Groupe de travail Réseau
Request for Comments : 4436
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft Corporation
J. Carlson, Sun Microsystems
S. Cheshire, Apple Computers
mars 2006

Détection du rattachement réseau dans IPv4 (DNAv4)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir 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 (2006). Tous droits réservés.

Résumé
Le temps nécessaire pour détecter un mouvement entre des réseaux et pour obtenir (ou continuer à utiliser) une configuration IPv4 peut être une fraction significative de la latence totale de transfert inter-cellulaire lorsque on se déplace entre des points de rattachement. Le présent document fait la synthèse, à partir de l'expérience du déploiement des hôtes qui prennent en charge le protocole de résolution d'adresse (ARP, *Address Resolution Protocol*), le protocole de configuration dynamique du serveur (DHCP, *dynamic host configuration protocol*), et les adresses de liaison locale IPv4, d'un ensemble d'étapes connues sous le nom de détection du rattachement réseau pour IPv4 (DNAv4, *Detecting Network Attachment for IPv4*) afin de diminuer la latence du transfert inter-cellulaire lors du déplacement entre des points de rattachement.

Table des matières

1. Introduction

Le temps nécessaire pour détecter un mouvement entre des réseaux et pour obtenir (ou continuer à utiliser) une configuration IPv4 peut être une fraction significative de la latence totale de transfert inter-cellulaire lorsque on se déplace entre des points de rattachement.

Le présent document fait la synthèse, à partir de l'expérience du déploiement des hôtes qui prennent en charge ARP [RFC826], DHCP [RFC2131], et les adresses de liaison locale IPv4 [RFC3927], d'un ensemble d'étapes connues sous le nom de détection du rattachement réseau pour IPv4 (DNAv4, *Detecting Network Attachment for IPv4*). DNAv4 optimise le cas (courant) de rattachement à un réseau de quelqu'un qui y a été connecté précédemment et tente de réutiliser une configuration antérieure (mais encore valide) en réduisant le délai de rattachement sur les LAN à quelques millisecondes. Comme cette procédure dépend du protocole ARP, elle ne convient pas pour une utilisation sur des supports qui n'acceptent pas ARP.

1.1 Applicabilité

DHCP est un mécanisme efficace et largement adopté pour qu'un hôte obtienne une adresse IP à utiliser sur une liaison réseau particulière, ou pour revalider une adresse obtenue précédemment via le mécanisme DHCP INIT-REBOOT [RFC2131].

Lorsque il obtient une nouvelle adresse, DHCP spécifie que le client DEVRAIT utiliser ARP pour vérifier que l'adresse offerte n'est pas déjà utilisée. Le processus de détection de conflit d'adresse [RFC5227] peut prendre jusqu'à sept secondes. En principe, cet intervalle de temps pourrait être raccourci, avec le compromis évident : moins un hôte passe de temps à attendre pour voir si un autre hôte utilise déjà l'adresse concernée, plus grand est le risque de conflits d'adresse inattendus.

Lorsque le client réussit à revalider une adresse obtenue précédemment en utilisant le mécanisme INIT-REBOOT, la spécification DHCP n'exige pas que le client effectue la détection de conflit d'adresse, de sorte que ce délai de sept secondes ne s'applique pas. Cependant, le serveur DHCP peut être lent à répondre ou peut être désactivé et ne pas répondre du tout, et les hôtes pourraient bénéficier d'un autre moyen pour déterminer rapidement si une adresse obtenue précédemment est valide pour être utilisée sur cette liaison particulière.

Lorsque le client se déplace entre des réseaux, la tentative de revalidation d'adresse peut échouer ; un NAK DHCP peut être reçu en réponse à une demande DHCP, causant le redémarrage du processus de configuration par le client en passant à l'état INIT. Si une adresse obtenue précédemment sur le nouveau réseau est encore fonctionnelle, DNAv4 permet à l'hôte de confirmer rapidement la nouvelle configuration, en sautant le redémarrage du processus de configuration et de détection de conflit.

Le mécanisme de remplacement spécifié par le présent document s'applique lorsque un hôte a une adresse DHCP précédemment allouée, qui n'a pas été retournée au serveur DHCP via un message DHCP RELEASE, et qui a encore du temps restant sur son allocation. Dans ce cas, l'hôte peut déterminer si il s'est rattaché à la liaison logique où l'utilisation de cette adresse est valide, en envoyant un paquet de demande ARP en envoi individuel à un routeur connu précédemment pour cette liaison (ou, dans le cas d'une liaison avec plus d'un routeur, en envoyant un ou plusieurs paquets de demande ARP en envoi individuel à un ou plusieurs de ces routeurs).

L'utilisation d'ARP en envoi individuel a un certain nombre d'avantages. Un de ceux-ci est que les paquets en envoi individuel imposent moins de charges au réseau que la diffusion de paquets, en particulier pour les réseaux 802.11 où les paquets en diffusion peuvent être envoyés à des débits aussi faibles que 1 Mbit/s. Un autre avantage est que si l'hôte n'est pas sur la liaison sur laquelle il espérait être, une demande de diffusion ARP pourrait polluer les antémémoires ARP des homologues sur cette liaison. Lorsque on utilise des adresses privées [RFC1918], un autre appareil pourrait légitimement utiliser la même adresse, et une demande de diffusion ARP pourrait déranger ses communications, causant la rupture des connexions TCP, et des problèmes similaires. Aussi, utiliser un paquet ARP en envoi individuel adressé à l'adresse MAC du routeur que l'hôte s'attend à trouver signifie que si l'hôte n'est pas sur la liaison attendue, il n'y aura pas d'appareil avec cette adresse MAC, et le paquet ARP va disparaître dans le vide sans causer aucun dommage.

Ces questions qui définissent l'applicabilité de DNAv4 nous conduisent à un certain nombre de conclusions :

- DNAv4 est une optimisation des performances. Son objet est d'accélérer un procès qui peut exiger jusqu'à quelques centaines de millisecondes (DHCP INIT-REBOOT), ainsi que de réduire de plusieurs secondes les délais de détection de conflit lorsque un hôte change de réseau.

- Au titre de l'optimisation des performances, il ne doit pas sacrifier l'exactitude. En d'autres termes, les faux positifs ne sont pas acceptables. DNAv4 ne doit pas conclure qu'un hôte est retourné sur une liaison visitée précédemment où il a une adresse IP fonctionnelle si ce n'est en fait pas le cas.

- Au titre de l'optimisation des performances, les faux négatifs sont acceptables. Ce n'est pas une exigence absolue que cette optimisation reconnaisse correctement une liaison visitée précédemment dans tous les cas possibles. Par exemple, si un routeur ignore des demandes ARP en envoi individuel, DNAv4 ne sera alors pas capable à l'avenir de détecter qu'il est retourné sur la même liaison. Ceci est acceptable parce que l'hôte fonctionne quand même correctement comme il le faisait sans DNAv4, seulement sans l'avantage de performances. Les utilisateurs et opérateurs de réseau qui désirent l'amélioration de performances offerte par DNAv4 peuvent mettre à niveau leurs routeurs pour qu'ils prennent en charge DNAv4.

- Au titre de l'optimisation des performances, lorsque DNAv4 ne réussit pas à procurer un avantage, il ne devrait ajouter que peu ou pas du tout de délai par rapport au traitement actuel de DHCP. En pratique, cela implique que le traitement DHCP doit s'effectuer en parallèle. Attendre l'échec de DNAv4 pour commencer le traitement DHCP peut considérablement augmenter le temps de traitement total, le contraire de l'effet désiré.

- Les essais ne coûtent pas cher. DNAv4 effectue ses essais en utilisant de petits paquets en envoi individuel. Un paquet ARP IPv4 sur un Ethernet fait juste 42 octets, y compris l'en-tête Ethernet. Cela signifie que le coût d'une tentative qui échoue est

faible tandis que le coût d'une opportunité manquée (en ayant la bonne adresse disponible comme candidate et en ne la choisissant pas pour l'essai pour une raison quelconque) est grand. Par suite, la meilleure tactique est souvent d'essayer toutes les configurations candidates possibles, plutôt que d'essayer de déterminer quelles candidates, s'il en est, pourraient être correctes pour cette liaison, sur la base d'une heuristique ou d'indications. Pour qu'une heuristique offre la perspective d'une façon potentiellement utile d'éliminer les configurations inappropriées de la liste des candidates, cette heuristique devrait (a) être rapide et peu coûteuse en calcul, par rapport à l'envoi d'un paquet de 42 octets en envoi individuel, et (b) avoir une forte probabilité de ne pas éliminer faussement une configuration candidate qui pourrait se trouver être la bonne.

- Le temps est limité. Si DNAv4 doit être efficace pour activer les relais à faible latence, il a besoin de s'achever en moins de 10 ms. Cela implique que toute heuristique utilisée pour éliminer les configurations candidates doit prendre au plus quelques millisecondes à calculer. Cela ne laisse pas beaucoup de place pour des heuristiques qui se fondent sur l'observation du trafic de couche de liaison ou Internet.

1.2 Exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Les mots-clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigences" [RFC2119].

1.3 Terminologie

Le présent document utilise les termes suivants :

ar$sha : champ de paquet ARP ; adresse du matériel envoyeur [RFC0826]. Adresse de matériel (MAC) de l'origine d'un paquet ARP.

ar$spa : champ de paquet ARP ; adresse de protocole de l'envoyeur [RFC0826]. Pour la résolution d'adresse IP, c'est l'adresse IPv4 de l'envoyeur du paquet ARP.

ar$tha : champ de paquet ARP ; adresse du matériel cible [RFC0826]. Adresse de matériel (MAC) de la cible d'un paquet ARP.

ar$tpa : champ de paquet ARP ; adresse du protocole cible [RFC0826]. Pour la résolution d'adresse IPv4, c'est l'adresse IPv4 pour laquelle on désire savoir l'adresse de matériel.

Client DHCP : un client DHCP ou "client" est un hôte Internet qui utilise le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) [RFC2131] pour obtenir des paramètres de configuration, comme une adresse réseau.

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

Liaison : facilité ou support de communication sur lequel les nœuds du réseau peuvent communiquer. Chaque liaison est associée à un minimum de deux points d'extrémité. Chaque point d'extrémité d'une liaison a un identifiant unique de couche de liaison.

Liaison morte : événement produit par la couche de liaison qui signifie un changement d'état associé au fait que l'interface n'est plus capable de communiquer les trames de données ; des périodes transitoires de fortes pertes de trames ne sont pas suffisantes. DNAv4 n'utilise pas l'indication "Liaison morte".

Couche de liaison : c'est la couche conceptuelle de logique de contrôle ou de traitement qui est chargée d'entretenir le contrôle de la liaison de données. Les fonctions de couche de liaison des données fournissent une interface entre la logique de couche supérieure et la liaison des données. La couche de liaison est celle qui est immédiatement en dessous de IP.

Liaison active : événement fourni par la couche de liaison qui signifie un changement d'état associé au fait que l'interface devient capable de communiquer des trames de données.

Point de rattachement : point d'extrémité de la liaison auquel l'hôte est actuellement connecté.

Adresse acheminable: dans la présente spécification, ce terme se réfère à toute adresse IPv4 en envoi individuel autre qu'une adresse IPv4 de liaison locale. Cela inclut les adresses privées comme spécifié dans "Allocation d'adresses pour internets privés" [RFC1918].

Adresse opérable : dans la présente spécification, ce terme se réfère à une adresse IPv4 statique, ou à une adresse allouée via DHCPv4 qui n'a pas été retournée au serveur DHCP via un message DHCP RELEASE, et dont le prêt n'a pas encore expiré.

2. Généralités

À la connexion sur un nouveau point de rattachement, l'hôte répond à une indication "Liaison active" de la part de la couche liaison en entreprenant la procédure DNAv4.

Pour chaque réseau auquel il se connecte, on suppose que l'hôte sauvegarde les paramètres suivants dans une mémorisation stable :
- l'adresse IPv4 et MAC d'un ou plusieurs nœuds sur le réseau,
- les paramètres de configuration IPv4, y compris l'identifiant de client DHCP, l'adresse allouée, et l'heure d'expiration du prêt.

À partir de l'ensemble des réseaux qui ont des adresses IPv4 opérables associées, l'hôte en choisit un sous ensemble et tente de confirmer la configuration pour chaque réseau, en utilisant l'essai d'accessibilité décrit au paragraphe 2.1.

Pour un réseau particulier, l'hôte DEVRAIT utiliser les adresses des routeurs locaux (de préférence les passerelles par défaut) comme ses nœuds d'essai. Si plus d'une adresse est connue, ces adresses peuvent être essayées en parallèle. Afin de s'assurer de la validité de la configuration, l'hôte DEVRAIT seulement configurer les routes pour lesquelles l'adresse de prochain bond réussit à l'essai d'accessibilité. Les autres routes DEVRAIENT être ré-apprises.

DNAv4 n'augmente pas de façon significative la probabilité d'un conflit d'adresse. L'essai d'accessibilité n'est effectué que pour un réseau où l'hôte a précédemment achevé la détection de conflit comme recommandé au paragraphe 2.2 de la spécification DHCP [RFC2131] et obtenu une configuration IPv4 opérable sur ce réseau. Les restrictions à l'envoi de demandes et réponses ARP sont décrites au paragraphe 2.1.1.

Un cas où DNAv4 n'augmente pas la probabilité d'un conflit d'adresse est quand :
- o un serveur DHCP remet un prêt d'adresse,
- o l'hôte qui a le prêt quitte le réseau,
- o le serveur DHCP a une coupure d'alimentation ou a une défaillance et est réamorcé,
- o le serveur DHCP, ayant échoué à sauvegarder les prêts sur une mémorisation stable, alloue la même adresse à un autre hôte,
- o le premier hôte revient, et ayant un prêt toujours valide pour le temps restant, commence à utiliser l'adresse allouée, entrant en conflit avec le nouvel hôte qui utilise maintenant cette adresse.

Alors que la Section 4 de la spécification DHCP [RFC2131] suppose que les serveurs DHCP sauvegardent leurs prêts dans une mémorisation persistante, presque aucune passerelle de NAT au niveau consommateur ne le fait. Les courtes durées de vie des prêts DHCP atténuent ce risque, bien que cela limite aussi les configurations opérables disponibles candidates pour les essais de DNAv4.

2.1 Essai d'accessibilité

L'hôte saute l'essai d'accessibilité pour un réseau si une des conditions suivante est vraie :

- L'hôte n'a pas d'adresse IPv4 opérable acheminable sur ce réseau. Dans ce cas, l'essai d'accessibilité ne peut pas confirmer que l'hôte a une adresse IPv4 opérable acheminable, de sorte qu'achever l'essai d'accessibilité ne servirait à rien.

- L'hôte ne connaît l'adresse d'aucun des nœuds d'essai sur ce réseau. Dans ce cas, les informations disponibles sont insuffisantes pour effectuer l'essai d'accessibilité.

- Si l'authentification DHCP [RFC3118] est configurée. L'essai d'accessibilité utilise ARP, qui n'est pas sûr. Les hôtes qui ont été configurés à tenter l'authentification DHCP NE DEVRAIENT PAS utiliser l'essai d'accessibilité. Les questions de sécurité sont discutées à la Section 4.

- Le contenu de l'option Identifiant de client DHCP que le client a utilisé pour obtenir la configuration candidate est différent de l'option Identifiant de client DHCP que le client a l'intention de présenter sur l'interface en question. Dans ce cas, il est prévu qu'un serveur DHCP va faire un accusé de réception négatif (NAK) à toute demande faite par le client pour acquérir ou étendre la configuration candidate, car les deux interfaces présentent des identités différentes

Si l'essai d'accessibilité réussit, l'hôte DEVRAIT continuer d'utiliser l'adresse IPv4 opérable acheminable associée au réseau confirmé, sans avoir besoin de la réacquérir. Une fois qu'une réponse d'essai d'accessibilité valide est reçue, la validation est achevée, et les réponses supplémentaires devraient être éliminées.

Si un client DHCPv4 est opérationnel, il est RECOMMANDÉ que l'hôte tente d'obtenir la configuration IPv4 via DHCPv4 en parallèle avec les essais d'accessibilité, l'hôte utilisant la première réponse retournée. Cela assure que la procédure DNAv4 ne va pas résulter en des délais supplémentaires dans le cas d'échec des essais d'accessibilité, ou lorsque l'envoi d'une DHCPREQUEST à partir de l'état INIT-REBOOT, comme décrit aux paragraphes 3.2 et 4.3.2 de la spécification DHCP [RFC2131], s'achève plus rapidement que les essais d'accessibilité.

Dans les situations où DNAv4 et DHCP sont tous deux utilisés sur la même liaison, il est possible que l'essai d'accessibilité s'achève avec succès, et qu'ensuite DHCP s'achève après avec un résultat différent. Si cela arrive, la mise en œuvre DEVRAIT abandonner les résultats de l'essai d'accessibilité et utiliser à la place le résultat de DHCP, sauf si l'adresse confirmée via l'essai d'accessibilité a été allouée manuellement (voir au paragraphe 2.4).

Lorsque l'essai d'accessibilité ne retourne pas de réponse, c'est normalement parce que l'hôte n'est pas rattaché au réseau dont la configuration est vérifiée. Dans ces circonstances, il y a peu d'intérêt à retransmettre agressivement les essais d'accessibilité qui ne fournissent pas de réponse. sauf si l'essai d'accessibilité ne retourne pas de réponse.

Lorsque DNAv4 et DHCP sont essayés en parallèle, une tactique est d'abandonner les retransmissions d'essai d'accessibilité et de permettre seulement au client DHCP de retransmettre. Afin de réduire la compétition entre les retransmissions DNAv4 et DHCP, une mise en œuvre DNAv4 qui retransmet peut utiliser la stratégie de retransmission décrite au paragraphe 4.1 de la spécification DHCP [RFC2131], en programmant les retransmissions DNAv4 entre les retransmissions DHCP.

Si une réponse est reçue à un essai d'accessibilité ou à un message DHCP, les retransmissions en instance sont annulées. Il est RECOMMANDÉ qu'une mise en œuvre DNAv4 ne retransmette pas plus de deux fois. Pour atténuer les conséquences d'indications "Liaison active" parasites, il est RECOMMANDÉ que la procédure DNAv4 ne soit pas effectuée plus d'une fois par seconde.

2.1.1 Format de paquet

L'essai d'accessibilité est effectué par l'envoi d'une demande ARP en envoi individuel. L'hôte DOIT régler l'adresse de protocole cible (ar$tpa) à l'adresse IPv4 du nœud essayé, et le champ d'adresse de protocole d'envoyeur (ar$spa) à sa propre adresse IPv4 candidate. La demande ARP DOIT utiliser l'adresse MAC de l'hôte comme source, et l'adresse MAC du nœud d'essai comme adresse de destination. L'hôte inclut son adresse MAC dans le champ d'adresse de matériel envoyeur (ar$sha) et règle le champ d'adresse de matériel cible (ar$tha) à 0.

Si une réponse ARP valide est reçue , où :
(a) l'adresse dans le champ Adresse de matériel envoyeur (ar$sha) est l'adresse MAC du nœud soumis à l'essai,
(b) l'adresse dans le champ Adresse de protocole d'envoyeur (ar$spa) est l'adresse IPv4 du nœud soumis à l'essai,
l'hôte peut conclure que sa candidate adresse IPv4 est valide pour ce réseau et peut continuer d'être utilisée, sous réserve de la ré-acquisition du prêt et du comportement d'expiration décrit au paragraphe 4.4.5 de la spécification DHCP [RFC2131].

Si une réponse ARP valide est reçue, l'adresse MAC dans le champ Adresse de matériel envoyeur (ar$sha) dans la réponse ARP est confrontée à l'adresse dans le champ Adresse de matériel cible (ar$tpa) de la demande ARP, et l'adresse IPv4 dans le champ Adresse de protocole envoyeur (ar$spa) de la réponse ARP est confrontée au champ Adresse de protocole cible (ar$tpa) de la demande ARP. Si une correspondance est trouvée, l'hôte continue d'utiliser cette adresse IPv4, sous réserve de la ré-acquisition du prêt et du comportement d'expiration décrit au paragraphe 4.4.5 de la spécification DHCP [RFC2131].

Le risque d'un conflit d'adresse est plus grand quand l'hôte se déplace entre des réseaux privés, car dans ce cas l'achèvement de la détection de conflit sur le premier réseau ne donne pas d'assurance contre un conflit d'adresse sur le nouveau réseau. Jusqu'à ce qu'un hôte ait confirmé le caractère opérationnel de sa configuration IPv4 par la réception d'une réponse à l'essai d'accessibilité, il NE DEVRAIT PAS répondre aux demandes ARP et NE DEVRAIT PAS diffuser de demandes ARP contenant son adresse dans le champ Adresse de protocole d'envoyeur (ar$spa).

L'envoi d'une demande d'écho ICMP [RFC0792] ne serait pas une façon acceptable de tester une configuration candidate, car l'envoi de tout paquet IP exige généralement un échange de demande/réponse ARP et, comme expliqué ci-dessus, les paquets

ARP ne peuvent pas être diffusés de façon sûre tant que la configuration candidate n'a pas été confirmée. Aussi, quand un hôte passe d'un réseau privé à un autre, une demande d'écho ICMP peut résulter en une réponse d'écho ICMP même si l'adresse MAC a changé, tant que l'adresse IPv4 reste la même. Cela peut se produire, par exemple, quand un hôte passe d'un réseau de rattachement à un autre en utilisant le préfixe 192.168/16. De plus, si le ping est envoyé avec un TTL > 1, une réponse d'écho ICMP peut être reçue d'un routeur hors liaison. Il en résulte que si l'adresse MAC du nœud d'essai n'est pas vérifiée, l'hôte peut confirmer le rattachement à tort, résultant potentiellement en un conflit d'adresse. Par suite, l'envoi d'une demande d'écho ICMP NE DEVRAIT PAS être utilisé comme substitut de l'essai d'accessibilité.

2.2 Acquisition de l'adresse IPv4

Si l'hôte a une adresse IPv4 opérable acheminable sur un ou plusieurs réseaux, et si DHCPv4 est activé sur l'interface, l'hôte DEVRAIT tenter d'acquérir une configuration IPv4 en utilisant DHCPv4, en parallèle avec un ou plusieurs essais d'accessibilité. Ceci se fait en entrant dans l'état INIT-REBOOT et en envoyant une DHCPREQUEST à l'adresse de diffusion, comme spécifié au paragraphe 4.4.2 de la spécification DHCP [RFC2131].

Si l'hôte n'a d'adresse IPv4 opérable acheminable sur aucun réseau, l'hôte entre dans l'état INIT et envoie un paquet DHCPDISCOVER à l'adresse de diffusion, comme décrit au paragraphe 4.4.1 de la spécification DHCP [RFC2131]. Si l'hôte prend en charge l'option Engagement rapide [RFC4039], il est possible que l'échange puisse être raccourci d'un échange de quatre messages à un échange de deux messages.

Si l'hôte ne reçoit pas de réponse à un DHCPREQUEST ou DHCPDISCOVER, il le retransmet comme spécifié au paragraphe 4.1 de la spécification DHCP [RFC2131].

Comme expliqué au paragraphe 4.4.4 de la spécification DHCP [RFC2131], un hôte dans l'état INIT ou REBOOTING qui connaît l'adresse d'un serveur DHCP peut l'utiliser dans le DHCPDISCOVER ou DHCPREQUEST plutôt que l'adresse de diffusion IPv4. Dans l'état INIT-REBOOT, une DHCPREQUEST est envoyée à l'adresse de diffusion afin que l'hôte reçoive une réponse, que l'adresse IPv4 précédemment configurée soit correcte ou non pour le réseau auquel il s'est connecté.

L'envoi d'une DHCPREQUEST à l'adresse d'envoi individuel dans l'état INIT-REBOOT n'est pas approprié, car si le client DHCP est passé sur un autre sous réseau, une réponse du serveur DHCP ne peut pas être réacheminée au client car la DHCPREQUEST va outrepasser le relais DHCP et contiendra une adresse de source invalide.

2.3 Adresses IPv4 de liaison locale

DNAv4 s'applique seulement aux adresses précédemment configurées qui ont une durée de vie de prêt associée, durant laquelle l'adresse peut légitimement être considérée comme réservée pour l'utilisation exclusive de l'hôte auquel elle est allouée. Les adresses allouées par DHCP répondent à cette description, mais les adresses IPv4 de liaison locale [RFC3927] ne le font pas car elles ne sont pas traitées par un serveur d'autorité et n'ont aucune durée de vie garantie utilisable.

La revendication d'un hôte sur une adresse IPv4 de liaison locale n'est valide que tant que cet hôte reste connecté à la liaison, la défendant activement contre les sondes pour cette adresse choisie. Aussitôt qu'un hôte ferme, reste inactif, ou se déconnecte par ailleurs d'une liaison, il renonce immédiatement à toute prétention qu'il pourrait avoir sur une adresse IPv4 de liaison locale sur cette liaison. Un hôte qui souhaite réclamer une adresse IPv4 de liaison locale précédemment utilisée DOIT effectuer le processus complet de sondage et d'annonces exigé par la "Configuration dynamique d'adresses IPv4 de liaison locale" de la [RFC3927] et NE DOIT PAS tenter d'utiliser DNAv4 comme raccourci pour outrepasser ce processus.

Lorsque l'hôte n'a d'adresse IPv4 opérable acheminable sur aucun réseau, il PEUT configurer une adresse IPv4 de liaison locale avant d'entrer dans l'état INIT et envoyer un paquet DHCPDISCOVER, comme décrit au paragraphe 2.3 de la spécification DHCP [RFC2131]. Lorsque un hôte peut confirmer qu'il reste connecté à un réseau sur lequel il possède une adresse IPv4 opérable acheminable, cette adresse devrait être utilisée, et l'adresse IPv4 de liaison locale est déconseillée, comme noté au paragraphe 1.9 de la spécification de liaison locale IPv4 [RFC3927].

Lorsque un hôte a une adresse IPv4 opérable acheminable sur un ou plusieurs réseaux mais que l'essai d'accessibilité ne peut pas confirmer la configuration et que le client DHCPv4 ne reçoit pas de réponse après avoir employé l'algorithme de retransmission, le paragraphe 3.2 de la spécification DHCP [RFC2131] déclare que le client PEUT choisir d'utiliser l'adresse réseau précédemment allouée et les paramètres de configuration pour le reste du prêt non encore expiré.

2.4 Adresses allouées manuellement

Une mise en œuvre peut utiliser DNAv4 pour confirmer la configuration d'adresses allouées manuellement. Cependant, une attention particulière est requise pour que cela produise des résultats fiables, de sorte que cela NE DEVRAIT PAS être activé par défaut.

Pour DNAv4, les adresses allouées manuellement peuvent être traitées comme équivalentes aux adresses allouées par DHCP avec une durée de vie infinie. Cela n'augmente pas significativement la probabilité d'un conflit d'adresses tant que l'adresse allouée manuellement est réservée par le serveur DHCP ou sort du domaine des adresses allouées par un serveur DHCP. Cependant, lorsque l'adresse allouée manuellement est dans un domaine d'adresses utilisé par un serveur DHCP, il est possible que l'hôte soit indisponible quand le serveur DHCP vérifie qu'il n'y a pas de conflit avant d'allouer l'adresse en question. Dans ce cas, un hôte qui utilise DNAv4 pourrait confirmer une adresse qui a été allouée à un autre hôte.

Normalement, une adresse est allouée manuellement sur un réseau parce que une allocation dynamique d'adresse ne convenait pas pour une raison quelconque. Donc, lorsque DNAv4 et DHCP fonctionnent en parallèle et que DNAv4 confirme une configuration manuelle, il peut n'être pas souhaitable de permettre que cette configuration soit outrepassée par DHCP, comme décrit au paragraphe 2.1. Cependant, une perte de paquet peut causer l'échec de l'essai d'accessibilité alors que DHCP s'achève avec succès, résultant en ce que l'hôte obtient une adresse dynamique alors qu'une adresse statique est désirée. Afin de fournir une reconfirmation fiable des adresses allouées manuellement, les essais d'accessibilité pour une configurations manuelle exigent une stratégie de retransmission plus agressive que ce qui est décrit au paragraphe 4.1 de la spécification DHCP [RFC2131]. Par exemple, des intervalles de retransmission plus courts et des retransmissions plus persistantes peuvent être nécessaires.

3. Considérations pour la sécurité

La détection de rattachement au réseau pour IPv4 (DNAv4, *Detecting Network Attachment for IPv4*) se fonde sur ARP et DHCP et hérite des faiblesses de sécurité de ces deux protocoles.

Le trafic ARP [RFC826] n'est pas sécurisé, de sorte qu'un attaquant qui obtient l'accès au réseau peut contrefaire une réponse à l'essai d'accessibilité décrit au paragraphe 2.1, conduisant celui qui interroge à conclure faussement qu'il est rattaché à un réseau auquel il n'est pas connecté.

De même, lorsque le trafic DHCPv4 n'est pas sécurisé, un attaquant pourrait se faire passer pour un serveur DHCPv4, afin de convaincre l'hôte qu'il est rattaché à un réseau particulier. Cette menace et d'autres en rapport avec DHCPv4 sont décrites dans "Authentification des messages DHCP" [RFC3118].

L'effet de ces attaques va normalement être limité à un déni de service, sauf si l'hôte utilise sa configuration IP pour d'autres objets, comme la configuration de la sécurité ou la détermination de la localisation. Par exemple, un hôte qui désactive son pare-feu personnel sur la foi de l'évidence qu'il est rattaché à son réseau domestique pourrait être compromis par la contrefaçon de l'essai d'accessibilité DNAv4. En général, l'ajustement de la configuration de sécurité sur la base de DNAv4 N'EST PAS RECOMMANDÉ.

Les hôtes qui dépendent d'une configuration IP sûre NE DEVRAIENT PAS utiliser DNAv4 mais DEVRAIENT plutôt utiliser l'authentification DHCP [RFC3118], éventuellement combinée avec l'option d'engagement rapide [RFC4039].

4. Références

4.1 Références normatives

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[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)

4.2 Références pour information

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001. *(P.S.)*

[RFC3927] S. Cheshire, B. Aboba, E. Guttman, "Configuration dynamique des adresses IPv4 de liaison locale", mai 2005. *(P.S.)*

[RFC4039] S. Park et autres, "Option d'engagement rapide pour le protocole de configuration dynamique d'hôte version 4 (DHCPv4)", mars 2005. *(P.S.)*

[RFC5227] S. Cheshire, "Détection de conflit d'adresses IPv4", juillet 2008. (*MàJ* RFC0826) *(P.S.)*

5. Remerciements

Les auteurs tiennent à remercier Greg Daley de Monash University, Erik Guttman et Erik Nordmark de Sun Microsystems, Ralph Droms de Cisco Systems, Ted Lemon de Nominum, John Loughney de Nokia, Thomas Narten de IBM et David Hankins de ISC de leurs contributions au présent document.

Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 818 4011
Fax : +1 425 936 7329
mél : bernarda@microsoft.com

James Carlson
Sun Microsystems, Inc
1 Network Drive
Burlington, MA 01803-2757
USA
téléphone : +1 781 442 2084
mél : james.d.carlson@sun.com

Stuart Cheshire
Apple Computer, Inc.
1 Infinite Loop
Cupertino, California 95014,
USA
téléphone: +1 408 974 3207
mél : rfc@stuartcheshire.org

Déclaration de droits de reproduction

Copyright (C) The Internet Society (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations qui y sont contenues sont fournis 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.

Propriété intellectuelle
L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou 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 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 faits 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.