Groupe de travail Réseau
Request for Comments : 5227
RFC mise à jour : 826
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 un des hôtes ou les deux. Le présent document décrit (i) une précaution simple qu'un hôte peut prendre à l'avance pour l'aider à empêcher cette mauvaise configuration de se produire, et (ii) si cette mauvaise configuration se produit, un mécanisme simple par lequel l'hôte peut détecter passivement, après coup, qu'elle s'est produite, afin que l'hôte ou l'administrateur puisse répondre en rectifiant le problème.

Table des Matières

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 (ARP, *Address Resolution Protocol*) existant fournit un moyen facile pour qu'un hôte détecte cette sorte de mauvaise configuration et la rapporte à l'utilisateur. La spécification DHCP [RFC2131] mentionne bièvement le rôle d'ARP pour détecter les mauvaises configurations, comme illustré dans les trois extraits suivants de la RFC 2131 :

- Le client DEVRAIT sonder 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) il DOIT envoyer un message DHCP

DECLINE au serveur

Malheureusement, la spécification DHCP ne donne pas de lignes directrices 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 même sur quelle sortes de paquets un hôte devrait être à l'écoute, 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 qu'il avait tort. Elle manque aussi à spécifier quelles précautions devrait prendre un client DHCP pour se garder contre des cas d'échec pathologiques, comme un serveur DHCP qui offre de façon répétée la même adresse, bien qu'elle ait fait plusieurs fois l'objet d'un DECLINE.

Les auteurs de la spécification DHCP peuvent avoir eu des justifications pour penser à ce moment que les réponses à ces questions semblaient trop simples, évidentes, et sans problème pour valoir la peine d'être mentionnées, 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 cette omission en spécifiant clairement les actions requises pour :

1. Déterminer si l'utilisation d'une adresse a une probabilité de 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 involontairement sur le point de commencer à utiliser la même adresse, et tous deux sont simultanément dans le processus de sondage pour déterminer si l'adresse peut être utilisée en toute sécurité (paragraphe 2.1.).

2. La détection passive ultérieure qu'un autre hôte sur le réseau utilise par inadvertance la même adresse. Même si tous les hôtes prennent des précautions pour éviter d'utiliser une adresse déjà utilisée, 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 brasseurs Ethernet ne fonctionne pas au moment de la configuration de l'adresse. Un hôte bien conçu va traiter non seulement les conflits détectés durant la configuration d'interface, mais aussi les conflits détectés ultérieurement, pour la durée entière de l'utilisation de l'adresse par l'hôte (paragraphe 2.4.).

3. La limitation du taux de 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 (ACD, *Address Conflict Detection*) IPv4 ne se limite pas aux clients DHCP. Quelle que soit la façon dont une adresse a été configurée, via une entrée manuelle par un utilisateur humain, via des informations reçues d'un serveur DHCP, ou via toute autre source d'informations de configuration, la détection de conflits est utile. Lorsque il détecte un conflit, l'agent de configuration devrait avoir notification de l'erreur. Dans le cas où l'agent de configuration est un utilisateur 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 d'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 de 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 choisi est en conflit avec un autre hôte sur le réseau. Le logiciel de configuration peut choisir de cesser l'opération réseau, ou il peut choisir automatiquement une nouvelle adresse afin que l'hôte puisse rétablir la connexité IP aussitôt que possible.

L'allocation des adresses IPv4 de liaison locale [RFC3927] peut être vue comme un cas particulier de ce mécanisme, où l'agent de configuration est un générateur de nombres pseudo aléatoires, et l'action qu'il entreprend lorsque un conflit lui est notifié est de prendre un numéro aléatoire différent et d'essayer à nouveau. En fait, c'est exactement comment l'adressage IPv4 de liaison locale a été mise en œuvre dans le Mac OS 9 dans les années 1998. Si le client DHCP échoue à obtenir une réponse d'un serveur DHCP, il va simplement fabriquer une fausse réponse 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, construisant une nouvelle adresse 169.254.x.x aléatoire autant de fois que nécessaire jusqu'à ce que cela réussisse. La mise en œuvre de ACD comme caractéristique standard de la pile réseau a pour effet collatéral que cela signifie 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 la [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

Quand 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 [RFC826] comme "ar$spa" (adresse de l'envoyeur du protocole) et "ar$tpa" (Adresse cible du protocole), respectivement. Pour l'usage de ARP décrit dans le présent 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 de zéros. L'adresse de matériel de l'envoyeur DOIT contenir l'adresse de matériel de l'interface d'envoi du paquet. Le champ "adresse IP de l'envoyeur" DOIT être réglée toute à zéro, pour éviter de polluer les antémémoires ARP dans les autres hôtes sur la même liaison dans le cas où l'adresse se trouverait 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 ("Quelqu'un utilise t-il cette adresse ?") et une déclaration implicite ("C'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, excepté que les champs d'adresse IP de l'envoyeur et de cible contiennent l'adresse IP annoncée. Il porte une déclaration plus forte qu'une sonde ARP, à savoir, "ceci est l'adresse que j'utilise maintenant."

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

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

1.2 Relations avec la RFC 826

Le présent document ne modifie aucune des règles de protocole de la RFC 826. Il ne modifie pas le format de paquet, ni la signification des champs. Les règles existantes pour "génération de paquet" et "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) en ajoutant un essai trivial qui devrait être effectué sur chaque paquet ARP reçu, pour faciliter la détection de conflit passif en cours. Cet essai supplémentaire ne crée aucun frais généraux de paquet supplémentaire sur le réseau (aucun paquet supplémentaire n'est envoyé) et une charge de CPU supplémentaire négligeable sur les hôtes, car chaque hôte qui met en œuvre ARP est *déjà* obligé de traiter chaque paquet ARP reçu conformément aux règles de réception de paquet spécifiées dans la [RFC0826]. Ces règles incluent déjà de vérifier si l'adresse IP d'envoyeur du paquet ARP apparaît dans une des entrées de l'antémémoire ARP de l'hôte ; l'essai supplémentaire est simplement de vérifier si l'adresse IP d'envoyeur est la *propre* adresse IP de l'hôte, potentiellement pas plus qu'une seule instruction machine supplémentaire dans de nombreuses architectures.

Comme le spécifie déjà la RFC 826, un paquet de demande ARP a deux fonctions, une assertion et une question :
* Assertion : les champs "ar$sha" (adresse de matériel de l'envoyeur) et "ar$spa" (adresse de protocole de l'envoyeur) servent ensemble d'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, en quelle adresse de matériel elle est transposée.

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

Certains lecteurs ont souligné qu'il était probablement impossible de poser une question vraiment pure ; poser toute question invite nécessairement à des spéculations sur pourquoi l'interrogateur veut connaître la réponse. Juste comme quelqu'un qui montre un siège vide et demande, "Quelqu'un est-il assis ici ?" implique un non-dit de "... parce que sinon je vais le faire," la même chose est vraie ici. Une sonde ARP avec une adresse IP d'envoyeur toute de zéros peut ostensiblement poser simplement une innocente question ("Y a t-il queIqu'un qui 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 précurseur de la revendication de l'adresse.

Par conséquent, si cette mise en œuvre est aussi, à ce moment précis, en train de poser la même question, elle devrait reconnaître qu'elles ne peuvent pas être toutes deux assises sur la même chaise, et donc qu'il serait prudent de demander un autre siège.

1.2.1 Réponses ARP en diffusion

Dans certaines applications de détection de conflit d'adresse (ACD, *Address Conflict Detection*) IPv4, il peut être avantageux de livrer les réponses ARP en utilisant la diffusion plutôt que l'envoi individuel parce que cela permet de détecter plus tôt les conflits d'adresses. 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 diffusion, parce que dans ce contexte le compromis entre l'accroissement du trafic de diffusion dans l'échange pour une fiabilité accrue et la tolérance aux fautes est réputé être approprié. Il peut y avoir d'autres futures spécifications où le même compromis est approprié. Des détails supplémentaires sont donnés au paragraphe 2.6, "Réponses ARP en diffusion".

La RFC 826 implique que les réponses aux demandes ARP soient généralement livrées en envoi individuel, mais il est aussi acceptable de livrer les réponses ARP en 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 la diffusion de couche de 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], l'anneau à jetons [802.5], et les LAN sans fil IEEE 802.11 [802.11], ainsi que d'autres technologies de couche de liaison qui opèrent à des débits de données d'au moins 1 Mbit/s, ont une latence d'aller-retour d'au plus une seconde, et utilisent ARP [RFC0826] pour transposer des adresses IP en adresses de matériel de couche de liaison. Partout où le présent document utilise le terme "IEEE 802", le texte s'applique églement à toutes ces technologies de réseau.

Les technologies de couche de liaison qui prennent en charge ARP mais opèrent 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 sondage. Sur ces sortes de liaisons, il peut être souhaitble de spécifier des valeurs différentes pour les paramètres suivants :

(a) PROBE_NUM, PROBE_MIN, et PROBE_MAX, le nombre et l'intervalle entre les sondes ARP (paragraphe 2.1)

(b) ANNOUNCE_NUM et ANNOUNCE_INTERVAL, le nombre et l'intervalle entre les annonces ARP (paragraphe 2.3)

(c) RATE_LIMIT_INTERVAL et MAX_CONFLICTS, contrôlant le débit maximum auquel les revendications d'adresse peuvent être tentées (paragraphe 2.1)

(d) DEFEND_INTERVAL, intervalle de temps entre ARP en conflit en dessous duquel un hôte NE DOIT PAS tenter de défendre son adresse, (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 adresse IP particulière est actuellement utilisée. Cependant, qui met en œuvre la détection de conflit d'adresse pour de tels réseau 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 la mettent en œuvre. Pour qu'un certain hôte qui met en œuvre la présente spécification soit protégé contre les conflits

d'adresses accidentels, tout ce qui est exigé est que les homologues sur la même liaison mettent correctement en œuvre le protocole ARP donné dans la RFC 826. Précisément, quand un hôte homologue reçoit une demande ARP où l'adresse de protocole cible de la demande ARP correspond à l'adresse IP (ou une des adresses) de cet hôte configurée sur cette interface, alors 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 les conflits entre deux hôtes qui utilisent la même adresse sur la même liaison physique. L'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 par des appareils sans compteur sur des réseaux privés sans compteurs tout autour du monde, et ceci ne crée pas de conflit, parce que ils sont sur des liaisons différentes. Il n'y aurait de conflit que si deux appareils de ce type devaient être connectés sur la même liaison, et quand cela arrive (c'est quelques fois le cas) c'est un parfait exemple de situation où l'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 être "sur la même liaison" si :
- quand tout hôte A,de cet ensemble, envoie un paquet à tout autre hôte B dans cet ensemble, en utilisant l'envoi individuel, la diffusion groupée, ou la diffusion, la charge utile entière de couche de liaison du paquet arrive non modifiée, et
- une diffusion envoyée sur cette liaison par tout hôte de cet ensemble d'hôtes peut être reçue par tout autre hôte de cet ensemble.

L'en-tête de couche de liaison peut être modifié, comme dans l'acheminement de source d'un anneau à jetons [802.5], mais pas la charge utile de couche de liaison. En particulier, si un appareil qui transmet un paquet modifie une partie quelconque de l'en-tête IP ou de la charge utile IP, le paquet n'est alors 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 concentrateurs, ou des commutateurs et être toujours considéré comme étant sur la même liaison pour les besoins du présent document, mais pas 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 les routeurs ou autres hôtes multi-rattachements, sans considération de si l'hôte/routeur transmet actuellement 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 la reconfiguration DHCP de la [RFC3203] deviennent de mise en œuvre courante) il n'y a aucun moyen pratique pour que le serveur DHCP informe les clients d'un changement d'adresse. Par conséquent, pour de tels appareils, le traitement de conflits par le tirage d'une nouvelle adresse IP n'est pas une bonne option. Dans ces 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 un autre appareil sur le réseau qui prétend avoir la même adresse IP va polluer les antémémoires ARP de l'homologue et empêcher une communication fiable, donc il est quand même utile d'informer l'opérateur. Si un conflit est détecté au moment où l'opérateur établit manuellement l'adresse fixe, il est alors utile d'informer immédiatement l'opérateur ; si un conflit est détecté ensuite, il est utile d'informer l'opérateur via un canal de communication asynchrone approprié. Mëme si une communication fiable via l'adresse conflictuelle n'est pas possible, il peut quand même être possible d'informer l'opérateur via quelque autre canal de communication qui fonctionne encore, comme via une autre interface sur le routeur, via une adresse IPv4 dynamique de liaison locale, via une adresse IPv6 qui fonctionne, ou même via une technologie non IP complètement différente comme un écran à rattachement local ou une console de série.

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

Cette section décrit le sondage initial pour déterminer en toute sécurité si une adresse est déjà utilisée, annoncer l'adresse choisie, la vérification de conflit en cours, et l'utilisation facultative de réponses ARP en diffusion pour fournir une détection de conflit plus rapide.

2.1 Sondage d'une adresse

Avant de commencer à utiliser une adresse IPv4 (qu'elle soit reçue d'une configuration manuelle, de DHCP, ou d'un autre moyen) 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 transite d'un état inactif à un état actif, quand un ordinateur se remet en activité, 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 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 c'est inutile à cause de la capacité des hôtes de découvrir passivement les conflits, comme décrit au paragraphe 2.4.

2.1.1 Détails du sondage

Un hôte sonde 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 de l'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 dans le cas où l'adresse se trouverait 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 demande ARP construite de cette façon, avec une "adresse IP d'envoyeur" toute de zéros, est appelée une "sonde ARP".

Quand il est prêt à commencer à sonder, l'hôte devrait attendre pendant un délai aléatoire choisi de façon uniforme dans la gamme de zéro à PROBE_WAIT secondes, et devrait alors envoyer PROBE_NUM paquets de sonde, chacun espacé uniformément et aléatoirement de PROBE_MIN à PROBE_MAX secondes. Ce délai initial aléatoire aide à s'assurer qu'un grand nombre d'hôtes alimentés en même temps n'envoient pas tous simultanément leurs paquets de sonde initiaux.

Si durant cette période, depuis le début du processus de sondage 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 sondée, alors l'hôte DOIT traiter cette adresse comme étant utilisée par un autre hôte, et devrait indiquer à l'agent de configuration (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 de cible du paquet est l'adresse qu'il sonde, et si l'adresse de matériel d'envoyeur du paquet n'est pas l'adresse de matériel d'une des interfaces de l'hôte, alors l'hôte DEVRAIT similairement traiter cela comme un conflit d'adresse et signaler une erreur à l'agent de configuration comme ci-dessus. Cela peut se produire si deux hôtes (ou plus) ont, pour une raison quelconque, été configurés par inadvertance avec la même adresse, et si tous deux sont simultanément en train de sonder cette adresse pour voir 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 concentrateurs Ethernet (souvent appelés des "répéteurs à mémoire tampon") et de nombreux points d'accès sans fil peuvent "rediffuser" tous paquets en diffusion reçus 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 voir ses propres paquets ARP renvoyés 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'adresses sur une interface donnée, il DOIT alors limiter le taux de sondage des nouvelles adresses sur cette interface à pas plus d'une nouvelle adresse tentée par RATE_LIMIT_INTERVAL. C'est pour empêcher des tempêtes catastrophiques d'ARP dans des cas d'échec pathologiques, comme celui d'un serveur DHCP défectueux qui alloue répétitivement la même adresse à chaque hôte qui en demande une. Cette règle de limitation de taux s'applique non seulement aux conflits rencontrés durant la phase de sondage initial, mais aussi aux conflits rencontrés plus tard, comme décrit au paragraphe 2.4 "Détection de conflit d'adresse en cours et défense d'adresse".

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

2.2 Temporisation plus courte sur des technologies réseau appropriées

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

Si il apparaît une situation où différents hôtes sur une liaison utilisent des paramètres de temporisation différents, cela ne cause 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 liaison mettent en œuvre le protocole tout court. Tout ce qui est exigé est que tous les hôtes mettent en œuvre ARP comme spécifié dans la [RFC0826], 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 arriver est que certains hôtes vont configurer leurs interfaces plus rapidement que d'autres. Au cas improbable où un conflit d'adresse ne serait pas détecté durant la phase de sondage d'adresse, le conflit va quand même être détecté par la détection de conflit d'adresse en cours décrite ci-dessous au paragraphe 2.4.

2.3 Annonce d'une adresse

Ayant sondé pour déterminer 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 la sonde ARP décrite précédemment, 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 qui restent d'un autre hôte qui aurait pu avoir utilisé précédemment la même adresse. L'hôte peut légitimement commencer à utiliser l'adresse IP immédiatement après voir envoyé la première des deux annonces ARP ; l'envoi de la seconde annonce ARP peut être achevé en asynchrone, concurremment avec les 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 ne se limite pas seulement au moment de la configuration initiale d'interface, quand un hôte envoie des sondes ARP. La détection de conflit d'adresse est un processus permament qui est actif tant qu'un hôte utilise une adresse. À tout moment, si un hôte reçoit un paquet ARP (de demande *ou* de réponse) où l'adresse IP de l'envoyeur est une des propres adresses IP de l'hôte configurée sur cette interface, mais où l'adresse de matériel de l'envoyeur ne correspond à aucune des adresses d'interface de l'hôte, c'est alors un paquet ARP en conflit, qui indique qu'un autre hôte pense aussi qu'il utilise à juste titre cette adresse. Pour résoudre le conflit d'adresse, un hôte DOIT répondre à un paquet ARP en conflit comme décrit en (a), (b), ou (c) ci-dessous :

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

(b) Si un hôte a actuellement des connexions TCP actives ou d'autres raisons de préférer garder la même adresse IPv4, et si il n'a pas vu d'autre paquet ARP en conflit dans les dernières DEFEND_INTERVAL secondes, il PEUT alors choisir de tenter de défendre son adresse en enregistrant l'heure à laquelle le paquet ARP en conflit a été reçu, et 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 de 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 en conflit que voit l'hôte, et si l'heure enregistrée pour le précédent paquet ARP en conflit est récente, dans les DEFEND_INTERVAL secondes, alors l'hôte DOIT cesser immédiatement d'utiliser cette adresse et signaler une erreur à l'agent de configuration comme décrit ci-dessus. C'est nécessaire pour assurer que deux hôtes ne sont pas bloqués dans une boucle sans fin où les deux hôtes essayent de défendre la même adresse.

(c) Si un hôte a été configuré de telle façon qu'il ne devrait abandonner son adresse sous aucun prétexte (peut-être parce qu'il est un appareil qui a besoin d'avoir une adresse IP bien connue stable, comme un routeur par défaut d'une liaison ou un serveur du DNS) il PEUT alors choisir de défendre son adresse indéfiniment. Si un tel hôte reçoit un paquet ARP en conflit, il devrait alors prendre les mesures appropriées pour enregistrer les informations utiles comme l'adresse Ethernet de source du paquet ARP, et informer un administrateur du problème. Le nombre de ces 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 récemment d'autre paquet ARP en conflit, dans les dernières DEFEND_INTERVAL secondes, il DOIT alors enregistrer l'heure de réception de ce paquet ARP en conflit, puis diffuser une seule annonce ARP, donnant ses propres adresses IP et de matériel. Ceci 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 en conflit que voit l'hôte, et si l'heure enregistrée pour le précédent paquet ARP en conflit est dans les DEFEND_INTERVAL secondes, alors l'hôte NE DOIT PAS envoyer d'autre annonce ARP défensive. Ceci est nécessaire pour assurer que deux hôtes mal configurés ne restent pas collés dans une boucle sans fin en inondant le réseau avec du trafic en diffusion pour essayer tous deux de défendre la même

adresse.

Un hôte qui souhaite avoir un fonctionnement fiable du réseau DOIT répondre aux paquets ARP en conflit comme décrit en (a), (b), ou (c) ci-dessus. Ignorer les paquets ARP en conflit résulte en des défaillances aléatoires du réseau qui peuvent être difficiles à diagnostiquer et très frustrantes pour les utilisateurs.

Une reconfiguration d'adresse forcée peut être perturbatrice, causant la coupure des connexions TCP (et d'autre couche transport). Cependant, de telles perturbations devraient être excessivement rares, et si une duplication d'adresse se produit de façon inattendue, 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 tenter activement de réinialiser toute connexion existante qui utilise cette adresse. Cela atténue certaines menaces sur la sécurité que fait peser la reconfiguration d'adresse, comme discuté à la Section 5.

Pour la plupart des machines client 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 être capable de conserver son adresse.

2.5 Continuation du fonctionnement

À partir du 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 usuelle exigée par la spécification ARP [RFC826]. Précisément, cela signifie que chaque fois qu'un hôte reçoit une demande ARP, qui n'est pas un paquet ARP en conflit comme décrit ci-dessus au paragraphe 2.4, où l'adresse IP cible de la demande ARP est une des propres adresses 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 pour les demandes ARP standard avec des adresses IP d'envoyeur non zéro et les 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, des conflits d'adresses devraient ne 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 utilisent 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 conflictuelle puisse persister pendant un bref instant avant d'être détectée. Supposons que deux hôtes, A et B, ait reçu par inadvertance la même adresse IP, X. Supposons de plus qu'au moment où ils sondent tous deux pour déterminer si l'adresse peut être utilisée en toute sécurité, la liaison de communication entre eux ne soit plus fonctionnelle pour une raison quelconque, de sorte qu'aucun d'eux ne détecte le conflit au moment de la configuration de l'interface. Supposons maintenant que la liaison de communication soit restaurée, et qu'un troisième hôte, C, diffuse une demande ARP pour l'adresse X. Ignorant 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 peut être un peu troublé, mais ni l'hôte A ni l'hôte B ne vont voir la réponse de l'autre, et aucun ne va immédiatement détecter 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 se propre demande ARP.

Si une détection de conflit plus rapide est désirée, cela peut être réalisé en ayant des hôtes qui envoient des réponses ARP en utilisant la diffusion de niveau liaison, au lieu d'envoyer seulement des demandes ARP via diffusion, et des réponses en envoi individuel. Ceci N'est PAS RECOMMANDÉ pour une utilisation générale, mais d'autres spécifications qui s'appuient sur l'ACD IPv4 peuvent choisir de spécifier des réponses ARP en diffusion si c'est approprié. Par exemple, "Configuration dynamique d'adresses IPv4 de liaison locale" [RFC3927] spécifie des réponses ARP en diffusion parce que dans ce contexte, la détection des conflits d'adresses utilisant l'ACD IPv4 n'est pas simplement une précaution de sauvegarde pour détecter les défaillances d'un autre mécanisme de configuration ; la détection des conflits d'adresses utilisant l'ACD IPv4 est le seul mécanisme de configuration.

Envoyer les réponses ARP en diffusion augmente le trafic de diffusion, mais dans le pire des cas, pas de plus d'un facteur

deux. Dans l'usage traditionnel de l'ARP, une réponse ARP en envoi individuel ne se produit qu'en réponse à une demande ARP en diffusion, donc les envoyer à la place en diffusion signifie qu'on génère au plus une réponse en diffusion en réponse à chaque demande en diffusion existante. Sur de nombreux réseaux, le trafic ARP est une proportion insignifiante du trafic total de sorte que le doubler ne fait pas de différence pratique. Cependant, cela peut n'être pas vrai de tous les réseaux, donc les réponses ARP en diffusion NE DEVRAIENT PAS être utilisées universellement. Les réponses ARP en diffusion devraient être utilisées lorsque le bénéfice d'une détection de conflit plus rapide surpasse le coût de l'accroissement du trafic de diffusion et de la charge accrue de traitement des paquets sur les hôtes du réseau participant.

3. Pourquoi les annonces ARP sont effectuées en utilisant des paquets Demande ARP et non des paquets Réponse ARP

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

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

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

Quoique en principe cela puisse sembler raisonnable, en pratique il y a deux raisons qui font pencher l'argument en faveur de l'utilisation des paquets de demande ARP. 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 "Stevens Networking" [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 dans Stevens. À ce stade, essayer de les obliger tous à passer à l'utilisation de paquets de réponse ARP serait vain.

La raison pratique est que les paquets de demande ARP ont plus de chances de fonctionner correctement avec plus de mises en œuvre ARP existantes, dont certaines peuvent ne pas mettre en œuvre la RFC 826 totalement correctement. 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, de sorte que cela ne devrait réellement pas avoir 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 ya plusieurs raisons pour qu'il y ait plus de chances qu'elles acceptent les demandes ARP gratuites que les réponses ARP gratuites :

* Une mise en œuvre ARP incorrecte peut s'attendre à ce que les réponses ARP soient seulement en envoi individuel. La RFC 826 ne dit pas cela, mais une mise en œuvre incorrecte peut le supposer ; le "principe de moindre surprise" impose que lorsque il y a deux façons ou plus de résoudre un problème de réseautage qui par ailleurs sont également bonnes, celle qui présente le moins de propriétés inhabituelles est celle qui aura probablement 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 en diffusion, et comme les paquets de réponse ARP ne le sont pas, recevoir un paquet de demande ARP en diffusion est moins surprenant que de recevoir un paquet de réponse ARP en diffusion.

* Une mise en œuvre ARP incorrecte peut s'attendre à ce que les réponses ARP soient seulement reçues en réponse aux demandes ARP qui ont été produites récemment par cette mise en œuvre. Des réponses non sollicitées inattendues 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 plusieurs façon dont une mise en œuvre ARP incorrecte pourrait plausiblement rejeter une réponse ARP (qui se produit généralement par suite d'une sollicitation du client) plutôt qu'une demande ARP (dont il est déjà attendu qu'elle se produise sans sollicitation).

4. Note historique

Certains lecteurs ont prétendu que "l'ARP gratuit", décrit dans Stevens [Ste94], fournit la détection d'adresse dupliquée, ce qui rendrait l'ACD inutile. Ceci est incorrect. Ce que Stevens décrit comme ARP gratuit est exactement le même paquet que ce à quoi se réfère le présent document par le terme plus descriptif de "annonce ARP". Cette mise en œuvre ARP traditionnel gratuite envoie seulement une annonce ARP quand une interface est configurée pour la première fois. Le résultat est que la victime (le détenteur de l'adresse existante) enregistre une erreur, et l'agessseur continue de fonctionner, souvent sans même détecter de problème. Les deux machines essaient alors normalement d'utiliser la même adresse IP, et échoue à fonctionner correctement parce que chacun réinitialise constamment les connexions TCP de l'autre. L'administrateur humain est supposé remarquer le message sur la machine victime et réparer les dommages après les faits. Normalement, cela va être fait en allant physiquement sur les machines en question, car dans cet état aucune n'est capable de garder une connexion TCP ouverte pendant assez longtemps pour faire quelque chose d'utile sur le réseau.

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

Cependant, le mises en œuvre de la détection de conflit d'adresse IPv4 devrait être conscientes de ce que, au moment de la rédaction du présent mémoire, ARP gratuit est encore largement déployé. Les étapes décrites aux paragraphes 2.1 et 2.4 du présent document aident à rendre un hôte robuste contre la mauvaise configuration et les conflits d'adresses, même quand l'autre hôte ne respecte pas les mêmes règles.

5. Considérations sur la sécurité

La détection de conflit d'adresse (ACD, *Address Conflict Detection*) IPv4 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 donnant sa propre adresse de matériel, prétendant ainsi être propriétaire de toutes les adresses du réseau.

La présente spécification ne rend pas pire cette vulnérabilité existante de l'ARP, et dans une certaine mesure l'améliore : au lieu d'échouer en silence sans indication de cause, les hôtes qui mettent en œuvre la présente spécification tentent soit de reconfigurer automatiquement, soit au moins d'informer l'utilisateur humain de ce qui arrive.

Si un hôte choisit volontairement une nouvelle adresse en réponse à un conflit d'ARP, comme décrit au point a) du paragraphe 2.4, cela rend potentiellement plus facile à un attaquant malveillant sur la même liaison de capturer les connexions TCP. Faire qu'un hôte réinitialise activement toute connexion existante avant d'abandonner une adresse aide à atténuer ce risque.

6. Remerciements

Le présent document résulte des dicussions du groupe de travail "Zeroconf" sur l'adressage de liaison locale IPv4 [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 au hasard d'une adresse) et quels éléments étaient génériques et applicables à tous les mécanismes de configuration d'adresse IPv4 (par exemple, la détection des conflits d'adresses). Les personnes suivantes ont fait de précieux commentaires dans le cours de ces travaux et/ou dans le processus ultérieur d'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. *(MàJ par* RFC8174)

7.1 Références pour information

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

[802.3] Norme ISO/CEI 8802-3, "Technologie de l'information - Télécommunications et échanges d'informations entre systèmes -- réseaux locaux et de zone métropolitaine – Exigences communes - Partie 3 : spécifications des méthodes d'accès d'accès multiple avec surveillance de signal et détection de collision (CSMA/CD) et de couche physique", (aussi ANSI/IEEE Std 802.3-1996), 1996.

[802.5] Norme ISO/CEI 8802-5 1995, "Technologie de l'information - Télécommunications et échanges d'informations entre systèmes -- réseaux locaux et de zone métropolitaine – Exigences spécifiques -- Partie 5: Méthode d'accès par anneau à jeton et spécification de la couche physique", (ANSI/IEEE 802.5, édition 1995).

[802.11] IEEE Std. 802.11-1999, "Technologie de l'information - Télécommunications et échanges d'informations entre systèmes -- réseaux locaux et de zone métropolitaine – Exigences spécifiques -- Partie 11 : spécifications du contrôle d'accès au support de LAN sans fil (MAC) et de couche physique (PHY)", 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 complète de droits de reproduction

mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations 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, le IETF TRUST 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 encloses ne viole 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 faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le 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.