

Groupe de travail Réseau  
**Request for Comments : 3527**  
 Catégorie : En cours de normalisation  
 Traduction Claude Brière de L'Isle

K. Kinnear & M. Stapp  
 R. Johnson & J. Kumarasamy  
 Cisco Systems  
 avril 2003

## Sous option de choix de liaison pour l'option d'information d'agent de relais dans DHCPv4

### 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 (2003). Tous droits réservés

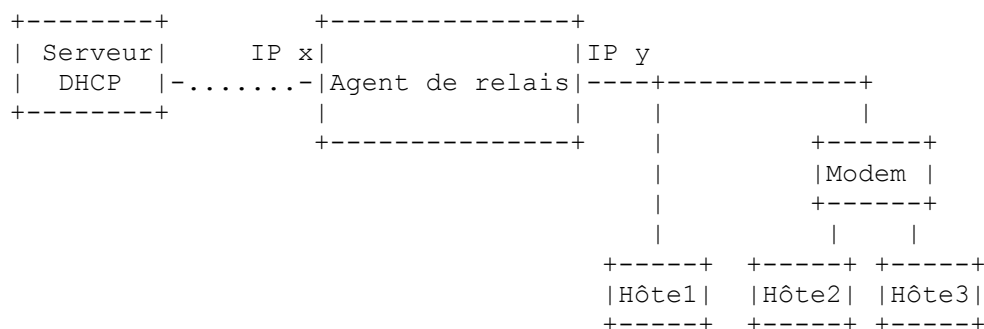
### Résumé

Le présent document décrit la sous option de choix de liaison de l'option Informations d'agent de relais pour le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*). Le paramètre giaddr spécifie une adresse IP qui détermine à la fois un sous-réseau, et par là une liaison sur laquelle réside un client DHCP, et une adresse IP qui peut être utilisée pour communiquer avec l'agent de relais. L'option de choix du sous-réseau permet de partager les fonctions du giaddr afin que lorsque une entité joue le rôle de mandataire DHCP, elle puisse spécifier le sous-réseau/liaison à partir duquel allouer une adresse IP, qui est différente de l'adresse IP au moyen de laquelle elle désire communiquer avec le serveur DHCP. Des situations analogues existent lorsque l'agent de relais a besoin de spécifier le sous-réseau/liaison sur lequel réside un client DHCP, qui est différente d'une adresse IP qui peut être utilisée pour communiquer avec l'agent de relais.

## 1. Introduction

Dans la [RFC2131], le giaddr spécifie une adresse IP qui détermine un sous-réseau (et de là une liaison) sur laquelle réside un client DHCP ainsi qu'une adresse IP qui peut être utilisée pour communiquer avec l'agent de relais. L'option de choix de sous-réseau [RFC3011] permet de partager ces fonctions du giaddr afin que lorsque une entité joue le rôle de mandataire DHCP, elle puisse spécifier le sous-réseau/liaison à partir duquel allouer une adresse IP différente de l'adresse IP au moyen de laquelle elle désire communiquer avec le serveur DHCP.

Des situations analogues existent lorsque l'agent de relais a besoin de spécifier le sous-réseau/liaison sur lequel un client DHCP réside, qui est différent d'une adresse IP qui peut être utilisée pour communiquer avec l'agent de relais. Considérons l'architecture suivante :



Dans l'approche habituelle, l'agent de relais mettrait l'adresse IP Y dans le giaddr de tout paquet qu'il transmet au serveur DHCP. Cependant, si pour une raison quelconque, l'adresse IP Y n'est pas accessible à partir du serveur DHCP, cette approche va échouer. Il y a plusieurs raisons qui font que IP y puisse être inaccessible depuis le serveur DHCP :

- o il peut y avoir une capacité de pare-feu dans l'élément de réseau dans lequel réside l'agent de relais qui ne permet pas au serveur DHCP d'accéder à l'agent de relais via IP y :
- o il peut n'y avoir pas de IP y. Un exemple serait le cas où il y a seulement un hôte et qu'on a une liaison point à point.

Dans ces cas, ou d'autres, l'agent de relais doit être capable de communiquer au serveur DHCP le sous-réseau/liaison à partir duquel allouer une adresse IP. L'adresse IP, qui va communiquer au serveur DHCP les informations de sous-réseau/liaison, ne peut pas être utilisée comme moyen de communiquer entre le serveur DHCP et l'agent de relais.

Comme l'agent de relais ne peut modifier la demande DHCP du client que de deux façons, le giaddr et l'option Informations d'agent de relais, il est nécessaire d'étendre l'option Informations d'agent de relais avec une nouvelle sous option, la sous-option Choix de liaison, pour permettre la séparation de la spécification du sous-réseau/liaison de l'adresse IP à utiliser lors de la communication avec l'agent de relais.

## 2. Terminologie

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].

Le présent document utilise les termes suivants :

"DHCP client" : hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration comme une adresse réseau.

"agent de relais DHCP" : agent de relais tiers qui transfère des messages BOOTP et DHCP entre les clients et serveurs résidant sur des sous-réseaux différents, selon les [RFC0951] et [RFC1542].

"serveur DHCP" : hôte Internet qui retourne les paramètres de configuration aux clients DHCP.

"liaison" : facilité ou support de communications sur lequel les nœuds peuvent communiquer à la couche liaison, c'est-à-dire, la couche immédiatement en dessous de IPv4. Des exemples sont les Ethernets (simples ou pontés) ; les liaisons PPP ; les réseaux X.25, de relais de trame, ou ATM ; et les "tunnels" de couche Internet (ou supérieure) tels que les tunnels sur IPv4 ou IPv6 lui-même.

"sous-réseau" : cela consiste (pour les besoins du présent document) en une gamme d'adresses acheminables. Il peut en exister un ou plusieurs au même moment sur une liaison.

## 3. Définition de la sous option de choix de liaison

La sous option Choix de liaison est utilisée par tout agent de relais DHCP qui désire spécifier un sous-réseau/liaison pour une demande de client DHCP qu'il relaye mais a besoin que la spécification du sous-réseau/liaison soit différente de l'adresse IP que le serveur DHCP devrait utiliser lorsque il communique avec l'agent de relais.

La sous-option contient une seule adresse IP qui est une adresse contenue dans un sous-réseau. La valeur pour l'adresse de sous-réseau est déterminée en prenant toute adresse IP sur le sous-réseau et en l'ajoutant par l'opération logique ET au gabarit de sous-réseau (c'est-à-dire que les bits du réseau et du sous-réseau sont laissés à part et les bits d'adresse restants sont mis à zéro). Cela détermine un seul sous-réseau, et lorsque on alloue une adresse IP, tous les autres sous-réseaux sur la même liaison vont aussi être considérés de la même manière qu'ils sont actuellement spécifiés pour le traitement du giaddr au premier point 4 du paragraphe 4.3.1 de la [RFC2131].

Dans les scénarios où cette sous-option est nécessaire, l'agent de relais l'ajoute chaque fois qu'il règle la valeur de giaddr (c'est-à-dire, sur tous les messages relayés au serveur DHCP).

Lorsque le serveur DHCP alloue une adresse et que cette sous-option est présente, le serveur DHCP DOIT alors allouer l'adresse sur :

- o le sous-réseau spécifié dans la sous-option Choix de liaison , ou
- o un sous-réseau sur la même liaison (aussi appelé un segment de réseau) que le sous-réseau spécifié par la sous-option Choix de liaison.

Le format de la sous-option est :

```

Ss/opt Longu. Adresse IP de sous-réseau
+-----+-----+-----+-----+-----+-----+
| 5   | 4   | a1  | a2  | a3  | a4  |
+-----+-----+-----+-----+-----+

```

Un agent de relais qui utilise cette sous-option DOIT supposer que le serveur qui reçoit la sous-option la prend en charge et utilise les informations disponibles dans la sous-option pour allouer correctement une adresse IP. Un agent de relais qui utilise cette sous-option NE DOIT PAS prendre d'actions différentes sur la base de ce que cette sous-option apparaît ou pas dans le paquet de réponse venant du serveur.

Il est important de s'assurer, en utilisant des techniques administratives, que tout agent de relais qui emploie cette sous-option est conduit à n'envoyer les paquets qu'à un serveur qui prend en charge cette sous-option.

Le prise en charge de cette sous-option n'exige pas de changement aux opérations ou caractéristiques du serveur DHCP autres que de choisir le sous-réseau (et la liaison) sur lequel allouer une adresse. Par exemple, le traitement de DHCPDISCOVER pour un sous-réseau inconnu devrait continuer de fonctionner sans changement.

Dans le cas d'un serveur DHCP qui reçoit un paquet contenant à la fois une option Choix de sous-réseau [RFC3011], et une sous-option Choix de liaison, les informations contenues dans la sous-option Choix de liaison DOIVENT être utilisées pour contrôler l'allocation d'une adresse IP de préférence aux informations contenues dans l'option Choix de sous-réseau.

Lorsque cette sous-option est présente et que le serveur prend en charge cette sous-option, le serveur NE DOIT PAS offrir une adresse qui n'est pas sur le sous-réseau demandé pour la liaison (segment de réseau) auquel ce sous-réseau est associé.

L'adresse IP à laquelle un serveur DHCP envoie une réponse DOIT être la même que celle qu'il aurait choisi en l'absence de cette sous-option.

#### **4. Considérations sur la sécurité**

Les attaques potentielles contre DHCP sont discutées à la section 7 de la spécification du protocole DHCP [RFC2131], ainsi que dans la spécification de l'authentification DHCP [RFC3118].

La sous-option Choix de liaison permet à un agent de relais de spécifier le sous-réseau/liaison sur lequel allouer une adresse pour un client DHCP. Étant donné que l'option Choix de sous-réseau existe déjà [RFC3011], aucun nouveau problème fondamental de sécurité n'est soulevé par l'existence de la sous-option Choix de liaison spécifiée dans le présent document au delà de ceux impliqués par l'option Choix de sous-réseau [RFC3011].

L'existence de l'une ou l'autre option de choix de sous-réseau ou sous-option de choix de liaison documentée ici permettrait à un client DHCP malveillant d'effectuer une attaque plus complète d'épuisement de réservoir d'adresses qu'il ne le pourrait sans l'utilisation de ces options, car le client ne serait plus restreint à attaquer les réservoirs d'adresses sur son seul sous-réseau local.

Il existe une protection mineure contre cette forme d'attaque qui utilise cette sous-option et qui n'est pas présente pour l'option de choix de sous-réseau, en ce qu'un agent de relais de confiance qui prend en charge l'option Information d'agent de relais DOIT éliminer un paquet qu'il reçoit avec un giaddr à zéro et une option Information d'agent de relais lorsque ce paquet arrive sur un circuit qui n'est pas "de confiance" ( paragraphe 2.1 de la [RFC3046]).

#### **5. Considérations relatives à l'IANA**

L'IANA a alloué dans l'espace de sous-options de l'agent de relais DHCP [RFC3046] une valeur de 5 à la sous-option Choix de liaison définie à la Section 3.

#### **6. Remerciements**

Eric Rosen a aidé les auteurs à comprendre le besoin de cette sous-option. Beaucoup du présent document a été emprunté, avec seulement des modifications mineures, au document qui décrit l'option Choix de sous-réseau [RFC3011].

## 7. Références

### 7.1 Références normatives

- [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. (DS) (Mà J par RFC3396, RFC4361, RFC5494, et RFC6849)
- [RFC3011] G. Waters, "Option de [sélection de sous-réseau](#) IPv4 pour DHCP", novembre 2000. (P.S.)
- [RFC3046] M. Patrick, "Option DHCP [Information d'agent de relais](#)", janvier 2001. (MàJ par RFC6607)

### 7.2 Références pour information

- [RFC0951] B. Croft et J. Gilmore, "[Protocole BOOTSTRAP](#) (BOOTP)", septembre 1985.
- [RFC1542] W. Wimer, "Précisions et extensions au protocole Bootstrap", octobre 1993. (D.S.)
- [RFC3118] R. Droms et W. Arbaugh, "[Authentification des messages](#) DHCP", juin 2001. (P.S.)

## 8. Déclaration de 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](mailto:ietf-ipr@ietf.org).

## 9. Adresses des auteurs

Kim Kinnear  
Cisco Systems  
1414 Massachusetts Ave  
Boxborough, Ma. 01719  
téléphone : (978) 936-0000  
mél : [kkinnear@cisco.com](mailto:kkinnear@cisco.com)

Mark Stapp  
Cisco Systems  
1414 Massachusetts Ave  
Boxborough, Ma. 01719  
téléphone: (978) 936-0000  
mél : [mjs@cisco.com](mailto:mjs@cisco.com)

Jay Kumarasamy  
Cisco Systems  
170 W. Tasman Dr.  
San Jose, CA 95134  
téléphone : (408) 526-4000  
mél : [jayk@cisco.com](mailto:jayk@cisco.com)

Richard Johnson  
Cisco Systems  
170 W. Tasman Dr.  
San Jose, CA 95134  
téléhone : (408) 526-4000  
mél : [raj@cisco.com](mailto:raj@cisco.com)

## 10. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003). 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 droits de reproduction ci-dessus et le présent 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 droits de reproduction 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 droits de reproduction 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 ses 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.