

Groupe de travail Réseau
Request for Comments : 3004
Catégorie : En cours de normalisation
novembre 2000
Traduction Claude Brière de L'Isle

G. Stump, IBM
R. Droms, Cisco Systems
Y. Gu, R. Vyaghrapuri, A. Demirtjis, Microsoft
B. Beser, Pacific Broadband Communications
J. Privat, Northstream AB

Option Classe d'utilisateur pour DHCP

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2000). Tous droits réservés.

Résumé

Cette option est utilisée par un client du protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) pour identifier facultativement le type ou la catégorie d'utilisateur ou applications qu'il représente. Les informations contenues dans cette option sont un champ opaque qui représente la classe d'utilisateur dont le client est membre. Sur la base de cette classe, un serveur DHCP choisit le réservoir d'adresses approprié pour allouer une adresse au client et les paramètres de configuration appropriés. Cette option devrait être configurable par un utilisateur.

1. Introduction

Les administrateurs DHCP peuvent définir des identifiants spécifiques d'une classe d'utilisateurs pour porter des informations sur la configuration logicielle d'un client ou sur les préférences de son utilisateur. Par exemple, l'option Classe d'utilisateur peut être utilisée pour configurer tous les clients des gens du département de comptabilité avec une imprimante différente des clients des gens du département commercial.

2. Terminologie des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT" et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

3. Terminologie DHCP

o "Client DHCP"

Un client DHCP ou "client" est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration tels qu'une adresse réseau.

o "Serveur DHCP"

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

o "Lien"

Un lien est une collection de paramètres de configuration, incluant au moins une adresse IP, associée à ou "liée à" un client DHCP. Les liens sont gérés par les serveurs DHCP.

4. Option Classe d'utilisateur

Cette option est utilisée par un client DHCP pour identifier facultativement le type ou la catégorie de l'utilisateur ou des applications qu'il représente. Un serveur DHCP utilise l'option Classe d'utilisateur pour choisir le réservoir d'adresses d'où il alloue une adresse et/ou pour choisir toute autre option de configuration.

Cette option est une option DHCP [RFC2131], [RFC2132].

Cette option PEUT porter plusieurs classes d'utilisateur. Les serveurs peuvent interpréter la signification de spécifications de classes multiples d'une façon qui dépend de la mise en œuvre ou d'une façon qui dépend de la configuration, et donc, l'utilisation de classes multiples par un client DHCP devrait se fonder sur la mise en œuvre spécifique de serveur et de la configuration qui sera utilisée pour traiter cette option Classe d'utilisateur.

Le format de cette option est le suivant :

```

Code   Long.      Valeur
+-----+-----+-----+-----+-----+-----+-----+-----+
| 77   | N   | Données de classe d'utilisateur ('Long.' octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

où Valeur consiste en une ou plusieurs instances de données de classe d'utilisateur. Chaque instance de données de classe d'utilisateur est formatée comme suit :

```

UC_Long_i   Données_de_classe_d'utilisateur_i
+-----+-----+-----+-----+-----+-----+-----+-----+
| L_i      | Données opaques (UC_Long_i' octets) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Chaque valeur de classe d'utilisateur (Données_de_classe_d'utilisateur_i) est indiquée comme champ opaque. La valeur dans UC_Long_i n'inclut pas le champ Longueur lui-même et DOIT être différente de zéro. Soit m le nombre de classes d'utilisateur portées dans l'option. La longueur de l'option comme spécifié dans Long. doit être la somme des longueurs de chacun des noms de classe plus m : $Long = UC_Long_1 + UC_Long_2 + \dots + UC_Long_m + m$. Si une ou des instances de données de classe d'utilisateur sont présentes, la valeur minimum de Long est deux ($Long = UC_Long_1 + 1 = 1 + 1 = 2$).

Le code pour cette option est 77.

Un serveur qui n'est pas équipé pour interpréter une des classes d'utilisateur spécifiée par un client DOIT l'ignorer (bien qu'il puisse en faire rapport). Si un serveur reconnaît une ou plusieurs classes d'utilisateur spécifiées par le client, mais ne reconnaît pas une ou plusieurs autres classes d'utilisateur spécifiées par le client, le serveur PEUT utiliser les classes d'utilisateur qu'il reconnaît.

Les clients DHCP qui mettent en œuvre cette option DEVRAIENT permettre aux usagers d'entrer une ou plusieurs valeurs de classe d'utilisateur.

5. Considérations relatives à l'IANA

L'option 77, que l'IANA a déjà allouée à cette fin, devrait être utilisée comme option Classe d'utilisateur pour DHCP.

6. Considérations pour la sécurité

DHCP ne fournit actuellement pas de mécanisme d'authentification ni de sécurité. Les expositions potentielles à des attaques sont discutées à la section 7 de la spécification du protocole [RFC2131].

L'absence de mécanisme d'authentification signifie qu'un serveur DHCP ne peut pas vérifier si un client ou un usager est autorisé à utiliser une certaine classe d'utilisateur. Cela introduit une vulnérabilité évidente lorsque on utilise l'option Classe d'utilisateur. Par exemple, si la classe d'utilisateur est utilisée pour distribuer un certain paramètre (par exemple, un serveur de base de données particulier) il n'y a aucun moyen d'authentifier un client et il est donc impossible de vérifier si un client est autorisé à utiliser ce paramètre.

7. Références

[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](#)*)

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

8. Remerciements

Le présent document se fonde sur des projets antérieurs de Glenn Stump, Ralph Droms, Ye Gu, Ramesh Vyaghrapuri et Burcak Beser. Merci à Ted Lemon, Steve Gonczi, Kim Kinnear, Bernie Volz, Richard Jones, Barr Hibbs et Thomas Narten pour leurs commentaires et suggestions.

9. Adresse des auteurs

Glenn Stump
IBM Networking Software
P.O. Box 12195
RTP, NC 27709
téléphone : 919 301 4277
mél : stumpga@us.ibm.com

Ralph Droms
Cisco Systems
300 Apollo Drive
Chelmsford, MA 01824
téléphone : 978 244 4733
mél : rdroms@cisco.com

Ye Gu
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : 425 936 8601
mél : yegu@microsoft.com

Ramesh Vyaghrapuri
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : 425 703 9581
mél : rameshv@microsoft.com

Burcak Beser
Pacific Broadband Communications
3103 North 1st Street
San Jose, CA 95134
téléphone : 408 468 6265
mél : Burcak@pacband.com

Ann Demirtjis
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
téléphone : 425 705 2254
mél : annd@microsoft.com

Jerome Privat
Northstream AB
Espace Beethoven 1
1200 Route des Lucioles
BP 302
06906 Sophia Antipolis Cedex
France
téléphone : +33 4 97 23 40 45
mél : jerome.privat@northstream.se

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2000). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de copyright ci-dessus et le présent et paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de copyright ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de copyright définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou 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.

Remerciement

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