Groupe de travail Réseau
Request for Comments : 3046
Catégorie : En cours de normalisation

M. Patrick, Motorola BCS
janvier 2001
Traduction Claude Brière de L'Isle

Option DHCP Informations d'agent de relais

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.

Résumé
Les plus nouvelles technologies d'accès à grande vitesse à l'Internet public mettent en place des modems à haut débit pour assurer le rattachement à d'un réseau de zone locale (LAN, *local area network*) d'un ou plusieurs hôtes dans des locaux d'utilisateurs. Il est avantageux d'utiliser le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) comme défini dans la [RFC2131] pour allouer des adresses IP à l'hôte dans des locaux d'utilisateur dans cet environnement. Cependant, un certain nombre de problèmes de sécurité et d'adaptabilité surviennent avec une telle utilisation "publique" de DHCP. Le présent document décrit une nouvelle option DHCP pour régler ces problèmes. Cette option étend l'ensemble des options DHCP tel que défini dans la [RFC2132].

La nouvelle option est appelée option Informations d'agent de relais et elle est insérée par l'agent de relais DHCP lorsque il transmet des paquets DHCP générés par un client à un serveur DHCP. Les serveurs qui reconnaissent l'option Informations d'agent de relais peuvent utiliser les informations pour mettre en œuvre une adresse IP ou autre politique d'allocation de paramètres. Le serveur DHCP fait écho à l'option à l'agent de relais dans les réponses de serveur à client, et l'agent de relais épluche l'option avant de transmettre la réponse au client.

L'option "Informations d'agent de relais" est organisée comme une seule option DHCP qui contient une ou plusieurs "sous-options" qui convoient des informations connues par l'agent de relais. Les sous-options initiales sont définies pour un agent de relais qui est colocalisé dans une unité d'accès de circuit public. Cela inclut un "Identifiant de circuit" pour le circuit entrant, et un "Identifiant distant" qui fournit un identifiant de confiance pour le modem à haut débit distant.

Table des matières

1. Introduction

1.1 Réseaux de données à commutation de circuits à haut débit

L'accès public à l'Internet se fait habituellement via un réseau de données à commutation de circuits. Aujourd'hui, ceci est principalement mis en œuvre avec des modems à numérotation téléphonique qui se connectent à un serveur d'accès distant. Mais des réseaux d'accès par circuit à plus grande vitesse incluent aussi le RNIS, l'ATM, le relais de trame, et les réseaux de données par câble. Tous ces réseaux peuvent être caractérisés comme une topologie en "étoile" où plusieurs utilisateurs se connectent à une "unité d'accès de circuit" via des circuits commutés ou permanents.

Avec les modems à numérotage, un seul PC hôte tente de se connecter au point central. Le protocole PPP est largement utilisé pour allouer les adresses IP à utiliser par un seul hôte PC.

Les technologies récentes de circuit à haut débit fournissent cependant fréquemment une interface de LAN (en particulier Ethernet) à un ou plusieurs PC hôtes. Il est souhaitable de prendre en charge l'allocation centralisée des adresses IP des ordinateurs hôtes qui se connectent sur de tels circuits via DHCP. Le serveur DHCP peut être, mais ne l'est généralement pas, mis en œuvre conjointement avec l'appareil de concentration d'accès de circuit centralisé. Le serveur DHCP est souvent connecté comme un serveur séparé sur le "LAN central" auquel le ou les appareils d'accès central sont rattachés.

Un modèle physique commun pou les circuits d'accès Internet à haut débit est présenté à la Figure 1, ci-dessous.

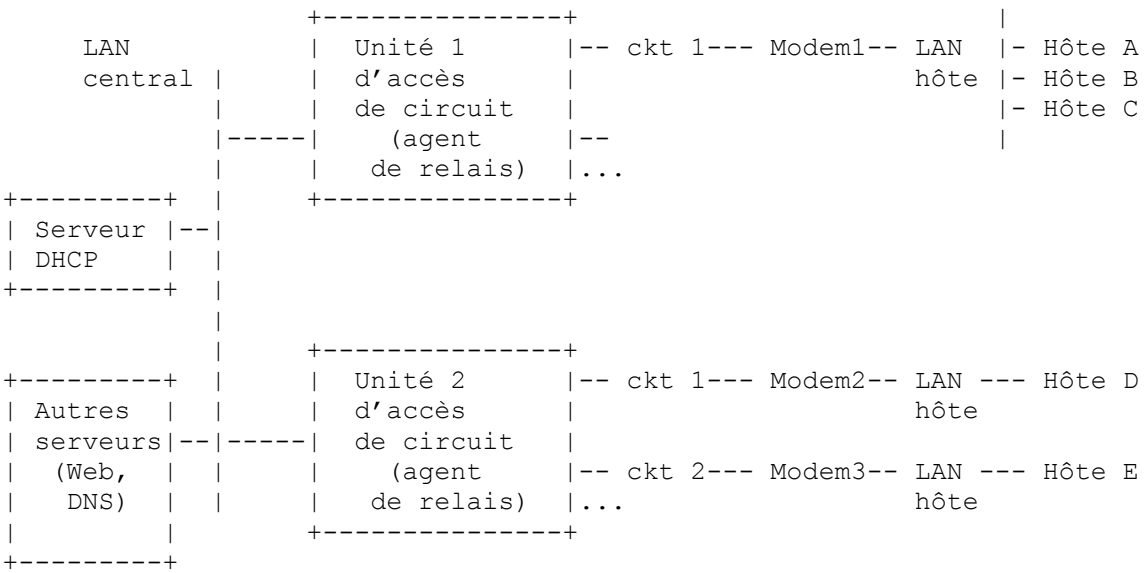


Figure 1 : Modèle DHCP de circuit d'accès haut débit

Noter que dans ce modèle, le "modem" connecte un LAN au site de l'utilisateur, plutôt qu'à un seul hôte. Plusieurs hôtes sont mis en œuvre sur ce site. Bien qu'il soit certainement possible de mettre en œuvre un routeur IP complet sur le site utilisateur, cela exige un équipement relativement coûteux (par rapport au coût d'un modem normal). De plus, un routeur exige une adresse IP non seulement pour chaque hôte, mais aussi pour le routeur lui-même. Finalement, un routeur sur le côté utilisateur exige un sous-réseau IP logique (LIS, *Logical IP Subnet*) dédié pour chaque utilisateur. Alors que ce modèle est approprié pour des environnements de relativement petits réseaux d'entreprise, il n'est pas adapté pour les grands réseaux avec accès public. Dans ce scénario, il est avantageux de mettre en œuvre un modèle de réseautage IP qui n'alloue pas une adresse IP au modem (ou autre appareil de réseautage sur le site utilisateur) et en particulier pas un LIS entier au LAN côté utilisateur.

Noter que l'utilisation de cette méthode pour obtenir des adresses IP signifie que les adresses IP ne peuvent être obtenues que lorsque la communication est disponible avec le site central. Certaines installations de LAN hôte peuvent utiliser un serveur DHCP local ou d'autres méthodes pour obtenir les adresses IP pour un usage domestique.

1.2 Agent de relais DHCP dans l'unité d'accès de circuit

Il est souhaitable d'utiliser DHCP pour allouer les adresses IP pour l'accès public aux circuits à haut débit. Un certain nombre d'unités d'accès de circuit (par exemple, les RAS, les systèmes de terminaison de modems câbles, les unités d'accès à l'ADSL, etc.) connectent à un LAN (ou à un internet local) auquel est rattaché un serveur DHCP.

Pour des raisons d'adaptabilité et de sécurité, il est avantageux de mettre en œuvre un "bond de routeur" à l'unité d'accès de circuit, un peu comme font aujourd'hui les RAS à haut débit. L'équipement d'accès de circuit agit à la fois comme un routeur envers les circuits et comme l'agent de relais DHCP.

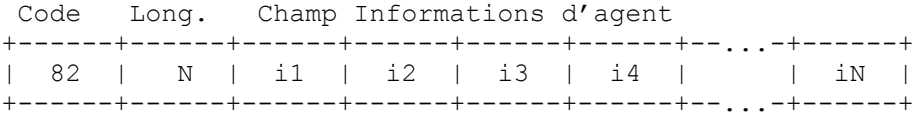
Les avantages de colocaliser l'agent de relais DHCP avec l'équipement d'accès de circuit sont que :
- les réponses en diffusion de DHCP peuvent être acheminées sur le seul circuit approprié, évitant la duplication de la diffusion de la réponse DCHP sur des milliers de circuits d'accès ;
- le même mécanisme utilisé pour identifier la connexion distante du circuit (par exemple, un identifiant d'utilisateur par un serveur d'accès distant agissant comme équipement d'accès de circuit) peut être utilisé comme identifiant d'hôte par DHCP, et utilisé pour l'allocation de paramètres. Cela inclut l'allocation centralisée des adresses IP aux hôtes. Cela donne un identifiant distant sûr à partir d'une source de confiance -- l'agent de relais.

Un certain nombre de questions se posent lors de la transmission de demandes DHCP provenant d'hôtes qui connectent des circuits haut débit à accès public à des connexions de LAN chez l'hôte. Beaucoup sont des questions de sécurité qui viennent de ce que des demandes de client DHCP proviennent de sources qui ne sont pas de confiance. Comment l'agent de relais sait-il sur quel circuit transmettre les réponses ? Comment le système empêche t-il les attaques IP par épuisement sur DHCP ? C'est quand un attaquant demande toutes les adresses IP disponibles à un serveur DHCP en envoyant des demandes avec des adresses MAC de clients falsifiés. Comment une adresse IP ou un LIS peut-il être alloué de façon permanente à un utilisateur ou modem particulier ? Comment empêche t-on "l'usurpation" des champs d'identifiant de clients utilisés pour allouer les adresses IP ? Comment empêche t-on le déni de service par "l'usurpation" des adresses MAC des autres clients ?

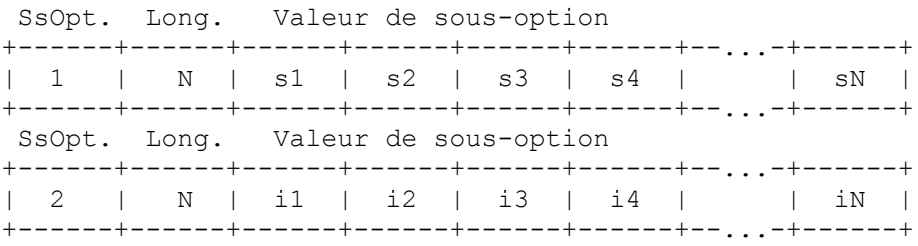
Toutes ces questions peuvent trouver leur solution en faisant que l'équipement d'accès de circuit, qui est un composant de confiance, ajoute des informations aux demandes des clients DHCP qu'il transmet au serveur DHCP.

2. Option Informations d'agent de relais

Le présent document définit une nouvelle option DHCP appelée Informations d'agent de relais. C'est une option "conteneur" pour les sous-options spécifiques fournies par l'agent. Le format de l'option Informations d'agent de relais est le suivant :



La longueur N donne le nombre total d'octets dans le champ Informations d'agent. Le champ Informations d'agent consiste en une séquence de triplets SsOpt/Longueur/Valeur pour chaque sous-option, codé de la façon suivante :



Aucune sous-option "de bourrage" n'est définie, et le champ Information NE DEVRA PAS se terminer par une sous-option 255. La longueur N de l'option Information d'agent DHCP devra inclure tous les octets des triplets code/longueur/valeur de la sous-option. Comme au moins une sous-option doit être définie, le minimum de longueur des informations d'agent de relais est deux (2). La longueur N des sous-options devra être le nombre d'octets dans seulement ce champ de valeur de la sous-option. Une longueur de sous-option peut être zéro. Les sous-options n'ont pas besoin d'apparaître dans l'ordre des codes de sous-option.

L'allocation initiale des sous-options d'agent de relais DHCP est la suivante :

Code de sous-option d'agent	Description de la sous-option
1	Sous-option d'agent Identifiant de circuit
2	Sous-option d'agent Identifiant distant

2.1 Fonctionnement de l'agent

L'ajout global de l'option Agent de relais DHCP DEVRAIT être configurable, et DEVRAIT être désactivé par défaut. Les agents de relais DEVRAIENT avoir des outils de configuration séparés pour contrôler si chaque sous-option est ajoutée aux paquets de client à serveur.

Un agent de relais DHCP qui ajoute un champ Informations d'agent de relais DEVRA l'ajouter à la dernière option (mais avant "Fin d'option" 255, si il est présent) dans le champ des options DHCP de tout BOOTP reconnu ou paquet DHCP transmis d'un client à un serveur.

Les agents de relais qui reçoivent un paquet DHCP provenant d'un circuit qui n'est pas de confiance avec giaddr réglé à zéro (ce qui indique qu'ils sont le routeur de premier bond) mais avec une option Informations d'agent de relais déjà présente dans le paquet DEVRA éliminer le paquet et incrémenter un compte d'erreur. Un circuit de confiance peut contenir un élément de réseau (pont) de confiance vers l'aval (plus près du client) entre l'agent de relais et le client qui PEUT ajouter une option d'agent de relais mais pas établir le champ giaddr. Dans ce cas, l'agent de relais N'AJOUTE PAS une "seconde" option d'agent de relais, mais transmet le paquet DHCP selon les opérations normales d'agent de relais DHCP, réglant le champ giaddr comme il paraît approprié.

Les mécanismes pour distinguer entre les circuits "de confiance" et "pas de confiance" sont spécifiques du type d'équipement de terminaison de circuit, et peuvent impliquer l'administration locale. Par exemple, un système de terminaison de modem câble peut considérer les paquets provenant de la plupart des modems câbles en amont comme "pas de confiance", mais un commutateur ATM qui est à l'extrémité de circuits virtuels (VC) commutés à travers un DSLAM peut considérer de tels VC comme "de confiance" et accepter une option d'agent de relais ajoutée par le DSLAM.

Les agents de relais PEUVENT être configurables à la taille maximum de paquet DHCP à créer après avoir ajouté l'option Informations d'agent. Les paquets qui, après ajout de l'option Informations d'agent de relais, dépasseraient cette taille maximum configurée devront être transmis SANS ajouter l'option Informations d'agent. Un compteur d'erreur DEVRAIT être incrémenté dans ce cas. En l'absence de cette configuration, l'agent NE DEVRA PAS augmenter une taille de paquet DHCP jusqu'à excéder la MTU de l'interface sur laquelle elle est transmise.

L'option Informations d'agent de relais à laquelle fait écho un serveur DOIT être retirée par l'agent de relais ou par l'élément de réseau aval de confiance qui l'a ajoutée lors de la transmission de la réponse de serveur à client en retour au client.

L'agent NE DEVRA PAS ajouter une option "Surcharge d'option" au paquet ou utiliser les champs "file" ou "sname" pour ajouter l'option Informations d'agent de relais. Il NE DEVRA PAS analyser ou retirer les options Informations d'agent de relais qui peuvent apparaître dans les champs sname ou file d'un paquet de serveur à client transmis à travers l'agent.

Le fonctionnement des agents de relais pour les différentes sous-options est spécifié avec cette sous-option.

Les agents de relais NE SONT PAS obligés de surveiller ou modifier les paquets DHCP générés par le client et adressés à une adresse de serveur en envoi individuel. Cela inclut les DHCP-REQUEST envoyées lors de l'entrée dans l'état RENEWING.

Les agents de relais NE DOIVENT PAS modifier les paquets DHCP qui utilisent l'en-tête d'authentification IPsec ou l'encapsulation de charge utile IPsec [RFC2401].

2.1.1 Demandes DHCP retransmises

Un agent de relais DHCP peut recevoir un paquet DHCP de client transmis d'un agent de relais BOOTP/DHCP plus proche du client. Un tel paquet aura une giaddr différente de zéro, et avoir déjà ou non une option Agent de relais DHCP.

Les agents de relais configurés pour ajouter une option Agent de relais qui reçoivent un paquet DHCP de client avec une giaddr différente de zéro DEVRONT éliminer le paquet si la giaddr simule une adresse giaddr mise en œuvre par l'agent local lui-même.

Autrement, l'agent de relais DEVRA transmettre tout paquet DHCP reçu avec une giaddr valide différente de zéro SANS ajouter d'option Agent de relais. Selon la [RFC2131], il ne devra pas non plus modifie la valeur de la giaddr.

2.2 Fonctionnement du serveur

Les serveurs DHCP qui n'ont pas la capacité de l'option Informations d'agent de relais vont ignorer l'option lorsque ils la reçoivent et ne vont pas y faire écho en réponse. C'est le comportement de serveur spécifié pour les options inconnues.

Les serveurs DHCP qui revendiquent la prise en charge de l'option Informations d'agent de relais DEVRONT faire écho au contenu entier de l'option Informations d'agent de relais dans toutes les réponses. Les serveurs DEVRAIENT copier l'option Informations d'agent de relais comme dernière option DHCP dans la réponse. Les serveurs NE DEVRONT PAS placer l'option Informations d'agent de relais en écho dans les champs sname ou file surchargés. Si un serveur n'est pas capable de copier un champ complet d'informations d'agent de relais dans une réponse, il DEVRA envoyer la réponse sans le champ Informations de relais, et DEVRAIT incrémenter un compteur d'erreur pour cette situation.

Le fonctionnement des serveurs DHCP pour les différentes sous-options est spécifié avec cette sous-option.

Noter que les agents de relais DHCP ne sont pas obligés de surveiller les messages DHCP en envoi individuel qui sont envoyés directement entre le client et le serveur (c'est-à-dire, ceux qui ne sont pas envoyés via un agent de relais). Cependant, certains agents de relais PEUVENT choisir de faire une telle surveillance et ajouter des options d'agent de relais. Par conséquent, les serveurs DEVRAIENT être prêts à traiter les options d'agent de relais dans des messages en envoi individuel, mais ils NE DOIVENT PAS s'attendre à ce qu'elles soient toujours là.

3. Sous-options d'informations d'agent de relais

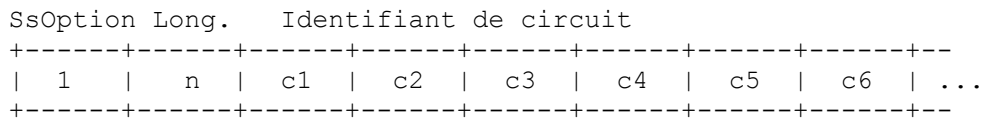
3.1 Sous-option d'agent Identifiant de circuit

Cette sous-option PEUT être ajoutée par les agents de relais DHCP qui terminent les circuits commutés ou permanents. Elle code un identifiant d'agent local du circuit d'où un paquet de client DHCP à serveur a été reçu. Elle est destinée à être utilisée par les agents pour relayer les réponses DHCP en retour sur le circuit approprié. Des utilisations possibles de ce champ incluent :

- le numéro d'interface du routeur
- le numéro d'accès de la plateforme de commutation
- le numéro d'accès du serveur d'accès distant
- le DLCI *(Data Link Connection Identifier,* identifiant de connexion de liaison de données) de relais de trame
- le numéro de circuit virtuel ATM
- le numéro de circuit virtuel de données par câble

Les serveurs PEUVENT utiliser l'identifiant de circuit pour IP et les autres politiques d'allocation de paramètres. L'identifiant de circuit DEVRAIT être considéré comme une valeur opaque, avec des politiques fondées seulement sur la correspondance exacte de chaîne ; c'est-à-dire que l'identifiant de circuit NE DEVRAIT PAS être analysé en interne par le serveur.

Le serveur DHCP DEVRAIT faire rapport de la valeur de l'identifiant de circuit d'agent des séquences actuelles dans les rapports statistiques (y compris dans sa MIB) et dans les journaux d'événements. Comme l'identifiant de circuit est seulement local sur un agent de relais particulier, un ID de circuit devrait être qualifié avec la valeur de la giaddr qui identifie l'agent de relais.



3.2 Sous-option Identifiant d'agent distant

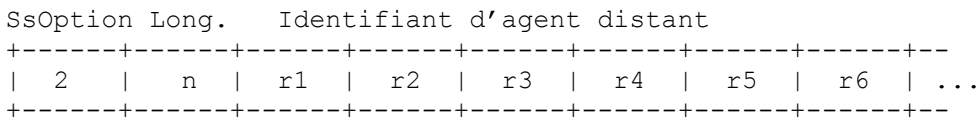
Cette sous-option PEUT être ajoutée par les agents de relais DHCP qui terminent des circuits commutés ou permanents et ont des mécanismes pour identifier l'extrémité d'hôte distant du circuit. Le champ Identifiant distant peut être utilisé pour coder, par exemple :

-- un "identifiant d'appelant" de numéro de téléphone pour une connexion numérotée
-- un "nom d'utilisateur" suggéré par un serveur d'accès distant
-- une adresse ATM d'appelant distant
-- un "identifiant de modem" d'un modem câble
-- l'adresse IP distante d'une liaison point à point
-- une adresse X.25 distante pour des connexions X.25

L'identifiant distant DOIT être unique au monde.

Les serveurs DHCP PEUVENT utiliser cette option pour choisir des paramètres spécifiques d'utilisateurs, hôtes, ou modems abonnés particuliers. L'option DEVRAIT être considérée comme une valeur opaque, avec des politiques fondées seulement sur une correspondance exacte de chaîne ; c'est-à-dire que l'option NE DEVRAIT PAS être analysée en interne par le serveur.

L'agent de relais PEUT utiliser ce champ en plus de, ou à la place, du champ Identifiant de circuit d'agent pour choisir le circuit sur lequel transmettre la réponse DHCP (par exemple, Offer, Ack, ou Nak). Les serveurs DHCP DEVRAIENT faire rapport de cette valeur dans tout rapport ou MIB associé à un client particulier.



4. Questions réglées

L'option d'agent de relais DHCP résout plusieurs problèmes dans un environnement où des hôtes qui ne sont pas de confiance accèdent à un internet via un réseau public de circuits. Cette résolution suppose que tout le trafic de protocole DHCP des hôtes publics traverse l'agent de relais DHCP et que le réseau IP entre l'agent de relais DHCP et le serveur DHCP n'est pas compromis.

Transmission en diffusion
L'équipement d'accès de circuit ne transmet la réponse DHCP qui est normalement en diffusion que sur le circuit indiqué dans l'identifiant de circuit d'agent.

Épuisement d'adresses DHCP
En général, le serveur DHCP peut avoir une extension pour tenir une base de données avec le "triplet" (adresse IP de client, adresse MAC de client, identifiant de client distant).
Le serveur DHCP DEVRAIT mettre en œuvre des politiques qui restreignent le nombre d'adresses IP à allouer à un seul identifiant distant.

Allocation statique
Le serveur DHCP peut utiliser l'identifiant distant pour choisir l'adresse IP à allouer. Il peut permettre l'allocation statique des adresses IP à des identifiants distants particuliers, et interdire une demande d'adresse d'un identifiant distant non autorisé.

Mystification IP
L'appareil d'accès au circuit peut associer l'adresse IP allouée par un serveur DHCP dans un paquet d'accusé de réception DHCP transmis au circuit auquel il a été transmis. L'appareil d'accès au circuit PEUT empêcher la transmission des paquets IP qui ont des adresses IP de source autres que celles qu'il a associé au circuit receveur. Cela empêche de simples attaques de mystification IP sur le LAN central, et la mystifications des autres hôtes IP.

Usurpation d'identifiant de client
En utilisant l'option d'identifiant d'agent distant fourni par l'agent, il n'est pas besoin pour le serveur DHCP d'utiliser le champ qui n'est pas de confiance et pas encore normalisé d'identifiant de client.

Usurpation d'adresse MAC
En associant une adresse MAC à un identifiant d'agent distant, le serveur DHCP peut empêcher d'offrir une adresse IP à un attaquant qui usurpe la même adresse MAC sur un identifiant distant différent.

5. Considérations pour la sécurité

DHCP tel qu'actuellement défini ne fournit pas de mécanisme d'authentification ou de sécurité. Les expositions potentielles aux attaques sont présentées à la section 7 de la spécification du protocole DHCP dans la [RFC2131].

Le présent document introduit des mécanismes pour contrer plusieurs attaques contre la sécurité du fonctionnement de l'allocation d'adresse IP, y compris l'usurpation IP, l'usurpation d'identifiant client, l'usurpation d'adresse MAC, et

l'épuisement des adresses du serveur DHCP. Il s'appuie sur une relation de confiance implicite entre l'agent de relais DHCP et le serveur DHCP, avec un client DHCP supposé non de confiance. Il introduit un nouvel identifiant, le "ID distant", qui est aussi supposé être de confiance. L'identifiant distant est fourni par le réseau ou modem d'accès et non par l'équipement dans les locaux du client. Les techniques cryptographiques ou autres pour authentifier l'ID distant sont certainement possibles et conseillées, mais elles sortent du domaine d'application du présent document.

Cette option vise les environnements dans lesquels l'infrastructure du réseau – l'agent de relais, le serveur DHCP, et le réseau entier dans lequel résident ces deux appareils – est de confiance et sûr. Tel qu'utilisé dans le présent document, le terme "de confiance" implique que le trafic DHCP non autorisé ne peut pas entrer dans le réseau de confiance sauf à travers un agent de relais de confiance, et que tous les appareils internes au réseau sont sûrs et de confiance. Les mises en œuvre potentielles de la présente option devraient prêter une considération attentive aux faiblesses potentielles de sécurité qui sont présentes dans ce modèle avant de mettre en œuvre l'option dans des réseaux réels.

Noter que tout mécanisme futur d'authentification des communications de client à serveur DHCP doit veiller à omettre l'option d'agent de relais DHCP des calculs d'authentification de serveur. C'est la principale raison de l'organisation de l'option Agent de relais DHCP comme une seule option avec des sous-options, et de l'exigence que l'agent de relais retire l'option avant de transmettre au client.

Bien qu'il sorte du domaine d'application du présent document de spécifier l'algorithme général de transmission des unités d'accès de circuits de données publics, noter que la retransmission automatique de paquets IP ou ARP en diffusion en retour vers l'aval expose à de sérieux risques pour la sécurité d'IP. Par exemple, si une diffusion de l'amont de DHCP-DISCOVER ou DHCP-REQUEST est rediffusée vers l'aval, tout hôte public peut aisément mystifier le serveur DHCP désiré.

6. Considérations pour l'IANA

L'IANA est priée de tenir un nouvel espace de noms de "sous-options d'agent de relais DHCP", situé dans le registre des paramètres BOOTP-DHCP. Les initiales de sous-options sont décrites à la section 2 du présent document.

L'IANA alloue les futures sous options d'agent de relais DHCP sous la politique de "consensus IETF" décrite dans la [RFC2434]. Les propositions de sous-options futures seront référencées symboliquement dans les projets Internet qui les décrivent, et l'IANA leur allouera des codes numériques lorsque ils seront approuvés pour publication comme RFC.

7. Notices de propriété intellectuelle

La présente section contient deux notices comme exigé par la [RFC2026] pour les documents en cours de normalisation.

L'IETF ne prend position sur la validité ou la portée d'aucun droit de propriété intellectuelle ou d'autres droits qui pourraient 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 non disponible ; pas plus qu'elle ne prétend qu'elle ait fait aucun effort pour identifier de tels droits. Des informations sur les procédures de l'IETF au sujet des droits dans la documentation en cours de normalisation et en rapport avec les normes peuvent être trouvées dans le BCP-11. Des copies des revendications de droits peuvent être disponibles à la publication et toutes les assurances de licences peuvent être rendues disponibles, ou le résultat de tentatives d'obtention d'une licence ou permission générale pour l'utilisation de tels droits de propriété par les mises en œuvre ou utilisateurs de la présente spécification peuvent être obtenus auprès du secrétariat de l'IETF.

Une revendication de droits de propriété intellectuelle a été notifiée à l'IETF à l'égard de tout ou partie de la spécification contenue dans le présent document. Pour d'autres informations, consulter la liste en ligne des revendications de droits.

8. Références

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378)

[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. *(M. à . par les RFC 3396 et 4361)*

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la RFC 5226)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir RFC4301*)

9. Glossaire

DSLAM *(Digital Subscriber Link Access Module)* module d'accès à une ligne d'abonné numérique
IANA *(Internet Assigned Numbers Authority)* Autorité d'allocation des numéros de l'Internet
LIS *(Logical IP Subnet)* sous-réseau logique IP
MAC *(Message Authentication Code)* code d'authentification de message
RAS *(Remote Access Server)* serveur d'accès distant

10. Adresse de l'auteur

Michael Patrick
Motorola Broadband Communications Sector
20 Cabot Blvd., MS M4-30
Mansfield, MA 02048
USA
téléphone : (508) 261-5707
mél : michael.patrick@motorola.com

Déclaration complète de droits de reproduction

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