

Groupe de travail Réseau
Request for Comments : 2563
Catégorie : En cours de normalisation

R. Troll, @Home Network
mai 1999
Traduction Claude Brière de L'Isle

Option DHCP pour désactiver l'auto-configuration sans état chez les clients IPv4

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 (1999). Tous droits réservés.

Résumé

Les systèmes d'exploitation (OS, *Operating System*) tentent maintenant de prendre en charge des réseaux ad hoc de deux systèmes ou plus, tout en conservant la configuration d'utilisateur au minimum. Pour s'accommoder de cela, en l'absence d'un mécanisme central de configuration (DHCP), certains OS choisissent automatiquement une adresse IP de liaison locale qui va leur permettre de communiquer seulement avec les autres hôtes sur la même liaison. Cette adresse ne va pas permettre à l'OS de communiquer au delà d'un routeur. Cependant, certains sites dépendent du fait qu'un hôte sans réponse DHCP n'aura pas d'adresse IP. Le présent document décrit un mécanisme par lequel les serveurs DHCP sont capables de dire aux clients qu'ils n'ont pas d'adresse IP à offrir, et que le client ne devrait pas générer de lui-même une adresse IP.

1. Introduction

Avec les ordinateurs qui prennent une part de plus en plus importante dans la vie courante, les systèmes d'exploitation doivent être capables de prendre en charge une plus large gamme d'environnements de fonctionnement. Un aspect de cette prise en charge est le choix d'une adresse IP. Le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) [RFC2131] fournit une superbe méthode par laquelle les administrateurs de site peuvent fournir des adresses IP (et autres paramètres réseau) aux appareils du réseau. Cependant, certains environnements de fonctionnement ne sont pas entretenus centralement, et les systèmes d'exploitation doivent maintenant être capables de traiter cela rapidement et facilement.

IPv6 tient compte de cela, et permet à une pile IPv6 d'allouer elle-même une adresse mondiale en l'absence de tout autre mécanisme de configuration [RFC2462]. Cependant, les concepteurs de système d'exploitation ne peuvent pas attendre partout la prise en charge de IPv6. Ils doivent être capables de supposer qu'ils vont avoir des adresses IPv4, afin qu'ils puissent communiquer les uns avec les autres même dans les plus petits réseaux.

Le présent document examine trois types de nœuds de réseau, et comment l'auto-configuration d'adresse IPv4 peut être désactivée au niveau du sous-réseau (ou même au niveau du nœud). Les trois types de nœud de réseau sont :

- * un nœud pour lequel l'administrateur de site va donner les informations de configuration,
- * un nœud sur un segment de réseau pour lequel il n'y a pas d'administrateur de site,
- * un nœud sur un segment de réseau qui a un administrateur de site central, et cet administrateur choisit de ne pas donner d'informations de configuration au nœud.

La différence entre le second et le troisième cas est le comportement des clients.

Dans un cas, le nœud peut s'allouer une adresse IP, et avoir la pleine connexité avec les autres nœuds sur la boucle locale. Dans le dernier cas, on ne dit pas au nœud ce qu'il doit faire, et bien qu'il puisse s'allouer lui-même une adresse réseau de la même manière que dans le cas n° 2, cela peut n'être pas ce que veut l'administrateur central.

Le premier scénario est traité par la norme DHCP actuelle. Cependant, la spécification DHCP actuelle [RFC2131] dit que les serveurs doivent ignorer en silence les demandes provenant d'hôtes qu'ils ne connaissent pas. À cause de cela, les clients DHCP sont dans l'incapacité de déterminer si ils sont sur un sous-réseau sans administration, ou avec une administration qui a choisi de ne pas donner d'adresses.

Le présent document décrit une méthode par laquelle les clients DHCP seront capables de déterminer si le réseau est ou non

administré centralement, lui permettant de déterminer intelligemment si il devrait ou non s'allouer lui-même une adresse de "liaison locale".

1.1 Conventions utilisées dans le document

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].

1.2 Terminologie

Client DHCP : c'est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration comme une adresse réseau.

Serveur DHCP : c'est un hôte Internet qui retourne des paramètres de configuration aux clients DHCP.

2. Option Auto-Configure

Ce code d'option est utilisé pour demander, et en avoir notification, si l'auto-configuration devrait être désactivée sur le sous-réseau local. L'option d'auto-configuration est un nombre de 8 bits.

Code	Longueur	Valeur
116	1	a

Le code de cette option est 116, et sa longueur est 1.

Ce code, avec l'allocation d'adresse IP, va permettre à un client DHCP de déterminer si il devrait ou non générer une adresse IP de liaison locale.

2.1 Valeurs de Auto-Configure

L'option auto-configure utilise les valeurs suivantes :

DoNotAutoConfigure	0
AutoConfigure	1

Lorsque un serveur répond avec la valeur "AutoConfigure", le client PEUT générer une adresse IP de liaison locale si c'est approprié. Cependant, si le serveur répond par "DoNotAutoConfigure", le client NE DOIT PAS générer une adresse IP de liaison locale, le laissant éventuellement sans adresse IP.

2.2 Comportement du client DHCP

Les clients qui ont des capacités d'auto-configuration DOIVENT ajouter l'option Auto-Configure à la liste des options incluse dans son message initial DHCPDISCOVER ([RFC2131] paragraphe 4.4.1). À ce moment, la valeur de l'option devrait être réglée à "AutoConfigure".

Lorsqu'un message DHCPOFFER est reçu, il est traité comme décrit au paragraphe 4.4.1 de la [RFC2131], avec une exception. Si le champ 'yiaddr' est 0x00000000, l'option Auto-Configure doit être consultée. Si cette option est réglée à "AutoConfigure", le DHCPOFFER DOIT alors être ignoré, et le client DHCP PEUT générer une adresse IP de liaison locale. Cependant, si cette option est réglée à "DoNotAutoConfigure", le DHCPOFFER DOIT alors être ignoré, et le client NE DOIT PAS générer une adresse IP de liaison locale.

Si un client DHCP reçoit un DHCPOFFER qui contient un champ 'yiaddr' de 0x00000000, et si le fanion Auto-Configure dit "DoNotAutoConfigure", en l'absence d'un DHCPOFFER avec un champ 'yiaddr' valide, le client DHCP NE DOIT PAS générer d'adresse IP de liaison locale. La durée pendant laquelle un client DHCP attend pour collecter d'autres DHCPOFFER dépend de la mise en œuvre.

2.4 Environnements mixtes

Les environnements qui contiennent un mélange de clients et serveurs qui prennent et ne prennent pas en charge l'option Auto-Configure ne posent pas de problème. Chaque transaction DHCP est entre un serveur et un client, et les scénarios mixtes possibles entre eux sont examinés ci-dessous.

2.4.1 Le client prend en charge, pas le serveur

Si un client DHCP envoie une demande qui contient l'étiquette Auto-Configure, un serveur DHCP qui ne sait pas ce qu'est cette étiquette va répondre normalement. Conformément au paragraphe 4.3.1 de la [RFC2131], le serveur NE DOIT PAS retourner une valeur pour ce paramètre.

Dans ce cas, le serveur va ou répondre par une DHCP OFFER valide, ou ne va pas répondre du tout. Dans les deux cas, un client DHCP qui prend en charge cette option ne va pas se soucier de l'état de l'option, et peut auto-configurer.

2.4.2 Les serveurs prennent en charge, pas le client

Si l'option Auto-Configure n'est pas présente dans le DHCPDISCOVER, le serveur ne va rien faire sur elle. Le client va s'auto-configurer si il ne reçoit pas de réponse et croit que c'est ce qu'il devrait faire.

Ce scénario NE DEVRAIT PAS se produire, car toute pile de protocoles qui met en œuvre un mécanisme d'auto-configuration DOIT aussi mettre en œuvre cette option.

2.5 Interaction avec les autres messages DHCP

Comme cette option n'affecte que le choix de l'adresse IP initiale, elle ne s'applique pas aux messages DHCP suivants. Si le client DHCP a reçu un prêt d'adresse d'un serveur DHCP, les messages DHCP futurs (RENEW, INFORM, ACK, etc.) n'ont pas besoin de rentrer dans un état d'auto-configuration.

Si le prêt du client DHCP arrive à expiration, le client revient à l'état INIT, et le DHCPDISCOVER initial est envoyé comme précédemment.

2.5.1 Messages DHCPRELEASE

Les DHCPRELEASE surviennent exactement comme décrit au paragraphe 4.4.6 de la [RFC2131]. Lorsque un client DHCP en a fini avec un prêt d'adresse, il PEUT notifier au serveur que c'est fini. Pour que cela se produise, le client DHCP a déjà reçu un prêt d'adresse de DHCP, et l'état de Auto-Configuration sur le réseau local importe peu.

2.5.2 Messages DHCPDECLINE

Un DHCPDECLINE est envoyé par le client DHCP lorsque il détermine que l'adresse réseau qu'il tente d'utiliser est déjà en service. Comme une adresse réseau a été essayée, il doit avoir eu une offre du serveur DHCP, et l'état de Auto-Configuration sur le réseau local n'a pas d'importance.

2.5.3 Messages DHCPINFORM

Les DHCPINFORM devraient être traités comme décrit au paragraphe 4.4.3 de la [RFC2131]. Aucun changement n'est nécessaire.

2.6 Options de message

Si le serveur DHCP voulait dire à un client pourquoi il ne lui est pas permis de s'autoconfigurer, il PEUT ajouter l'option Message à la réponse. Cette option est définie au paragraphe 9.9 de la [RFC2132].

Si le client DHCP reçoit une réponse avec l'option Message établie, il DOIT fournir cette information à l'administrateur du client DHCP. Comment cette information est fournie dépend de la mise en œuvre.

3. Considérations pour la sécurité

DHCP ne fournit actuellement par lui-même aucun mécanisme d'authentification ni de sécurité. Les expositions potentielles à une attaque sont discutées à la section 7 de la spécification du protocole DHCP [RFC2131].

Ce mécanisme n'ajoute pas d'autre attaque potentielle. Un usager malveillant sur un sous-réseau peut répondre à toutes les demandes DHCP avec des réponses disant aux clients DHCP qu'ils ne devraient pas s'autoconfigurer sur la boucle locale. Sur un réseau où l'auto-configuration est exigée, cela serait cause que tous les clients DHCP ne choisissent pas d'adresse.

4. Remerciements

Cette idée a été lancée à une réunion conjointe du groupe de solutions communes / Microsoft chez Microsoft en mai 1998. La pile IP dans Win98 et NT5 s'alloue elle-même une adresse IP (dans un sous-réseau spécifique) en l'absence d'une réponse de serveur DHCP, et cela cause des maux de tête à de nombreux sites qui s'appuient en fait sur des machines qui ne prennent pas d'adresse IP lorsque les serveurs DHCP ne les connaissent pas.

Walter Wong a proposé une solution qui pourrait permettre aux serveurs DHCP de dire aux clients de ne pas faire cela. Sa solution initiale ne fonctionnerait pas sans de légères modifications à DHCP lui-même. Le présent document décrit ces modifications.

5. Considérations pour l'IANA

L'IANA a alloué le numéro d'option 116 à cette option.

6. 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 RFC3396 et 4361*)
- [RFC2132] S. Alexander et R. Droms, "Options DHCP et [Extensions de fabricant BOOTP](#)", mars 1997.
- [RFC2462] S. Thomson, T. Narten, "[Autoconfiguration d'adresse IPv6 sans état](#)", décembre 1998. (*Obsolète, voir RFC4862*) (D.S.)

7. Adresse de l'auteur

Ryan Troll
@Home Network
425 Broadway
Redwood City, CA 94063
USA
téléphone : (650) 556-6031
mél : rtroll@corp.home.net

8. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des

normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

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