Groupe de travail Réseau
Request for Comments : 4702
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Stapp, Cisco Systems
B. Volz, Cisco Systems
Y. Rekhter, Juniper Networks
octobre 2006

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

Résumé
Le présent document décrit une option du protocole de configuration dynamique d'hôte pour IPv4 (DHCPv4, *Dynamic Host Configuration Protocol for IPv4*) qui peut être utilisée pour échanger des informations sur le nom de domaine pleinement qualifié d'un client DHCPv4 et sur la responsabilité de la mise à jour des enregistrements de ressource du DNS relatifs à l'allocation d'adresse du client.

Table des matières

1. Introduction

Le DNS ([RFC1034], [RFC1035]) conserve (entre autres choses) les informations sur la transposition entre les noms de domaine pleinement qualifiés (FQDN, *Fully Qualified Domain Name*) [RFC1594] des hôtes et les adresses IP allouées au hôtes. Les informations sont conservées dans deux types d'enregistrements de ressource (RR, *Resource Record*) : A et PTR. La spécification de mise à jour du DNS [RFC2136] décrit un mécanisme qui permet aux informations du DNS d'être mises

à jour sur un réseau.

Le protocole de configuration dynamique d'hôte pour IPv4 (DHCPv4, *Dynamic Host Configuration Protocol for IPv4*) (ou juste DHCP dans le présent document) [RFC2131] fournit un mécanisme par lequel un hôte (un client DHCP) peut acquérir certaines informations de configuration, ainsi que son adresse. Le présent document spécifie une option DHCP, l'option FQDN de client, qui peut être utilisée par les clients et serveurs DHCP pour échanger des informations sur le nom de domaine pleinement qualifié du client pour une adresse et qui a la responsabilité de mettre à jour le DNS avec les RR A et PTR associés.

1.1 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].

1.2 Modèles de fonctionnement

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

1. Le client DHCP met à jour le RR A, le serveur DHCP met à jour le RR PTR.
2. Le serveur DHCP met à jour les deux RR A et PTR.

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

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

Note : un troisième cas est accepté : le client demande que le serveur n'effectue pas de mise à jour. Cependant, ce cas est présumé être rare à cause des problèmes d'autorité.

Il est considéré qu'il relève de la politique locale de permettre aux clients et serveurs DHCP d'effectuer les mises à jour du DNS aux zones. Le présent document n'exige aucune politique administrative spécifique et n'en propose pas. De plus, la présente spécification s'applique seulement aux processus de client et serveur DHCP ; elle ne s'applique pas aux autres processus qui initient les mises à jour du DNS.

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

2. Option FQDN de client

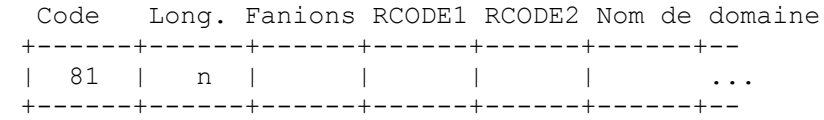
Pour mettre à jour la transposition d'adresse IP en FQDN, un serveur DHCP a besoin de connaître le FQDN du client auquel le serveur prête l'adresse. Pour permettre au client de porter son FQDN au serveur, le présent document définit une nouvelle option DHCP, appelée "FQDN de client". L'option FQDN de client contient aussi des fanions, que les serveurs DHCP peuvent utiliser pour porter aux clients des informations sur les mises à jour du DNS, et deux RCODE déconseillés.

Les clients PEUVENT envoyer l'option FQDN de client, en réglant les valeurs de fanions appropriées, dans leurs messages DHCPDISCOVER et DHCPREQUEST. Si un client envoie l'option FQDN de client dans son message DHCPDISCOVER, il DOIT envoyer l'option dans les messages DHCPREQUEST suivants malgré le changement du contenu de l'option.

Une seule option FQDN de client PEUT apparaître dans un message, bien qu'elle puisse être instanciée dans un message comme plusieurs options [RFC3396]. Les clients et serveurs DHCP qui prennent en charge cette option DOIVENT mettre en œuvre l'enchaînement d'options DHCP [RFC3396]. Dans la terminologie de la [RFC3396], l'option FQDN de client est une option qui exige l'enchaînement.

Le code de cette option est 81. Longueur contient le nombre d'octets qui suivent le champ Longueur, et la valeur minimum est 3 (octets).

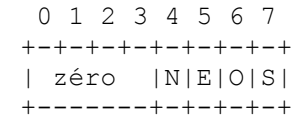
Le format de l'option FQDN de client est :



La figure ci-dessus suit les conventions de la [RFC2132].

2.1 Champ Fanions

Le format du champ Fanions de un octet est :



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

Le bit "E" indique le codage du champ Nom de domaine. 1 indique le format canonique du réseau, sans compression, comme décrit au paragraphe 3.1 de la [RFC1035]. Ce codage DEVRAIT être utilisé par les clients et DOIT être pris en charge par les serveurs. 0 indique un codage ASCII maintenant déconseillé (voir au paragraphe 2.3.1). Un serveur DOIT utiliser le même codage qu'utilisé par le client. Un serveur qui ne prend pas en charge le codage ASCII déconseillé DOIT ignorer les options FQDN de client qui utilisent ce codage.

Les bits restants dans le champ Fanions sont réservés pour de futures allocations. Les clients et serveurs DHCP qui envoient l'option FQDN de client DOIVENT régler à zéro les bits zéro et ils DOIVENT ignorer ces bits.

2.2 Champs RCODE

Les deux champs d'un octet RCODE1 et RCODE2 sont déconseillés. Un client DEVRAIT les régler à 0 quand il envoie l'option et DEVRAIT les ignorer à réception. Un serveur DEVRAIT les régler à 255 quand il envoie l'option et DOIT les ignorer à réception.

Comme cette option avec ces champs est déjà largement utilisée, les champs sont conservés. Ces champs étaient à l'origine définis pour être utilisés par un serveur DHCP pour indiquer au client DHCP le code de réponse de tout RR A (RCODE1) ou PTR (RCODE2) mis à jour du DNS qu'il a effectué, ou une valeur de 255 était utilisée pour indiquer qu'une mise à jour avait été initiée mais pas encore achevée. Chacun de ces champs fait un octet. Ces champs ont été définis avant EDNS0 [RFC2671], qui décrit un mécanisme pour étendre la longueur d'un RCODE DNS à 12 bits, qui est une autre raison pour les

déconseiller.

Si le client a besoin de confirmer que la mise à jour du DNS a été faite, il PEUT utiliser une interrogation du DNS pour vérifier si la transposition est à jour. Cependant, selon la charge sur les serveurs DHCP et DNS et les délais de propagation du DNS, le client peut seulement déduire le succès. Si les informations ne sont pas 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 avoir déjà mis à jour leurs antémémoires.

2.3 Champ Nom de domaine

La partie Nom de domaine de l'option porte tout ou partie du FQDN d'un client DHCP. Les données dans le champ Nom de domaine DEVRAIENT apparaître dans le format canonique du réseau comme spécifié au paragraphe 3.1 de la [RFC1035]. Si le client DHCP utilise le format canonique du réseau, il DOIT régler le bit "E" dans le champ Fanions à 1. 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 doit 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.

2.3.1 Codage ASCII déconseillé

Une population substantielle de clients a mis en œuvre un projet antérieur de la présente spécification, qui permettait un codage ASCII du champ Nom de domaine. Les mises en œuvre de serveurs DEVRAIENT être conscientes que les clients qui envoient l'option FQDN de client avec le bit "E" réglé à 0 utilisent un codage ASCII du champ Nom de domaine. Les serveurs PEUVENT être prêts à retourner une version codée en ASCII du champ Nom de domaine à de tels clients. Les serveurs qui ne sont pas prêts à retourner une version codée en ASCII DOIVENT ignorer l'option FQDN de client si le bit "E" est 0. L'utilisation du codage ASCII dans cette option DEVRAIT être considérée comme déconseillée.

Un client DHCP qui utilise le codage ASCII avait la permission de suggérer une seule étiquette si il n'était pas configuré avec un nom de domaine pleinement qualifié. De tels clients envoient une seule étiquette comme une série de caractères ASCII dans le champ Nom de domaine, excluant le caractère "." (point).

Les clients et serveurs DEVRAIENT suivre les règles de jeu de caractères de la Section 4 de la [RFC0952], ("Hypothèses") dans les cinq premières phrases, telles que modifiées par le paragraphe 2.1 de la [RFC1123]. Cependant, les mises en œuvre DEVRAIENT aussi savoir que certains logiciels de client peuvent envoyer des données destinées à être dans d'autres jeux de caractères. La présente spécification n'exige pas la prise en charge d'autres jeux de caractères.

3. Comportement du client DHCP

Ce qui suit décrit le comportement d'un client DHCP qui met en œuvre l'option FQDN de client.

3.1 Interaction avec les autres options

D'autres options DHCP PEUVENT porter des données relatives au champ Nom de domaine de l'option FQDN de client. L'option Nom d'hôte de la [RFC2132], par exemple, contient une représentation en chaîne ASCII du nom d'hôte du client. En général, un client n'a pas besoin d'envoyer des données redondantes, et donc, les clients qui envoient l'option FQDN de client dans leurs messages NE DOIVENT PAS envoyer aussi l'option Nom d'hôte. Les clients qui reçoivent les deux options Nom d'hôte et l'option FQDN de client d'un serveur DEVRAIENT préférer les données d'option FQDN de client. La Section 4 donne pour instruction aux serveurs d'ignorer l'option Nom d'hôte dans les messages de client qui incluent l'option FQDN de client.

3.2 Le client désire mettre à jour des RR

Si un client qui possède/maintient son propre FQDN veut être responsable de la mise à jour de la transposition de FQDN en adresse IP pour le FQDN et la ou les adresses utilisées par le client, le client DOIT inclure l'option FQDN de client dans le message DHCPREQUEST qu'il génère. Un client DHCP PEUT choisir d'inclure l'option FQDN de client dans ses messages DHCPDISCOVER ainsi que dans ses messages DHCPREQUEST. Les bits "S", "O", et "N" dans le champ Fanions de l'option DOIVENT être à 0.

Une fois que la configuration DHCP du client est achevée (le client reçoit un message DHCPACK et achève avec succès une vérification finale sur les paramètres passés dans le message) le client PEUT générer une mise à jour pour le RR A (associé au FQDN du client) sauf si le serveur a réglé le bit "S" à 1. Si le bit "S" est 1, le client DHCP NE DEVRAIT PAS initier une 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 DHCP 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.

3.3 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 IP pour le FQDN et la ou les adresses utilisées par le client. Afin d'informer le serveur de ce choix, le client DEVRAIT inclure l'option FQDN de client dans son message DHCPREQUEST et PEUT inclure l'option FQDN de client dans son DHCPDISCOVER. Le bit "S" dans le champ Fanions de l'option DOIT être 1, et les bits "O" et "N" DOIVENT être 0.

3.4 Le client ne désire aucune mise à jour du DNS par le serveur

Un client peut choisir de demander que le serveur n'effectue pas de 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 son message DHCPREQUEST et PEUT inclure l'option FQDN de client dans son DHCPDISCOVER. Le bit "N" dans le champ Fanions de l'option DOIT être 1, et les bits "S" et "O" DOIVENT être 0.

Une fois que la configuration DHCP du client est achevée (le client reçoit un message DHCPACK et achève avec succès une vérification finale sur les paramètres passés dans le message) le client PEUT générer ses mises à jour du DNS pourvu que le bit "N" du serveur soit à 1. Si le bit "N" du serveur est à 0, le serveur PEUT effectuer les mises à jour de RR PTR ; il PEUT aussi effectuer les mises à jour de RR A si le bit "S" est à 1.

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

Comme il y a une possibilité que le serveur DHCP soit configuré à compléter ou remplacer un nom de domaine qu'envoie le client, le client PEUT trouver utile d'envoyer l'option FQDN de client dans ses messages DHCPDISCOVER. Si le serveur DHCP retourne des données de nom de domaine différentes dans son message DHCPOFFER, le client pourrait utiliser ces données pour effectuer sa propre mise à jour éventuelle de RR A, ou pour former l'option FQDN de client qu'il envoie dans son message DHCPREQUEST. Il n'est pas exigé que le client envoie des données d'option FQDN de client identiques dans ses messages DHCPDISCOVER et DHCPREQUEST. 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 causer la mise à jour par le serveur DHCP du nom associé à l'enregistrement PTR et, si le serveur a mis à jour l'enregistrement A qui représente le client, à supprimer cet enregistrement et à tenter 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 IP à un serveur ne va pas recevoir d'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 (voir au paragraphe 2.2).

Si un client libère son prêt avant l'heure d'expiration du prêt et si il est responsable de la mise à jour de son RR A, le client DEVRAIT supprimer le RR A associé à l'adresse prêtée avant d'envoyer un message DHCPRELEASE. De même, si un client était responsable de la mise à jour de son RR A, mais est incapable de renouveler son prêt, le client DEVRAIT tenter de supprimer le RR A avant l'expiration du prêt. Un client DHCP qui n'a pas été capable de supprimer un RR A qu'il a ajouté (parce qu'il a perdu l'usage de son adresse IP DHCP) DEVRAIT tenter de le notifier à son administrateur, peut-être

en émettant un message dans le journal d'événements.

Un client qui désire effectuer des mises à jour du DNS sur des RR A NE DEVRAIT PAS le faire si l'adresse du client est une adresse privée [RFC1918].

4. Comportement du serveur DHCP

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 examine sa configuration et les bits de fanion dans l'option FQDN de client du client pour déterminer comment répondre :

- Si le bit "E" du client est 0 et si le serveur ne prend pas en charge le codage ASCII (paragraphe 2.3.1) le serveur DEVRAIT ignorer 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. Le serveur copie le bit "E" du client.

- Si le bit "N" du client est 1 et si la configuration du serveur lui permet d'honorer la demande du client qu'il n'y ait pas de mise à jour du DNS initiée 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 A 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. Le serveur DOIT utiliser le même format de codage (ASCII ou DNS binaire) qu'utilisé par le client dans l'option FQDN de client dans sa DHCPDISCOVER ou DHCPREQUEST, et il DOIT régler le bit "E" dans le champ Fanions de l'option en conséquence.

Si un client envoie les deux options FQDN de client et Nom d'hôte, le serveur DEVRAIT ignorer l'option Nom d'hôte.

Le serveur DEVRAIT régler les champs RCODE1 et RCODE2 à 255 avant d'envoyer le message FQDN de client au client dans un DHCPOFFER ou DHCPACK.

4.1 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 1 dans le champ Fanions de l'option FQDN de client dans les messages DHCPACK à envoyer au client. Cependant, le serveur DEVRAIT supprimer tous les RR qu'il a précédemment ajoutés via les mises à jour du DNS pour le client.

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

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

Le serveur PEUT effectuer ces mises à jour même si le DHCPREQUEST du client ne portait pas l'option FQDN de client. Le serveur NE DOIT PAS initier de mises à jour du DNS quand il répond aux messages DHCPDISCOVER provenant d'un client.

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

Si la mise à jour de RR A du DNS du serveur n'est pas achevée après que le serveur a répondu au client DHCP, l'interaction du serveur avec le serveur DNS PEUT causer le changement par le serveur DHCP du nom de domaine qu'il associe au

client. Cela peut arriver, 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 DHCP va changer entre deux échanges DHCP.

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

Quand un serveur détecte qu'un prêt sur une adresse qu'il a prêtée à un client a expiré, le serveur DEVRAIT supprimer tous les RR PTR qu'il avait ajoutés via les mises à jour du DNS. De plus, si le serveur avait ajouté un RR A au nom du client, le serveur DEVRAIT aussi supprimer le RR A.

Quand un serveur termine un prêt sur une adresse avant l'heure d'expiration du prêt (par exemple, en envoyant un DHCPNAK à un client) le serveur DEVRAIT supprimer tout RR PTR qu'il avait associé à l'adresse via une mise à jour du DNS. De plus, si le serveur avait pris la responsabilité d'un RR A, le serveur DEVRAIT aussi supprimer ce RR A.

5. TTL de RR DNS

Les RR associés à des clients DHCP peuvent être plus volatiles que des RR configurés de façon 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 au DNS retournent des enregistrements qui se réfèrent à des allocations d'adresse DHCP qui ont expiré ou ont été libérées.

Le couplage entre serveurs DNS primaires, secondaires, et d'antémémoire 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 le monde réel, cela représente rarement un problème significatif. La plupart des clients gérés par DHCP font rarement l'objet d'une recherche par nom 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 durées de vie pour les RR ajoutés par suite d'une activité d'allocation d'adresse IP par DHCP DEVRAIENT être inférieures au temps de prêt initial. Le TTL de RR d'un enregistrement DNS ajouté NE DEVRAIT PAS excéder 1/3 du temps de prêt, mais NE DEVRAIT PAS être moins de 10 minutes. On reconnaît que les administrateurs individuels vont avoir des exigences variables : les serveurs et clients DHCP DEVRAIENT permettre aux administrateurs de configurer les TTL et des limites supérieures et inférieures sur les valeurs de TTL, soit comme intervalle de temps absolu, soit comme pourcentage du temps de prêt.

Alors que clients et serveurs PEUVENT mettre à jour le TTL des enregistrements lorsque le prêt est sur le point d'expirer, il n'est pas exigé qu'ils le fassent, car cela mettrait une charge supplémentaire sur le DNS sans grande contrepartie.

6. Conflits de mise à jour du DNS

Le présent document ne résout pas comment un client ou serveur DHCP empêche les conflits de noms. Le présent document traite seulement comment un client et un serveur DHCP négocient qui va effectuer les mises à jour du DNS et le nom de domaine pleinement qualifié demandé ou utilisé.

Les mises en œuvre du présent travail vont devoir considérer comment les conflits de noms seront empêchés. Si une mise à jour du DNS a besoin d'un jeton de sécurité afin de réussir à effectuer les mises à jour du DNS sur un nom spécifique, un conflit de nom ne peut survenir que si plusieurs mises à jour reçoivent un jeton de sécurité pour ce nom. Ou, si les domaines pleinement qualifiés se fondent sur l'adresse spécifique liée à un client, il n'y aura pas de conflit. Ou, une technique de résolution de conflit de nom comme décrite dans "Résolution des conflits de noms" [RFC4703] DEVRAIT être utilisée.

7. Considérations relatives à l'IANA

L'IANA a déjà alloué le numéro d'option DHCP 81 à l'option FQDN de client. Comme le présent document décrit l'utilisation de l'option, il est demandé à l'IANA de faire référence au présent document pour l'option 81.

8. 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 DHCP 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 DHCP soit responsable de la mise à jour d'une transposition de FQDN en adresse IP ou que ce soit de la responsabilité du serveur DHCP 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 IP pour son FQDN).

Qu'un serveur DHCP soit toujours responsable de la mise à jour de transposition de FQDN en adresse IP (en plus de la mise à jour de transposition d'adresse IP en FQDN) sans considération des souhaits d'un client DHCP 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 DHCP effectue les mises à jour du DNS au nom d'un client, le serveur DHCP devrait être sûr du nom DNS à utiliser pour le client, et de l'identité du client.

Actuellement, il est difficile aux serveurs DHCP de développer une grande confiance dans les identités de leurs clients, étant donnée l'absence d'authentification de l'identité de la part du protocole DHCP lui-même. 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. Si l'authentification DHCP [RFC3118] devient largement déployée, cela peut devenir plus courant.

Un exemple de situation qui offre des assurances supplémentaires est quand le client DHCP est connecté à un réseau de modems câbles du système de réseau câblé multimédia (MCNS, *Multimedia Cable Network System*) et le système de terminaison de modem câble (CMTS, *cable modem termination system*) c'est-à-dire, où l'extrémité de tête assure que l'usurpation d'adresse MAC ne se produit simplement pas. Un autre exemple de configuration qui pourrait être de confiance est celle où les clients obtiennent l'accès réseau via un serveur d'accès réseau qui utilise PPP. Le NAS lui-même pourrait obtenir les adresses IP via DHCP, en codant l'identification d'un client dans l'option Identifiant de client DHCP. Dans ce cas, le serveur d'accès réseau ainsi que le serveur DHCP pourraient fonctionner dans un environnement de confiance, auquel cas le serveur DHCP pourrait être configuré à faire confiance que l'authentification de l'utilisateur et la procédure d'autorisation du serveur d'accès distant sont suffisantes, et pourrait donc faire confiance à l'identification de client codée dans l'identifiant de client DHCP.

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

9. Remerciements

Tous nos remerciements à Mark Beyer, Jim Bound, Ralph Droms, Robert Elz, Peter Ford, Olafur Gudmundsson, Edie Gunter, Andreas Gustafsson, David W. Hankins, R. Barr Hibbs, Kim Kinnear, Stuart Kwan, Ted Lemon, Ed Lewis, Michael Lewis, Josh Littlefield, Michael Patton, Pekka Savola, Jyrki Soini, et Glenn Stump de leur relecture et commentaires.

10. Références

10.1 Références normatives

[RFC0952] K. Harrenstien, M. Stahl, E. Feinler, "Spécification du tableau des hôtes de l'Internet du DOD", octobre 1985.

[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)

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989. *(MàJ par* RFC7766)

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

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

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

[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.

[RFC3396] T. Lemon et S. Cheshire, "Codage d'options longues dans le protocole de configuration dynamique d'hôte (DHCPv4)", novembre 2002.

[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.)*

10.2 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.)*

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

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.) (Remplacée par* RFC6891)

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

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001. *(P.S.)*

Adresses des auteurs

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
téléphone : 978.936.1535
mél : mjs@cisco.com

Bernie Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
téléphone : 978.936.0382
mél : volz@cisco.com

Yakov Rekhter
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
téléphone : 408.745.2000
mél : yakov@juniper.net

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).