Groupe de travail Réseau
Request for Comments : 4703
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Stapp, Cisco Systems
B. Volz, Cisco Systems, Inc.

octobre 2006

Résolution de conflits de nom de domaine pleinement qualifié (FQDN) entre clients protocole de configuration dynamique d'hôte (DHCP)

Résumé
Le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) fournit un mécanisme pour la configuration d'hôte qui inclut une allocation dynamique des adresses IP et des noms de domaines pleinement qualifiés. Pour maintenir des transpositions précises de nom en adresse IP et d'adresse IP en nom dans le DNS, ces adresses allouées dynamiquement et les noms de domaine pleinement qualifiés (FQDN, *fully qualified domain name*) exigent des mises à jour du DNS. Le présent document identifie les situations dans lesquelles des conflits d'utilisation de nom de domaine pleinement qualifié peuvent survenir entre des clients et serveurs DHCP, et il décrit une stratégie d'utilisation d'enregistrement de ressource (RR, *resource record*) DHCID du DNS pour résoudre ces conflits.

Table des matières

1. Introduction

"Option FQDN de client" [RFC4702] inclut une description du fonctionnement de clients et serveurs [RFC2131] qui utilisent l'option FQDN de client DHCPv4. "Option FQDN de client DHCPv6 " [RFC4704] inclut une description du fonctionnement des clients et serveurs [RFC3315] qui utilisent l'option FQDN de client DHCPv6. Par l'utilisation de

l'option FQDN de client, les clients et serveurs DHCP peuvent négocier le FQDN de client et l'allocation de la responsabilité de la mise à jour des RR A et/ou AAAA de client DHCP. Le présent document identifie les situations dans lesquelles des conflits d'utilisation des FQDN peuvent survenir entre des clients et serveurs DHCP, et il décrit une stratégie d'utilisation de l'enregistrement de ressource DHCID du DNS [RFC4701] pour résoudre ces conflits.

Dans tous les cas, qu'un site permettre que tous, certains, ou aucun, serveurs et clients DHCP effectuent les mises à jour du DNS [RFC2136], [RFC3007] 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 aucune. La gamme des politiques possibles est très large, depuis des sites où seuls les serveurs DHCP ont reçu des accréditifs que les serveurs DNS vont accepter, aux sites où chaque client DHCP individuel a été configuré avec des accréditifs qui permettent au client de modifier son propre FQDN. Les mises en œuvre conformes PEUVENT prendre en charge certaines ou toutes ces possibilités. 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.

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].

Le présent document suppose la familiarité avec la terminologie du DNS définie dans la [RFC1035] et la terminologie DHCP définie dans les [RFC2131] et [RFC3315].

Un FQDN, ou nom de domaine pleinement qualifié, est le nom complet d'un système, plutôt que juste son nom d'hôte. Par exemple, "venera" est un nom d'hôte, et "venera.isi.edu" est un FQDN. Voir la [RFC1983].

Les spécifications DOCSIS *(Data-Over-Cable Service Interface)* sont définies par CableLabs.

3. Problèmes de mise à jour du DNS dans les environnements DHCP

Il y a deux situations de mise à jour du DNS qui exigent une attention particulière dans les environnements DHCP : les cas où plus d'un client DHCP a été configuré avec le même FQDN, et les cas où plus d'un serveur DHCP a reçu l'autorité pour effectuer les mises à jour du DNS dans une zone. Dans ces cas, il est possible que les enregistrements du DNS soient modifiés de façon incohérente sauf si ceux qui mettent à jour ont un mécanisme qui leur permet de détecter les situations anormales. Si ceux qui mettent à jour le DNS peuvent détecter ces situations, les administrateurs de site peuvent configurer le comportement de mise à jour de façon à ce que les politiques de site soient appliquées. La présente spécification décrit un mécanisme conçu pour permettre à ceux qui mettent à jour de détecter ces situations et suggère que les mises en œuvre de DHCP utilisent ce mécanisme par défaut.

3.1 Mauvaise configuration de client

Les administrateurs peuvent souhaiter conserver une relation biunivoque entre les clients DHCP actifs et les FQDN, et conserver la cohérence entre les RR A, AAAA, et PTR d'un client. Les clients qui ne sont pas représentés dans le DNS, ou les clients qui partagent par inadvertance un FQDN avec un autre client peuvent rencontrer un comportement incohérent ou peuvent n'être pas capables d'obtenir l'accès à des ressources du réseau. Que chaque client DHCP soit configuré avec un FQDN par son administrateur ou que le serveur DHCP soit configuré à distribuer le FQDN du client, la cohértence des données du DNS dépend entièrement de la précision de la procédure de configuration. Les sites qui déploient la [RFC3007] peuvent configurer des accréditifs pour chaque client et son FQDN alloué d'une façon qui soit plus résistante à l'erreur, car le FQDN et les accréditifs doivent tous deux correspondre.

Considérons un exemple dans lequel deux clients DHCP dans le réseau "exemple.com" sont tous deux configurés avec le nom d'hôte "foo". Il est permis aux clients d'effectuer leurs propres mises à jour du DNS. Le premier client, client A, est configuré via DHCP. Il ajoute un RR A à "foo.exemple.com", et son serveur DHCP ajoute le RR PTR correspondant à son adresse IP allouée. Quand le second client, client B, s'amorce, il est aussi configuré via DHCP, et il commence aussi à mettre à jour "foo.exemple.com".

À ce point, les administrateurs de "exemple.com" peuvent souhaiter établir une politique sur les FQDN de clients DHCP. Si

la politique est que chaque client qui s'amorce devrait remplacer tout RR A existant qui correspond à son FQDN, le client B peut continuer, bien que le client A puisse rencontrer des problèmes. Dans cet exemple, le client B remplace le RR A associé à "foo.exemple.com". Le client A doit avoir un moyen de reconnaître que le RR associé à "foo.exemple.com" contient maintenant des information pour le client B, de sorte qu'il peut éviter de modifier le RR. Quand l'adresse allouée au client A arrive à expiration, par exemple, il ne devrait pas supprimer un RR qui reflète l'adresse IP allouée par DHCP au client B.

Si la politique est que le premier client DHCP qui a un certain FQDN devrait être le seul client associé à ce FQDN, le client B doit être capable de déterminer si il n'est pas le client associé à "foo.exemple.com". Il se pourrait que le client A se soit amorcé le premier, et que le client B devrait choisir un autre FQDN. Ou il se pourrait que B se soit amorcé sur un nouveau sous réseau et ait reçu une nouvelle allocation d'adresse IP, auquel cas B devrait mettre à jour le DNS avec sa nouvelle adresse IP. Il doit soit conserver l'état persistant sur la dernière adresse IP qui lui a été allouée (en plus de son adresse IP actuelle) soit il doit avoir un autre moyen de détecter que c'était la dernière mise à jour de "foo.exemple.com" afin de mettre en œuvre la politique du site.

3.2 Multiples serveurs DHCP

Il est possible de s'arranger pour que les serveurs DHCP effectuent les mises à jour de RR A et/ou AAAA au nom d'un de leurs clients. Si un seul serveur DHCP gère tous les clients DHCP d'un site, il peut tenir une base de données des FQDN utilisés et peut vérifier cette base de données avant d'allouer un FQDN à un client. Une telle base de données est cependant nécessairement propriétaire, et cette approche ne fonctionne que si pas plus d'un serveur DHCP est déployé.

Quand plusieurs serveurs DHCP sont déployés, les serveurs exigent un moyen pour coordonner les identités des clients DHCP. Considérons l'exemple dans lequel le client DHCPv4 A s'amorce, obtient une adresse IP du serveur S1, présentant le nom d'hôte "foo" dans une option FQDN de client [RFC4702] dans son message DHCPREQUEST. Le serveur S1 met à jour le FQDN "foo.exemple.com", ajoutant un RR A contenant l'adresse IP allouée à A. Le client passe ensuite à un autre sous réseau, desservi par le serveur S2. Quand le client A s'amorce sur le nouveau sous réseau, le serveur S2 va lui allouer une nouvelle adresse IP et va tenter d'ajouter un RR A contenant la nouvelle adresse IP allouée au FQDN "foo.exemple.com". À ce point, sans un mécanisme de communication permettant à S2 de demander à S1 (et à tout autre serveur DHCP qui met à jour la zone) ce qu'il en est du client, S2 n'a pas de moyen de savoir si le client A est actuellement associé au FQDN, ou si A est un client différent configuré avec le même FQDN. Si les serveurs ne peuvent pas distinguer entre ces situations, ils ne peuvent pas appliquer les politiques de dénomination du site.

4. Utilisation du RR DHCID

Une solution à ces deux problèmes est que celui qui met à jour (un client ou serveur DHCP) soit capable de déterminer quel client DHCP a été associé à un FQDN, afin d'offrir aux administrateurs l'opportunité de configurer le comportement de mise à jour.

À cette fin, un RR DHCID, spécifié dans la [RFC4701], est utilisé pour associer les informations d'identification de client à un FQDN et les RR A, AAAA, et PTR associés à ce FQDN. Quand un client ou serveur ajoute des RR A, AAAA, ou PTR pour un client, il ajoute aussi un RR DHCID qui spécifie une identité unique de client, sur la base des données provenant du message DHCP du client. Dans ce modèle, un seul client est associé à un FQDN donné à la fois.

En associant ces informations de propriété à chaque FQDN, la coopération des mises à jour du DNS peut déterminer si leur client est actuellement associé à un FQDN particulier et mettre en œuvre la politique administrative configurée de façon appropriée. De plus, les clients DHCP qui ont actuellement des FQDN peuvent passer d'un serveur DHCP à un autre sans perdre leur FQDN.

L'algorithme spécifique qui utilise le RR DHCID pour signaler la propriété du client est expliqué ci-dessous. L'algorithme ne fonctionne que dans le cas où les entités qui mettent à jour coopèrent toutes -- cette approche est seulement indicative et n'est pas un substitut de la sécurité du DNS, pas plus qu'elle n'est remplacée par la sécurité du DNS.

5. Procédures de mise à jour du DNS

5.1 Codes de retour d'erreur

Certains RCODE définis dans la [RFC2136] indiquent que le serveur DNS de destination n'a pas pu effectuer une mise à jour, c'est-à-dire, FORMERR, SERVFAIL, REFUSED, NOTIMP. Si un de ces RCODE est retourné, celui qui met à jour DOIT terminer sa tentative. D'autres RCODE [RFC2845] peuvent indiquer qu'il y a des problèmes avec la clé utilisée et peuvent signifier d'essayer une clé différente, si il en est de disponible, ou de terminer l'opération. Parce que certaines erreurs peuvent indiquer une mauvaise configuration de celui qui met à jour ou du serveur DNS, celui qui met à jour PEUT tenter de signaler à son administrateur qu'une erreur s'est produite, par exemple, par un message dans le journal d'événements.

5.2 Considération de client à la fois IPv4 et IPv6

Au moment de la publication du présent document, une petite minorité de clients DHCP prennent en charge à la fois IPv4 et IPv6. On prévoit cependant qu'une transition va prendre un certain temps, et que plus de sites auront des clients à double pile présents. Les clients IPv6 exigent des mises à jour des RR AAAA ; les clients IPv4 exigent des mises à jour des RR A. Les administrateurs de déploiements mixtes vont probablement souhaiter permettre à un seul FQDN de contenir des RR A et AAAA provenant du même client.

Les sites qui souhaitent permettre qu'un seul FQDN contienne les deux RR A et AAAA DOIVENT utiliser les clients et serveurs DHCPv4 qui prennent en charge l'utilisation de l'identifiant DHCP unique (DUID, *DHCP Unique Identifier*) pour les identifiants de client DHCPv4 afin que ce DUID soit utilisé dans le calcul des RDATA du RR DHCID par les deux DHCPv4 et DHCPv6 pour le client ; voir la [RFC4361]. Autrement, un client à double pile qui utilise des identifiants de client DHCPv4 de style plus ancien (voir les [RFC2131] et [RFC2132]) va seulement être capable d'avoir son enregistrement soit A, soit AAAA dans le DNS sous un seul FQDN à cause des conflits de RR DHCID qui en résultent.

5.3 Ajout de RR A et/ou AAAA au DNS

Quand un client ou serveur DHCP à l'intention de mettre à jour des RR A et/ou AAAA, il commence par la demande UPDATE du paragraphe 5.3.1.

Comme la séquence de mise à jour ci-dessous peut résulter en des boucles, les mises en œuvre DEVRAIENT limiter le nombre total de tentatives pour une seule transaction.

5.3.1 Demande initiale de RR DHCID

Celui qui met à jour prépare une demande DNS UPDATE qui inclut comme prérequis l'assertion que le FQDN n'existe pas. La section de mise à jour de la demande tente d'ajouter le nouveau FQDN et sa transposition d'adresse IP (les RR A et/ou AAAA) et le RR DHCID avec son identité unique de client.

Si la demande UPDATE réussit, la mise à jour de RR A et/ou AAAA est maintenant complète (et la mise à jour de client est finie, tandis qu'un serveur procéderait alors à effectuer une mise à jour de RR PTR).

Si la réponse au UPDATE retourne YXDOMAIN, celui qui met à jour peut maintenant conclure que le FQDN prévu est utilisé et procède comme indiqué au paragraphe 5.3.2.

Si tout autre état est retourné, celui qui met à jour NE DEVRAIT PAS tenter une mise à jour (voir au paragraphe 5.1).

5.3.2 Mise à jour du DNS quand le FQDN est utilisé

Celui qui met à jour tente ensuite de confirmer que le FQDN n'est pas utilisé par quelque autre client en préparant une demande UPDATE dans laquelle il y a deux prérequis. Le premier prérequis est que le FQDN existe. Le second est que le FQDN désiré a un RR DHCID qui lui est rattaché et dont le contenu correspond à l'identité du client. La section mise à jour de la demande UPDATE contient :

1. Une suppression de tous les RR A existants sur le FQDN si c'est une mise à jour de RR A ou AAAA et si celui qui met à jour ne désire pas d'enregistrement A sur le FQDN, ou si cette mise à jour est l'ajout d'un RR A et qu'il désire seulement une seule adresse IP sur le FQDN.

2. Une suppression des RR AAAA existants sur le FQDN si celui qui met à jour ne désire pas d'enregistrements AAAA sur le FQDN, ou si cette mise à jour est l'ajout d'un RR AAAA et que celui qui met à jour désire seulement une seule adresse IP sur le FQDN.

3. Un (ou des) ajouts du RR A qui correspond au lien DHCP si c'est une mise à jour de RR A.

4. Des ajouts de RR AAAA qui correspondent aux liens DHCP si c'est une mise à jour de AAAA.

La suppression des RR A ou AAAA dépend de celui qui met à jour, ou de sa politique. Par exemple, si celui qui met à jour est le client, ou est configuré comme le seul serveur DHCP pour la liaison sur laquelle le client est situé, il peut trouver avantageux de supprimer tous les RR A et/ou AAAA et d'ajouter ensuite l'ensemble actuel de RR A et/ou AAAA, si il en est, pour le client.

Si la demande UPDATE réussit, celui qui met à jour peut conclure que le client actuel était le dernier client associé au FQDN, et que le FQDN contient maintenant les RR A et/ou AAAA à jour. La mise à jour est maintenant achevée (et un client qui met à jour a terminé, tandis qu'un serveur procéderait alors à effectuer une mise à jour de RR PTR).

Si la réponse à la demande UPDATE retourne NXDOMAIN, le FQDN n'est plus utilisé, et celui qui met à jour revient au traitement du paragraphe 5.3.1.

Si la réponse à la demande UPDATE retourne NXRRSET, il y a deux possibilités : il n'y a pas de RR DHCID pour le FQDN, ou le RR DHCID ne correspond pas. Dans les deux cas, celui qui met à jour revient au paragraphe 5.3.3.

5.3.3 FQDN utilisé par un autre client

Comme le FQDN paraît être utilisé par un autre client ou n'est associé à aucun client, celui qui met à jour DEVRAIT choisir un autre FQDN et redémarrer le processus de mise à jour avec ce nouveau FQDN ou terminer la mise à jour avec un échec.

Les techniques qui peuvent être envisagées pour ôter les ambiguïtés de FQDN incluent d'ajouter un suffixe ou préfixe à la portion Nom d'hôte du FQDN ou de générer un nom d'hôte au hasard.

5.4 Ajout d'entrées de RR PTR au DNS

Le serveur DHCP soumet une demande UPDATE DNS qui supprime tous les RR PTR associés à l'adresse IP allouée au client et ajoute un RR PTR dont les données sont le FQDN du client (éventuellement désambigüé). Le serveur PEUT aussi ajouter un RR DHCID comme spécifié à la Section 4, et dans ce cas, il va inclure une suppression de tous les RR DHCID associés à l'adresse IP allouée au client, et va ajouter un RR DHCID pour le client.

Il n'est pas besoin de valider le RR DHCID pour les mises à jour de PTR car le ou les serveurs DHCP n'allouent qu'une seule adresse à un seul client à la fois.

5.5 Suppression d'entrées du DNS

La considération la plus importante lors de la suppression d'entrées du DNS est d'être sûr que l'entité qui supprime une entrée du DNS ne supprime qu'une entrée qu'elle a ajoutée, ou pour laquelle un administrateur lui a explicitement alloué cette responsabilité.

Quand le temps de prêt d'une adresse ou sa durée de validité arrive à expiration ou qu'un client DHCP produit une demande DHCPRELEASE [RFC2131] ou Release [RFC3315], le serveur DHCP DEVRAIT supprimer le RR PTR qui correspond au lien DHCP, si on avait réussi à en ajouter un. La demande UPDATE du serveur DEVRAIT certifier que le nom de domaine (champ PTRDNAME) dans l'enregistrement PTR correspond au FQDN du client dont l'adresse a expiré ou a été libérée et devrait supprimer tous les RR pour le FQDN.

L'entité choisie pour traiter les enregistrements A ou AAAA pour ce client (le client ou le serveur) DEVRAIT supprimer les enregistrements A ou AAAA qui ont été ajoutés quand l'adresse a été allouée au client.Cependant, celui qui met à jour ne devrait supprimer le RR DHCID que si il ne reste pas de RR A ou AAAA pour le client.

Afin d'effectuer cette suppression de RR A ou AAAA, celui qui met à jour prépare une demande UPDATE qui contient un

prérequis qui affirme que le RR DHCID existe et dont les données sont l'identité du client décrite à la Section 4 et contient une section mise à jour qui supprime le RR A ou AAAA spécifique du client.

Si la demande UPDATE réussit, celui qui met à jour prépare une seconde demande UPDATE qui contient trois prérequis et une section mise à jour qui supprime tous les RR pour le FQDN. Le premier prérequis affirme que le RR DHCID existe et que ses données sont l'identité de client décrite à la Section 4. Le second prérequis affirme qu'il n'y a pas de RR A. Le troisième prérequis affirme qu'il n'y a pas de RR AAAA.

Si l'une ou l'autre des demandes échoue, celui qui met à jour NE DOIT PAS supprimer le FQDN. Il se peut que le client dont l'adresse a expiré soit passé sur un autre réseau et qu'il ait obtenu une adresse d'un serveur différent, ce qui a causé le remplacement du RR A ou AAAA du client. Ou, les données du DNS peuvent avoir été supprimées ou altérées par un administrateur.

5.6 Mise à jour d'autres RR

Les procédures décrites dans le présent document ne couvrent que les mises à jour des RR A, AAAA, PTR, et DHCID. La mise à jour des autres types de RR sort du domaine d'application du présent document.

6. Considérations de sécurité

Les administrateurs doivent être attentifs à ne pas permettre de mises à jour non sécurisées du DNS sur des zones, qu'elles soient ou non exposées à l'Internet mondial. Les clients et serveurs DHCP DEVRAIENT utiliser une forme d'authentification de demande de mise à jour (par exemple, TSIG [RFC2845]) 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 peut être fondé sur le modèle de sécurité qui est utilisé avec le protocole de mise à jour dynamique 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 peut être fondé sur le modèle de sécurité qui est utilisé avec les mises à jour dynamiques 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 FQDN 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'une entité d'authentification de la part du protocole DHCP lui-même. Il y a de nombreuses façons pour un serveur DHCP de développer un FQDN à utiliser pour un client, mais seulement dans certaines circonstances relativement rares 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 par un modem câble DOCSIS, et que le système de terminaison de modem câble (CMTS, *cable modem termination system*) (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 serveur d'accès réseau (NAS, *Network Access Server*) 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 NAS 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 NAS sont suffisantes, et pourrait donc faire confiance à l'identification de client codée dans l'identifiant de client DHCP.

7. 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, et Glenn Stump de leur relecture et commentaires.

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)

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (MàJ 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.

[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)

[RFC4701] M. Stapp et autres, "Enregistrement de ressource (RR) du DNS pour le codage des informations du protocole de configuration dynamique d'hôte (DHCP) ", octobre 2006. *(P.S.)*

8.2 Références pour information

[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)

[RFC1983] G. Malkin, "Glossaire des utilisateurs de l'Internet", FYI 18, août 1996.

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

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[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.)*

[RFC4361] T. Lemon, B. Sommerfeld, "Identifiants de client spécifique de nœud pour le protocole de configuration dynamique d'hôte version 4 (DHCPv4)", février 2006. (*MàJ* RFC2131, RFC2132, RFC3315) *(P.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.)*

[RFC4704] B. Volz, "Option de nom de domaine pleinement qualifié (FQDN) de client du protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", octobre 2006. *(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

Déclaration complète de droits de reproduction

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