Groupe de travail Réseau
Request for Comments : 5527
RFC mise à jour : 0826
Catégorie : Sur la voie de la normalisation

S. Cheshire, Apple Inc.
juillet 2008

Traduction Claude Brière de L'Isle

Détection de conflit d'adresse IPv4

Résumé
Quand deux hôtes sur la même liaison tentent d'utiliser la même adresse IPv4 en même temps (sauf dans de rares cas particuliers où cela a été arrangé par une coordination préalable) des problèmes s'ensuivent pour l'un ou les deux hôtes. Le présent document décrit (i) une simple précaution que peut prendre un hôte à l'avance pour aider à empêcher cette mauvaise configuration de se produire, et (ii) si cette configuration se présente, un simple mécanisme par lequel un hôte peut détecter passivement, après coup, que cela s'est produit, afin que l'hôte ou l'administrateur puisse rectifier le problème.

Table des matières

1. Introduction....1
1.1 Conventions et terminologie utilisée dans le document....2
1.2 Relations avec la RFC0826....3
1.3 Applicabilité....4
2. Vérification d'adresse, annonce, détection de conflit, et défense....5
2.1 Vérification d'une adresse....5
2.2 Temporisations plus courtes sur les technologies de réseau appropriées....6
2.3 Annonce d'une adresse....6
2.4 Détection de conflit d'adresse en cours et défense d'adresse....7
2.5 Poursuite du fonctionnement....8
2.6 Réponses ARP en diffusion....8
3. Pourquoi les annonces ARP sont-elles effectuées avec des paquets de demande ARP et pas des paquets de réponse ARP ?...8
4. Note historique....9
5. Considérations pour la sécurité....9
6. Remerciements....10
7. Références....10
7.1 Références normatives....10
7.2 Références pour information....10
Adresse de l'auteur....11
Déclaration de droits de reproduction....11

1. Introduction

Historiquement la configuration accidentelle de deux hôtes Internet avec la même adresse IP a souvent été un problème ennuyeux et difficile à diagnostiquer.

C'est malheureux, parce que le protocole de résolution d'adresse existant (ARP, *Address Resolution Protocol*) donne à un hôte un moyen facile pour détecter cette sorte de mauvaise configuration et la rapporter à l'utilisateur. La spécification DHCP [RFC2131] mentionne brièvement le rôle de ARP dans la détection de mauvaises configurations, comme l'illustrent les trois extraits suivants de la RFC 2131 :

- le client DEVRAIT vérifier la nouvelle adresse reçue, par exemple, avec ARP,
- le client DEVRAIT effectuer une vérification finale sur les paramètres (par exemple, ARP pour l'adresse réseau allouée)
- si le client détecte que l'adresse est déjà utilisée (par exemple, en utilisant ARP) le client DOIT envoyer un message DHCPDECLINE au serveur.

Malheureusement, la spécification DHCP ne donne aucune ligne directrice aux mises en œuvre concernant le nombre de paquets ARP à envoyer, l'intervalle entre les paquets, le temps d'attente total avant de conclure qu'une adresse peut être utilisée en toute sécurité, ou bien sûr quelle sorte de paquets un hôte devrait attendre, afin de faire cette détermination. Elle laisse non spécifiée l'action qu'un hôte devrait entreprendre si, après avoir conclu qu'une adresse peut être utilisée en toute sécurité, il découvre ensuite que c'était faux. Elle manque aussi à spécifier quelles précautions devrait prendre un client DHCP pour se garder contre des cas de défaillance pathologiques, comme un serveur DHCP qui OFFRE de façon répétée la même adresse, bien qu'elle ait été DECLINÉE plusieurs fois.

Les auteurs de la spécification DHCP peuvent avoir eu raison de penser en ce temps là que les réponses à ces questions semblaient si simples, évidentes, et directes qu'il ne valait pas la peine de les mentionner, mais malheureusement cela a laissé la charge de la conception du protocole à chaque mise en œuvre individuelle. Le présent document cherche à remédier à ces omissions en spécifiant clairement les actions requises pour :

1. déterminer si l'utilisation d'une adresse va probablement conduire à un conflit d'adressage. Cela inclut (a) le cas où l'adresse est déjà activement utilisée par un autre hôte sur la même liaison, et (b) le cas où deux hôtes sont par inadvertance sur le point de commencer à utiliser la même adresse, et tous deux sont simultanément en train de vérifier si l'adresse peut être utilisée en toute sécurité (paragraphe 2.1.).

2. la détection passive ultérieure qu'un autre hôte sur le réseau est, par inadvertance, en train d'utiliser la même adresse. Même si tous les hôtes respectent les précautions pour éviter d'utiliser une adresse qui est déjà en service, des conflits peuvent quand même se produire si deux hôtes sont hors communication au moment de la configuration initiale de l'interface. Cela pourrait se produire avec des interfaces de réseau sans fil si les hôtes sont temporairement hors de portée, ou avec des interfaces Ethernet si la liaison entre deux plates-formes Ethernet n'est pas en fonction au moment de la configuration d'adresse. Un hôte bien conçu va traiter non seulement les conflits détectés durant la configuration d'interface, mais aussi les conflits détectés plus tard, pendant toute la durée où l'hôte utilise l'adresse (paragraphe 2.4.).

3. la limitation en débit des tentatives d'acquisition d'adresse dans le cas d'un nombre excessif de conflits répétés (paragraphe 2.1.).

L'utilité de la détection de conflit d'adresse IPv4 (ACD, *Address Conflict Detection*) n'est pas limitée aux clients DHCP. Quelle que soit la façon dont une adresse a été configurée, via entrée manuelle par un humain, via des informations reçues d'un serveur DHCP, ou via toute autre source d'informations de configuration, la détection des conflits est utile. Quand un conflit est détecté, l'erreur devrait être notifiée à l'agent de configuration. Dans le cas où l'agent de configuration est un humain, cette notification peut prendre la forme d'un message d'erreur sur un écran, d'une notification du protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) ou un message d'erreur envoyé via un message de texte à un téléphone mobile. Dans le cas d'un serveur DHCP, cette notification prend la forme d'un message DHCP DECLINE envoyé au serveur. Dans le cas d'une configuration par une autre sorte de logiciel, cette notification prend la forme d'une indication d'erreur au logiciel en question, pour l'informer que l'adresse qu'il a choisie est en conflit avec un autre hôte sur le réseau. Le logiciel de configuration peut choisir de cesser de fonctionner sur le réseau, ou il peut automatiquement choisir une nouvelle adresse afin que l'hôte puisse rétablir la connexité IP aussitôt que possible.

L'allocation d'adresses IPv4 de liaison locale de la [RFC3927] peut être vue comme un cas particulier de ce mécanisme, où l'agent de configuration est un générateur de nombre pseudo aléatoire, et l'action qu'il exerce lorsque on lui notifie un conflit est de prendre un nombre aléatoire différent et d'essayer à nouveau. En fait, c'est exactement comment l'adressage IPv4 de liaison locale a été mis en œuvre dans le Mac OS 9 en 1998. Si le client DHCP échoue à obtenir une réponse d'un serveur DHCP, il va simplement fabriquer une réponse factice contenant une adresse 169.254.x.x aléatoire. Si le module ARP a rapporté un conflit pour cette adresse, le client DHCP va alors essayer à nouveau, fabriquant une nouvelle adresse 169.254.x.x aléatoire autant de fois que nécessaire jusqu'à ce qu'il réussisse. Mettre en œuvre ACD comme caractéristique standard de la pile de réseautage a pour effet collatéral que la moitié du travail de l'adressage IPv4 de liaison locale est déjà fait.

1.1 Conventions et terminologie utilisée dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Chaque fois que le présent document utilise le terme "adresse IP d'envoyeur" ou "adresse IP cible" dans le contexte d'un paquet ARP, il se réfère aux champs du paquet ARP identifiés dans la spécification ARP [RFC0826] comme respectivement "ar$spa" (adresse de protocole d'envoyeur) et "ar$tpa" (adresse de protocole cible). Pour l'usage de ARP décrit dans ce document, chacun de ces champs contient toujours une adresse IPv4.

Dans le présent document, le terme "sonde ARP" est utilisé pour se référer à un paquet de demande ARP, diffusé sur la liaison locale, avec une "adresse IP d'envoyeur" toute à zéro. L'adresse de matériel d'envoyeur DOIT contenir l'adresse de matériel de l'interface qui envoie le paquet. Le champ "adresse IP d'envoyeur" DOIT être réglé tout à zéro, pour éviter de polluer les antémémoires ARP dans les autres hôtes sur la même liaison dans le cas où l'adresse se révélerait être déjà utilisée par un autre hôte. Le champ "adresse de matériel cible" est ignoré et DEVRAIT être réglé tout à zéro. Le champ "adresse IP cible" DOIT être réglé à l'adresse sondée. Une sonde ARP porte à la fois une question ("y a t-il quelqu'un qui utilise cette adresse ?") et une déclaration implicite ("Ceci est l'adresse que j'espère utiliser.").

Dans le présent document, le terme "annonce ARP" est utilisé pour se référer à un paquet de demande ARP, diffusé sur la liaison locale, identique à la sonde ARP décrite ci-dessus, sauf que les champs d'adresse IP de l'envoyeur et de la cible contiennent tous deux l'adresse IP annoncée. Elle porte une déclaration plus forte que la sonde ARP, à savoir, "Ceci est l'adresse que j'utilise maintenant".

Les constantes de temps utilisées dans ce protocole sont référencées à la Section 2, qui décrit en détails le fonctionnement du protocole. (Noter que les valeurs mentionnées ici sont des constantes fixes ; elle ne sont pas destinées à être modifiables par les mises en œuvre, les opérateurs, ou les utilisateurs finaux. Ces constantes ont reçu des noms symboliques pour faciliter la rédaction de normes futures qui pourront vouloir faire référence au présent document avec des valeurs différentes pour ces constantes ; cependant, aucune de ces futures normes n'existe pour l'instant.)

PROBE_WAIT : 1 seconde (délai aléatoire initial)
PROBE_NUM : 3 (nombre de paquets de sonde)
PROBE_MIN : 1 seconde (délai minimum avant de répéter la sonde)
PROBE_MAX : 2 secondes (délai maximum avant de répéter la sonde)
ANNOUNCE_WAIT : 2 secondes (délai avant d'annoncer)
ANNOUNCE_NUM : 2 (nombre de paquets d'annonce)
ANNOUNCE_INTERVAL : 2 secondes (délai entre paquets d'annonce)
MAX_CONFLICTS : 10 (nombre maximum de conflits avant de limiter le débit)
RATE_LIMIT_INTERVAL 60 secondes (délai entre tentatives successives)
DEFEND_INTERVAL : 10 secondes (intervalle minimum entre ARP défensifs)

1.2 Relations avec la RFC0826

Le présent document ne modifie aucune des règles du protocole de la RFC 826. Il ne modifie pas le format de paquet, ni la signification des champs. Les règles existantes de "génération de paquet" et de "réception de paquet" s'appliquent exactement comme spécifié dans la RFC 826.
Le présent document étend la RFC 826 en spécifiant :
(1) qu'une demande ARP spécifique devrait être générée quand une interface est configurée, pour découvrir si l'adresse est déjà utilisée, et
(2) qu'un essai supplémentaire trivial devrait être effectué sur chaque paquet ARP reçu, pour faciliter la détection passive de conflit en cours. Cet essai supplémentaire ne crée pas de surcharge additionnelle sur le réseau (aucun paquet supplémentaire n'est envoyé) et une charge de CPU négligeable sur les hôtes, car tout hôte qui met en œuvre ARP est *déjà* obligé de traiter tout paquet ARP reçu conformément aux règles de réception de paquet spécifiées dans la RFC 826. Ces règles incluent déjà de vérifier si l'adresse IP d'envoyeur du paquet ARP apparaît dans une des entrées de l'antémémoire de l'hôte ARP ; l'essai supplémentaire est simplement de vérifier si l'adresse IP d'envoyeur est la propre adresse IP de l'hôte, potentiellement comme une seule instruction de machine supplémentaire sur de nombreuses architectures.

Comme il est déjà spécifié dans la RFC 826, un paquet de demande ARP sert deux fonctions, une assertion et une question :
- Assertion : les champs "ar$sha" (Adresse du matériel envoyeur) et "ar$spa" (Adresse du protocole envoyeur) servent ensemble à l'assertion d'un fait : que l'adresse de protocole déclarée est transposée en l'adresse de matériel déclarée.
- Question : les champs "ar$tha" (Adresse de matériel cible, zéro) et "ar$tpa" (Adresse de protocole cible) servent de question, demandant, pour l'adresse de protocole déclarée, à quelle adresse de matériel elle est transposée.

Le présent document précise ce que signifie d'avoir l'une sans l'autre.

Certains lecteurs ont fait remarquer qu'il est probablement impossible de poser une vraie question pure ; poser toute question invite nécessairement à des spéculations sur pourquoi l'interrogateur veut savoir la réponse. Tout comme quelqu'un qui montre une chaise vide et demande, "Quelqu'un est il assis ici ?" implique en sous entendu "... parce que dans ce cas, je vais la prendre". la même chose est vraie ici. Une sonde ARP avec une "adresse IP d'envoyeur" toute de zéros peut ostensiblement être simplement en train de poser une question innocente ("Est ce que quelqu'un utilise cette adresse ?") mais une mise en œuvre intelligente qui sait comment fonctionne la détection de conflit d'adresse IPv4 devrait être capable de reconnaître cette question comme le précurseur de la revendication de cette adresse.

Par conséquent, si une mise en œuvre est aussi, à ce moment exact, dans le processus de poser la même question, elle devrait reconnaître qu'elles ne peuvent toutes deux occuper le même siège, de sorte qu'il serait prudent d'en demander un autre.

1.2.1 Réponses de diffusion ARP

Dans certaines applications de la détection de conflit d'adresse IPv4 (ACD, *Address Conflict Detection*) il peut être avantageux de livrer les réponses ARP en utilisant la diffusion plutôt que l'envoi individuel parce que cela permet que les conflits d'adresse soient détectés plus tôt. Par exemple, la "configuration dynamique des adresses IPv4 de liaison locale" [RFC3927] utilise ACD exactement comme spécifié ici, mais spécifie de plus que les réponses ARP devraient être envoyées en utilisant la diffusion, parce que dans ce contexte le compromis de l'augmentation du trafic de diffusion avec une fiabilité et une tolérance aux fautes améliorées est réputé être approprié. Il pourrait y avoir de futures spécifications où le même compromis serait approprié. Des détails supplémentaires sont donnés au paragraphe 2.6, "Réponses ARP en diffusion".

La RFC 826 implique que les réponses aux demandes ARP sont généralement livrées en utilisant l'envoi individuel, mais il est aussi acceptable de livrer les réponses ARP en utilisant la diffusion. Les règles de réception de paquet de la RFC 826 spécifient que le contenu du champ "ar$spa" devrait être traité "avant" d'examiner le champ "ar$op", de sorte que tout hôte qui met correctement en œuvre l'algorithme de réception de paquet spécifié dans la RFC 826 va traiter correctement les réponses ARP livrées via une diffusion de couche liaison.

1.3 Applicabilité

La présente spécification s'applique à tous les réseaux de zone locale (LAN, *Local Area Network*) IEEE 802 [802], incluant Ethernet [802.3], les anneaux à jetons [802.5], et les LAN sans fil IEEE 802.11 [802.11], ainsi qu'aux autres technologies de couche de liaison qui opèrent à des débits de données d'au moins 1 Mbit/s, qui ont une latence d'aller-retour d'au plus une seconde, et utilisent ARP [RFC826] pour transposer les adresses IP en adresses de matériel de couche de liaison. Chaque fois que le présent document utilise le terme "IEEE 802", le texte s'applique également à toutes les technologies de réseau.

Les technologies de couche de liaison qui prennent en charge ARP mais fonctionnent à des débits inférieurs à 1 Mbit/s ou des latences supérieures à une seconde vont quand même fonctionner correctement avec ce protocole, mais peuvent avoir plus souvent à traiter des conflits tardifs détectés après l'achèvement de la phase de sonde. Sur ces sortes de liaisons, il peut être souhaitable de spécifier des valeurs différentes pour les paramètres suivants :

(a) PROBE_NUM, PROBE_MIN, et PROBE_MAX, le nombre de sondes ARP, et l'intervalle entre elles, expliqué au paragraphe 2.1.

(b) ANNOUNCE_NUM et ANNOUNCE_INTERVAL, le nombre d'annonces ARP, et l'intervalle entre elles, expliqué au paragraphe 2.3.

(c) RATE_LIMIT_INTERVAL et MAX_CONFLICTS, contrôlant le débit maximum auquel la revendication d'adresse peut être tentée, expliqué au paragraphe 2.1.

(d) DEFEND_INTERVAL, l'intervalle de temps entre les ARP en conflit en dessous duquel un hôte NE DOIT PAS tenter de défendre son adresse, expliqué au paragraphe 2.4.

Les technologies de couche de liaison qui ne prennent pas en charge ARP peuvent être capables d'utiliser d'autres techniques pour déterminer si une certaine adresse IP est actuellement utilisée. Cependant, la mise en œuvre de la détection de conflit d'adresse pour de tels réseaux sort du domaine d'application de ce document.

Pour que le protocole spécifié dans le présent document soit efficace, il n'est pas nécessaire que tous les hôtes sur la liaison le mettent en œuvre. Pour qu'un hôte qui met en œuvre la présente spécification soit protégé contre un conflit d'adresses accidentel, tout ce qui est exigé est que les homologues sur la même liaison mettent correctement en œuvre le protocole ARP comme spécifié à la RFC 826. Pour être précis, quant un hôte reçoit une demande ARP où l'adresse de protocole cible de la demande ARP correspond à la ou les (une des) adresses IP de cet hôte configurées sur cette interface, tant qu'il répond de façon appropriée avec une réponse ARP correctement formatée, l'hôte qui interroge va être capable de détecter que l'adresse est déjà utilisée.

Les spécifications du présent document permettent aux hôtes de détecter des conflits entre deux hôtes utilisant la même adresse sur la même liaison physique. ACD ne détecte pas les conflits entre deux hôtes qui utilisent la même adresse sur des liaisons physiques différentes, et bien sûr, il ne le devrait pas. Par exemple, l'adresse 10.0.0.1 [RFC1918] est utilisée sur des appareils sans comptage sur des réseaux privés sans comptage partout dans le monde, et ce n'est pas un conflit, parce qu'ils sont sur des liaisons différentes. Il n'y aurait de conflit que si deux de ces appareils se trouvaient être connectés à la même liaison, et quand

cela arrive (quelques fois) c'est un parfait exemple de situation où ACD est extrêmement utile pour détecter et rapporter (et/ou corriger automatiquement) cette erreur.

Pour les besoins du présent document, un ensemble d'hôtes est considéré comme étant "sur la même liaison" si :
- quand un hôte, A, de cet ensemble, envoie un paquet à tout autre hôte, B, de cet ensemble, en utilisant l'envoi individuel, la diffusion, ou la diffusion groupée, la charge utile entière de paquet de couche de liaison arrive non modifiée, et
- une diffusion envoyée sur cette liaison par tout hôte de cet ensemble d'hôtes peut être reçue par chaque autre hôte de cet ensemble.

L'en-tête de couche de liaison peut être modifié, comme dans l'acheminement de source d'anneau à jeton [802.5], mais pas la charge utile de couche de liaison. En particulier, si un appareil qui transmet un paquet modifie une partie de l'en-tête IP ou de la charge utile IP, le paquet n'est plus considéré comme étant sur la même liaison. Cela signifie que le paquet peut passer à travers des appareils comme des répéteurs, des ponts, des plates-formes, ou des commutateurs et être toujours considéré comme étant sur la même liaison pour les besoins du présent document, mais par à travers un appareil comme un routeur IP qui décrémente le TTL ou modifie autrement l'en-tête IP.

Lorsque le présent document utilise le terme "hôte", il s'applique également aux interfaces sur des routeurs ou autres hôtes multi rattachements, sans considérer si l'hôte/routeur est actuellement en train de transmettre des paquets. Dans de nombreux cas, un routeur va être une infrastructure critique de réseau avec une adresse IP qui est bien connue localement et est supposée être relativement constante. Par exemple, l'adresse du routeur par défaut est un des paramètres qu'un serveur DHCP communique normalement à ses clients, et (au moins jusqu'à ce que des mécanismes comme "DHCP Reconfigure" [RFC3203] soient largement mis en œuvre) il n'y a aucun moyen pratique pour que le serveur DHCP informe les clients si cette adresse change. Par conséquent, pour de tels appareils, le traitement des conflits en prenant une nouvelle adresse IP n'est pas une bonne option. Dans ce cas, l'option (c) du paragraphe 2.4 ("Détection de conflit d'adresse en cours et défense d'adresse") s'applique.

Cependant, même quand un appareil est configuré manuellement avec une adresse fixe, avoir d'autres appareils sur le réseau qui revendiquent la possession de la même adresse IP va polluer les mémoires tampon ARP des homologues et empêcher une communication fiable, et il est toujours utile d'en informer l'opérateur. Si un conflit est détecté au moment où l'opérateur établit l'adresse manuelle fixe, il est alors utile d'informer immédiatement l'opérateur ; si un conflit est détecté plus tard, il est utile d'informer l'opérateur via un canal de communication asynchrone approprié.

Même si une communication fiable n'est pas possible via l'adresse en conflit, il peut quand même être possible d'informer l'opérateur via quelque autre canal de communication toujours opérationnel, comme via une autre interface sur le routeur, via une adresse IPv4 de liaison locale dynamique, via une adresse IPv6, ou même via une technologie non IP complètement différente comme un écran ou console série à rattachement local.

2. Vérification d'adresse, annonce, détection de conflit, et défense

Cette section décrit les vérifications initiales pour déterminer en toute sécurité si une adresse est déjà utilisée, en annonçant l'adresse choisie, en vérifiant si il y a conflit, et avec l'utilisation facultative des réponses ARP en diffusion pour fournir une détection plus rapide du conflit.

2.1 Vérification d'une adresse

Avant de commencer à utiliser une adresse IPv4 (qu'elle soit reçue d'une configuration manuelle, de DHCP, ou par d'autres moyens) un hôte qui met en œuvre la présente spécification DOIT vérifier si l'adresse est déjà utilisée, en diffusant des paquets de sonde ARP. Cela s'applique aussi quand une interface réseau passe d'un état inactif à un état actif, quand un ordinateur sort d'un état de veille, quand un changement d'état de liaison signale qu'un câble Ethernet a été connecté, quand une interface sans fil 802.11 s'associe à une nouvelle station de base, ou quand tout autre changement de la connexité se produit lorsque un hôte devient activement connecté à une liaison logique.

Un hôte NE DOIT PAS effectuer cette vérification périodiquement. Ce serait un gaspillage de la bande passante du réseau, et ce n'est pas nécessaire à cause de la capacité des hôtes à découvrir passivement les conflits, comme décrit au paragraphe 2.4.

2.1.1 Détails de la vérification

Un hôte vérifie pour voir si une adresse est déjà utilisée en diffusant une demande ARP pour l'adresse désirée. Le client DOIT remplir le champ Adresse de matériel envoyeur de la demande ARP avec l'adresse de matériel de l'interface à travers laquelle il envoie le paquet. Le champ Adresse IP de l'envoyeur DOIT être réglé tout à zéro ; c'est pour éviter de polluer les antémémoires ARP dans les autres hôtes sur la même liaison au cas où l'adresse se révélerait être déjà utilisée par un autre hôte. Le champ

Adresse de matériel cible est ignoré et DEVRAIT être réglé tout à zéro. Le champ Adresse IP cible DOIT être réglé à l'adresse à vérifier. Une demande ARP construite de cette façon, avec une adresse IP d'envoyeur toute à zéro est appelée une "sonde ARP".

Quand il est prêt à commencer la vérification, l'hôte devrait alors attendre pendant un intervalle de temps aléatoire choisi uniformément dans la gamme de zéro à PROBE_WAIT secondes, et devrait alors envoyer PROBE_NUM paquets de sonde, espacés chacun de façon aléatoire et uniforme, de PROBE_MIN à PROBE_MAX secondes les uns des autres. Ce délai initial aléatoire aide à s'assurer qu'un grand nombre d'hôtes mis sous tension au même moment ne vont pas tous envoyer simultanément leur paquet de sonde initial.

Si durant cette période, depuis le début du processus de vérification jusqu'à ANNOUNCE_WAIT secondes après l'envoi du dernier paquet de sonde, l'hôte reçoit un paquet ARP (demande ou réponse) sur l'interface où le sondage est effectué, où l'adresse IP d'envoyeur du paquet est l'adresse à vérifier, l'hôte DOIT alors traiter cette adresse comme étant utilisée par un autre hôte, et devrait indiquer à l'agent configureur (opérateur humain, serveur DHCP, etc.) que l'adresse proposée n'est pas acceptable.

De plus, si durant cette période l'hôte reçoit une sonde ARP où l'adresse IP cible du paquet est l'adresse qui fait l'objet de la vérification, et où l'adresse de matériel d'envoyeur du paquet n'est pas l'adresse de matériel d'une des interfaces de l'hôte, l'hôte DEVRAIT alors de la même façon traiter cela comme un conflit d'adresse et signaler une erreur à l'agent configureur comme ci-dessus. Cela peut se produire si deux (ou plus) hôtes ont, pour une raison quelconque, été configurés par inadvertance avec la même adresse, et que tous deux sont simultanément en train de vérifier si elle peut être utilisée en toute sécurité.

Note : La vérification que l'adresse de matériel d'envoyeur du paquet n'est pas l'adresse de matériel d'une des interfaces de l'hôte est importante. Certaines sortes de plates-formes Ethernet (souvent appelées "répéteur à mémoire tampon") et de nombreux points d'accès sans fil "rediffusent" tout paquet reçu en diffusion à tous les receveurs, incluant l'envoyeur original lui-même. Pour cette raison, la précaution décrite ci-dessus est nécessaire pour s'assurer qu'un hôte n'est pas dans la confusion quand il voit ses propres paquets ARP revenir en écho.

Un hôte qui met en œuvre la présente spécification DOIT prendre des précautions pour limiter le taux d'envoi des sondes pour les nouvelles adresses candidates : si l'hôte rencontre MAX_CONFLICTS, ou plus, conflits d'adresse sur une certaine interface, l'hôte DOIT limiter le taux de vérification de nouvelles adresses sur cette interface à pas plus d'une nouvelle adresse tentée par RATE_LIMIT_INTERVAL. C'est pour empêcher de catastrophiques tempêtes ARP dans des cas d'échec pathologiques, comme d'un serveur DHCP défectueux qui alloue de façon répétée la même adresse à chaque hôte qui lui en demande une. Cette règle de taux de limitation s'applique non seulement aux conflits rencontrés durant la phase initiale de vérification mais aussi aux conflits rencontrés plus tard, décrits au paragraphe 2.4 "Détection de conflit d'adresse en cours et défense d'adresse".

Si ANNOUNCE_WAIT secondes après la transmission de la dernière sonde ARP aucune réponse ARP de conflit ni sonde ARP n'a été reçue, l'hôte a bien déterminé que l'adresse désirée peut être utilisée en toute sécurité.

2.2 Temporisations plus courtes sur les technologies de réseau appropriées

Des technologies de réseau peuvent émerger pour lesquelles sont appropriés de plus courts délais que ceux exigés par le présent document. Une publication ultérieure de l'IETF pourra être produite pour fournir des lignes directrices pour des valeurs différentes pour PROBE_WAIT, PROBE_NUM, PROBE_MIN, et PROBE_MAX sur ces technologies.

Si il apparaît une situation où les différents hôtes d'une liaison utilisent des paramètres de temporisation différents, cela ne pose aucun problème. Ce protocole ne dépend pas de ce que tous les hôtes sur une liaison mettent en œuvre la même version du protocole ; bien sûr, ce protocole ne dépend pas de ce que tous les hôtes sur une même liaison mettent en œuvre le protocole. Tout ce qui est exigé est que les hôtes mettent en œuvre ARP comme spécifié dans la RFC 826, et répondent correctement aux demandes ARP qu'ils reçoivent. Dans la situation où différents hôtes utilisent des paramètres de temporisation différents, tout ce qui va se produire est que certains hôtes vont configurer leurs interfaces plus rapidement que d'autres. Dans le cas peu probable où un conflit d'adresse ne serait pas détecté durant la phase de vérification d'adresse, le conflit va quand même être détecté par la détection de conflit d'adresse en cours décrit au paragraphe 2.4.

2.3 Annonce d'une adresse

Ayant vérifié qu'une adresse désirée peut être utilisée en toute sécurité, un hôte qui met en œuvre la présente spécification DOIT alors annoncer qu'il commence à utiliser cette adresse en diffusant des annonces ARP ANNOUNCE_NUM, espacées de ANNOUNCE_INTERVAL secondes. Une annonce ARP est identique à une sonde ARP décrite ci-dessus, sauf que maintenant les adresses IP d'envoyeur et de cible sont toutes deux réglées à la nouvelle adresse IPv4 choisie par l'hôte. L'objet de ces annonces ARP est de s'assurer que les autres hôtes sur la liaison n'ont pas d'entrées d'antémémoire ARP périmées laissées sur

un autre hôte qui auraient pu utiliser précédemment la même adresse. L'hôte peut légitimement commencer à utiliser l'adresse IP immédiatement après l'envoi de la première des deux annonces ARP ; l'envoi de la seconde annonce ARP peut être réalisé en asynchrone, en concurrence avec d'autres opérations de réseautage que l'hôte peut souhaiter effectuer.

2.4 Détection de conflit d'adresse en cours et défense d'adresse

La détection de conflit d'adresse n'est pas limitée au seul moment de la configuration initiale d'interface, quand un hôte est en train d'envoyer des sondes ARP. La détection de conflit d'adresse est un processus continu qui est en effet aussi longtemps qu'un hôte utilise une adresse. À tout moment, si un hôte reçoit un paquet ARP (Demande ou Réponse) où "l'adresse IP d'envoyeur" est (une des) la propre adresse IP de l'hôte configurée sur cette interface, mais où "l'adresse de matériel d'envoyeur" ne correspond à aucune des propres adresses d'interface de l'hôte, c'est alors un paquet ARP de conflit, qui indique qu'un autre hôte pense aussi qu'il est légitimement en train d'utiliser cette adresse. Pour résoudre le conflit d'adresse, un hôte DOIT répondre à un paquet ARP de conflit comme décrit en (a), (b), ou (c) ci-dessous :

(a) À réception d'un paquet ARP de conflit, un hôte PEUT choisir de cesser immédiatement d'utiliser l'adresse, et de signaler une erreur à l'agent de configuration comme décrit précédemment.

(b) Si un hôte a actuellement une connexion TCP active ou d'autres raisons de préférer garder la même adresse IPv4, et qu'il n'a pas vu d'autres paquets ARP de conflit depuis les dernières DEFEND_INTERVAL secondes, il PEUT alors choisir de tenter de défendre son adresse en enregistrant l'heure de réception du paquet ARP de conflit, et ensuite de diffuser une seule annonce ARP, donnant ses propres adresses IP et de matériel comme adresses d'envoyeur de l'ARP, avec l'adresse IP cible réglée à sa propre adresse IP, et l'adresse de matériel cible réglée toute à zéro. Cela fait, l'hôte peut alors continuer d'utiliser l'adresse normalement sans autre action particulière. Cependant, si ce n'est pas le premier paquet ARP de conflit que l'hôte a vu, et si l'heure enregistré pour le paquet ARP de conflit précédent est récente, dans les DEFEND_INTERVAL secondes, l'hôte DOIT alors immédiatement cesser d'utiliser cette adresse et signaler une erreur à l'agent de configuration comme décrit précédemment. Ceci est nécessaire pour assurer que deux hôtes ne restent pas englués dans une boucle sans fin avec les deux hôtes essayant de défendre la même adresse.

(c) Si un hôte a été configuré de façon à ce qu'il n'abandonne son adresse dans aucune circonstance (peut-être parce que c'est un type d'appareil qui a besoin d'une adresse IP stable et bien connue, comme un routeur par défaut d'une liaison ou un serveur DNS) il PEUT alors choisir de défendre indéfiniment son adresse. Si un tel hôte reçoit un paquet ARP de conflit, il devrait alors prendre les mesures appropriées pour enregistrer des informations utiles comme une adresse Ethernet de source du paquet ARP, et informer un administrateur du problème. Le nombre de telles notifications devrait être contrôlé de façon appropriée pour empêcher qu'un nombre excessif de rapports d'erreur soient générés. Si l'hôte n'a pas vu d'autre paquets ARP de conflit récemment, dans les dernières DEFEND_INTERVAL secondes, il DOIT alors enregistrer l'heure de réception du paquet ARP de conflit, et ensuite diffuser une seule annonce ARP, donnant ses propres adresses IP et de matériel. Cela fait, l'hôte peut alors continuer d'utiliser normalement l'adresse sans autre action particulière. Cependant, si ce n'est pas le premier paquet ARP de conflit que voit l'hôte, et si l'heure enregistrée pour le précédent paquet ARP de conflit est dans les DEFEND_INTERVAL secondes, l'hôte NE DOIT alors PAS envoyer une autre annonce ARP défensive. Ceci est nécessaire pour s'assurer que deux hôtes mal configurés ne restent pas englués dans une boucle sans fin en inondant le réseau avec du trafic de diffusion alors qu'ils essayent tous deux de défendre la même adresse.

Un hôte qui souhaite assurer un fonctionnement réseau fiable DOIT répondre aux paquets ARP de conflit comme décrit en (a), (b), ou (c) ci-dessus. Ignorer les paquets ARP de conflit résulte en des défaillances de réseau aléatoires qu'il peut être difficile de diagnostiquer et qui sont très frustrantes pour l'utilisateur humain.

Une reconfiguration d'adresse forcée peut être perturbante, causant la rupture de connexions TCP (et d'autre couche transport). Cependant, de telles perturbations devraient être excessivement rares, et si une duplication d'adresse accidentelle se produit, la perturbation de la communication est inévitable. Il n'est pas possible que deux hôtes différents utilisant la même adresse IP sur le même réseau fonctionnent de façon fiable.

Avant d'abandonner une adresse à cause d'un conflit, les hôtes DEVRAIENT activement tenter de réinitialiser toutes connexions existantes en utilisant cette adresse. Cela atténue certaines menaces sur la sécurité que fait peser la reconfiguration d'adresse, comme exposé à la Section 5.

Pour la plupart des machines clients qui n'ont pas besoin d'une adresse IP fixe, demander immédiatement à l'agent de configuration (utilisateur humain, client DHCP, etc.) de configurer une nouvelle adresse aussitôt que le conflit est détecté est le meilleur moyen de restaurer une communication utile aussi vite que possible. Le mécanisme décrit ci-dessus de diffusion d'une seule annonce ARP pour défendre l'adresse atténue un peu le problème, en aidant à améliorer les chances qu'un des deux hôtes en conflit puisse conserver son adresse.

2.5 Poursuite du fonctionnement

Depuis le moment où un hôte envoie sa première annonce ARP, jusqu'au moment où il cesse d'utiliser cette adresse IP, l'hôte DOIT répondre aux demandes ARP de la façon habituelle exigée par la spécification ARP [RFC0826]. Précisément, cela signifie que chaque fois qu'un hôte reçoit une demande ARP, ce n'est pas un paquet ARP de conflit comme décrit ci-dessus au paragraphe 2.4, où l'adresse IP de cible de la demande ARP est (une des) la propre adresse IP de l'hôte configurée sur cette interface, l'hôte DOIT répondre avec une réponse ARP comme décrit dans la RFC 826. Cela s'applique également aux demandes ARP standard avec des adresses IP d'envoyeur non zéro et aux demandes de sonde avec des adresses IP d'envoyeur toutes de zéros.

2.6 Réponses ARP en diffusion

Dans un réseau bien géré avec des adresses allouées manuellement, ou un réseau avec un serveur DHCP fiable et des clients DHCP fiables, un conflit d'adresse ne devrait se produire que dans de rares scénarios de défaillance, de sorte que la surveillance passive décrite au paragraphe 2.4 est adéquate. Si deux hôtes sont en train d'utiliser la même adresse IP, alors tôt ou tard un hôte ou l'autre va diffuser une demande ARP, que l'autre va voir, permettant que le conflit soit détecté et par conséquent résolu.

Il est cependant possible qu'une configuration de conflit puisse persister pendant un bref instant avant d'être détectée. Supposons que deux hôtes, A et B, aient par inadvertance alloué la même adresse IP, X. Supposons de plus qu'au moment où ils vérifient tous deux si l'adresse peut être utilisée en toute sécurité, la liaison de communication entre eux ne soit pas fonctionnelle pour une raison quelconque, de sorte que ni l'un ni l'autre ne détecte le conflit au moment de la configuration d'interface. Supposons maintenant que la liaison de communication est restaurée, et qu'un troisième hôte, C, diffuse une demande ARP pour l'adresse X. Ignorants de tout conflit, les deux hôtes A et B vont envoyer des réponses ARP en envoi individuel à l'hôte C. L'hôte C va voir les deux réponses, et être un peu étonné, mais ni l'hôte A ni l'hôte B ne vont voir la réponse de l'autre, et aucun d'eux ne va détecter immédiatement qu'il y a un conflit à résoudre. Les hôtes A et B vont continuer d'ignorer le conflit jusqu'à ce que l'un ou l'autre diffuse une demande ARP de son propre chef.

Si on désire une détection de conflit plus rapide, ce peut être réalisé en faisant que les hôtes envoient des réponses ARP en utilisant la diffusion de niveau liaison, au lieu de n'envoyer que les demandes ARP via la diffusion, et les réponses via l'envoi individuel. Ceci n'est PAS RECOMMANDÉ en utilisation générale, mais d'autres spécifications construites sur l'ACD IPv4 pourront choisir de spécifier des réponses ARP diffusées si c'est approprié. Par exemple, "Configuration dynamique des adresses IPv4 de liaison locale" [RFC3927] spécifie des réponses ARP en diffusion parce que dans ce contexte, la détection de conflit d'adresse utilisant l'ACD IPv4 n'est pas simplement une précaution de sauvegarde pour détecter les défaillances de certains autres mécanismes de configuration ; la détection de conflit d'adresse utilisant l'ACD IPv4 est le seul mécanisme de configuration.

L'envoi des réponses ARP en utilisant la diffusion n'augmente pas le trafic de diffusion, mais dans le pire des cas, de pas plus qu'un facteur deux. Dans l'usage traditionnel d'ARP, une réponse ARP en envoi individuel ne se produit qu'en réponse à une demande ARP en diffusion, de sorte que les envoyer en diffusion signifie qu'on génère au plus une réponse en diffusion en réponse à chaque demande diffusée existante. Sur de nombreux réseaux, le trafic ARP est une proportion si insignifiante du trafic total que le doubler ne fait en pratique pas de différence. Cependant, ceci peut n'être pas vrai de tous les réseaux, de sorte que la diffusion des réponses ARP NE DEVRAIT PAS être utilisée de façon universelle. La diffusion des réponses ARP devrait être utilisée lorsque l'avantage d'une détection de conflit plus rapide compense le coût d'un trafic de diffusion accru et d'une augmentation de la charge de traitement des paquets sur les hôtes du réseau participants.

3. Pourquoi les annonces ARP sont-elles effectuées avec des paquets de demande ARP et pas des paquets de réponse ARP ?

Durant les délibérations de l'IETF sur la détection de conflit d'adresse IPv4 de 2000 à 2008, une question a été posée de façon répétée : "Les annonces ARP ne devraient elles pas être effectuées en utilisant des paquets de réponse ARP gratuits ?"

Cette remarque semble raisonnable. Une réponse ARP conventionnelle est une réponse à une question. Si en fait aucune question n'a été posée, il serait raisonnable de décrire une telle réponse comme gratuite.

Le terme de "réponse gratuite" semble s'appliquer parfaitement à une annonce ARP : une réponse à une question implicite qu'en fait personne n'a posée.

Cependant si cela peut sembler raisonnable en principe, en pratique il y a deux raisons qui font pencher la balance en faveur de l'utilisation de paquets de demande ARP. L'une est un précédent historique, et l'autre est pragmatique.

Le précédent historique est que (comme décrit à la Section 4) ARP gratuit est documenté dans le réseautage de Stevens [Ste94] comme utilisant des paquets de demande ARP. BSD Unix, Microsoft Windows, Mac OS 9, Mac OS X, etc., utilisent tous des paquets de demande ARP comme décrit par Stevens. À ce stade, essayer de rendre obligatoire qu'ils se mettent tous à utiliser des paquets de réponse ARP serait futile.

La raison pratique est que les paquets de demande ARP vont probablement fonctionner correctement avec plus de mises en œuvre ARP existantes, dont certaines ne peuvent pas mettre en œuvre entièrement correctement la RFC 826. Les règles de réception de paquet de la RFC 826 déclarent que le opcode est la dernière chose à vérifier dans le traitement de paquet, donc cela ne devrait pas avoir réellement d'importance, mais il peut y avoir des mises en œuvre "créatives" qui ont un traitement de paquet différent selon le champ "ar$op", et il y a plusieurs raisons pour qu'elles acceptent plus probablement les demandes ARP gratuites que les réponses ARP gratuites :

- Une mise en œuvre incorrecte d'ARP peut s'attendre à ce que les réponses ARP ne soient envoyées qu'en envoi individuel. La RFC 826 ne dit pas cela, mais une mise en œuvre incorrecte peut le supposer ; le "principe de moindre surprise" dit que lorsque il y a deux façons ou plus de résoudre un problème de réseautage et qu'elles sont par ailleurs également bonnes, celle qui a le moins de propriétés inhabituelles est celle qui a le plus de chances d'avoir le moins de problèmes d'interopérabilité avec les mises en œuvre existantes. Une annonce ARP a besoin de diffuser les informations à tous les hôtes sur la liaison. Comme les paquets de demande ARP sont toujours diffusés, et que les paquets de réponse ARP ne le sont pas, recevoir un paquet de demande ARP via diffusion est moins surprenant que de recevoir un paquet de réponse ARP via diffusion.

- Une mise en œuvre ARP incorrecte peut s'attendre à ce que les réponses ARP ne soient reçues qu'en réponse aux demandes ARP qui ont été produites récemment par cette mise en œuvre. Les réponses inattendues non sollicitées peuvent être ignorées.

- Une mise en œuvre ARP incorrecte peut ignorer les réponses ARP où "ar$tha" ne correspond pas à son adresse de matériel.

- Une mise en œuvre ARP incorrecte peut ignorer les réponses ARP où "ar$tpa" ne correspond pas à son adresse IP.

En résumé, il y a plus de façons pour qu'une mise en œuvre ARP incorrecte puisse plausiblement rejeter une réponse ARP (qui se produit généralement par suite d'une sollicitation du client) qu'une demande ARP (dont il est déjà attendu qu'elle se produise non sollicitée).

4. Note historique

Certains lecteurs ont prétendu que "ARP gratuit", comme décrit dans Stevens [Ste94], fournit une détection d'adresse dupliquée, rendant ACD inutile. Ceci est incorrect. Ce que Stevens décrit comme ARP gratuit est exactement le même paquet auquel le présent document se réfère sous le terme plus descriptif de "annonce ARP". Cette mise en œuvre d'ARP gratuit traditionnel envoie une seule annonce ARP quand une interface est configurée. Le résultat est que la victime (le détenteur existant de l'adresse) enregistre une erreur, et l'offenseur continue de fonctionner, souvent sans même détecter de problème. Les deux machines commencent alors normalement à essayer d'utiliser la même adresse IP, et échouent à fonctionner correctement parce que chacune est constamment en train de réinitialiser la connexion TCP de l'autre. On attend de l'administrateur humain qu'il remarque le message enregistré sur la machine de la victime et qu'il répare les dommages après les faits. Normalement cela doit être fait en allant physiquement sur les machines en question, car dans cet état aucune n'est capable de garder la connexion TCP ouverte pendant assez longtemps pour faire quelque chose d'utile sur le réseau.

ARP gratuit ne donne en fait pas de détection efficace d'adresse dupliquée et (en janvier 2008) de nombreux résultats de tête d'une recherche sur Google sur la phrase "ARP gratuit" sont des articles décrivant comment le désactiver.

Cependant, les mises en œuvre de la détection de conflit d'adresse IPv4 devraient être conscientes que, à ce jour, ARP gratuit est toujours largement déployé. Les étapes décrites aux paragraphes 2.1 et 2.4 de ce document aident à rendre un hôte robuste contre la mauvaise configuration et le conflit d'adresse, même quand l'autre hôte ne respecte pas les règles du jeu.

5. Considérations pour la sécurité

La détection de conflit d'adresse IPv4 (ACD) se fonde sur ARP [RFC826] et hérite des faiblesses de sécurité de ce protocole. Un hôte malveillant peut envoyer des paquets ARP frauduleux sur le réseau, interférant avec le fonctionnement correct des autres hôtes. Par exemple, il est facile à un hôte de répondre à toutes les demandes ARP avec des réponses qui donnent sa propre adresse de matériel, revendiquant ainsi la propriété de toutes les adresses du réseau.

La présente spécification ne rend pas pires les faiblesses existantes d'ARP, et par certains côté, les améliore : au lieu d'échouer en silence sans indiquer pourquoi, les hôtes qui mettent en œuvre la présente spécification tentent de reconfigurer automatiquement, ou au moins informent l'utilisateur humain de ce qui se passe.

Si un hôte choisit de plein gré une nouvelle adresse en réponse à un conflit ARP, comme décrit au paragraphe 2.4, alinéa (a), cela facilité potentiellement la capture de la connexion TCP par des attaquants malveillants sur la même liaison. Faire qu'un hôte réinitialise activement toutes les connexions existantes avant d'abandonner une adresse aide à atténuer ce risque.

6. Remerciements

Le présent document résulte de discussions au sein du groupe de travail Zeroconf sur l'adressage IPv4 de liaison locale [RFC3927], où il n'était pas clair pour de nombreux participants quels éléments de la gestion d'adresse de liaison locale étaient spécifiques de cet espace de problème particulier (par exemple, choix aléatoire d'une adresse) et quels éléments étaient génériques et applicables à tous les mécanismes de configuration d'adresse IPv4 (par exemple, la détection de conflit d'adresse). Les personnes suivantes ont fait de précieux commentaires pendant le cours de ce travail et/ou les étapes suivantes de l'édition de ce document : Bernard Aboba, Randy Bush, Jim Busse, James Carlson, Alan Cox, Spencer Dawkins, Pavani Diwanji, Ralph Droms, Donald Eastlake III, Alex Elder, Stephen Farrell, Peter Ford, Spencer Giacalone, Josh Graessley, Erik Guttman, Myron Hattig, Mike Heard, Hugh Holbrook, Richard Johnson, Kim Yong-Woon, Marc Krochmal, Rod Lopez, Rory McGuire, Satish Mundra, Thomas Narten, Erik Nordmark, Randy Presuhn, Howard Ridenour, Pekka Savola, Daniel Senie, Dieter Siegmund, Valery Smyslov, Mark Townsley, Oleg Tychev, et Ryan Troll.

7. Références

7.1 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.

7.2 Références pour information

[802] ANSI/IEEE Std 802, "IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture", 1990.

[802.3] ISO/CEI 8802-3, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", (aussi ANSI/IEEE Std 802.3-1996), 1996.

[802.5] ISO/CEI 8802-5, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 5: Token ring access method and physical layer specifications", (aussi ANSI/IEEE Std 802.5-1998), 1998.

[802.11] IEEE Std. 802.11-1999, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC3203] Y. T'Joens, C. Hublet, P. De Schrijver, "Extension DHCP Reconfigure", décembre 2001. (*MàJ par* RFC6704) *(P.S.)*

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

[Ste94] W. Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, 1994.

Adresse de l'auteur

Stuart Cheshire
Apple Inc.
1 Infinite Loop
Cupertino
California 95014
USA

téléphone : +1 408 974 3207
mél : rfc@stuartcheshire.org

Déclaration de droits de reproduction

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