Groupe de travail Réseau
Request for Comments : 3397
Catégorie : En cours de normamisation
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
S. Cheshire, Apple Computer, Inc.
novembre 2002

Option Recherche de domaine du protocole de configuration dynamique d'hôte (DHCP)

Résumé
Le présent document définit une nouvelle option du protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) qui est passée du serveur DHCP au client DHCP pour spécifier la liste de recherche de domaine utilisée lors de la résolution des noms d'hôte avec le DNS.

Table des Matières

1. Introduction

Le protocole de configuration dynamique d'hôte (DHCP) [RFC2131] fournit un mécanisme pour la configuration des hôtes. La [RFC2132] et la [RFC2937] permettent aux serveurs DHCP de passer des informations de configuration de service de noms aux clients DHCP. Dans certaines circonstances, il est utile pour le client DHCP d'être configuré avec la liste de recherche de domaine. Le présent document définit une nouvelle option DHCP qui est passée du serveur DHCP au client DHCP pour spécifier la liste de recherche de domaine utilisée lors de la résolution des noms d'hôtes avec le DNS. Cette option ne s'applique qu'au DNS et ne s'applique pas aux autres mécanismes de résolution de noms.

1.1 Terminologie

Le présent document utilise les termes suivants :

Client DHCP
Un client DHCP ou "client" est un hôte Internet qui utilise DHCP pour obtenir les paramètres de configuration comme une adresse réseau.

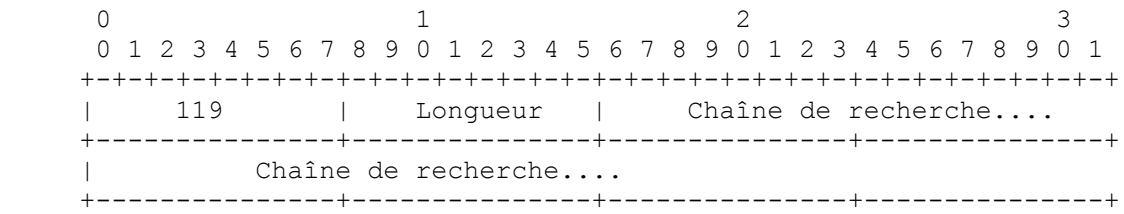
Serveur DHCP
Un serveur DHCP ou "serveur" est un hôte Internet qui retourne les paramètres de configuration aux clients DHCP.

1.2 Langage des exigences

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

2. Format de l'option Recherche de domaine

Le code de cette option est 119.



Dans le diagramme ci-dessus, Chaîne de recherche est une chaîne qui spécifie la liste de recherche. Si la longueur de la liste de recherche excède le maximum permissible dans une seule option (255 octets) plusieurs options PEUVENT alors être utilisées, comme décrit dans "Codage de longues options dans le protocole de configuration dynamique d'hôte (DHCPv4)" [RFC3396].

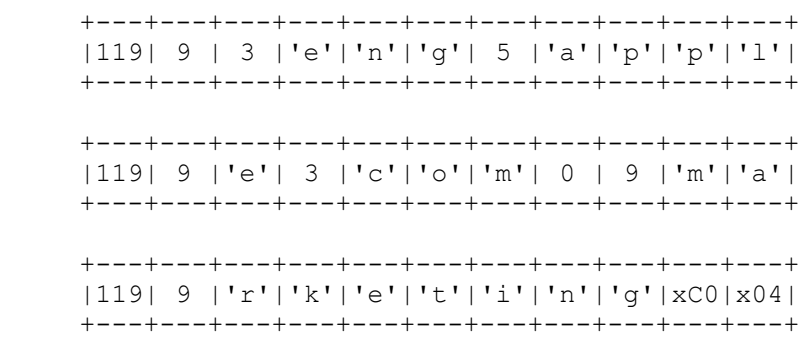
Pour permettre de coder la liste de recherche de façon compacte, les chaînes de recherche dans la liste de recherche DOIVENT être enchaînées et codées en utilisant la technique décrite au paragraphe 4.1.4 de "Noms de domaines – mise en œuvre et spécification" [RFC1035]. Dans ce schéma, un nom de domaine entier ou une liste d'étiquettes à la fin d'un nom de domaine est remplacé par un pointeur sur une occurrence antérieure du même nom. En dépit de sa complexité, cette technique est précieuse car l'espace disponible pour coder les options DHCP est limité, et il est vraisemblable qu'une chaîne de recherche d'un domaine va contenir des instances répétées du même nom de domaine. Donc, la compression de nom DNS est à la fois utile et vraisemblablement efficace.

Pour l'usage de la présente spécification, le pointeur se réfère au décalage au sein de la portion de données de l'option DHCP (non inclus l'octet de code de l'option DHCP précédente ou l'octet de longueur de l'option DHCP).

Si plusieurs options de recherche de domaine sont présentes, les portions de données de toutes les options de recherche de domaine sont alors enchaînées ensemble comme spécifié dans "Codage de longues options dans le protocole de configuration dynamique d'hôte (DHCPv4)" [RFC3396] et le pointeur indique un décalage au sein du bloc de données de l'agrégat complet.

3. Exemple

Voici un exemple de codage d'une liste de recherche consistant en "eng.apple.com." et "marketing.apple.com.":



Notes :
- Le codage a été séparé (pour cet exemple) en trois options de recherche de domaine. Toutes les options de recherche de domaine sont logiquement enchaînées en un bloc de données avant d'être interprétées par le client.
- Le codage de "eng.apple.com." se termine par un zéro, l'étiquette de la racine nulle, pour marquer la fin du nom, comme exigé par la RFC1035.

- Le codage de "marketing" (pour "marketing.apple.com.") se termine par le pointeur de compression de deux octets C004 (hex), qui pointe sur offset 4 dans le bloc agrégé complet des données de l'option Recherche de domaine, où un autre nom de domaine validement codé peut être trouvé pour compléter le nom ("apple.com.").

Chaque nom de domaine de recherche doit se terminer soit par un zéro, soit par un pointeur de compression de deux octets. Si le receveur est en cours du décodage d'un nom de domaine lorsque il atteint la fin du bloc agrégé complet des données de l'option de liste de recherche, sans trouver un zéro ou un pointeur de compression valide de deux octets, le nom partiellement lu DOIT alors être éliminé comme invalide.

4. Considérations pour la sécurité

Des attaques potentielles contre DHCP sont discutées à la Section 7 de la spécification du protocole DHCP [RFC2131], ainsi que dans la spécification d'authentification DHCP [RFC3118]. En particulier, en utilisant l'option de recherche de domaine, un serveur DHCP félon pourrait être capable de rediriger le trafic sur un autre site.

Par exemple, un usager qui demande une connexion à "myhost", s'attendant à joindre "myhost.bigco.com" pourrait à la place être dirigé sur "myhost.roguedomain.com". Noter que la prise en charge de DNSSEC [RFC2535] ne va pas détourner cette attaque, car les enregistrements de ressource pour "myhost.roguedomain.com" peuvent être légitimement signés. Cela fait de l'option Recherche de domaine une avenue toute tracée pour les attaques par un serveur DHCP félon plutôt que de fournir une option de serveur DHCP illégitime (décrite dans la [RFC2132]).

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

1 utilisent des listes de recherche seulement sur spécification explicité ; aucune liste de recherche implicite ne devrait être utilisée ;
2 résolvent un nom qui contient un ou des points en essayant d'abord un FQDN et si cela échoue, avec un nom de domaine local (ou liste de recherche si spécifié) ajouté ;
3 résolvent un nom ne contenant pas de point en l'annexant 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 :

a les mises en œuvre d'hôte de l'option Recherche de domaine DEVRAIENT aussi mettre en œuvre les recommandations de la liste de recherche de la section 6 de la [RFC1536] ;
b lorsque des paramètres DNS tels que Liste de recherche de domaine ou Serveurs DNS ont été configurés manuellement, ces paramètres NE DEVRAIENT PAS être outrepassés par DHCP ;
c les mises en œuvre de l'option Recherche de domaine PEUVENT exiger l'authentification DHCP [RFC3118] avant d'accepter une option Recherche de domaine.

5. Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

[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)*

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(Mise à jour par les RFC 3396 et 4361)*

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001.

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

6. Références pour information

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

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

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

[RFC2937] C. Smith, "Option de recherche de service de nom pour DHCP", septembre 2000. *(P.S.)*

7. Considérations relatives à l'IANA

L'IANA a alloué le code d'option DHCP 119 à l'option Recherche de domaine.

8. Remerciements

Les auteurs tiennen à remercier Michael Patton, Erik Guttman, Olafur Gudmundsson, Thomas Narten, Mark Andrews, Erik Nordmark, Myron Hattig, Keith Moore, et Bill Manning de leur commentaires sur ce mémoire.

9. Déclaration de propriété intellectuelle

10. Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 706 6605
mél : bernarda@microsoft.com

Stuart Cheshire
Apple Computer, Inc.
1 Infinite Loop
Cupertino
California 95014
téléphone : +1 408 974 3207
mél : rfc@stuartcheshire.org

11. Déclaration complète de droits de reproduction

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