Groupe de travail Réseau
Request for Comments : 5107
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Johnson, Cisco Systems, Inc.
J. Jumarasamy, Cisco Systems, Inc.
K. Kinnear, Cisco Systems, Inc.
M. Stapp, Cisco Systems, Inc.
février 2008

Sous option Outrepasser l'identifiant de serveur DHCP

Résumé
Le présent mémoire définit une nouvelle sous option de l'option d'informations de relais DHCP qui permet au relais DHCP de spécifier une nouvelle valeur pour l'option Identifiant de serveur, insérée par le serveur DHCP. Cela permet au relais DHCP d'agir comme le serveur DHCP actuel afin que les demandes DHCP RENEW viennent au relais au lieu d'aller directement au serveur. Cela donne au relais l'opportunité d'inclure l'option d'agent de relais avec les sous options appropriées même sur les messages DHCP RENEW.

Table of Contents

1. Introduction

Il y a de nombreuses situations où un agent de relais DHCP est impliqué, et il peut facilement insérer une option Informations d'agent de relais [RFC3046] avec les sous options appropriées dans les messages DHCP DISCOVER. Une fois que le prêt a été accordé, les futurs messages DHCP REQUEST envoyés par un client dans l'état RENEWING sont cependant envoyés directement au serveur DHCP, comme spécifié dans l'option Identifiant de serveur. Dans ce cas, le relais peut ne pas voir ces messages DHCP REQUEST (selon la topologie du réseau) et ne peut donc pas insérer l'option Informations d'agent de relais dans les messages DHCP REQUEST.

Cette sous option d'agent de relais DHCP, Outrepasser l'identifiant de serveur, permet à l'agent de relais de dire au serveur DHCP quelle valeur placer dans l'option Identifiant de serveur [RFC2132]. En utilisant cela, le relais peut forcer un hôte dans l'état RENEWING à envoyer des messages DHCP REQUEST à l'agent de relais plutôt que directement au serveur. L'agent de relais a alors l'opportunité d'insérer l'option Informations d'agent de relais avec les sous options appropriées et relayer le DHCP REQUEST au serveur réel. De cette façon, le serveur DHCP va obtenir les mêmes informations d'agent de relais lors des renouvellements (comme les Circuit-ID, Remote-ID, Classe d'appareil, etc.) que fournies dans le message DHCP DISCOVER initial.

En bref, cette nouvelle sous option permet au relais DHCPv4 de fonctionner de la même façon que celle dont fonctionne actuellement le relais DHCPv6 [RFC3315].

2. Conventions

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].

3. Terminologie

Le présent document utilise la terminologie DHCP comme défini au paragraphe 1.5 de la [RFC2131], à l'exception du terme "agent de relais DHCP" qui remplace "agent de relais BOOTP".

Un autre terme est utilisé dans ce document :

o RENEW DHCP REQUEST : message DHCP REQUEST envoyé par un client dans l'état RENEWING.

4. Définition de la sous option Outrepasser l'identifiant de serveur

Le format de la sous option est :

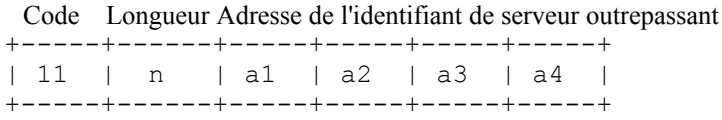

Figure 1

La longueur de l'option (n) est 4. Les octets "a1" à "a4" spécifient la valeur qui DOIT être insérée dans l'option Identifiant de serveur par le serveur DHCP lorsque il répond.

Les serveurs DHCP qui mettent en œuvre cette sous option Informations d'agent de relais DOIVENT utiliser cette valeur, si elle est présente dans un message DHCP reçu d'un client, comme valeur à insérer dans l'option Identifiant de serveur dans la réponse correspondante. Le serveur DHCP doit aussi enregistrer l'adresse dans la sous option pour l'utiliser dans les messages suivants au client DHCP jusqu'à ce que soit reçu le prochain message DHCP de l'agent de relais DHCP.

Si un serveur DHCP ne comprend pas ou ne met pas en œuvre cette sous option Informations de relais, il va ignorer la sous option, et donc va insérer sa propre adresse d'interface appropriée dans l'option Identifiant de serveur. Dans ce cas, le relais DHCP ne va pas recevoir de messages RENEW DHCP REQUEST de la part du client. Quand il configure un agent de relais DHCP à utiliser cette sous option, l'administrateur de l'agent de relais devrait tenir compte de si le serveur DHCP auquel le message va être relayé va comprendre correctement cette sous option.

Quand il sert un message DHCP REQUEST, le serveur DHCP va normalement chercher l'option Identifiant de serveur pour vérifier que l'adresse qui y est spécifiée est une des adresses associées au serveur DHCP, ignorant en silence la DHCP REQUEST si elle ne correspond pas à une adresse d'interface de serveur DHCP configurée. Si le message DHCP REQUEST contient la sous option Outrepasser l'identifiant de serveur, une comparaison devrait cependant être faite entre l'adresse dans cette sous option et dans l'option Identifiant de serveur. Si la sous option Outrepasser l'identifiant de serveur et l'option Identifiant de serveur spécifient toutes deux la même adresse, alors le serveur devrait accepter le message DHCP REQUEST au traitement, sans considération de si l'option Identifiant de serveur correspond ou non à une interface de serveur DHCP.

L'agent de relais DHCP devrait remplir le champ giaddr quand il relaye le message, tout comme il le ferait normalement.

Dans une situation où l'agent de relais DHCP est configuré à transmettre les messages à plus d'un serveur, il DEVRAIT transmettre tous les messages DHCP à tous les serveurs. Cela s'applique aussi aux messages RENEW DHCP REQUEST. L'intention est que l'agent de relais DHCP ne devrait pas avoir besoin de conserver les informations d'état sur le prêt DHCP.

Les agents de relais DHCP qui mettent en œuvre cette sous option DEVRAIENT aussi mettre en œuvre et utiliser la sous option Fanions d'agent de relais DHCPv4 [RFC5010] afin de spécifier si l'agent de relais DHCP a reçu le message original

en diffusion ou en envoi individuel. Le serveur DHCP qui reçoit un message contenant la sous option Outrepasser l'identifiant de serveur peut utiliser ces informations supplémentaires dans le traitement du message.

Noter que si l'agent de relais DHCP devient inaccessible au client DHCP ou perd l'accès réseau au serveur DHCP, les messages RENEW DHCP REQUEST ultérieurs provenant du client DHCP ne pourront pas être traités correctement et le prêt du client DHCP pourrait arriver à péremption.

5. Considérations sur la sécurité

L'authentification de message dans DHCP pour l'utilisation intradomaine où l'échange hors bande d'un secret partagé est faisable est définie dans la [RFC3118]. Les expositions potentielles à l'attaque sont discutées à la Section 7 de la spécification du protocole DHCP dans la [RFC2131].

L'option Informations d'agent de relais DHCP dépend d'une relation de confiance entre l'agent de relais DHCP et le serveur DHCP, comme décrit à la Section 5 de la [RFC3046]. Bien que l'introduction d'options frauduleuses d'informations d'agent de relais DHCP puisse être prévenue par un périmètre de défense qui bloque ces options sauf si l'agent de relais DHCP est de confiance, une défense plus en profondeur utilisant la sous option d'authentification de l'option Informations d'agent de relais DHCP [RFC4030] DEVRAIT être aussi déployée.

Si un agent de relais DHCP félon était inséré entre le client DHCP et le serveur DHCP, il pourrait rediriger les clients sur lui-même en utilisant cette sous option. Cela permettrait à un tel système de refuser ultérieurement les demandes DHCP RENEW et donc forcerait les clients à cesser d'utiliser les adresses qui leur sont allouées. Cela pourrait aussi permettre au relais félon de changer, insérer, ou supprimer les options DHCP dans les messages DHCP ACK et d'étendre les prêts au delà de ce que le serveur a permis. L'authentification DHCP [RFC3118] et/ou l'option d'authentification Informations d'agent de relais DHCP [RFC4030] pourrait traiter ce cas. (Noter que, comme c'est toujours le cas, l'absence d'authentification DHCP permettrait à un agent de relais DHCP félon de changer l'option Outrepasser l'identifiant de serveur sans être détecté dans les messages DHCP OFFER et DHCP ACK. Cette menace n'est pas nouvelle pour la sous option Outrepasser l'identifiant de serveur.)

Le présent document n'ajoute aucune nouvelle vulnérabilité à celles qui étaient déjà présentes, sauf dans le cas où l'authentification DHCP est déjà en place, et que les clients DHCP exigent son utilisation. Il est suggéré que l'authentification DHCP et l'authentification d'option d'agent de relais DHCP DEVRAIENT être déployées quand cette option est utilisée, ou une protection devrait être fournie contre l'insertion d'agents de relais DHCP félons entre le client et le serveur.

Cette sous option de relais n'est pas destinée, par elle-même, à procurer d'avantage de sécurité supplémentaire.

7. Considérations relatives à l'IANA

L'IANA a alloué un numéro de sous option (11) pour la sous option Outrepasser l'identifiant de serveur dans l'espace de noms de sous options de l'option Informations d'agent de relais DHCP [RFC3046].

7. Droits de propriété intellectuelle et droit de reproduction

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) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC3046] M. Patrick, "Option DHCP Information d'agent de relais", janvier 2001. (*MàJ par* RFC6607)

[RFC5010] K. Kinnear et autres, "Sous-option Fanions d'agent de relais du protocole de configuration dynamique d'hôte, version 4 (DHCPv4)", septembre 2007. *(P.S.)*

8.2 Références pour information

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

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

[RFC4030] M. Stapp, T. Lemon, "Sous-option d'authentification de l'option d'agent de relais pour le protocole de configuration dynamique d'hôte (DHCP)", mars 2005. *(P.S.)*

Adresse des auteurs

Richard A. Johnson
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US
téléhone : +1 408 526 4000
mél : raj@cisco.com

Jay Kumarasamy
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US
téléphone : +1 408 526 4000
mél : jayk@cisco.com

Kim Kinnear
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US
téléphone : +1 408 526 4000
mél : kkinnear@cisco.com

Mark Stapp
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US
téléphone : +1 408 526 4000
mél : mjs@cisco.com

Déclaration complète de droits de reproduction