Groupe de travail Réseau
Request for Comments : 4704
Catégorie : Sur la voie de la normalisation

B. Volz, Cisco Systems, Inc.
octobre 2006
Traduction Claude Brière de L'Isle

Option de nom de domaine pleinement qualifié (FQDN) de client du protocole de configuration dynamique d'hôte (DHCPv6)

Résumé
Le présent document spécifie une nouvelle option du protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) qui peut être utilisée pour échanger des informations sur le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) d'un client DHCPv6 et sur la responsabilité de la mise à jour des enregistrements de ressource (RR, *resource record*) du DNS relatives aux allocations d'adresse du client.

Table des matières

1. Introduction

Le DNS ([RFC1034], [RFC1035]) contient (entre autres choses) les informations sur la transposition entre les noms de domaine pleinement qualifiés (FQDN) [RFC1594] des hôtes et les adresses IPv6 allouées aux hôtes. Les informations sont maintenues dans deux types d'enregistrements de ressource (RR) : AAAA et PTR [RFC3596]. La spécification de mise à jour du DNS [RFC2136] décrit un mécanisme qui permet que les informations du DNS soient mises à jour sur un réseau.

Le protocole de configuration dynamique d'hôte pourIPv6 (DHCPv6) [RFC3315] fournit un mécanisme par lequel un hôte (un client DHCPv6) peut acquérir certaines informations de configuration, ainsi que sa ou ses adresses IPv6 à états pleins.

Le présent document spécifie une nouvelle option DHCPv6, l'option FQDN de client, qui peut être utilisée par les clients et serveurs DHCPv6 pour échanger des informations sur le nom de domaine pleinement qualifié de client et sur qui a la responsabilité de mettre à jour le DNS avec les RR AAAA et PTR associés.

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].

On suppose le lecteur familiarisé avec le protocole de mise à jour du DNS [RFC2136] et avec DHCPv6 et sa terminologie, comme définie dans la [RFC3315].

3. Modèles de fonctionnement

Quand un client DHCPv6 acquiert une adresse, un administrateur de site peut désirer que le RR AAAA pour le FQDN du client et le RR PTR pour l'adresse acquise soient mis à jour. Donc, deux transactions séparées de mise à jour du DNS peuvent se produire. Acquérir une adresse via DHCPv6 implique deux entités : un client DHCPv6 et un serveur DHCPv6. En principe, chacune de ces entités pourrait effectuer aucune, une, ou les deux transactions de mise à jour du DNS. Cependant, en pratique, toutes les permutations n'ont pas de sens. L'option FQDN de client DHCPv6 est principalement destinée à opérer dans les deux cas suivants :
1. Le client DHCPv6 met à jour le RR AAAA ; le serveur DHCPv6 met à jour le RR PTR.
2. Le serveur DHCPv6 met à jour les deux RR AAAA et PTR.

La seule différence entre ces deux cas est si la transposition de FQDN en adresse IPv6 est mise à jour par un client ou par un serveur DHCPv6. La transposition d'adresse IPv6 en FQDN est mise à jour par un serveur DHCPv6 dans les deux cas.

La raison des deux est importante, tandis que les autres cas sont peu probables, et elle a à voir avec l'autorité sur les noms de domaines DNS respectifs. Un client DHCPv6 peut avoir l'autorité sur la transposition de ses propres RR AAAA, ou cette autorité peut être restreinte au serveur pour empêcher le client de faire une liste d'adresses arbitraires ou d'associer ses adresses à des noms de domaine arbitraires. Dans tous les cas, la seule place raisonnable pour l'autorité sur les RR PTR associés à l'adresse est dans le serveur DHCPv6 qui alloue l'adresse.

Note : un troisième cas est pris en charge dans lequel le client demande que le serveur n'effectue aucune mise à jour. Cependant, ce cas est présumé être rare à cause des problèmes d'autorité.

Dans tous les cas, qu'un site permette à tous les serveurs et clients DHCPv6, à certains, ou à aucun, d'effectuer les mises à jour du DNS dans les zones qu'ils contrôlent est entièrement une affaire de politique administrative locale. Le présent document n'exige aucune politique administrative spécifique et n'en propose pas. La gamme des politiques possibles est très large, des sites où seulement les serveurs DHCPv6 ont reçu des accréditifs que les serveurs du DNS vont accepter, aux sites où chaque client DHCPv6 individuel a été configuré avec des accréditifs qui permettent au client de modifier son propre nom de domaine. Les mises en œuvre conformes PEUVENT prendre en charge certaines de ces possibilités ou toutes. De plus, la présente spécification s'applique seulement aux processus de client et serveur DHCPv6 ; elle ne s'applique pas aux autres processus qui initient les mises à jour du DNS.

Le présent document décrit une nouvelle option DHCPv6 que peut utiliser un client pour porter tout ou partie de son nom de domaine à un serveur DHCPv6. La politique spécifique de site détermine si les serveurs DHCPv6 peuvent utiliser ou non les noms que les clients offrent, et ce que les serveurs DHCPv6 font dans les cas où les clients ne fournissent pas de nom de domaine.

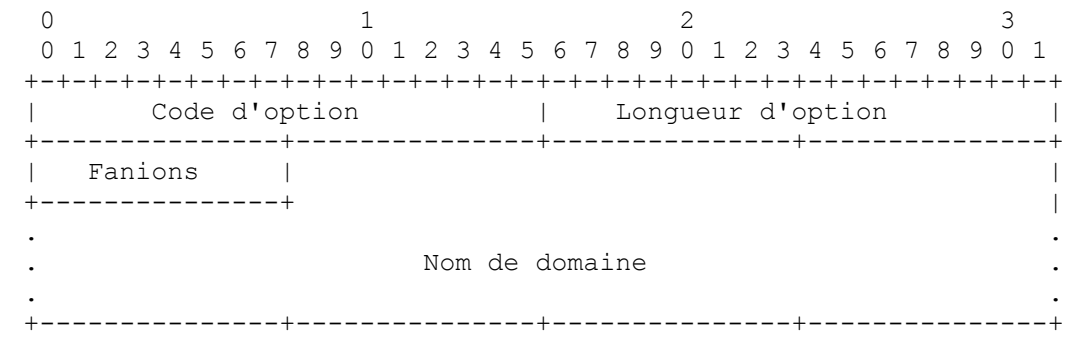
4. Option FQDN de client DHCPv6

Pour mettre à jour la transposition d'adresse IPv6 en FQDN, un serveur DHCPv6 a besoin de savoir le FQDN du client pour les adresses des liens IA_NA du client. Pour permettre au client de porter son FQDN au serveur, le présent document définit une nouvelle option DHCPv6 appelée "FQDN de client". L'option FQDN de client contient aussi des fanions

qu'utilisent les clients et serveurs DHCPv6 pour négocier qui fait quelles mises à jour.

Le code de cette option est 39. Sa longueur minimum est 1 octet.

Le format de l'option FQDN de client DHCPv6 est montré ci-dessous :



Code d'option : OPTION_CLIENT_FQDN (39)

Longueur d'option : 1 + longueur du nom de domaine.

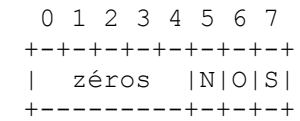
Fanions : bits de fanions utilisés entre client et serveur pour négocier qui effectue quelles mises à jour.

Nom de domaine : le nom de domaine partiel ou pleinement qualifié (avec la longueur d'option - 1)

L'option FQDN de client DOIT apparaître seulement dans le champ Options d'un message et s'applique à toutes les adresses pour tous les liens IA_NA dans la transaction.

4.1 Champ Fanions

Le format du champ Fanions est :



Le bit "S" indique si le serveur DEVRAIT ou NE DEVRAIT PAS effectuer les mises à jour de RR AAAA (de FQDN en adresse) du DNS. Un client règle le bit à 0 pour indiquer que le serveur NE DEVRAIT PAS effectuer les mises à jour et à 1 pour indiquer que le serveur DEVRAIT effectuer les mises à jour . L'état du bit dans la réponse du serveur indique l'action à entreprendre par le serveur ; si c'est 1, le serveur a pris la responsabilité des mises à jour de RR AAAA pour le FQDN.

Le bit "O" indique si le serveur a outrepassé la préférence du client pour le bit "S". Un client DOIT régler ce bit à 0. Un serveur DOIT régler ce bit à 1 si le bit "S" dans sa réponse au client ne correspond pas au bit "S" reçu du client.

Le bit "N" indique si le serveur NE DEVRAIT PAS effectuer du tout de mise à jour du DNS. Un client règle ce bit à 0 pour demander que le serveur DEVRAIT effectuer les mises à jour (du RR PTR et éventuellement du RR AAAA sur la base du bit "S") ou à 1 pour demander que le serveur NE DEVRAIT PAS effectuer du tout de mise à jour du DNS. Un serveur règle le bit "N" pour indiquer si le serveur DEVRA (0) ou NE DEVRA PAS (1) effectuer les mises à jour du DNS. Si le bit "N" est à 1, le bit "S" DOIT être 0.

Les bits restants du champ Fanions sont réservés pour des allocations futures. Les clients et serveurs DHCPv6 qui envoient l'option FQDN de client DOIVENT mettre à zéro ces bits, et ils DOIVENT les ignorer à réception.

4.2 Champ Nom de domaine

La partie Nom de domaine de l'option porte tout ou partie du FQDN d'un client DHCPv6. Les données dans le champ Nom de domaine DOIVENT être codées comme décrit à la Section 8 de la [RFC3315]. Afin de déterminer si le FQDN a changé entre les échanges de messages, le client et le serveur NE DOIVENT PAS altérer le contenu du champ Nom de domaine

sauf si le FQDN a réellement changé.

Un client PEUT être configuré avec un nom de domaine pleinement qualifié ou avec un nom partiel qui n'est pas pleinement qualifié. Si un client connaît seulement une partie de son nom, il PEUT envoyer un nom qui n'est pas pleinement qualifié, indiquant qu'il connaît une partie du nom mais pas nécessairement la zone dans laquelle le nom va être incorporé.

Pour envoyer un nom de domaine pleinement qualifié, le champ Nom de domaine est réglé au nom de domaine codé du DNS incluant l'étiquette de longueur zéro de terminaison. Pour envoyer un nom partiel, le champ Nom de domaine est réglé au nom de domaine codé du DNS sans l'étiquette de longueur zéro de terminaison.

Un client PEUT aussi laisser vide le champ Nom de domaine si il désire que le serveur fournisse un nom.

Les serveurs DEVRAIENT envoyer le nom de domaine pleinement qualifié complet dans les options FQDN de client.

5. Comportement du client DHCPv6

On décrit ci-après le comportement d'un client DHCPv6 qui met en œuvre l'option FQDN de client.

Un client DOIT seulement inclure l'option FQDN de client dans les messages SOLICIT, REQUEST, RENEW, ou REBIND.

Un client qui envoie l'option FQDN de client DOIT aussi inclure l'option dans l'option Demande d'option si il s'attend à ce que le serveur inclue l'option FQDN de client dans toutes les réponses.

5.1 Le client désire mettre à jour les RR AAAA

Si un client qui possède/maintient son propre FQDN veut être responsable de la mise à jour de la transposition de FQDN en adresse IPv6 pour le FQDN et la ou les adresses utilisés par le client, le client DOIT inclure l'option FQDN de client dans le message SOLICIT avec engagement rapide, REQUEST, RENEW, et REBIND généré par le client. Un client PEUT choisir d'inclure l'option FQDN de client dans ses messages SOLICIT. Les bits "S", "O", et "N" dans le champ Fanions de l'option DOIVENT être à 0.

Une fois que la configuration DHCPv6 du client est achevée (le client reçoit un message REPLY et réalise avec succès une vérification finale des paramètres passés dans le message) le client PEUT générer une mise à jour pour les RR AAAA (associés au FQDN du client) sauf si le serveur a réglé le bit "S" à 1. Si le bit "S" est 1, le client DHCPv6 NE DEVRAIT PAS initier de mise à jour pour le nom dans le champ Nom de domaine de l'option FQDN de client retournée par le serveur. Cependant, un client DHCPv6 qui est explicitement configuré avec un FQDN PEUT ignorer l'état du bit "S" si le nom retourné par le serveur correspond au nom configuré du client.

5.2 Le client désire que le serveur fasse les mises à jour du DNS

Un client peut choisir de déléguer au serveur la responsabilité de la mise à jour de la transposition de FQDN en adresse IPv6 pour le FQDN et la ou les adresses utilisés par le client. Afin d'informer le serveur de ce choix, le client DEVRAIT inclure l'option FQDN de client dans ses messages SOLICIT avec engagement rapide, REQUEST, RENEW, et REBIND, et PEUT inclure l'option FQDN de client dans son SOLICIT. Le bit "S" dans le champ Fanions dans l'option DOIT être 1, et les bits "O" et "N" DOIVENT être à 0.

5.3 Le client désire qu'il n'y ait pas de mises à jour du DNS par le serveur

Un client peut choisir de demander que le serveur n'effectue aucune mise à jour du DNS en son nom. Afin d'informer le serveur de ce choix, le client DEVRAIT inclure l'option FQDN de client dans ses messages SOLICIT avec engagement rapide, REQUEST, RENEW, et REBIND, et PEUT inclure l'option FQDN de client dans son SOLICIT. Le bit "N" bit dans le champ Fanions dans l'option DOIT être 1, et les bits "S" et "O" DOIVENT être à 0.

Une fois que la configuration DHCPv6 du client est achevée (le client reçoit un message REPLY et réalise avec succès une vérification finale des paramètres passés dans le message) le client PEUT générer ses mises à jour du DNS pourvu que le

bit "N" du serveur soit 1. Si le bit "N" du serveur est 0, le serveur PEUT effectuer les mises à jour de RR PTR ; il PEUT aussi effectuer les mises à jour de RR AAAA si le bit "S" est 1.

5.4 Questions de mise à jour de nom de domaine et du DNS

Comme il y a une possibilité que le serveur DHCPv6 soit configuré à compléter ou remplacer un nom de domaine que le client envoie, le client PEUT trouver utile d'envoyer l'option FQDN de client dans ses messages SOLICIT. Si le serveur DHCPv6 retourne des données différentes de nom de domaine dans son message ADVERTISE, le client pourrait utiliser ces données pour effectuer sa propre mise à jour éventuelle de RR AAAA, ou pour former l'option FQDN de client qu'il envoie dans ses messages suivants. Il n'est pas exigé que le client envoie des données d'option FQDN de client identiques dans ses messages SOLICIT, REQUEST, RENEW, ou REBIND. En particulier, si un client a envoyé l'option FQDN de client à son serveur, et si la configuration du client change de telle sorte que sa notion de son nom de domaine change, il PEUT envoyer les nouvelles données de nom dans une option FQDN de client quand il communique à nouveau avec le serveur. Cela PEUT être cause que le serveur DHCPv6 mette à jour le nom associé aux enregistrements PTR et, si le serveur a mis à jour l'enregistrement AAAA qui représente le client, qu'il supprime cet enregistrement et tente une mise à jour pour le nom de domaine actuel du client.

Un client qui délègue la responsabilité de la mise à jour de la transposition de FQDN en adresse IPv6 à un serveur ne va recevoir aucune indication (ni positive ni négative) de la part du serveur sur si le serveur a été capable d'effectuer la mise à jour. Le client PEUT utiliser une interrogation du DNS pour vérifier si la transposition est à jour. Cependant, selon la charge sur les serveurs DHCPv6 et DNS et les délais de propagation du DNS, le client peut seulement déduire le succès. Si les informations se trouvent ne pas être à jour dans le DNS, les serveurs d'autorité pourraient ne pas avoir achevé les mises à jour ou les transferts de zone, ou les résolveurs d'antémémoire peuvent ne pas avoir encore mis à jour leurs antémémoires.

Si un client libère une adresse avant l'heure d'expiration de la durée de vie valide et si le client est responsable de la mise à jour de son RR AAAA, le client DEVRAIT supprimer le RR AAAA associé à l'adresse avant d'envoyer un message RELEASE. De même, si un client est responsable de la mise à jour de ses RR AAAA, mais est incapable de renouveler les durées de vie pour une adresse, le client DEVRAIT tenter de supprimer le RR AAAA avant que la durée de vie de l'adresse ne soit plus valide. Un client DHCPv6 qui n'a pas été capable de supprimer un RR AAAA qu'il avait ajouté DEVRAIT tenter de le notifier à son administrateur, peut-être en émettant un message dans le journal d'événements.

Un client NE DEVRAIT PAS effectuer de mises à jour du DNS sur les RR AAAA pour des adresses d'envoi individuel non mondiales [RFC4291] ou des adresses temporaires [RFC3041].

6. Comportement du serveur DHCPv6

On décrit ci-après le comportement d'un serveur DHCPv6 qui met en œuvre l'option FQDN de client quand le message du client inclut l'option FQDN de client.

Les serveurs DOIVENT seulement inclure une option FQDN de client dans les messages ADVERTISE et REPLY si le client a inclus une option FQDN de client et si l'option FQDN de client est demandée par l'option Demande d'option dans le message du client auquel le serveur répond.

On décrit ci-après le comportement d'un serveur DHCP qui met en œuvre l'option FQDN de client quand le message du client inclut l'option FQDN de client.

- Le serveur règle à 0 les bits "S", "O", et "N" dans sa copie de l'option qu'il va retourner au client.

- Si bit "N" du client est 1 et si la configuration du serveur lui permet d'honorer la demande du client de ne pas avoir de mises à jour du DNS initiées par le serveur, le serveur règle le bit "N" à 1.

- Autrement, si le bit "S" du client est 1 et si la configuration du serveur lui permet d'honorer la demande du client que le serveur initie les mises à jour de RR AAAA du DNS, le serveur règle le bit "S" à 1. Si le bit "S" du serveur ne correspond pas au bit "S" du client, le serveur règle le bit "O" à 1.

Le serveur PEUT être configuré à utiliser le nom fourni dans l'option FQDN de client du client, ou il PEUT être configuré à modifier le nom fourni ou à substituer un nom différent. Le serveur DEVRAIT envoyer sa notion de FQDN complet pour le client dans le champ Nom de domaine. Le serveur PEUT simplement copier le champ Nom de domaine de l'option

FQDN de client que le client a envoyé au serveur.

6.1 Quand effectuer les mises à jour du DNS

Le serveur NE DEVRAIT PAS effectuer de mises à jour du DNS si le bit "N" est à 1 dans le champ Fanions de l'option FQDN de client dans les messages REPLY à envoyer au client. Cependant, le serveur DEVRAIT supprimer tous les RR qu'il avait ajoutés précédemment via des mises à jour du DNS pour le client.

Le serveur PEUT effectuer la mise à jour du RR PTR du DNS (sauf si le bit "N" est à 1).

Le serveur PEUT effectuer la mise à jour du RR AAAA du DNS si le bit "S" est à 1 dans le champ Fanions de l'option FQDN de client dans le message REPLY à envoyer au client.

Le serveur PEUT effectuer ces mises à jour même si le message du client ne portait pas l'option FQDN de client. Le serveur NE DOIT PAS initier des mises à jour du DNS quand il répond par un message ADVERTISE au client.

Le serveur PEUT compléter ses mises à jour du DNS (RR PTR ou PTR et RR AAAA) avant ou après l'envoi du message REPLY au client.

Si la mise à jour du RR AAAA du DNS par le serveur ne s'achève pas avant que le serveur ait répondu au client DHCPv6, l'interaction du serveur avec le serveur DNS PEUT être cause que le serveur DHCPv6 change le nom de domaine qu'il a associé au client. Cela peut se produire, par exemple, si le serveur détecte et résout un conflit de nom de domaine [RFC4703]. Dans ce cas, le nom de domaine que le serveur retourne au client DHCPv6 va changer entre deux échanges DHCPv6.

Si le serveur a effectué précédemment des mises à jour du DNS pour le client et si les informations du client n'ont pas changé, le serveur PEUT sauter les mises à jour supplémentaires du DNS.

Quand un serveur reçoit un RELEASE ou DECLINE pour une adresse, détecte que la durée de vie valide sur une adresse que le serveur lie à un client a expiré, ou termine un lien sur une adresse avant l'heure d'expiration du lien (par exemple, en envoyant un REPLY avec une durée de vie valide de zéro pour une adresse) le serveur DEVRAIT supprimer tous les RR PTR qu'il avait associés à l'adresse via une mise à jour du DNS. De plus, si le serveur a pris la responsabilité des RR AAAA, le serveur DEVRAIT aussi supprimer les RR AAAA.

7. TTL de RR du DNS

Les RR associés aux clients DHCP peuvent être plus volatiles que les RR à configuration statique. Les clients et serveurs DHCP qui effectuent des mises à jour dynamiques devraient tenter de spécifier des durées de vie d'enregistrement de ressource qui reflètent cette volatilité, afin de minimiser la possibilité que les réponses aux interrogations du DNS retournent des enregistrements qui se réfèrent à des allocations DHCP d'adresse IP qui ont expiré ou ont été libérées.

Le couplage entre serveurs primaires, secondaires, et d'antémémoire du DNS est "souple" ; c'est une partie fondamentale de la conception du DNS. Cette souplesse rend impossible d'empêcher toutes les situations possibles dans lesquelles un résolveur peut retourner un enregistrement reflétant une adresse IP allouée par DHCP qui a expiré ou a été libérée. Dans la réalité, cela représente rarement, si il en est, un problème significatif. La plupart des clients gérés par DHCP sont rarement recherchés par noms dans le DNS, et le déploiement de IXFR [RFC1995] et NOTIFY [RFC1996] peut réduire la latence entre les mises à jour et leur visibilité sur les serveurs secondaires.

On suggère ces lignes directrices de base pour les mises en œuvre. En général, les TTL pour les RR ajoutés par suite d'une activité DHCP d'allocation d'adresse IP DEVRAIENT être inférieurs à la durée de vie initiale. Le TTL de RR sur un enregistrement DNS ajouté NE DEVRAIT PAS excéder 1/3 de la durée de vie, mais NE DEVRAIT PAS être moins de 10 minutes. On reconnaît que les administrateurs individuels auront des exigences variées : les serveurs et clients DHCP DEVRAIENT permettre aux administrateurs de configurer les TTL et des limites supérieures et inférieures des valeurs de TTL, soit comme un intervalle en temps absolu, soit comme un pourcentage de la durée de vie du prêt.

Bien que clients et serveurs PUISSENT mettre à jour le TTL sur les enregistrements lorsque la durée de vie est sur le point d'expirer, il n'est pas exigé qu'ils le fassent car cela fait peser une charge supplémentaire sur le système du DNS sans véritable contrepartie.

8. Conflits de mise à jour du DNS

Le présent document ne traite pas de la façon dont un client ou serveur DHCPv6 prévient les conflits de nom. Le présent document traite seulement comment un client et un serveur DHCPv6 négocient le nom de domaine pleinement qualifié et qui va effectuer les mises à jour du DNS.

Les mises en œuvre de ce travail vont devoir considérer comment empêcher les conflits de noms. Si une mise à jour du DNS a besoin d'un jeton de sécurité afin d'effectuer avec succès les mises à jour du DNS sur un nom spécifique, des conflits de noms ne peuvent survenir que si plusieurs mises à jour reçoivent un jeton de sécurité pour ce nom. Ou, si les domaines pleinement qualifiés se fondent sur le lien d'adresse spécifique avec un client, les conflits n'auront pas lieu. Ou, une technique de résolution de conflit de noms comme décrite dans "Résolution des conflits de noms" [RFC4703]) DEVRAIT être utilisé.

9. Considérations relatives à l'IANA

L'IANA a alloué le code d'option DHCPv6 de 39 à l'option FQDN de client.

10. Considérations de sécurité

Les mises à jour non authentifiées du DNS peuvent conduire à une confusion terrible, par une attaque malveillante ou par une mauvaise configuration accidentelle. Les administrateurs doivent être attentifs à ne pas permettre de mises à jour non sécurisées du DNS sur des zones qui sont exposées à l'Internet mondial. Les clients et serveurs DHCPv6 devraient tous utiliser une forme de procédure d'authentification d'origine des demandes de mettre à jour (par exemple, la mise à jour dynamique sécurisée du DNS [RFC3007]) quand ils effectuent des mises à jour du DNS.

Qu'un client DHCPv6 soit responsable de la mise à jour d'une transposition de FQDN en adresse IPv6 ou que ce soit de la responsabilité du serveur DHCPv6 est une affaire de site local. Le choix entre les deux alternatives est probablement fondé sur le modèle de sécurité qui est utilisé avec le protocole de mise à jour du DNS (par exemple, seul un client peut avoir des accréditifs suffisants pour effectuer les mises à jour de transposition de FQDN en adresse IPv6 pour son FQDN).

Qu'un serveur DHCPv6 soit toujours responsable de la mise à jour de transposition de FQDN en adresse IPv6 (en plus de la mise à jour de transposition d'adresse IPv6 en FQDN) sans considération des souhaits d'un client DHCPv6 individuel, est aussi une affaire de site local. Le choix entre les deux alternatives est probablement fondé sur le modèle de sécurité qui est utilisé avec les mises à jour du DNS. Dans les cas où un serveur DHCPv6 effectue les mises à jour du DNS au nom d'un client, le serveur DHCPv6 devrait être sûr du nom DNS à utiliser pour le client, et de l'identité du client.

Selon la présence ou le type d'authentification utilisé avec l'option Authentification, un serveur DHCPv6 peut n'avoir qu'une confiance limitée dans l'identité de ses clients. Il y a de nombreuses façons pour un serveur DHCP de développer un nom DNS à utiliser pour un client, mais seulement dans certaines circonstances relativement inhabituelles le serveur DHCP pourra tenir pour certaine l'identité du client.

Il est critique de mettre en œuvre une résolution de conflit appropriée, et les considérations de sécurité de la résolution de conflit de la [RFC4703] s'appliquent ici.

11. Remerciements

Tous nos remerciements à Mark Stapp et Yakov Rekhter, car le présent document se fonde sur l'option FQDN de client DHCPv4 [RFC4702], et à Ralph Droms, Ted Lemon, Josh Littlefield, Kim Kinnear, Pekka Savola, et Mark Stapp pour leur relecture et leurs commentaires.

12. Références

12.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

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

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

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

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

[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)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

[RFC4703] M. Stapp, B. Volz, "Résolution des conflits de nom de domaine pleinement qualifié (FQDN) entre clients du protocole de configuration dynamique d'hôte (DHCP)", octobre 2006. *(P.S.)*

12.2 Références pour information

[RFC1594] A. Marine, J. Reynolds, G. Malkin, "Réponses aux questions les plus fréquentes des "nouveaux utilisateurs de l'Internet"", mars 1994. *(Information, remplacée par la* RFC2664)

[RFC1995] M. Ohta, "Transferts de zone par incréments dans le DNS", RFC 1995, août 1996.

[RFC1996] P. Vixie, "Mécanisme de notification rapide des changements de zone (DNS NOTIFY)", août 1996. *(P.S.)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000.

[RFC3596] S. Thomson et autres, "Extensions au DNS pour la prise en charge de IPv6", octobre 2003. *(D.S.)*

[RFC4702] M. Stapp et autres, "Option de nom de domaine pleinement qualifié (FQDN) de client du protocole de configuration dynamique d'hôte (DHCP)", octobre 2006. *(P.S.)*

Adresse de l'auteur

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

téléphone : +1 978 936 0382
mél : volz@cisco.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la 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 actuellement assuré par l'activité de soutient administratif de l'IETF (IASA).