrogation mal formée)*.

4.1.2.2 Option Client Data

L'option Client Data *(données de client)* est utilisée pour encapsuler les données pour un seul client sur une seule liaison dans un message LEASEQUERY-REPLY.

Le format de l'option Client Data est :



Code d'option : OPTION_CLIENT_DATA (45)

Longueur d'option : longueur, en octets, du champ Options de client encapsulées.

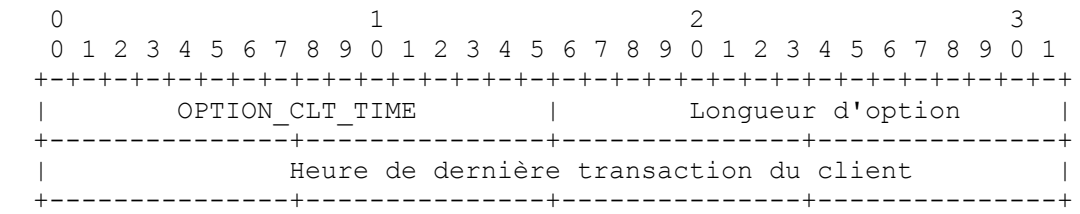
Options de client : options associées à ce client.

Les options de client encapsulées incluent les options OPTION_CLIENTID, OPTION_IAADDR, OPTION_IAPREFIX, et OPTION_CLT_TIME et d'autres options spécifiques du client et demandées par le demandeur dans le OPTION_ORO des options d'interrogation de OPTION_LQ_QUERY. Le serveur DOIT retourner toutes les adresses allouées à états pleins du client et les préfixes délégués, avec une durée de vie valide non zéro, sur la liaison.

4.1.2.3 Option Heure de dernière t ransaction du client

L'option Heure de dernière transaction du client est encapsulée dans une OPTION_CLIENT_DATA et identifie la durée écoulée depuis la dernière communication du serveur avec le client, en secondes.

Le format de l'option Heure de dernière transaction du client est :



Code d'option : OPTION_CLT_TIME (46)

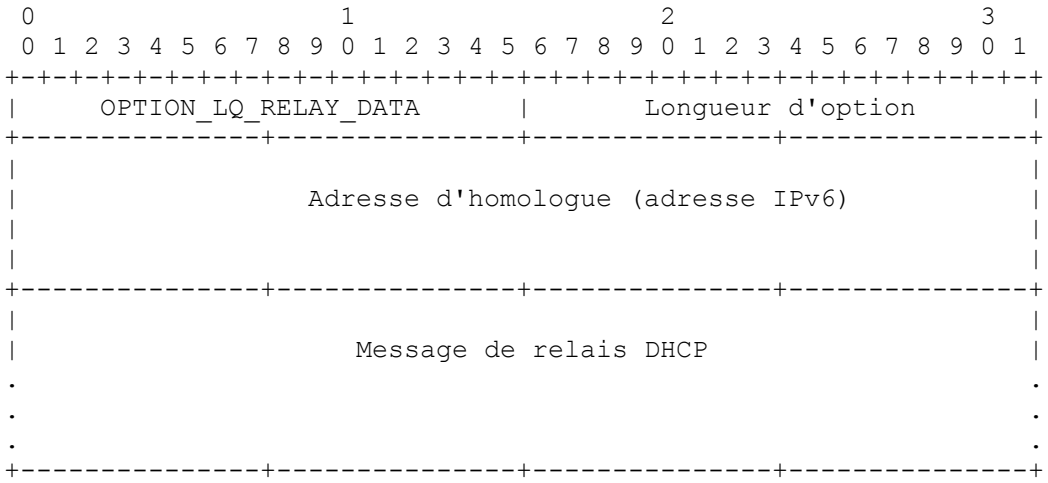
Longueur d'option : 4

Heure de dernière transaction du client : nombre de secondes depuis la dernière commmunication du serveur avec le client (sur cette liaison). Heure de dernière transaction du client est une valeur positive et reflète le nombre de secondes depuis la dernière communication du serveur avec le client (sur cette liaison).

4.1.2.4 Option Relay Data

L'option Relay Data *(données de relais)* n'est utilisée que dans un message LEASEQUERY-REPLY et fournit à l'agent de relais les informations utilisées quand le client a communiqué pour la dernière fois avec le serveur.

Le format de l'option Relay Data est :



Code d'option : OPTION_LQ_RELAY_DATA (47)

Longueur d'option : 16 + longueur du message de relais DHCP.

Adresse d'homologue : adresse de l'agent de relais duquel le message relayé a été reçu par le serveur.

Message de relais DHCP : dernier message complet relayé, à l'exclusion du message OPTION_RELAY_MSG du client, reçu par le serveur.

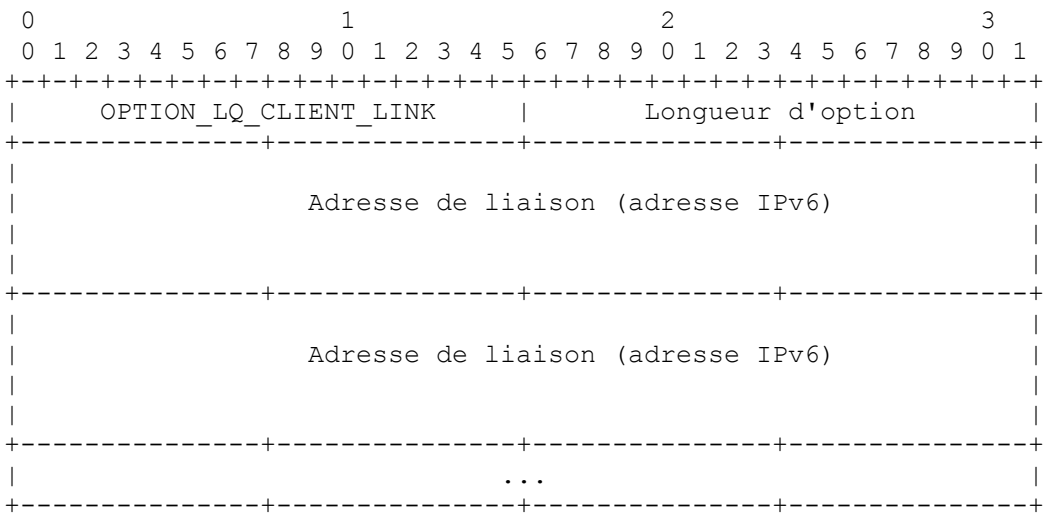
Cette option est utilisée par le serveur pour retourner les informations complètes d'agent de relais pour un client. Elle NE DOIT PAS être retournée si le serveur n'a pas ces informations, soit parce que le client a communiqué directement (sans agent de relais) avec le serveur, soit parce que le serveur n'a pas conservé ces informations.

Si il est retourné, le message de relais DHCP DOIT contenir un message valide (peut être multi bonds) RELAY-FORW comme le plus récemment reçu par le serveur pour le client. Cependant, l'option (la plus interne) OPTION_RELAY_MSG contenant le message du client DOIT avoir été supprimée.
Cette option DEVRAIT n'être retournée que si elle a été demandée par le OPTION_ORO de OPTION_LQ_QUERY.

4.1.2.5 Option Client Link

L'option Client Link n'est utilisée que dans un message LEASEQUERY-REPLY et identifie les liaisons sur lesquelles le client a un ou plusieurs liens. Elle est utilisée en réponse à une interrogation quand aucune adresse de liaison n'a été spécifiée et que le client se trouve être sur plus d'une liaison.

Le format de l'option Client Link est :



Code d'option : OPTION_LQ_CLIENT_LINK (48)

Longueur d'option : longueur de la liste des liaisons en octets ; doit être a multiple de 16.

Adresse de liaison : adresse mondiale utilisée par le serveur pour identifier la liaison sur laquelle le client est situé.

Un serveur peut répondre à une interrogation par un identifiant de client, où l'adresse de liaison 0::0 a été spécifiée, avec cette option si le client se trouve être sur plusieurs liaisons. Le demandeur peut alors répéter l'interrogation une fois pour chaque adresse de liaison retournée dans la liste, en spécifianr l'adresse de liaison retournée. Si le client est sur une seule liaison, le serveur DEVRAIT retourner les données du client dans une option OPTION_CLIENT_DATA.

4.1.3 Codes d'état

Les nouveaux codes d'état suivants sont définis :

UnknownQueryType *(type d'interrogation inconnu)* (7) - le type d'interrogation est inconnu ou non pris en charge par le serveur.

MalformedQuery *(interrogation mal formée)* (8) - L'interrogation n'est pas valide ; par exemple, une option d'interrogation exigée manque dans la OPTION_LQ_QUERY.

NotConfigured *(non configurée)* (9) - le serveur n'a pas l'adresse ou liaison cible dans sa configuration.

NotAllowed *(interdit)* (10) - le serveur ne permet pas au demandeur de produire ce LEASEQUERY.

4.1.4 Paramètres de transmission et de retransmission

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

Paramètre	Par défaut	Description
LQ_TIMEOUT	1 s	Temporisation de LEASEQUERY initial
LQ_MAX_RT	10 s	Valeur maximum de temporisation LEASEQUERY
LQ_MAX_RC	5	Maximum de tentatives d'essai LEASEQUERY

4.2 Validation de message

4.2.1 LEASEQUERY

Les demandeurs et clients DOIVENT éliminer tous les messages LEASEQUERY reçus. Les serveurs DOIVENT éliminer tout message LEASEQUERY reçu qui satisfait une des conditions suivantes :
- o le message n'inclut pas d'option OPTION_CLIENTID ;
- o le message inclut une option OPTION_SERVERID mais le contenu de l'option OPTION_SERVERID ne correspond pas à l'identifiant du serveur ;
- o le message n'inclut pas d'option OPTION_LQ_QUERY.

4.2.2 LEASEQUERY-REPLY

Les demandeurs DOIVENT éliminer tous les messages LEASEQUERY-REPLY reçus qui satisfont uae des conditions suivantes :
- o le message n'inclut pas d'option OPTION_SERVERID ;
- o le message n'inclut pas d'option OPTION_CLIENTID, ou le contenu de l'option OPTION_CLIENTID ne correspond pas au DUID du demandeur ;
- o le champ "transaction-id" dans le message ne correspond pas à la valeur utilisée dans le message d'origine.

Les serveurs et agents de relais (sur l'accès de serveur 547 [RFC3315]) DOIVENT éliminer tout message LEASEQUERY-REPLY reçu.

4.3 Comportement du demandeur Leasequery DHCPv6

Ce paragraphe décrit comment un demandeur initie la restitution des données de prêt des serveurs DHCPv6.

4.3.1 Création de LEASEQUERY

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

Le demandeur DOIT inclure une option OPTION_CLIENTID pour s'identifier auprès du serveur.

Le demandeur DOIT inclure ue option OPTION_LQ_QUERY et régler le type d'interrogation, l'adresse de liaison, et les options d'interrogation comme approprié pour le type d'interrogation (paragraphe 4.1.2.1).

Le demandeur DEVRAIT inclure une option OPTION_SERVERID si il n'envoie pas en individuel le LEASEQUERY et attend seulement une réponse d'un serveur spécifique.

4.3.2 Transmission de LEASEQUERY

Le demandeur PEUT être configuré à utiliser une liste d'adresses de destination, qui PEUT inclure des adresses d'envoi individuel, l'adresse de diffusion groupée All_DHCP_Servers *(tous serveurs DHCP)* ou d'autres adresses choisies par l'administrateur du réseau. Si le demandeur n'a pas été explicitement configuré, il PEUT utiliser par défaut l'adresse de diffusion groupée All_DHCP_Servers.

Le demandeur DEVRAIT envoyer un LEASEQUERY à un ou plusieurs serveurs DHCPv6 connus pour posséder des informations d'autorité sur la cible de l'interrogation.

En l'absence d'informations concernant les serveurs DHCPv6 qui pourraient posséder des informations d'autorité sur la cible de l'interrogation, le demandeur DEVRAIT envoyer le LEASEQUERY à tous les serveurs DHCPv6 que le demandeur connait ou avec lesquels il est configuré. Par exemple, le demandeur PEUT envoyer le LEASEQUERY à l'adresse de diffusion groupée All_DHCP_Servers.

Le demandeur transmet les messages LEASEQUERY conformément à la Section 14 de la [RFC3315], en utilisant les paramètres suivants :

IRT : LQ_TIMEOUT
MRT : LQ_MAX_RT
MRC : LQ_MAX_RC
MRD : 0

Si l'échange de messages échoue, le demandeur effectue une action fondée sur la politique locale du demandeur. Des exemples d'actions que le demandeur pourrait effectuer incluent de :
- o choisir un autre serveur sur une liste de serveurs connus du demandeur ;
- o envoyer à plusieurs serveurs en diffusion groupée à l'adresse All_DHCP_Servers ;
- o terminer la demande.

4.3.3 Réception de LEASEQUERY-REPLY

Une LEASEQUERY-REPLY réussie est sans option OPTION_STATUS_CODE (ou une option OPTION_STATUS_CODE avec un code de succès). Il y a trois variantes :

1. Si le serveur avait des liens pour le client demandé, le message inclut une option OPTION_CLIENT_DATA et le demandeur extrait les données du client de la LEASEQUERY-REPLY et met à jour sa base de données d'informations de liens. Si les OPTION_CLIENT_DATA ne contiennent pas de OPTION_CLT_TIME, le demandeur DEVRAIT éliminer en silence l'option OPTION_CLIENT_DATA.

2. Si le serveur a trouvé des liens pour le client sur plusieurs liaisons, le message inclut une option

OPTION_CLIENT_LINK. Le demandeur va devoir produire à nouveau des messages LEASEQUERY en utilisant chacune des adresses de liaison retournées pour obtenir les liens du client.

3. Si le serveur n'avait pas de liens pour le client, ni l'option OPTION_CLIENT_DATA ni l'option OPTION_CLIENT_LINK ne vont être présentes.

Une LEASEQUERY-REPLY non réussie est celle qui a une OPTION_STATUS_CODE avec un code d'erreur. Selon le code d'état, le demandeur peut essayer un serveur différent (comme pour NotAllowed, NotConfigured, et UnknownQueryType) essayer une interrogation différente ou corrigée (comme pour UnknownQueryType et MalformedQuery) ou terminer l'interrogation.

4.3.4 Traitement de données de client DHCPv6 provenant de plusieurs sources

Un demandeur peut recevoir des données de prêt sur le même client provenant du même serveur DHCPv6 en réponse à différents types de LEASEQUERY. Si un LEASEQUERY est envoyé à plusieurs serveurs, le demandeur peut recevoir de plusieurs serveurs des données de prêt sur le même client DHCPv6. Ce paragraphe décrit comment le demandeur traite plusieurs sources de données de prêt sur le même client DHCPv6 provenant du même serveur ou de serveurs différents.

Les données de client provenant de différentes sources peuvent être disjointes ou se chevaucher. Les relations de disjonction et de chevauchement peuvent apparaître entre des données provenant du même serveur ou de serveurs différents.

Si les données de client provenant de deux sources sur le même client sont de types ou valeurs différents, alors les données sont disjointes. Un exemple de données de différents types est quand un demandeur reçoit un prêt d'adresse IPv6 d'un serveur et un prêt de préfixe d'un autre serveur, tous deux alloués au même client. Un exemple de valeurs différentes (mais de même type) est quand un demandeur reçoit deux prêts d'adresse IPv6 de deux serveurs différents, tous deux alloués au même client, mais les prêts sont sur deux adresses IPv6 différentes. Si le demandeur reçoit des données de client disjointes de différentes sources, il DEVRAIT les fusionner.

Si les données de client provenant de deux sources sur le même client sont de même type et valeur, alors les données sont en chevauchement. Un exemple de données en chevauchement est quand un demandeur reçoit un prêt sur la même adresse IPv6 de deux serveurs différents. Les données de client en chevauchement sont aussi appelées des données en conflit.

Le demandeur DEVRAIT utiliser le OPTION_CLT_TIME pour résoudre les conflits de données provenant de serveurs différents, et DEVRAIT accepter les données avec le OPTION_CLT_TIME le plus récent.

4.4 Comportement du serveur Leasequery DHCPv6

Un serveur DHCPv6 envoie des messages LEASEQUERY-REPLY en réponse aux messages LEASEQUERY valides qu'il reçoit pour retourner les adresses allouées à états pleins, les préfixes délégués, et autres informations qui correspondent à l'interrogation.

4.4.1 Réception des messages LEASEQUERY

À réception d'un message LEASEQUERY valide, le serveur DHCPv6 localise le client demandé, collecte les données sur le client, et construit et retourne une LEASEQUERY-REPLY. Un message LEASEQUERY ne peut pas être utilisé pour allouer, libérer, ou modifier autrement des liens ou autres informations de configuration.

Le serveur construit un message LEASEQUERY-REPLY en réglant le champ "msg-type" à LEASEQUERY-REPLY, et en copiant l'identifiant de transaction provenant du message LEASEQUERY dans le champ Identifiant de transaction.

Si le type d'interrogation dans l'option OPTION_LQ_QUERY n'est pas une valeur connue ou prise en charge, le serveur ajoute une option OPTION_STATUS_CODE avec le code d'état UnknownQueryType et envoie la LEASEQUERY-REPLY au demandeur. Si les options d'interrogation ne contiennent pas les options exigées pour le type d'interrogation, le serveur ajoute une option OPTION_STATUS_CODE avec le code d'état MalformedQuery et envoie la LEASEQUERY-REPLY au client.

Un serveur peut aussi restreindre les messages LEASEQUERY, ou les types d'interrogation à certains demandeurs. Dans ce cas, le serveur PEUT éliminer le message LEASEQUERY ou PEUT ajouter une option OPTION_STATUS_CODE avec le

code d'état NotAllowed et envoyer la LEASEQUERY-REPLY au demandeur.

Si la OPTION_LQ_QUERY spécifiait une adresse de liaison non zéro, le serveur DOIT utiliser l'adresse de liaison pour trouver la liaison appropriée pour le client. Pour une QUERY_BY_ADDRESS, si l'adresse de liaison 0::0 a été spécifiée, le serveur utilise l'adresse provenant de l'option OPTION_IAADDR pour trouver la liaison appropriée pour le client. Dans l'un et l'autre de ces cas, si le serveur n'est pas capable de trouver la liaison, il DEVRAIT retourner une option OPTION_STATUS_CODE avec l'état NotConfigured et envoyer la LEASEQUERY-REPLY au demandeur.

Pour une QUERY_BY_CLIENTID, si une adresse de liaison 0::0 a été spécifiée, le serveur DOIT chercher toutes ses liaisons pour le client. Si le client n'est trouvé que sur une seule liaison, le serveur DEVRAIT retourner ces données de client dans une option OPTION_CLIENT_DATA. Si le client est trouvé sur plus d'une seule liaison, le serveur DOIT retourner la liste des liaisons dans l'option OPTION_CLIENT_LINK ; le serveur NE DOIT PAS retourner de données de client.

Autrement, le serveur utilise les données dans la OPTION_LQ_QUERY pour initier l'interrogation. Le résultat de l'interrogation va être zéro ou un client. Il va résulter en l'ajout de zéro ou une option OPTION_CLIENT_DATA à la LEASEQUERY-REPLY.

4.4.2 Construction de l'OPTION_CLIENT_DATA du client

Une option OPTION_CLIENT_DATA dans un message LEASEQUERY-REPLY DOIT au minimum contenir les options suivantes :
1. OPTION_CLIENTID *(option Identifiant de client)*
2. OPTION_IAADDR et/ou OPTION_IAPREFIX *(option d'adresse/préfixe d'association d'identité)*
3. OPTION_CLT_TIME

Selon les liens que le client a sur une liaison, des options OPTION_IAADDR, OPTION_IAPREFIX, ou les deux peuvent être présentes.

L'option OPTION_CLIENT_DATA DEVRAIT inclure les options demandées dans le OPTION_ORO de l'option OPTION_LQ_QUERY dans le message LEASEQUERY et qu'il est acceptable de retourner sur la base de la liste des "options sensibles", discutées ci-dessous .

Les serveurs DHCPv6 DEVRAIENT être configurables avec une liste des "options sensibles" qui ne doivent pas être retournées au demandeur quand elles sont spécifiées dans le OPTION_ORO de l'option OPTION_LQ_QUERY dans le message LEASEQUERY. Aucune option figurant dans cette liste NE DOIT être retournée à un demandeur, même si elles sont demandées par ce demandeur.

4.4.3 Transmission des messages LEASEQUERY-REPLY

Le serveur envoie le message LEASEQUERY-REPLY comme décrit dans le paragraphe "Transmission des messages de réponse" de la [RFC3315].

5. Considérations sur la sécurité

Les concentrateurs d'accès sont supposés être les demandeurs courants d'interrogations de prêt. Les concentrateurs d'accès qui utilisent le glanage DHCPv6 (c'est-à-dire, [RAAN]), rafraîchi avec des messages LEASEQUERY, vont conserver des informations précises de client/lien. Cela assure que le concentrateur d'accès peut transmettre du trafic de données à la destination prévue dans le réseau d'accès large bande, peut effectuer la vérification de l'adresse de source IPv6 des datagrammes provenant du réseau d'accès, et peut chiffrer le trafic qui ne peut être déchiffré que par le modem d'accès prévu (par exemple, [DOCSIS] et [BPPIS]). Donc, la capacité leasequery permet à un concentrateur d'accès de fournir une sécurité considérablement améliorée.

La Section "Considérations sur la sécurité" de la [RFC3315] détaille les menaces générales pour DHCPv6, et donc pour les messages LEASEQUERY. La Section "Authentification des messages DHCP" de la [RFC3315] décrit la sécurisation de la communication entre agents de relais et serveurs, ainsi que des clients et serveurs. Si le demandeur est un concentrateur d'accès, la sécurité fondée sur IPsec [RFC4301] comme décrite au paragraphe 21.1 de la [RFC3315] DEVRAIT être utilisée. Les autres types de demandeurs sont essentiellement des clients DHCPv6. Donc, l'authenticafition DHCPv6, à la

Section 21 de la [RFC3315], est un mécanisme approprié pour sécuriser les messages LEASEQUERY et LEASEQUERY-REPLY. Comme le nombre de demandeurs et serveurs leasequery dans un domaine administratif est relativement faible, tous les problèmes de distribution de clés partagées sont minimisés.

Après la mise en œuvre des approches ci-dessus, le serveur DHCPv6 devrait ne communiquer qu'avec des demandeurs LEASEQUERY de confiance, de sorte que les besoins de sécurité devraient être satisfaits.

Cependant, tout le trafic n'a pas pour origine directe ces demandeurs de confiance. Par exemple, des agents de relais de confiance peuvent relayer des messages LEASEQUERY provenant de demandeurs qui ne sont pas de confiance ou d'ailleurs dans le réseau. Ceci DEVRAIT être empêché au moins au périmètre des agents de relais (ou sur tous les agents de relais sauf si les messages LEASEQUERY relayés sont exigés pour certains demandeurs). Les serveurs DHCPv6 PEUVENT être configurés à éliminer les messages LEASEQUERY relayés ou à restreindre le chaînage de relais.

Les serveurs DHCPv6 DEVRAIENT aussi fournir la capacité de restreindre les informations retournées pour un client dans une LEASEQUERY-REPLY même à un demandeur LEASEQUERY de confiance, comme décrit au paragraphe 4.4.2.

Comme même des concentrateurs d'accès de confiance peuvent générer des demandes LEASEQUERY par suite d'une activité externe au concentrateur d'accès, les concentrateurs d'accès DEVRAIENT minimiser le potentiel d'attaques de déni de service sur les serveurs DHCPv6 en minimisant la génération de messages LEASEQUERY. En particulier, le concentrateur d'accès DEVRAIT employer la mise en mémoire tampon négative (c'est-à-dire, mettre en mémoire tampon le fait qu'une interrogation récente particulière a échoué à retourner les données de client) et les restrictions d'adresse lorsque possible (c'est-à-dire, ne pas envoyer de message LEASEQUERY pour des adresses en dehors de la gamme des réseaux d'accès large bande rattachés). Ensemble, ces mécanismes limitent le concentrateur d'accès à la transmission d'un message LEASEQUERY (en excluant les messages réessayés) par adresse légitime de réseau d'accès large bande après un événement de réamorçage.

Les attaques de déni de service par inondation de paquets peuvent résulter en l'épuisement des ressources de traitement, empêchant donc le serveur de servir les clients DHCPv6 légitimes et réguliers ainsi que les demandeurs LEASEQUERY DHCPv6 légitimes, déniant les configurations aux clients DHCPv6 légitimes ainsi que les informations de prêt aux demandeurs LEASEQUERY DHCPv6 légitimes. Bien que ces attaques soient peu probables quand on communique seulement avec des demandeurs LEASEQUERY de confiance, la possibilité existe toujours que la confiance soit mal placée, que les techniques de sécurité soient compromises, ou même que des demandeurs de confiance puissent avoir des bogues. Donc, les techniques pour se défendre contre les attaques de déni de service par inondation de paquets sont toujours une bonne idée, et elles incluent un bon périmètre de sécurité, comme mentionné précédemment, et la limitation du taux de trafic DHCPv6 par les agents de relais, d'autres éléments de réseau, ou le serveur lui-même.

Une façon d'attaquer un concentrateur d'accès (par opposition à un serveur DHCPv6) comme un demandeur LEASEQUERY est l'établissement d'un serveur malveillant avec l'intention de fournir des informations de prêt ou d'acheminement incorrectes dans le concentrateur d'accès, déjouant la vérification de l'adresse de source IPv6, et empêchant un acheminement correct. Ce type d'attaque peut être minimisé en utilisant IPsec comme décrit au paragraphe 21.1 de la [RFC3315].

6. Considérations relatives à l'IANA

L'IANA a alloué les nouveaux types de messages DHCPv6 suivants dans le registre tenu à http://www.iana.org/assignments/dhcpv6-parameters :

LEASEQUERY
LEASEQUERY-REPLY

L'IANA a alloué les nouveaux codes d'option DHCPv6 dans le registre tenu à http://www.iana.org/assignments/dhcpv6-parameters :

OPTION_LQ_QUERY
OPTION_CLIENT_DATA
OPTION_CLT_TIME
OPTION_LQ_RELAY_DATA
OPTION_LQ_CLIENT_LINK

L'IANA a alloué t les nouveaux codes d'état DHCPv6 suivants dans le registre tenu à http://www.iana.org/assignments/dhcpv6-parameters :

UnknownQueryType
MalformedQuery
NotConfigured
NotAllowed

L'IANA a créé un nouveau registre pour les codes de type d'interrogation d'option OPTION_LQ_QUERY dans le registre tenu à http://www.iana.org/assignments/dhcpv6-parameters avec les allocations initiales suivantes :

QUERY_BY_ADDRESS 1
QUERY_BY_CLIENTID 2

Le nouveaux codes de type d'interrogation d'option OPTION_LQ_QUERY sont alloués par action de normalisation, comme défini dans la [RFC2434].

7. Remerciements

Merci à Ralph Droms, Richard Johnson, Josh Littlefield, Hemant Singh, Pak Siripunkaw, Markus Stenberg, et Ole Troan de leurs apports, idées, et relecture durant la production de ce document.

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3633] O. Troan, R. Droms, "Options de préfixes IPv6 pour le protocole de configuration dynamique d'hôte (DHCP) version 6", décembre 2003. (*MàJ par la* RFC6603) *(P.S. ; Obsolète voir* RFC8415)

[RFC4388] R. Woundy, K. Kinnear, "Protocole Leasequery dans le protocole de configuration dynamique d'hôte (DHCP)", février 2006. *(P.S.)*

8.2 Références pour information

[BPPIS] CableLabs, "Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification CM-SP-BPI+_I12-050812", août 2005, disponible à http://www.cablemodem.com/.

[DOCSIS] SCTE Data Standards Subcommittee, "Data-Over-Cable Service Interface Specifications: DOCSIS 1.0 Baseline Privacy Interface Specification SCTE 22-2 2002", 2002, disponible à http://www.scte.org/standards/.

[MULPI] CableLabs, "Data-Over-Cable Service Interface Specifications: DOCSIS 3.0, MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I04-070518", mai 2007, disponible à http://www.cablemodem.com/.

[RAAN] Droms, R., "DHCPv6 Relay Agent Assignment Notification (RAAN) Option", Travail en cours, novembre 2006.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

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

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

Adresse des auteurs

John Jason Brzozowski
Comcast Cable
1800 Bishops Gate Boulevard
Mt. Laurel, NJ 08054
USA
téléphone : +1 856 324 2671
mél : john_brzozowski@cable.comcast.com

Kim Kinnear
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
téléphone : +1 978 936 0000
mél : kkinnear@cisco.com

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
téléphone : +1 978 936 0000
mél : volz@cisco.com

Shengyou Zeng
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
téléphone : +1 978 936 0000
mél : szeng@cisco.com

Déclaration complète de droits de reproduction

présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).