Groupe de travail Réseau
Request for Comments : 3993
Catégorie : Normes

R. Johnson
T. Palaniappan
M. Stapp
Cisco Systems, Inc.

Mars 2005

Sous-option ID d’abonné pour l’option d’agent de relais du protocole de configuration dynamique d’hôte (DHCP)

Statut du présent Mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à discussion et suggestions en vue de son amélioration. Prière de se rapporter à l’édition en cours des "Internet Official Protocol Standards" (*normes officielles du protocole Internet*) (STD 1) pour connaître l’état de la normalisation et le statut du présent protocole. La distribution du présent mémo n’est pas soumise à restrictions.

Déclaration de copyright

Résumé

Le présent mémo définit une nouvelle sous-option d’identifiant d’abonné pour l’option d’information de l’agent de relais du protocole de configuration dynamique d’hôte (DHCP). La sous-option permet à un agent de relais DHCP d’associer un "ID d’abonné" stable aux messages client DHCP d’une façon indépendante du client et de l’infrastructure réseau physique sous jacente.

Table des matières

1. Introduction

DHCP (RFC 2131 [2]) fournit des adresses IP et des informations de configuration pour les clients IPv4. Il comporte une fonction d'agent de relais dans laquelle les processus au sein de l'infrastructure du réseau reçoivent les messages en diffusion provenant des clients et les transmettent aux serveurs DHCP comme messages en mono diffusion. Dans les environnements de réseau tels que des données DOCSIS sur câble et xDSL, il s'est révélé utile que l'agent de relais ajoute des informations au message DHCP avant de le transmettre, en utilisant l'option d'information d'agent de relais (RFC 3046 [3]).

Les serveurs qui reconnaissent l'option d'agent de relais la répercutent dans leurs réponses, et une partie des informations ajoutées par les relais peut être utilisée pour aider un appareil périphérique à retourner efficacement des réponses aux clients. Les informations que fournissent les relais peuvent aussi être utilisées dans la prise de décision du serveur sur les paramètres d'adresse et de configuration que le client devrait recevoir.

Dans de nombreux environnements de fournisseur de service, il est souhaitable d'associer des informations spécifiques du fournisseur à des messages DHCP du client. Cela est souvent fait en utilisant l'option d'information de l'agent de relais. La RFC 3046 définit les sous-options d'ID distant et d'ID de circuit qui servent à transporter de telles informations. Les valeurs de ces sous-options sont cependant habituellement fondées sur une ressource du réseau telle qu'une adresse IP d'un appareil d'accès au réseau, un identifiant de circuit virtuel ATM, ou un identifant de modem câble DOCSIS. Il en résulte que les valeurs portées dans ces sous options dépendent de la configuration physique du réseau. Si un client se connecte au réseau du fournisseur de service par des chemins différents, différentes valeurs sont portées dans les sous options dépendantes du réseau.

2. Terminologie pour les 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" doivent être interprétés comme décrit par la [RFC2119].

3. La sous option ID d'abonné

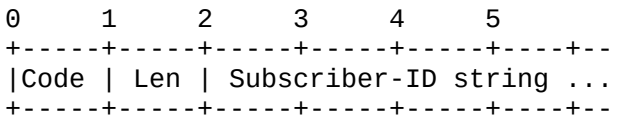
Dans les environnements complexes de fournisseur de service, la connections de la configuration DHCP d'un utilisateur et des informations administratives est nécessaire. La sous-option d'ID d'abonné porte une valeur qui peut être indépendante de la configuration physique du réseau à travers lequel l'abonné est connecté. Cette valeur complète les sous-options d'option d'agent de relais fondées sur le réseau exposées à la section 2, et peut aussi bien être utilisée en complément de celle-ci. L'"ID d'abonné" allouée par le fournisseur est destinée à être stable tandis que les utilisateurs se connectent par différents chemins, et alors que surviennent des changements de réseau.

Les informations d'ID d'abonné permettent au fournisseur de service d'allouer/activer des actions spécifiques de l'abonné ; par exemple, d'allouer l'adresse IP de l'hôte et le gabarit du sous-réseau, la configuration DNS, ou le déclenchement de la comptabilité. Cette sous-option est découplée de la structure physique du réseau d'accès, de sorte que lorsque l'abonné se déplace, par exemple, d'un point d'accès à l'autre, cela ne requière pas de reconfiguration aux serveurs DHCP du fournisseur de service.

L'ID d'abonné est une chaîne ASCII ; le codage de cette chaîne est défini au paragraphe 3.1. Le contenu sémantique de la chaîne d'ID d'abonné est, bien sûr, spécifique du fournisseur. La présente spécification n'établit aucune exigence de sémantique sur les données de la chaîne.

3.1. Format de sous option

Le présent mémo définit une nouvelle sous-option d'option d'agent de relais DHCP qui porte une valeur "ID d'abonné". La valeur est une chaîne ASCII. La sous-option prend une forme similaire à celle de nombreuses autres sous-options d'option d'informations de relais :



Le code pour la sous-option est 6.

Le champ d'un octet Len est la longueur de la chaîne ID, en octets.
La longueur minimum de la chaîne ID est 1 octet.

Le "ID d'abonné" est une chaîne NVT ASCII [4]. La chaîne NE DOIT PAS être de terminaison NULLE, car la longueur est spécifiée dans le champ "Len".

4. Comportement de l'agent de relais

Les agents de relais DHCP PEUVENT être configurés de façon à inclure une sous-option ID d'abonné s'ils incluent une option d'informations d'agent de relais dans les messages DHCP relayés. Les chaînes d'ID d'abonné elles-mêmes sont allouées et configurées par des mécanismes qui sont en dehors du champ d'application du présent mémo.

5. Comportement du serveur DHCP

La présente sous-option fournit des informations supplémentaires au serveur DHCP. S'il est configuré pour prendre en charge cette option, le serveur DHCP peut utiliser ces informations en plus des autres données d'option d'agent de relais et des autres options incluses dans les messages client DHCP afin d'allouer une adresse IP et/ou d'autres paramètres de configuration au client. Il n'y a pas de traitement supplémentaire spécial pour cette sous-option.

6. Considérations sur la sécurité

L'authentification de message en DHCP pour utilisation intradomaine lorsque l'échange hors bande d'un secret partagé est faisable est définie dans la RFC 3118 [5]. La possibilité d'exposition à des attaques est discutée à la section 7 de la spécification du protocole DHCP dans la RFC 2131 [2].

L'option d'agent de relais DHCP dépend d'une relation de confiance entre l'agent de relais DHCP et le serveur, comme décrit à la section 5 de la RFC 3046. Des données frauduleuse d'option d'agent de relais pourraient conduire à un vol de service ou à l'épuisement de ressources limitées (comme des adresses IP) par des clients non autorisés. Un hôte qui tripote des données d'agent de relais associées à des messages DHCP d'un autre hôte pourrait dénier le service à cet hôte, ou interférer avec son fonctionnement en amenant le serveur DHCP à lui allouer des paramètres de configuration inappropriés.

Alors que l'introduction d'options frauduleuses d'agent de relais peut être empêchée par un périmètre de défense qui bloque ces options sauf si l'agent de relais est de confiance, une défense plus en profondeur utilisant l'authentification pour les options d'agent de relais via la sous-option d'authentification [6] ou IPSec [7] DEVRAIT aussi être développée.

Il y a plusieurs champs de données dans un message DHCP convoyant de l'information qui peuvent identifier un hôte individuel sur le réseau. Ils incluent le chaddr, l'option ID de client, et les options hostname et client-fqdn. Selon le type d'identifiant choisi, la sous-option ID d'abonné peut aussi convoyer des informations qui identifient un hôte spécifique ou un utilisateur spécifique sur le réseau. En pratique, ces informations ne sont pas exposée en dehors du réseau interne du fournisseur de service, où les messages DHCP sont habituellement confinés. Les administrateurs qui configurent des données qui vont être utilisées dans les sous-options d'identifiant d'abonné DHCP devraient veiller à utiliser des identifiants appropriés aux types de réseau qu'ils administrent. Si des messages DHCP voyagnet en-dehors du propre réseau du fournisseur de service, ou si les valeurs de la sous-option peuvent devenir visible pour d'autres utilisateurs, cela peut soulever des problèmes de confidentialité pour le fournisseur d'accès ou le fournisseur de service.

7. Considérations relatives à l'IANA

L'IANA a alloué une valeur de 6 dans les codes de sous-option de l'option d'informations d'agent de relais DHCP [3] pour la sous-option ID d'abonné décrite dans le présent document.

8. Remerciements

Le présent document est le résultat du travail effectué au sein de Cisco Systems. Des remerciements particuliers à Andy Sudduth pour ses commentaires en relecture.

9. Références

9.1. Références normatives

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels" *(Mots clé à utiliser dans les RFC pour indiquer les niveaux d'exigence)*, BCP 14, RFC 2119, mars 1997.

[2] Droms, R., "Dynamic Host Configuration Protocol" *(Protocole de configuration dynamique d'hôte)*, RFC 2131, mars 1997.

[3] Patrick, M., "DHCP Relay Agent Information Option" *(Option d'informations d'agent de relais DHCP)*, RFC 3046, janvier 2001.

[4] Postel, J. et J. Reynolds, "Telnet Protocol Specification" *(Spécification du protocole Telnet)*, STD 8, RFC 854, mai 1983.

9.2. Références informatives

[5] Droms, R. et W. Arbaugh, "Authentication for DHCP Messages" *(Authentification des messages DHCP)*, RFC 3118, juin 2001.

[6] Stapp, M., "The Authentication Suboption for the DHCP Relay Agent Option" *(Sous-option d'authentification pour l'option d'agent de relais DHCP)*, travail en cours.

[7] Droms, R., "Authentication of Relay Agent Options Using IPSec" *(Authentification des options d'agent de relais avec IPsec)*, travail en cours.

Adresse des auteurs

Richard Johnson	Theyn Palaniappan	Mark Stapp
Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.
170 W. Tasman Dr.	170 W. Tasman Dr.	1414 Massachusetts Ave.
San Jose, CA 95134	San Jose, CA 95134	Boxborough, MA 01719
USA	USA	USA
tél : 408.526.4000	tél : 408.526.4000	tél : 978.936.0000
mél : raj@cisco.com	mél : athenmoz@cisco.com	mél : mjs@cisco.com

Déclaration de copyright

IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait 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 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 fourni par Internet Society.