Groupe de travail Réseau
Request for Comments : 3646
Catégorie : En cours de normalisation

R. Droms, éditeur, Cisco Systems
décembre 2003
Traduction Claude Brière de L'Isle

Options de configuration du DNS pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)

Résumé
Le présent document décrit les options du protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) pour passer une liste des serveurs de noms DNS récurrents disponibles et une liste de recherche de domaines à un client.

1. Introduction

Le présent document décrit deux options pour passer les informations de configuration qui se rapportent au service des noms de domaines (DNS, *Domain Name Service*) ([RFC1034] et [RFC1035]) dans DHCPv6 ([RFC3315]).

2. Terminologie

Les mots-clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" lorsque ils apparaissent dans le présent document sont à interpréter comme décrit dans le BCP 14, [RFC 2119].

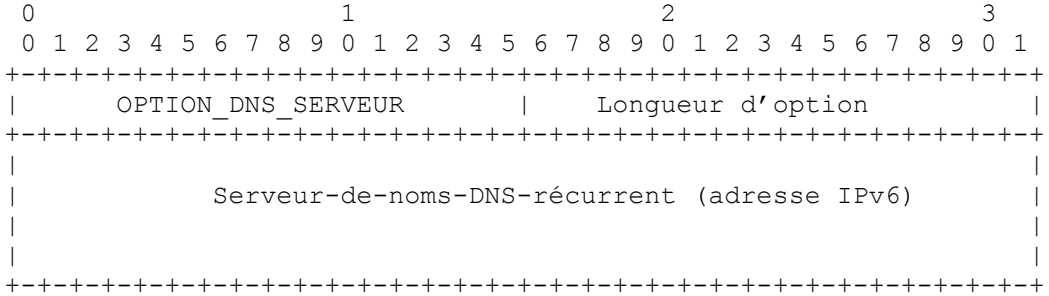
Tout au long du présent document, sauf spécification contraire, l'acronyme DHCP se réfère à DHCP pour IPv6 (DHCPv6) comme spécifié dans la [RFC3315].

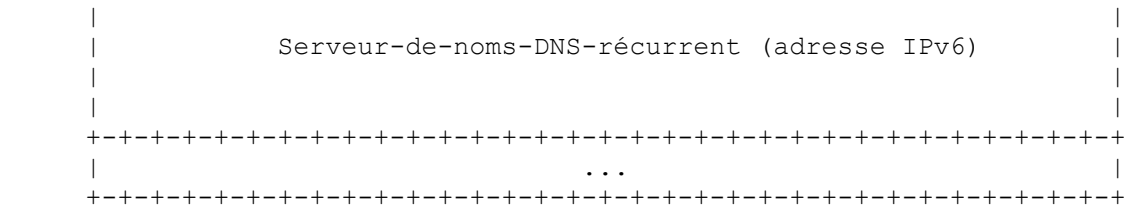
Le présent document utilise la terminologie spécifique d'IPv6 et de DHCP comme défini à la section 4 "Terminologie" de la [RFC3315].

3. Option Serveur de noms DNS récurrent

L'option Serveur de noms DNS récurrent fournit une liste d'une ou plusieurs adresses IPv6 de serveurs de noms DNS récurrents auxquels le résolveur DNS d'un client PEUT envoyer des interrogations DNS [RFC1035]. Les serveurs DNS sont énumérés dans l'ordre de préférence de l'utilisation par le résolveur du client.

Le format de l'option Serveur de noms DNS récurrent est :



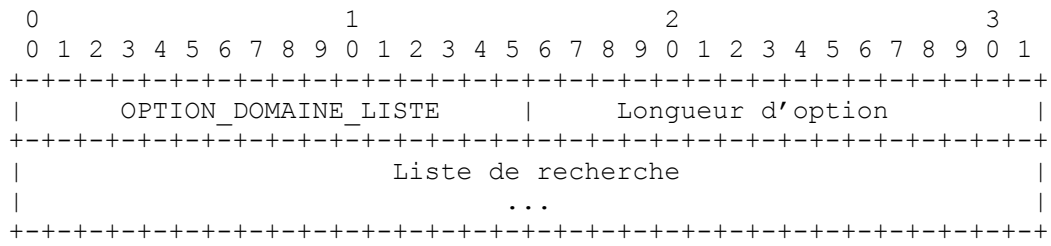


Code d'option : OPTION_DNS_SERVEUR (23).
Longueur d'option : Longueur de la liste des serveurs de noms DNS récurrents en octets, doit être un multiple de 16.
Serveur-de-noms-DNS-récurrent : Adresse IPv6 du serveurs de noms DNS récurrent.

4. Option Liste de recherche de domaine

L'option Liste de recherche de domaine spécifie la liste de recherche de domaines que le client va utiliser pour la résolution des noms d'hôtes avec le DNS. Cette option ne s'applique pas aux autres mécanismes de résolution de noms.

Le format de l'option Liste de recherche de domaines est :



Code d'option : OPTION_DOMAINE_LISTE (24).
Longueur d'option : Longueur du champ 'Liste de recherche' en octets.
Liste de recherche : Spécification de la liste des noms de domaines dans la liste de recherche de domaines.

La liste des noms de domaines dans la "liste de recherche" DOIT être codée comme spécifié dans la section 8, "Représentation et usage des noms de domaines" de la [RFC3315].

5. Présentation de ces options

L'option Serveur de noms DNS récurrent NE DOIT PAS apparaître dans un autre message que les suivants : Sollicite, Annonce, Demande, Renouveler, Relier, Demande-d'informations, et Réponse.

L'option Liste de recherche de domaine NE DOIT PAS apparaître dans un autre message que les suivants : Sollicite, Annonce, Demande, Renouvelle, Relier, Demande-d'informations, et Réponse.

6. Considérations pour la sécurité

L'option Serveur de noms DNS récurrent peut être utilisée par un serveur DHCP intrus pour causer l'envoi par des clients DHCP d'interrogations DNS à un serveur de noms DNS récurrent intrus. Le résultat de ces interrogations DNS mal dirigées peut être utilisé pour usurper des noms du DNS.

Pour éviter des attaques à travers l'option Serveur de noms DNS récurrent, le client DHCP DEVRAIT exiger l'authentification DHCP (voir la section 21 "Authentification des messages DHCP" de la RFC 3315) avant d'installer une liste de serveurs de noms DNS récurrents obtenus par DHCP authentifié.
L'option Liste de recherche de domaine peut être utilisée par un serveur DHCP intrus pour amener les clients DHCP à rechercher à travers des domaines invalides des noms de domaines incomplètement spécifiés. Le résultat de ces recherches mal dirigées peut être utilisé pour usurper des noms DNS. Noter que la prise en charge de DNSSEC [RFC2535] ne va pas éviter cette attaque, parce que les enregistrements de ressources dans les domaines invalides peuvent être légitimement signés.

Le degré de vulnérabilité d'un hôte aux attaques via une option invalide de recherche de domaine est déterminé en partie par le comportement du résolveur DNS. La [RFC1535] contient un exposé des faiblesses de la sécurité à l'égard des listes de recherche de domaine implicites aussi bien qu'explicites, et formule des recommandations sur le traitement des listes de recherche par les résolveurs. La Section 6 de la [RFC1536] traite aussi de cette vulnérabilité, et recommande que les résolveurs :

1. N'utilisent des listes de recherche que lorsque explicitement spécifié ; aucune liste de recherche implicite ne devrait être utilisée.
2. Résolvent un nom qui contient des points en l'essayant d'abord comme FQDN et si cela échoue, avec les noms dans la liste de recherche associée.
3. Résolvent un nom ne contenant pas de point en l'ajoutant directement à la liste de recherche, mais là encore, aucune liste de recherche implicite ne devrait être utilisée.

Afin de minimiser les faiblesses potentielles, il est recommandé que :

1. Les hôtes qui mettent en œuvre l'option de recherche de domaine DEVRAIENT aussi mettre en œuvre les recommandations sur la liste de recherche de la section 6 de la RFC1536.
2. Lorsque des paramètres DNS tels que la liste de recherche de domaines ou des serveurs DNS ont été configurés manuellement, ces paramètres NE DEVRAIENT PAS être outrepassés par DHCP.
3. Un hôte DEVRAIT exiger l'utilisation de l'authentification DHCP (Voir à la section 21 "Authentification des messages DHCP" de la RFC3315) avant d'accepter une option de recherche de domaine.

7. Considérations relatives à l'IANA

L'IANA a alloué un code d'option à l'option Serveur de noms DNS récurrent (23) et à l'option Liste de domaine de recherche (24) à partir de l'espace de code d'option DHCP défini à la section "Considérations relatives à l'IANA" de la [RFC3315].

8. Remerciements

Cette option faisait à l'origine partie de la spécification DHCPv6, écrite par Jim Bound, Mike Carney, Charlie Perkins, Ted Lemon, Bernie Volz et Ralph Droms.
L'analyse de l'attaque potentielle à travers la liste de recherche de domaine est tirée de la spécification de l'option Recherche de domaine de DHCPv4, [RFC3397].
Merci à Rob Austein, Alain Durand, Peter Koch, Tony Lindstrom et Pekka Savola pour leurs contributions au présent document.

9. Références

9.1 Références normatives

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

[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.

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

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC1536] A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller, "Erreurs courantes de mise en œuvre du DNS et corrections suggérées", octobre 1993. *(Information)*

9.2 Références pour information

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1535] E. Gavron, "Problème de sécurité et proposition de correction avec le logiciel courant du DNS", octobre 1993. *(Information)*

[RFC3397] B. Aboba, S. Cheshire, "Option Recherche de domaine du protocole de configuration dynamique d'hôte (DHCP)", novembre 2002. *(P.S.)*

Déclaration de droits de propriété intellectuelle

Adresse de l'auteur

Ralph Droms, Editor
Cisco Systems
1414 Massachusetts Ave.
Boxboro, MA 01719
USA
téléphone : +1 978 936 1674
mél : rdroms@cisco.com

Déclaration complète de droits de reproduction

Remerciement

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