Groupe de travail Réseau
Request for Comments : 3927
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Cheshire, Apple Computer
B. Aboba, Microsoft Corporation
E. Guttman, Sun Microsystems
mai 2005

Configuration dynamique des adresses IPv4 de liaison locale

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright
Copyright (C) The Internet Society (2005). Tous droits réservés.

Résumé
Pour participer à un internet IP de large zone, un hôte doit être configuré avec des adresses IP pour ses interfaces, soit manuellement par l'utilisateur soit automatiquement à partir d'une source située dans le réseau, comme un serveur du protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*). Malheureusement, de telles informations de configuration d'adresse peuvent n'être pas toujours disponibles. Il est donc avantageux pour un hôte d'être capable de dépendre d'un sous-ensemble utile de fonctions de réseautage IP même lorsque aucune configuration d'adresse n'est disponible. Le présent document décrit comment un hôte peut automatiquement configurer une interface avec une adresse IPv4 au sein du préfixe 169.254/16 qui est valide pour la communication avec d'autres appareils connectés à la même liaison physique (ou logique).

Les adresses IPv4 de liaison locale ne conviennent pas pour les communications avec des appareils qui ne sont pas directement connectés à la même liaison physique (ou logique) et ne sont utilisées que lorsque des adresses stables, acheminables, ne sont pas disponibles (comme sur des réseaux ad hoc ou isolés). Le présent document ne recommande pas que des adresses IPv4 de liaison locale et des adresses acheminables soient connectées simultanément sur la même interface.

Table des Matières

1. Introduction

Comme la popularité du protocole Internet continue d'augmenter, il devient de plus en plus intéressant d'être capable d'utiliser des outils IP familiers comme FTP non seulement pour la communication mondiale, mais aussi pour la communication locale. Par exemple, deux personnes avec des ordinateurs portables qui prennent en charge des LAN sans fils IEEE 802.11 [802.11] peuvent se rencontrer et souhaiter échanger des fichiers. Il est souhaitable pour ces personnes d'être capables d'utiliser un logiciel d'application IP sans l'inconvénient d'avoir à configurer manuellement des adresses IP statiques ou d'établir un serveur DHCP [RFC2131].

Le présent document décrit une méthode par laquelle un hôte peut automatiquement configurer une interface avec une adresse IPv4 dans le préfixe 169.254/16 qui soit valide pour une communication de liaison locale sur cette interface. C'est particulièrement précieux dans des environnements où aucun autre mécanisme de configuration n'est disponible. Le préfixe IPv4 169.254/16 est enregistré à cette fin auprès de l'IANA. L'allocation des adresses IPv6 de liaison locale est décrite dans la [RFC2462] "Autoconfiguration d'adresse IPv6 sans état".

La communication de liaison locale en utilisant des adresses IPv4 de liaison locale ne convient que pour la communication avec d'autres appareils connectés à la même liaison physique (ou logique). La communication de liaison locale utilisant les adresses IPv4 de liaison locale ne convient pas pour une communication avec des appareils non directement connectés à la même liaison physique (ou logique).

Microsoft Windows 98 (et ultérieur) et Mac OS 8.5 (et ultérieur) prennent déjà en charge cette capacité. Le présent document normalise cet usage, prescrit des règles sur la façon dont les adresses IPv4 de liaison locale doivent être traitées par les hôtes et routeurs. En particulier, il décrit comment les routeurs doivent se comporter à réception de paquets qui ont des adresses IPv4 de liaison locale dans l'adresse de source ou de destination. Par rapport aux hôtes, il discute de la revendication et de la défense des adresses, de la maintenance des adresses IPv4 de liaison locale et acheminables sur la même interface, et les questions de multi rattachement.

1.1 Exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119] "Mots clés à utiliser dans les RFC ...".

1.2 Terminologie

Le présent document décrit l'adressage de liaison locale pour la communication IPv4 entre deux hôtes sur une seule liaison. Un ensemble d'hôtes est considéré comme étant "sur la même liaison" si :

- pour tout hôte A de cet ensemble qui envoie un paquet à tout autre hôte B de cet ensemble, en utilisant l'envoi individuel, la diffusion groupée, ou la diffusion, la charge utile de couche liaison entière 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 liaison peut être modifié, comme dans l'acheminement de source par anneau à jetons *(Token Ring Source Routing)* [802.5], mais pas la charge utile de couche 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 diminue le TTL ou modifie autrement l'en-tête IP.

Le présent document utilise le terme "adresse acheminable" pour se référer à toute adresse IPv4 en envoi individuel valide en dehors du préfixe 169.254/16 qui peut être transmise via des routeurs. Cela inclut toutes les adresses IP mondiales et les adresses privées telles que des réseaux 10/8 [RFC1918], mais pas des adresses de rebouclage telles que 127.0.0.1.

Partout où le présent document utilise le terme "hôte" pour décrire l'utilisation des adresses IPv4 de liaison locale, le texte s'applique également aux routeurs lorsque ils sont la source ou la destination prévue des paquets qui contiennent des adresses IPv4 de liaison locale de source ou de destination.

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

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 de l'envoyeur DOIT contenir l'adresse du matériel de l'interface qui envoie le paquet. Le champ 'adresse de matériel de l'envoyeur' est ignoré et DEVRAIT être réglé tout à zéro. Le champ 'adresse IP cible' DOIT être réglé à l'adresse à sonder. 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 décrit ci-dessus, excepté que les champs d'envoyeur et d'adresse IP cible contiennent l'adresse IP annoncée.

Les constantes sont présentées en majuscules. Leurs valeurs sont données à la Section 9.

1.3 Applicabilité

La présente spécification s'applique à tous les réseaux de zone locale (LAN, *Local Area Network*) IEEE 802 [802], y compris Ethernet [802.3], anneau à jetons [802.5] et LAN sans fils 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, ont une latence d'aller-retour d'au plus une seconde, et prennent en charge ARP [RFC0826]. Partout où le présent document utilise le terme "IEEE 802", le texte s'applique également à toutes ces 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 supérieure à la seconde peuvent devoir spécifier des valeurs différentes pour les paramètres suivants :

(a) le nombre et l'intervalle entre les sondes ARP, voir PROBE_NUM, PROBE_MIN, PROBE_MAX définis au paragraphe 2.2.1.

(b) le nombre et l'intervalle entre les annonces ARP, voir ANNOUNCE_NUM et ANNOUNCE_INTERVAL définis au paragraphe 2.4.

(c) le débit maximum auquel les revendications d'adresse peuvent être tentées, voir RATE_LIMIT_INTERVAL et MAX_CONFLICTS définis au paragraphe 2.2.1.

(d) l'intervalle de temps entre les ARP en conflit en dessous duquel un hôte DOIT reconfigurer au lieu de tenter de défendre son adresse, voir DEFEND_INTERVAL défini au paragraphe 2.5.

Les technologies de couche 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, l'application de mécanismes de revendication et de défense à de tels réseaux sort du domaine d'application du présent document.

La présente spécification est destinée à être utilisée avec de petits réseaux ad hoc - une seule liaison contenant seulement quelques hôtes. Bien que les 65024 adresses IPv4 de liaison locale soient disponibles en principe, tenter d'utiliser toutes ces

adresses sur une seule liaison résulterait en une forte probabilité de conflits d'adresses, exigeant d'un hôte qu'il passe un temps conséquent à trouver une adresse disponible.

Les opérateurs de réseaux avec plus de 1300 hôtes sur une seule liaison peuvent vouloir envisager de diviser cette unique liaison en deux sous réseaux ou plus. Un hôte qui se connecte à une liaison qui a déjà 1300 hôtes, qui choisit au hasard une adresse de liaison locale IPv4 a 98 % de chances de choisir une adresse de liaison locale IPv4 inutilisée au premier essai. Un hôte a 99,96 % de chances de choisir une adresse de liaison locale IPv4 en deux essais. La probabilité qu'il doive faire plus de dix essais est d'environ 1 sur 10^17.

1.4 Considérations sur le protocole de couche application

Les adresses IPv4 de liaison locale et leur configuration dynamique ont de profondes implications sur les applications qui les utilisent. Ceci est discuté à la Section 6. De nombreuses applications supposent fondamentalement que les adresses des homologues de communication sont acheminables, relativement stables et uniques. Cette hypothèse ne tient plus avec les adresses IPv4 de liaison locale, ou un mélange d'adresses de liaison locale et d'adresses IPv4 acheminables.

Donc, alors que de nombreuses applications vont fonctionner correctement avec des adresses IPv4 de liaison locale, ou un mélange d'adresses IPv4 de liaison locale et d'adresses IPv4 acheminables, d'autres ne peuvent faire cela qu'après une modification, ou vont posséder des capacités réduites ou partielles.

Dans certains cas, il peut être infaisable de modifier l'application pour qu'elle fonctionne dans de telles conditions.

Les adresses IPv4 de liaison locale devraient donc n'être utilisées que lorsque des adresses stables, acheminables, ne sont pas disponibles (comme sur des réseaux ad hoc ou isolés) ou dans des situations contrôlées où ces limitations et leur impact sur les applications sont compris et acceptés. Le présent document ne recommande pas que les adresses IPv4 de liaison locale et les adresses acheminables soient configurées simultanément sur la même interface.

L'utilisation des adresses IPv4 de liaison locale dans une communication hors liaison va vraisemblablement causer des échecs d'application. Cela peut survenir au sein de toute application qui inclut des adresses incorporées, si une adresse IPv4 de liaison locale est incorporée lors d'une communication avec un hôte qui n'est pas sur la liaison. Des exemples d'applications qui incorporent des adresses sont IPsec, Kerberos 4/5, FTP, RSVP, SMTP, SIP, X-Windows/Xterm/Telnet, Real Audio, H.323, et SNMP [RFC3027].

Pour empêcher l'utilisation des adresses IPv4 de liaison locale dans la communication hors liaison, les mesures de précaution suivantes sont conseillées :

a. Les adresses IPv4 de liaison locale NE DOIVENT PAS être configurées dans le DNS. La transposition des adresses IPv4 en noms d'hôte est conventionnellement faite en produisant des interrogations au DNS sur des noms de la forme "x.x.x.x.in-addr.arpa". Lorsque c'est utilisé pour des adresses de liaison locale, qui n'ont de signification que sur la liaison locale, il est inapproprié d'envoyer de telles interrogations au DNS au delà de la liaison locale. Les clients DNS NE DOIVENT PAS envoyer d'interrogations DNS pour des noms qui entrent dans le domaine "254.169.in-addr.arpa.". Les serveurs de noms récurrents du DNS qui reçoivent des interrogations provenant de clients non conformes pour des noms dans le domaine "254.169.in-addr.arpa." DOIVENT par défaut retourner le RCODE 3, affirmation d'autorité qu'un tel nom n'existe pas dans le système des noms de domaine.

b. Les noms qui se résolvent en adresses acheminables devraient être utilisés dans les applications chaque fois qu'ils sont disponibles. Les noms qui ne peuvent se résoudre que sur la liaison locale (comme par l'utilisation de protocoles comme la résolution de nom de diffusion groupée sur liaison locale [RFC4795]) NE DOIVENT PAS être utilisés dans la communication hors liaison. Les adresses IPv4 et les noms qui ne peuvent être résolus que sur la liaison locale NE DEVRAIENT PAS être transmis au delà de la liaison locale. Les adresses IPv4 de liaison locale DEVRAIENT être envoyées seulement lorsque une adresse de liaison locale est utilisée comme adresse de source et/ou destination. Ce fort conseil devrait dissuader les adresses et noms de portée limitée de quitter le contexte dans lequel elles/ils s'appliquent.

c. Si des noms résolubles en adresses acheminables mondialement ne sont pas disponibles, mais si des adresses mondialement acheminables le sont, elles devraient être utilisées à la place des adresses IPv4 de liaison locale.

1.5 Questions d'autoconfiguration

Les mises en œuvre de l'autoconfiguration d'adresse IPv4 de liaison locale DOIVENT s'attendre à des conflits d'adresses, et DOIVENT être prêts à les traiter en douceur par le choix automatique d'une nouvelle adresse chaque fois qu'est détecté un conflit, comme décrit à la Section 2. Cette exigence de détection et de traitement des conflits d'adresse s'applique durant toute la période où un hôte utilise une adresse de liaison locale IPv4 de 169.254/16, et pas seulement durant la

configuration initiale d'interface. Par exemple, les conflits d'adresse peuvent survenir bien après qu'un hôte a achevé l'amorçage si deux réseau précédemment séparés sont joints, comme décrit à la Section 4.

1.6 Interdiction d’autres utilisations

Noter que les adresses dans le préfixe 169.254/16 NE DEVRAIENT PAS être configurées manuellement ou par un serveur DHCP. La configuration manuelle ou DHCP peut causer l'utilisation par un hôte d'une adresse dans le préfixe 169.254/16 sans suivre les règles particulières concernant la détection de dupliqués et la configuration automatique qui relèvent de ces adresses dans ce préfixe. Bien que la spécification DHCP [RFC2131] indique qu'un client DHCP DEVRAIT sonder une adresse nouvellement reçue avec ARP, ceci n'est pas obligatoire. De même, bien que la spécification DHCP recommande qu'un serveur DHCP DEVRAIT sonder une adresse en utilisant une demande d'écho ICMP avant de l'allouer, ceci n'est pas obligatoire, et même si le serveur le fait, les adresses IPv4 de liaison locale ne sont pas acheminables, de sorte qu'un serveur DHCP non directement connecté à une liaison ne peut pas détecter si un hôte sur cette liaison utilise déjà l'adresse IPv4 de liaison locale désirée.

Les administrateurs qui souhaitent configurer leurs propres adresses locales (en utilisant la configuration manuelle, un serveur DHCP, ou tout autre mécanisme non décrit dans le présent document) devraient utiliser un des préfixes d'adresse privée existants [RFC1918], et non le préfixe 169.254/16.

1.7 Interfaces multiples

Des considérations supplémentaires s'appliquent aux hôtes qui prennent en charge plus d'une interface active et où une ou plusieurs de ces interfaces acceptent la configuration d'adresse IPv4 de liaison locale. Ces considérations sont discutées à la Section 3.

1.8 Communication avec des adresses acheminables

Il y a des cas où des appareils qui ont une adresse de liaison locale configurée ont besoin de communiquer avec un appareil qui a une adresse acheminable configurée sur la même liaison physique, et vice versa. Les règles du paragraphe 2.6 permettent cette communication.

Cela permet, par exemple, qu'un ordinateur portable avec seulement une adresse acheminable pour communiquer avec les serveurs de la Toile mondiale utilise son adresse acheminable mondialement tout en imprimant en même temps ces pages de la Toile sur une imprimante locale qui a seulement une adresse IPv4 de liaison locale.

1.9 Quand configurer une adresse IPv4 de liaison locale

Avoir des adresses de plusieurs portées différentes allouées à une interface, sans moyen adéquat de déterminer dans quelles circonstances chaque adresse devrait être utilisée, conduit à de la complexité pour les applications et à la confusion des utilisateurs. Un hôte qui a une adresse sur une liaison peut communiquer avec tous les autres appareils sur cette liaison, que ces appareils utilisent des adresses de liaison locale ou des adresses acheminables. Pour ces raisons, un hôte NE DEVRAIT PAS avoir à la fois une adresse acheminable et une adresse de liaison locale IPv4 en fonctionnement configurées sur la même interface. Le terme "adresse en fonctionnement" est utilisé pour signifier une adresse qui fonctionne effectivement pour la communication dans le contexte de réseau actuel (voir ci-dessous). Lorsque une adresse acheminable en fonctionnement est disponible sur une interface, l'hôte NE DEVRAIT PAS allouer aussi une adresse IPv4 de liaison locale sur cette interface. Cependant, durant la transition (dans l'une ou l'autre direction) entre l'utilisation d'une adresse acheminable et une adresse IPv4 de liaison locale toutes deux PEUVENT être en service à la fois sous réserve des règles suivantes :

1. L'allocation d'une adresse IPv4 de liaison locale sur une interface se fonde seulement sur l'état de l'interface, et est indépendante de tous les autres protocoles tels que DHCP. Un hôte NE DOIT PAS altérer son comportement et utiliser d'autres protocoles comme DHCP parce que l'hôte a alloué une adresse IPv4 de liaison locale à une interface.

2. Si un hôte trouve qu'une interface qui était précédemment configurée avec une adresse IPv4 de liaison locale a maintenant une adresse de fonctionnement acheminable disponible, l'hôte DOIT utiliser l'adresse acheminable lorsque il initie une nouvelle communication, et DOIT cesser d'annoncer la disponibilité de l'adresse IPv4 de liaison locale par tout mécanisme par lequel cette adresse a été portée à la connaissance des autres. L'hôte DEVRAIT continuer d'utiliser l'adresse IPv4 de liaison locale pour les communications déjà en cours, et PEUT continuer d'accepter de nouvelles communications adressées à l'adresse IPv4 de liaison locale. Les moyens par lesquels une adresse de fonctionnement acheminable pourrait devenir disponible sur une interface incluent :
   * la configuration manuelle

   * l'allocation d'adresse par DHCP
   * l'itinérance de l'hôte sur un réseau sur lequel une adresse allouée antérieurement devient fonctionnelle.

3. Si un hôte trouve qu'une interface n'a plus d'adresse de fonctionnement acheminable disponible, il PEUT identifier une adresse IPv4 de liaison locale utilisable (comme décrit à la Section 2) et allouer cette adresse à l'interface. Les moyens par lesquels une adresse de fonctionnement acheminable pourrait cesser d'être disponible sur une interface incluent :
   * le retrait de l'adresse de l'interface par configuration manuelle;
   * l'expiration du prêt de l'adresse allouée au moyen de DHCP,
   * l'itinérance de l'hôte sur un nouveau réseau sur lequel l'adresse n'est plus fonctionnelle.

La détermination par le système qu'une adresse est "fonctionnelle" n'est pas tranchée de façon claire et de nombreux changements dans le contexte du système (par exemple, des changements de routeur) peuvent affecter la fonctionnalité d'une adresse. En particulier l'itinérance d'un hôte d'un réseau à l'autre va vraisemblablement – mais pas de façon certaine – changer la fonctionnalité d'une adresse configurée mais la détection d'un tel changement n'est pas toujours triviale.

"Détection des rattachements au réseau (DNA) dans IPv4" [RFC4436] donne une discussion plus approfondie de l'allocation d'adresse et de la détermination de la fonctionnalité.

2. Sélection d'adresse, défense et livraison

La section suivante explique l'algorithme de choix d'adresse IPv4 de liaison locale, comment sont défendues les adresses IPv4 de liaison locale, et comment sont livrés les paquets IPv4 avec des adresses IPv4 de liaison locale.

Les hôtes des systèmes d'exploitation Windows et Mac qui mettent déjà en œuvre l'auto configuration d'adresse IPv4 de liaison locale sont compatibles avec les règles présentées dans cette section. Cependant, si un problème d'interopérabilité était découvert, le présent document, et aucune mise en œuvre antérieure, définît la norme.

2.1 Choix d'une adresse de liaison locale

Lorsque un hôte souhaite configurer une adresse IPv4 de liaison locale, il choisit une adresse en utilisant un générateur de nombre pseudo aléatoire avec une distribution uniforme dans la gamme de 169.254.1.0 à 169.254.254.255 inclus.

Le préfixe IPv4 169.254/16 est enregistré auprès de l'IANA à cette fin. Les 256 premières adresses et les dernières 256 adresses dans le préfixe 169.254/16 sont réservées pour utilisation future et NE DOIVENT PAS être choisies par un hôte qui utilise ce mécanisme de configuration dynamique.

L'algorithme de génération de nombre pseudo aléatoire DOIT être choisi de telle sorte que des hôtes différents ne génèrent pas la même séquence de nombres. Si l'hôte a accès à des informations persistantes qui sont différentes pour chaque hôte, comme son adresse MAC IEEE 802, le générateur de nombres pseudo aléatoires DEVRAIT alors être alimenté en utilisant une valeur dérivée de ces informations. Cela signifie que même sans utiliser d'autre mémorisation persistante, un hôte va normalement choisir la même adresse IPv4 de liaison locale chaque fois qu'il est amorcé, ce qui peut être pratique pour le débogage et d'autres raisons opérationnelles. Alimenter le générateur de nombres pseudo aléatoires en utilisant l'horloge en temps réel ou toutes autres informations qui sont (ou peuvent être) identiques dans chaque hôte N'EST PAS convenable pour cela, parce qu'un groupe d'hôtes qui sont tous mis sous tension en même temps vont alors tous générer la même séquence, d'où résultera une série sans fin de conflits lorsque les hôtes se déplacent en cœur à travers exactement la même séquence pseudo aléatoire, en conflit sur chaque adresse qu'ils sondent.

Les hôtes qui sont équipés d'une mémorisation persistante PEUVENT, pour chaque interface, enregistrer l'adresse IPv4 qu'ils ont choisie. À l'amorçage, les hôtes qui ont une adresse précédemment enregistrée DEVRAIENT utiliser cette adresse comme premier candidat lors du sondage. Cela augmente la stabilité des adresses. Par exemple, si un groupe d'hôtes est éteint la nuit, alors lorsque ils sont mis sous tension le matin suivant, ils vont reprendre en utilisant les mêmes adresses, au lieu de prendre des adresses différentes et d'avoir éventuellement à résoudre les conflits qui surviennent.

2.2 Revendication d'une adresse de liaison locale

Après qu'il a choisi une adresse IPv4 de liaison locale, un hôte DOIT essayer de voir si l'adresse IPv4 de liaison locale est déjà utilisée avant de commencer à l'utiliser. Lorsque une interface réseau passe d'un état inactif à l'état actif, l'hôte ne sait pas de quelles adresses IPv4 de liaison locale il peut actuellement se servir sur cette liaison, car le point de rattachement peut avoir changé ou l'interface réseau peut avoir été inactive lorsque un conflit d'adresse s'est produit.

Si l'hôte devait immédiatement commencer à utiliser une adresse IPv4 de liaison locale qui est déjà utilisée par un autre hôte, cela perturberait cet autre hôte. Comme il est possible que l'hôte ait changé son point de rattachement, une adresse acheminable peut être obtenue sur le nouveau réseau, et donc on ne peut pas supposer qu'une adresse IPv4 de liaison locale est préférable.

Avant d'utiliser l'adresse IPv4 de liaison locale (par exemple, en l'utilisant comme adresse de source dans un paquet IPv4, ou comme adresse d'envoyeur IPv4 dans un paquet ARP) un hôte DOIT effectuer l'essai décrit ci-dessous pour mieux s'assurer que l'utilisation de cette adresse IPv4 de liaison locale ne va pas causer de perturbation.

Des exemples d'événements qui impliquent une interface qui devient active incluent :
Amorçage/démarrage
Réveil de sommeil (si l'interface réseau était inactive durant le sommeil)
Activation d'une interface réseau précédemment inactive
Changement d'état de liaison d'un matériel IEEE 802 (approprié pour le type de support et les mécanismes de sécurité qui s'appliquent) indique qu'une interface est devenue active.
Association à une station de base sans fil ou à un réseau ad hoc.

Un hôte NE DOIT PAS effectuer cette vérification périodiquement. Ce serait un gaspillage de la bande passante du réseau, et c'est inutile du fait de la capacité des hôtes de découvrir passivement les conflits, comme décrit au paragraphe 2.5.

2.2.1 Détails de la vérification

Sur une couche de liaison comme IEEE 802 qui prend en charge ARP, la détection de conflit se fait en utilisant des sondes ARP. Sur les technologies de couche de liaison qui ne prennent pas en charge ARP, d'autres techniques peuvent être disponibles pour déterminer si une adresse IPv4 particulière est actuellement utilisée. Cependant, l'application des mécanismes de revendication et défense à de tels réseaux sort du domaine d'application du présent document.

Un hôte sonde pour voir si une adresse est déjà utilisé 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 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 révèlerait être déjà utilisée par un autre hôte. Le champ 'adresse du matériel cible' est ignorée et DEVRAIT être réglé toute 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 à zéro est appelée une "sonde ARP".

Lorsque il est prêt à sonder, 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 les paquets de sonde PROBE_NUM, chacun de ces paquets sonde espacés aléatoirement, séparés de PROBE_MIN à PROBE_MAX secondes. Si durant cette période, du commencement du processus de sondage jusqu'à ANNOUNCE_WAIT secondes après l'envoi du dernier paquet sonde, l'hôte reçoit tout paquet ARP (demande *ou* réponse) sur l'interface où le sondage est effectuée où 'l'adresse IP d'envoyeur' du paquet est l'adresse sondée, puis l'hôte DOIT traiter cette adresse comme étant utilisée par un autre hôte, et DOIT choisir une nouvelle adresse pseudo aléatoire et répéter le processus. De plus, si durant cette période, l'hôte reçoit une sonde ARP où 'l'adresse IP cible' du paquet est l'adresse qu'il sonde, et si l' adresse de matériel envoyeur du paquet n'est pas l'adresse de matériel de l'interface que l'hôte tente de configurer, l'hôte DOIT alors traiter cela comme un conflit d'adresse et choisir une nouvelle adresse comme ci-dessus. Cela peut se produire si deux (ou plus) hôtes tentent de configurer la même adresse IPv4 de liaison locale au même moment.

Un hôte devrait tenir un compteur du nombre de conflits d'adresses qu'il a rencontré dans le processus d'essai d'acquisition d'une adresse, et si le nombre de conflits excède MAX_CONFLICTS, l'hôte DOIT alors limiter le taux d'envoi de sondes pour les nouvelles adresses à pas plus d'une nouvelle adresse par RATE_LIMIT_INTERVAL. Ceci est pour empêcher une tempête d'ARP catastrophique dans les cas d'échecs pathologiques, comme celui d'un hôte pirate qui répond à toutes les sondes ARP, causant des boucles infinies pour les hôtes légitimes qui tentent de choisir une adresse utilisable.

Si, ANNOUNCE_WAIT secondes après la transmission de la dernière sonde ARP, aucune réponse ARP de conflit ou aucune sonde ARP n'a été reçue, l'hôte a alors revendiqué avec succès l'adresse IPv4 de liaison locale désirée.

2.3 Temporisations plus courtes

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

2.4 Annonce d'une adresse

Ayant sondé pour déterminer une unique adresse à utiliser, l'hôte DOIT alors annoncer sa revendication d'adresse en diffusant des annonces ARP ANNOUNCE_NUM, espacées chacune de ANNOUNCE_INTERVAL secondes. Une annonce ARP est identique à la sonde ARP décrite ci-dessus, sauf que maintenant les adresses IP d'envoyeur et de cible sont toutes deux réglées à l'adresse IPv4 nouvellement choisie de 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 d'un autre hôte qui pourrait avoir antérieurement utilisé la même adresse.

2.5 Détection de conflit et défense

La détection de conflit d'adresses n'est pas limitée à la phase du choix d'adresse, lorsque un hôte envoie des sondes ARP. La détection de conflit d'adresse est un processus permanent qui s'effectue tant qu'un hôte utilise une adresse IPv4 de liaison locale. À tout moment, si un hôte reçoit an paquet ARP (demande *ou* réponse) sur une interface où l'adresse IP d'envoyeur est l'adresse IP que l'hôte a configuré pour cette interface, mais si l'adresse de matériel envoyeur ne correspond pas à l'adresse de matériel de cette interface, c'est alors un paquet ARP de conflit, indiquant un conflit d'adresse.

Un hôte DOIT répondre à un paquet ARP de conflit comme décrit en (a) ou en (b) :

(a) À réception d'un paquet ARP de conflit, un hôte PEUT choisir de configurer immédiatement une nouvelle adresse IPv4 de liaison locale comme décrit ci-dessus ou

(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 de conflit dans les dernières DEFEND_INTERVAL secondes, il PEUT alors choisir de tenter de défendre son adresse en enregistrant l'heure à laquelle a été reçu le paquet ARP de conflit, et diffuser ensuite une seule annonce ARP, donnant ses propres adresses IP et de matériel comme adresses d'envoyeur de l'ARP. Ayant fait cela, l'hôte peut ensuite continuer à 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 enregistrée pour le précédent paquet ARP de conflit est récente, dans les DEFEND_INTERVAL secondes, l'hôte DOIT alors immédiatement cesser d'utiliser cette adresse et configurer une nouvelle adresse IPv4 de liaison locale comme décrit ci-dessus. Ceci est nécessaire pour assurer que deux hôtes ne sont pas entrés dans une boucle sans fin où chacun essaye de défendre la même adresse.

Un hôte DOIT répondre aux paquets ARP de conflit comme décrit soit en (a) soit en (b) ci-dessus. Un hôte NE DOIT PAS ignorer les paquets ARP de conflit.

Une reconfiguration d'adresse forcée peut être perturbatrice, causant la rupture des connexions TCP. Cependant, on suppose que de telles perturbations seront rares, et si une duplication d'adresse imprévue se produit, l'interruption de la communication est inévitable, sans considération de la façon dont les adresses ont été allouées. Il n'est pas possible que deux hôtes différents qui utilisent 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 rétablir toute connexion existante en utilisant cette adresse. Cela diminue certaines menaces pour la sécurité posées par la reconfiguration d'adresse, comme exposé à la Section 5.

Configurer immédiatement une nouvelle adresse aussitôt que le conflit est détecté est la meilleure façon 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 soit capable de conserver son adresse.

Tous les paquets ARP (*réponse* comme demande) qui contiennent une 'adresse IP d'envoyeur' de liaison locale DOIVENT être envoyés en utilisant la diffusion de couche de liaison au lieu de l'envoi individuel de couche de liaison. Cela aide la détection en temps utile des adresses dupliquées. Un exemple illustrant comment cela aide est donné à la Section 4.

2.6 Usage de l'adresse et règles de transmission

Un hôte qui met en œuvre la présente spécification doit se conformer à des règles supplémentaires, qu'il ait ou non une interface configurée avec une adresse IPv4 de liaison locale.

2.6.1 Usage de l'adresse de source

Comme chaque interface sur un hôte peut avoir une adresse IPv4 de liaison locale en plus de zéro, une ou plusieurs autres adresses configurées par d'autres moyens (par exemple, manuellement ou via un serveur DHCP) un hôte peut devoir faire un choix sur l'adresse de source à utiliser quand il envoie un paquet ou initie une connexion TCP.

Lorsque une adresse IPv4 de liaison locale et une adresse acheminable sont toutes deux disponibles sur la même interface, l'adresse acheminable devrait être préférée comme adresse de source pour les nouvelles communications, mais les paquets envoyés de ou à l'adresse IPv4 de liaison locale sont quand même livrés comme prévu. L'adresse IPv4 de liaison locale peut continuer d'être utilisée comme adresse de source dans les communications où le passage à une adresse préférée causerait l'échec des communications à cause des exigences d'un protocole de couche supérieure (par exemple, une connexion TCP existante). Voir plus de détails au paragraphe 1.7.

Un hôte multi rattachements a besoin de choisir une interface de sortie que la destination soit ou non une adresse IPv4 de liaison locale. Les détails de ce processus sortent du domaine d'application de la présente spécification. Après le choix d'une interface, l'hôte multi rattachements devrait envoyer les paquets qui impliquent des adresses IPv4 de liaison locale comme spécifié dans le présent document, comme si l'interface choisie était la seule interface de l'hôte. Voir à la Section 3 plus d'explications sur les hôtes multi rattachements.

2.6.2 Règles de transmission

Quelle que soit l'interface utilisée, si l'adresse de destination est dans le préfixe 169.254/16 (à l'exclusion de l'adresse 169.254.255.255, qui est l'adresse de diffusion pour le préfixe de liaison locale) l'envoyeur DOIT consulter ARP pour l'adresse de destination et ensuite envoyer son paquet directement à la destination sur la même liaison physique. Ceci DOIT être fait que l'interface soit configurée avec une adresse IPv4 de liaison locale ou une adresse acheminable.

Dans de nombreuses piles de réseau, réaliser cette fonctionnalité peut être simplement d'ajouter une entrée de tableau d'acheminement qui indique que 169.254/16 est directement accessible sur la liaison locale. Cette approche ne va pas fonctionner pour les routeurs ou des hôtes multi rattachements. Voir à la Section 3 plus d'éléments sur les hôtes multi rattachements.

L'hôte NE DOIT PAS envoyer de paquet avec une adresse IPv4 de liaison locale de destination à un routeur pour transmission.

Si l'adresse de destination est une adresse d'envoi individuel en dehors du préfixe 169.254/16, l'hôte DEVRAIT alors utiliser une adresse de source IPv4 acheminable appropriée, si il peut. Si pour une raison quelconque l'hôte choisit d'envoyer le paquet avec une adresse de source IPv4 de liaison locale (par exemple, aucune adresse acheminable n'est disponible sur l'interface choisie) il DOIT alors consulter ARP pour l'adresse de destination puis envoyer son paquet, avec une adresse de source IPv4 de liaison locale et une adresse de destination IPv4 acheminable, directement à sa destination sur la même liaison physique. L'hôte NE DOIT PAS envoyer le paquet à un routeur pour transmission.

Dans le cas d'un appareil avec une seule interface et seulement une adresse IPv4 de liaison locale, cette exigence peut être paraphrasée par "ARP pour tout".

Dans de nombreuses piles de réseau, réaliser ce comportement de "ARP pour tout" peut être simplement de n'avoir pas de routeur IP principal configuré, en ayant l'adresse de routeur principal IP configurée à 0.0.0.0, ou en ayant l'adresse IP du routeur principal réglée à la même adresse IPv4 de liaison locale de l'hôte. Le comportement suggéré dans les hôtes multi rattachements est décrit à la Section 3.

2.7 Les paquets de liaison locale ne sont pas transmis

Un réglage par défaut raisonnable pour les applications qui envoient à partir d'une adresse IPv4 de liaison locale est de mettre explicitement le TTL IPv4 à 1. Ceci n'est pas approprié dans tous les cas car certaines applications peuvent exiger que le TTL IPv4 soit réglé à d'autres valeurs.

Un paquet IPv4 dont l'adresse de source et/ou de destination est le préfixe 169.254/16 NE DOIT PAS être envoyé pour transmission à un routeur, et tout appareil réseau qui reçoit un tel paquet DOIT NE PAS le transmettre, sans considération du TTL dans l'en-tête IPv4. De même, un routeur ou autre hôte NE DOIT PAS répondre sans discrimination à toutes les demandes ARP pour des adresses dans le préfixe 169.254/16. Un routeur peut, bien sûr, répondre aux demandes ARP pour une ou plusieurs adresses IPv4 de liaison locale qu'il a légitimement revendiquées pour son propre usage conformément au protocole de revendication et défense décrit dans le présent document.

Cette restriction s'applique aussi aux paquets de diffusion groupée. Les paquets IPv4 avec une adresse de source de liaison locale NE DOIVENT PAS être transmis en dehors de la liaison locale même si ils ont une adresse de destination de diffusion groupée.

2.8 Les paquets de liaison locale sont locaux

La règle de non transmission signifie que les hôtes peuvent supposer que toutes les adresses de destination 169.254/16 sont "sur la liaison" et directement accessibles. Le préfixe d'adresse 169.254/16 NE DOIT PAS être mis en sous réseaux. La présente spécification utilise la détection de conflit d'adresse fondée sur ARP, qui fonctionne par diffusion sur le sous réseau local. Comme de telles diffusions ne sont pas transmises, si le sous réseautage était permis, les conflits d'adresses pourraient alors rester indétectés.

Cela ne signifie pas qu'il est interdit aux appareils de liaison locale de faire aucune communication en dehors de la liaison locale. Les hôtes IP qui mettent en œuvre les deux adresses IPv4 de liaison locale et l'acheminable conventionnelle peuvent quand même utiliser leurs adresses acheminables sans restriction comme ils le font aujourd'hui.

2.9 Considérations sur le protocole de couche supérieure

Des considérations similaires s'appliquent aux couches au-dessus de IP.

Par exemple, les concepteurs de pages de la Toile (y compris celles qui sont générées automatiquement) NE DEVRAIENT PAS inclure de liens incorporant des adresses IPv4 de liaison locale si ces pages sont visibles à partir d'hôtes qui sont en dehors de la liaison locale où les adresses sont valides.

Comme les adresses IPv4 de liaison locale peuvent changer à tout moment et avoir une portée limitée, les adresses IPv4 de liaison locale NE DOIVENT PAS être mémorisées dans le DNS.

2.10 Problèmes de confidentialité

Une autre raison pour restreindre la portée des adresses IPv4 de liaison locale à l'extérieur de la liaison locale est le souci de confidentialité. Si les adresses IPv4 de liaison locale sont déduites d'un hachage de l'adresse MAC, on peut avancer qu'elles pourraient être indirectement associées à un individu, et par là, utilisées pour retracer les activités de cet individu. Au sein de la liaison locale, les adresses de matériel dans les paquets sont toutes directement observables, de sorte que tant que les adresses IPv4 de liaison locale ne quittent pas la liaison locale, elles ne fournissent pas plus d'informations à un intrus que ce qui pourrait être glané par une observation directe des adresses de matériel.

2.11 Interaction avec le client DHCPv4 et les automates à états IPv4 de liaison locale

Comme exposé dans l'Appendice A, les premières mises en œuvre de liaison locale IPv4 ont modifié l'automate à état DHCP. L'expérience du terrain montre que ces modifications réduisent la fiabilité du service DHCP.

Un appareil qui met en œuvre à la fois une liaison locale IPv4 et un client DHCPv4 ne devrait pas altérer le comportement du client DHCPv4 pour s'accommoder de la configuration de liaison locale IPv4. En particulier, la configuration d'une adresse IPv4 de liaison locale, qu'un serveur DHCP réponde actuellement ou non, n'est pas une raison suffisante pour défaire la configuration d'un prêt DHCP valide, pour empêcher le client DHCP de tenter d'acquérir une nouvelle adresse IP, pour changer les temporisateurs DHC, ou pour changer le comportement de l'automate à états DHCP de quelque autre façon.

Un exposé plus complet de ce problème figure dans "Détection du rattachement réseau (DNA) dans IPv4" [RFC4436].

3. Considérations pour les interfaces multiples

Les considérations mentionnées ici s'appliquent aussi chaque fois qu'un hôte a plusieurs adresses IP, qu'il ait ou non plusieurs interfaces physiques. D'autres exemples d'interfaces multiples incluent des points d'extrémité logiques différents (tunnels, réseaux privés virtuels, etc.) et des réseaux logiques multiples sur le même support physique. Ceci est souvent appelé "multi rattachements".

Les hôtes qui ont plus d'une interface active et qui choisissent de mettre en œuvre la configuration dynamique des adresses IPv4 de liaison locale sur une ou plusieurs de ces interfaces vont devoir faire face à divers problèmes. Cette section fait la liste de ces problèmes mais ne fait rien de plus qu'indiquer comment on peut les résoudre. Au moment de la rédaction de ce document, il n'y a pas de baguette magique qui résolve ces problèmes dans tous les cas, d'une façon générale. Les mises en œuvre doivent examiner ces questions avant de mettre en œuvre le protocole spécifié dans le présent document sur un système qui peut avoir plus d'une interface active au titre de la pile TCP/IP capable de multi rattachements.

3.1 Adresses à portée limitée

Un hôte peut être rattaché à plus d'un réseau en même temps. Il serai bien qu'un seul espace d'adresses soit utilisé dans tous les réseau, mais ce n'est pas le cas. Les adresses utilisées dans un réseau, qu'il soit un réseau derrière un NAT ou une liaison sur laquelle les adresses IPv4 de liaison locale sont utilisées, ne peuvent pas être utilisées dans un autre réseau et ont le même effet.

Ce serait aussi bien si les adresses n'étaient pas exposées aux applications, mais elles le sont. La plupart des logiciels qui utilisent TCP/IP et qui attendent des messages reçoivent de n'importe quelle interface à un certain numéro d'accès, pour un certain protocole de transport. Les applications ne sont généralement au courant (et ne se soucient) que de ce qu'elles ont reçu un message. L'application connaît l'adresse de l'envoyeur auquel l'application va répondre.

Le premier problème de portée d'adresse est celui du choix de l'adresse de source. Un hôte multi rattachements a plus d'une adresse. Quelle adresse devrait être utilisée comme adresse de source lors de l'envoi à une certaine destination ? Cette question reçoit généralement sa réponse en se référant à un tableau d'acheminement, qui exprime sur quelle interface (avec quelle adresse) envoyer, et comment envoyer (doit on transmettre à un routeur, ou envoyer directement). Le choix est rendu compliqué par les adresses à portée limitée parce que la gamme d'adresses dans laquelle réside la destination peut être ambiguë. Le tableau peut n'être pas capable de donner une bonne réponse. Ce problème est lié au choix du prochain bond, qui est discuté au paragraphe 3.2.

Le second problème de l'adresse à portée limitée survient des paramètres à portée qui sortent de leur portée. Ceci est discuté à la Section 7.

Il est possible de surmonter ces problèmes. Une façon de le faire est d'exposer les informations de portée aux applications afin qu'elles sachent toujours dans quelle portée est un homologue. De cette façon, l'interface correcte pourrait être choisie, et une procédure sûre pourrait être suivie par rapport aux adresses de transmission et aux autres paramètres à portée limitée. D'autres approches sont possibles. Aucune de ces méthodes n'a été normalisée pour IPv4 ni n'est spécifiée dans le présent document. Une bonne conception d'API pourrait mitiger les problèmes, soit en exposant les portées d'adresses aux applications 'au courant des adresses à portée limitée', soit en encapsulant habilement les informations et la logique de portée afin que les applications fassent les bonnes choses sans se soucier de la limitation de portée d'adresse.

Une mise en œuvre pourrait entreprendre de résoudre ces problèmes, mais ne peut pas simplement les ignorer. Avec une expérience suffisante, on espère que des spécifications vont émerger pour explique comment surmonter les problèmes des adresses à portée limitée multi rattachements.

3.2 Adresse ambiguë

C'est un problème central pour l'accessibilité des adresses IPv4 de liaison locale de destination sur plus d'une interface. Que devrait faire un hôte lorsque il a besoin d'envoyer à la liaison locale de destination L et que L peut être résolu en utilisant ARP sur plus d'une liaison ? Même si une adresse de liaison locale ne peut se résoudre que sur une liaison à un certain moment, il n'est pas garanti qu'elle va rester non ambiguë à l'avenir. Des hôtes supplémentaires sur d'autres interfaces peuvent revendiquer aussi l'adresse L.

Une possibilité est de n'accepter ceci que dans le cas où l'application exprime spécifiquement de quelle interface envoyer.

Il n'y a pas de norme ou de solution évidente à ce problème. Les logiciels d'application existants écrits pour la suite de protocoles IPv4 sont largement incapables de traiter l'ambiguïté d'adresse. Cela n'empêche pas une mise en œuvre de trouver une solution, d'écrire des applications qui sont capables de l'utiliser, et de fournir un hôte qui peut prendre en charge la configuration dynamique des adresses IPv4 de liaison locale sur plus d'une interface. Cette solution ne va cependant presque sûrement pas être généralement applicable aux logiciels existants et être transparente pour les couches supérieures.

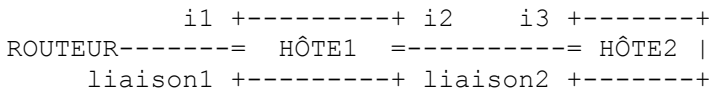
Étant donné que la pile IP doit avoir son interface sortante associée à un paquet qui doit être envoyé à une adresse de destination de liaison locale, le choix de l'interface doit être fait. L'interface sortante ne peut pas être déduite des paramètres d'en-tête du paquet comme l'adresse de source ou de destination (par exemple, en utilisant la recherche dans le tableau de transmission). Donc, l'association de l'interface sortante doit être faite explicitement par d'autre moyens. La spécification ne stipule pas ces moyens.

3.3 Interaction avec les hôtes qui ont des adresses acheminables

La présente spécification fait attention à la transition de l'utilisation des adresses IPv4 de liaison locale aux adresses acheminables (voir le paragraphe 1.5). L'intention est de permettre à un hôte avec une seule interface de d'abord prendre en charge la configuration de la liaison locale puis de passer en douceur à l'utilisation d'une adresse acheminable. Comme l'hôte qui passe à l'utilisation d'une adresse acheminable peut avoir temporairement plus d'une adresse active, les questions

d'adresse à portée limitée décrites au paragraphe 3.1 vont s'appliquer. Lorsque un hôte acquiert une adresse acheminable, il n'a pas besoin de conserver son adresse de liaison locale pour la communication avec d'autres appareils sur la liaison qui n'utilisent eux-mêmes que des adresses de liaison locale : tout hôte conforme à la présente spécification sait que, sans considération de l'adresse de source, une liaison locale IPv4 de destination doit être atteinte en transmettant directement à la destination, et non via un routeur ; il n'est pas nécessaire que cet hôte ait une adresse de source de liaison locale pour envoyer à une adresse de destination de liaison locale.

Un hôte qui a une adresse IPv4 de liaison locale peut envoyer à une destination qui n'a pas une adresse IPv4 de liaison locale. Si l'hôte n'est pas multi rattachements, la procédure est simple et non ambiguë : utiliser ARP et transmettre directement aux destinations sur la liaison est le chemin par défaut. Si l'hôte est multi rattachements, la politique d'acheminement est cependant plus complexe, en particulier si une des interfaces est configurée avec une adresse acheminable et le chemin par défaut est (sensiblement) dirigé sur un routeur accessible par cette interface. L'exemple suivant illustre ce problème et y donne une solution courante.



Dans la figure ci-dessus, HÔTE1 est connecté à liaison1 et liaison2. L'interface i1 est configurée avec une adresse acheminable, tandis que i2 est une adresse IPv4 de liaison locale. HÔTE1 a son chemin par défaut réglé à l'adresse du ROUTEUR, par i1. HÔTE1 va acheminer aux destinations dans 169.254/16 à i2, envoyant directement à la destination.

HÔTE2 a une adresse IPv4 configurée (liaison non locale) allouée à i3.

En utilisant un protocole de résolution ou de découverte de service, HÔTE1 peut découvrir l'adresse de HÔTE2. Comme l'adresse de HÔTE2 n'est pas dans 169.254/16, la politique d'acheminement de HÔTE1 va envoyer les datagrammes à HÔTE2, via i1, au ROUTEUR. Sauf si il y a un chemin de ROUTEUR à HÔTE2, les datagrammes envoyés de HÔTE1 à HÔTE2 ne vont pas l'atteindre.

Une solution à ce problème est qu'un hôte tente d'accéder à chaque hôte en local (en utilisant ARP) pour lequel il reçoit un message d'erreur ICMP injoignable (codes de message ICMP 0, 1, 6 ou 7 [RFC0792]). L'hôte essaye toutes ses liaisons rattachées à la façon d'un round robin. Cela a été mis en œuvre avec succès pour des hôtes IPv6, pour circonvenir exactement ce problème. Dans les termes de l'exemple, sur l'échec de l'HÔTE1 à joindre l'HÔTE2 via le ROUTEUR, il va tenter de transmettre à l'HÔTE2 via i2 et réussir.

Il est aussi possible de surmonter ce problème en utilisant les techniques décrites au paragraphe 3.2, ou d'autres moyens non exposés ici. La présente spécification ne fournit pas de solution standard, ni n'empêche une mise en œuvre de prendre en charge les configurations multi rattachements pourvu quelle traite les problèmes de cette section pour les applications qui seront prises en charge sur l'hôte.

3.4 Réponse auto immune non intentionnelle

Il faut faire attention si un hôte multi rattachements peut prendre en charge plus d'une interface sur la même liaison, dont toutes prennent en charge l'autoconfiguration de liaison locale IPv4. Si ces interfaces tentent d'allouer la même adresse, elles vont défendre l'hôte contre lui-même – causant l'échec de l'algorithme de revendication. La solution la plus simple à ce problème est de faire fonctionner l'algorithme indépendamment sur chaque interface configurée avec des adresses IPv4 de liaison locale.

En particulier, les paquets ARP qui paraissent revendiquer une adresse qui est allouée à une interface spécifique n'indiquent un conflit que si elles sont reçues sur cette interface et si leur adresse de matériel est sur une autre interface.

Si un hôte a deux interfaces sur la même liaison, les revendiquer et les défendre sur ces interfaces doit assurer qu'elles se terminent sur des adresses différentes juste comme si elles étaient sur des hôtes différents. Noter que certaines des façons dont un hôte peut se retrouver lui-même avec deux interfaces sur la même liaison peuvent être imprévues et non évidentes, comme lorsque un hôte a Ethernet et 802.11 sans fil, mais ces deux liaisons sont (éventuellement sans que l'utilisateur de l'hôte le sache) pontées ensemble.

4. Réparation de partitions de réseau

Les hôtes sur des liaisons réseau disjointes peuvent configurer la même adresse IPv4 de liaison locale. Si ces liaisons réseau séparées sont ultérieurement jointes ou pontées ensemble, il peut alors y avoir deux hôtes qui sont maintenant sur la même

liaison, qui essayent d'utiliser la même adresse. Lorsque l'un ou l'autre hôte tente de communiquer avec un autre hôte sur le réseau, il va à un moment diffuser un paquet ARP qui va permettre aux hôtes en question de détecter qu'il y a un conflit d'adresse.

Lorsque ces conflits d'adresses sont détectés, la reconfiguration forcée qui suit peut créer des perturbations, causant la rupture des connexions TCP. Cependant, on estime que de telles perturbations seront rares. Il devrait être assez peu courant que des réseaux soient joints alors que des hôtes sont actifs sur ces réseaux. Aussi, 65 024 adresses sont disponibles pour l'utilisation des liaisons locales IPv4, de sorte que même lorsque deux petits réseaux sont joints, les chances de conflit pour un certain hôte sont très faibles.

Lorsque on joint deux grands réseaux (définis comme des réseaux avec un nombre substantiel d'hôtes par segment) il y a plus de chances de conflit. Dans de tels réseaux, il est probable que la jonction de segments précédemment séparés va résulter en ce qu'un ou plusieurs hôtes aient besoin de changer leur adresse IPv4 de liaison locale, avec perte subséquente des connexions TCP. Dans les cas où séparation et réunion sont fréquentes, comme dans des réseau pontés à distance, cela pourrait se révéler dérangeant. Cependant, sauf si le nombre d'hôtes sur les segments joints est très important, le trafic résultant de la jonction et de la résolution du conflit d'adresse qui s'ensuit sera faible.

L'envoi des réponses ARP qui ont des adresses d'envoyeur de liaison locale IPv4 via diffusion au lieu d'envoi individuel assure que ces conflits peuvent être détectés aussitôt qu'ils deviennent des problèmes potentiels, mais pas avant. Par exemple, si deux liaisons de réseaux disjoints sont jointes, où les hôtes A et B ont été tous deux configurés avec la même adresse de liaison locale, X, ils peuvent rester dans cet état jusqu'à ce que A, B ou quelque autre hôte tente d'initier une communication. Si un autre hôte C envoie maintenant une demande ARP pour l'adresse X, et si les hôtes A et B répondent tous deux avec les réponses ARP conventionnelles en envoi individuel, l'hôte C pourrait être dans la confusion, mais A et B ne sauraient toujours pas qu'il y a un problème car ni l'un ni l'autre n'auraient vu le paquet de l'autre. L'envoi de ces réponses via diffusion permet à A et B de voir chacun les paquets ARP de conflit et de répondre en conséquence.

Noter qui l'envoi d'ARP périodiques gratuits pour tenter de détecter ces conflits plus tôt n'est pas nécessaire, gâche la bande passante du réseau, et peut en fait être nuisible. Par exemple, si les liaisons réseau n'ont été jointes que brièvement, et ont été séparée à nouveau avant qu'aucune nouvelle communication impliquant A ou B ait été initiée, le conflit temporaire aurait alors été bénin et aucune reconfiguration forcée n'aurait été requise. Déclancher une reconfiguration forcée inutile dans ce cas n'aurait servi à rien d'utile. Les hôtes NE DEVRAIENT PAS envoyer d'ARP périodiques gratuits.

5. Considérations pour la sécurité

L'utilisation d'adresses IPv4 de liaison locale peut ouvrir un hôte du réseau à de nouvelles attaques. En particulier, un hôte qui antérieurement n'avait pas d'adresse IP, et pas de pile IP en cours, n'était pas susceptible d'attaques fondées sur IP. En configurant une adresse qui fonctionne, l'hôte peut maintenant être vulnérable aux attaques fondées sur IP.

Le protocole ARP [RFC0826] n'est pas sûr. Un hôte malveillant peut envoyer des paquets ARP frauduleux sur le réseau, interférer avec le fonctionnement correct d'autres hôtes. Par exemple, il est facile pour un hôte de répondre à toutes les demandes ARP avec des réponses donnant sa propre adresse de matériel, revendiquant par là la propriété de toutes les adresses du réseau.

Note : Il y a certaines sortes de liaisons locales, comme les LAN sans fil, qui ne fournissent aucune sécurité physique. À cause de l'existence de ces liaisons, il serait très malavisé qu'une mise en œuvre suppose que lorsque un appareil ne communique qu'avec la liaison locale il peut se dispenser des précautions de sécurité normales. Manquer à mettre en œuvre les mesures de sécurité appropriées peut exposer les usagers à des risques considérables.

Un hôte qui met en œuvre la configuration de liaison locale IPv4 a une vulnérabilité supplémentaire à la reconfiguration et l'interruption sélective. Il est possible à un attaquant sur la liaison de produire des paquets ARP qui amèneraient un hôte à couper toutes ses connexions en le faisant passer à une nouvelle adresse. L'attaquant pourrait forcer l'hôte qui met en œuvre la configuration de liaison locale IPv4 à choisir certaines adresses, ou toujours l'empêcher d'achever un choix d'adresse. Cette menace est distincte de celle posée par les ARP frauduleux, décrite dans le paragraphe précédent.

Les mises en œuvre et les utilisateurs devraient aussi noter qu'un nœud qui abandonne une adresse et reconfigure, comme exigé au paragraphe 2.5, offre la possibilité qu'un autre nœud puisse facilement et avec succès capturer les connexions TCP existantes.

Les développeurs doivent savoir que l'architecture du protocole Internet s'attend à ce que chaque appareil ou hôte du réseau mette en œuvre la sécurité adéquate pour protéger les ressources auxquelles l'appareil ou hôte a accès, y compris le réseau lui-même, contre les menaces connues ou crédibles. Bien que l'utilisation des adresses IPv4 de liaison locale puisse réduire

le nombre de menaces auxquelles est exposé un appareil, les mises en œuvre d'appareils qui prennent en charge le protocole Internet ne doivent pas supposer que le réseau local d'un consommateur est libéré de tous les risques pour la sécurité.

Bien qu'il y ait de nombreuse sortes d'appareils, , ou d'environnements particuliers, pour lesquels la sécurité fournie par le réseau est adéquate pour protéger les ressources auxquelles peut accéder l'appareil, il serait trompeur de faire une déclaration générale visant à dire que l'exigence de fourniture de la sécurité est réduite pour les appareils qui utilisent des adresses IPv4 de liaison locale comme seul moyen d'accès.

Dans tous les cas, que les adresses IPv4 de liaison locale soient utilisées ou non, il est nécessaire que la mise en œuvre des appareils qui prennent en charge le protocole Internet analyse les menaces connues et crédibles auxquelles un appareil ou hôte spécifique pourrait être soumis, et dans la mesure où c'est faisable, de fournir les mécanismes de sécurité qui améliorent ou réduisent les risques associés à de telles menaces.

6. Considérations sur la programmation des applications

L'utilisation des adresses IPv4 de liaison locale autoconfigurées présente des défis supplémentaires aux auteurs d'applications et peut résulter en l'échec du logiciel d'application existant.

6.1 Changements d'adresse, échec et récupération

Les adresses IPv4 de liaison locale utilisées par une application peuvent changer avec le temps. Certains logiciels d'application vont échouer lorsque ils rencontrent un changement d'adresse. Par exemple, les connexions de client TCP existantes seront interrompues, les serveurs dont les adresses changent devront être redécouverts, les lectures et écritures bloquées vont sortir avec une condition d'erreur, et ainsi de suite.

Les fabricants qui produisent des logiciels d'application qui seront utilisés sur des mises en œuvre IP qui prennent en charge la configuration d'adresse IPv4 de liaison locale DEVRAIENT détecter et inclure les événements de changement d'adresse. Les fabricants qui produisent des mises en œuvre de IPv4 qui prennent en charge la configuration d'adresse IPv4 de liaison locale DEVRAIENT exposer les événements de changement d'adresse aux applications.

6.2 Transmission limitée des localisateurs

Les adresses IPv4 de liaison locale NE DOIVENT PAS être transmises via un protocole d'application (par exemple dans un URL) à une destination qui n'est pas sur la même liaison. Ceci est exposé au paragraphe 2.9 et à la Section 3.

Les logiciels d'application répartie existants qui transmettent les informations d'adresse peuvent échouer. Par exemple, FTP [RFC0959] (lorsque il n'utilise pas le mode passif) transmet l'adresse IP du client. Supposons qu'un client démarre et obtienne sa configuration IPv4 à un moment où il a seulement une adresse de liaison locale. Ultérieurement, l'hôte obtient une adresse IP mondiale, et le client contacte un serveur FTP en dehors de la liaison locale. Si le client FTP transmet sa vieille adresse de liaison locale au lieu de sa nouvelle adresse IP mondiale dans la commande FTP "port", le serveur FTP va alors être incapable d'ouvrir une connexion de données avec le client, et le fonctionnement de FTP va échouer.

6.3 Ambiguïté d'adresse

Les logiciels d'application qui fonctionnent sur un hôte multi rattachements qui acceptent la configuration d'adresse IPv4 de liaison locale sur plus d'une interface peuvent échouer. Cela se produit parce que le logiciel d'application suppose que une adresse IPv4 n'est pas ambiguë, et qu'il peut se référer à seulement un hôte. Les adresses IPv4 de liaison locale sont uniques seulement sur une liaison. Un hôte rattaché à plusieurs liaisons peut facilement rencontrer une situation où la même adresse est présente sur plus d'une interface, ou la première sur une interface, la dernière sur une autre ; en tous cas associée à plus d'un hôte. La plupart des logiciels existant ne sont pas préparés à cette ambiguïté. À l'avenir, des interfaces de programmation d'application pourraient être développées pour prévenir ces problèmes. La question est discutée à la Section 3.

7. Considérations sur les routeurs

Un routeur NE DOIT PAS transmettre un paquet avec une adresse IPv4 de liaison locale de source ou de destination, sans considération de la configuration du chemin par défaut du routeur ou des chemins obtenus de protocoles d'acheminement dynamiques.

Un routeur qui reçoit un paquet avec une adresse IPv4 de liaison locale de source ou de destination NE DOIT PAS transmettre le paquet. Cela empêche la transmission de paquets en retour sur le segment de réseau d'où ils sont originaires, ou à tout autre segment.

8. Considérations relatives à l'IANA

L'IANA a alloué le préfixe 169.254/16 pour l'usage décrit dans le présent document. Les 256 premières et dernières adresses dans cette gamme (169.254.0.x et 169.254.255.x) sont allouées par action de normalisation, comme défini dans "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA" (BCP 26) [RFC2434]. Aucun autre service de l'IANA n'est demandé par le présent document.

9. Constantes

Les constantes de temporisation suivantes sont utilisées dans le présent protocole ; elles ne sont pas destinées à être configurables par l'utilisateur.

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

10. Références

10.1 Références normatives

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

[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.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

10.2 Références pour information

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

[802.3] ISO/IEC 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 norme ANSI/IEEE 802.3-1996), 1996.

[802.5] ISO/IEC 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 norme ANSI/IEEE 802.5-1998), 1998.

[802.11] "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", IEEE Std. 802.11-1999, 1999.

[RFC0959] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", STD 9, octobre 1985. *(MàJ par* RFC7151)

[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*)*

[RFC2462] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", décembre 1998. (*Obsolète, voir* RFC4862) *(D.S.)*

[RFC3027] M. Holdrege, P. Srisuresh, "Complications de protocole avec le traducteur d'adresse réseau IP", janvier 2001. *(Info.)*

[RFC4436] B. Aboba et autres, "Détection des rattachements au réseau dans IPv4 (DNAv4)", mars 2006. *(P.S.)*

[RFC4795] B. Aboba et autres, "Résolution de nom de diffusion groupée sur liaison locale (LLMNR)", janvier 2007. *(Information)*

Remerciements

On souhaite remercier de leurs contributions (par ordre alphabétique) Jim Busse, Pavani Diwanji, Donald Eastlake 3rd, Robert Elz, Peter Ford, Spencer Giacalone, Josh Graessley, Brad Hards, Myron Hattig, Hugh Holbrook, Christian Huitema, Richard Johnson, Kim Yong-Woon, Mika Liljeberg, Rod Lopez, Keith Moore, Satish Mundra, Thomas Narten, Erik Nordmark, Philip Nye, Howard Ridenour, Daniel Senie, Dieter Siegmund, Valery Smyslov, et Ryan Troll.

Appendice A Mises en œuvre antérieures

A.1 Apple Mac OS 8.x et 9.x.

Le système d'exploitation Mac choisit l'adresse IP de façon pseudo aléatoire. L'adresse choisie est sauvegardée dans une mémorisation persistante pour la poursuite de l'utilisation après réamorçage, lorsque c'est possible.

Le système d'exploitation Mac envoie neuf paquets DHCP DISCOVER, avec un intervalle de deux secondes entre les paquets. Si aucune réponse n'est reçue d'une de ces demandes (18 secondes), il va s'autoconfigurer.

Si il découvre qu'une adresse choisie est utilisée, le système d'exploitation Mac va choisir une nouvelle adresse aléatoire et essayer à nouveau, à un taux limité à une tentative au plus toutes les deux secondes.

Les systèmes d'OS Mac autoconfigurés vérifient la présence d'un serveur DHCP toutes les cinq minutes. Si un serveur DHCP est trouvé mais si le système d'exploitation Mac ne réussit pas à obtenir un nouveau prêt, il conserve l'adresse IP autoconfigurée existante. Si le système d'exploitation Mac réussit à obtenir un nouveau prêt d'adresse, il élimine toutes les connexions existantes sans avertissement. Cela peut causer la perte des sessions en cours pour les utilisateurs. Une fois qu'un nouveau prêt d'adresse est obtenu, le système d'exploitation Mac ne va plus allouer d'autre connexion sur l'adresse IP autoconfigurée.

Les systèmes d'OS Mac n'envoient pas de paquets adressés à une adresse de liaison locale à la passerelle par défaut si il en est une présente ; ces adresses sont toujours résolues sur le segment local.

Les systèmes d'OS Mac envoient par défaut tous les paquets sortants en envoi individuel avec un TTL de 255. Tous les paquets en diffusion et en diffusion groupée sont aussi envoyés avec un TTL de 255 si ils ont une adresse de source dans le préfixe 169.254/16.

Le système d'exploitation Mac met en œuvre la détection du support lorsque le matériel (et le logiciel du pilote) le prend en charge. Aussitôt que la connexité réseau est détectée, un DHCP DISCOVER va être envoyé sur l'interface. Cela signifie que les systèmes vont immédiatement sortir du mode autoconfiguré aussitôt que la connexité est restaurée.

A.2 Apple Mac OS X Version 10.2

Le système d'exploitation Mac X choisit l'adresse IP de façon pseudo aléatoire. L'adresse choisie est sauvegardée en mémoire afin qu'elle puisse être réutilisée durant les tentatives successives d'autoconfiguration durant un seul amorçage du système.

L'autoconfiguration d'une adresse de liaison locale dépend des résultats du processus DHCP. DHCP envoie deux paquets, avec des temporisations de une et deux secondes. Si aucune réponse n'est reçue (au bout de trois secondes) il commence l'autoconfiguration. DHCP continue d'envoyer des paquets en parallèle pendant un total de 60 secondes.

Au début de l'autoconfiguration, il génère dix adresses IP uniques de façon aléatoire, et sonde chacune d'elles à son tour pendant deux secondes. Il arrête de sonder après avoir trouvé une adresse non utilisée, ou si la liste des adresses est épuisée.

Si DHCP ne réussit pas, il attend cinq minutes avant de recommencer. Une fois que DHCP a réussi, l'adresse de liaison locale autoconfigurée est abandonnée. Le sous réseau de liaison locale reste cependant configuré.

L'autoconfiguration n'est tentée que sur une seule interface à tout instant.

Le système d'exploitation Mac X assure que l'interface connectée qui a la plus forte priorité est associée au sous réseau de liaison locale. Les paquets adressés à une adresse de liaison locale ne sont jamais envoyés à la passerelle par défaut, s'il en est une présente. Les adresses de liaison locale sont toujours résolues sur le segment local.

Le système d'exploitation Mac X met en œuvre la détection de support lorsque le matériel et le pilote la prennent en charge. Lorsque le support réseau indique qu'il a été connecté, le processus d'autoconfiguration recommence, et tente de réutiliser l'adresse de liaison locale précédemment allouée. Lorsque le support réseau indique qu'il a été déconnecté, le système attend quatre secondes avant de déconfigurer l'adresse et le sous réseau de liaison locale. Si la connexion est restaurée avant ce moment, le processus d'autoconfiguration recommence. Si la connexion n'est pas restaurée avant ce moment, le système choisit une autre interface à autoconfigurer.

Le système d'exploitation Mac X envoie par défaut tous les paquets sortants en envoi individuel avec une durée de vie de 255. Tous les paquets en diffusion et en diffusion groupée sont aussi envoyés avec un TTL de 255 si ils ont une adresse de source dans le préfixe 169.254/16.

A.3 Microsoft Windows 98/98SE

Les systèmes Windows 98/98SE choisissent leur adresse IPv4 de liaison locale de façon pseudo aléatoire. L'algorithme de choix d'adresse se fonde sur le calcul d'un hachage sur l'adresse MAC de l'interface, de sorte qu'une large collection d'hôtes devrait obéir à une distribution de probabilité uniforme en choisissant des adresses dans l'espace d'adresses 169.254/16. Déduire l'adresse IPv4 de liaison locale initiale de l'adresse MAC de l'interface assure aussi que les réamorçages des systèmes vont obtenir la même adresse autoconfigurée, sauf si un conflit est détecté.

Dans l'état INIT, le client DHCP Windows 98/98SE envoie un total de quatre DHCP DISCOVER, avec un intervalle entre les paquets de six secondes. Lorsque aucune réponse n'est reçue après les quatre paquets (24 secondes) il va autoconfigurer une adresse.

Le compte des essais d'autoconfiguration pour les systèmes Windows 98/98SE est de 10. Après dix essais d'adresse IPv4 autoconfigurée, et ayant trouvé que toutes sont prises, l'hôte va s'amorcer sans adresse IPv4.

Les systèmes Windows 98/98SE autoconfigurés vérifient la présence d'un serveur DHCP toutes les cinq minutes. Si un serveur DHCP est trouvé mais si Windows 98 ne réussit pas à obtenir un nouveau prêt d'adresse, il conserve l'adresse IPv4 de liaison locale autoconfigurée existante. Si Windows 98/98SE réussit à obtenir un nouveau prêt, il élimine toutes les connexions existantes sans avertissement. Cela peut causer la perte des sessions en cours des utilisateurs. Une fois qu'un nouveau prêt est obtenu, Windows 98/98SE ne va plus allouer d'autre connexion en utilisant l'adresse IPv4 de liaison locale autoconfigurée .

Les systèmes Windows 98/98SE qui ont une adresse IPv4 de liaison locale n'envoient pas de paquets adressés à une adresse IPv4 de liaison locale à la passerelle par défaut si il en est une présente; ces adresses sont toujours résolues sur le segment local.

Les systèmes Windows 98/98SE envoient par défaut tous les paquets sortants en envoi individuel avec un TTL de 128. La configuration du TTL est effectuée en réglant à la valeur appropriée la clé du registre Windows du type REG_DWORD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\ Parameters\DefaultTTL. Cependant, ce TTL par défaut va s'appliquer à tous les paquets. Bien que cette facilité puisse être utilisée pour régler le TTL par défaut à 255,

elle ne peut être utilisée pour régler le TTL par défaut des paquets IPv4 de liaison locale à un (1), tout en permettant que d'autres paquets soient envoyés avec un TTL supérieur à un.

Les systèmes Windows 98/98SE ne mettent pas en œuvre la détection du support. Cela signifie que les questions de connexité du réseau (comme un câble débranché) peuvent empêcher un système de contacter le serveur DHCP, causant par là son autoconfiguration. Lorsque le problème de connectivité est réglé (comme lorsque le câble est reconnecté) la situation ne va pas se corriger immédiatement. Comme le système ne détecte pas la reconnexion, il va rester en mode autoconfiguré jusqu'à ce qu'une tentative soit faite d'atteindre le serveur DHCP.

Le serveur DHCP inclus avec le partage de connexion Internet (ICS, *Internet Connection Sharing*) de Windows 98SE (une mise en œuvre de NAT) alloue par défaut dans l'espace d'adresses privées de 192.168/16.

Cependant, il est possible de changer le préfixe d'allocation via une clé de registre, et aucune vérification n'est faite pour empêcher l'allocation dans le préfixe IPv4 de liaison locale. Lorsque il est ainsi configuré, l'ICS Windows 98SE va réécrire les paquets provenant du préfixe IPv4 de liaison locale et les transmettre au delà de la liaison locale. L'ICS Windows 98SE n'achemine pas automatiquement pour le préfixe IPv4 de liaison locale, de sorte que les hôtes qui obtiennent des adresses via DHCP ne peuvent pas communiquer avec les appareils qui sont seulement autoconfigurés.

Il existe d'autres passerelles locales qui allouent par défaut des adresses dans le préfixe IPv4 de liaison locale. Les systèmes Windows 98/98SE peuvent utiliser une adresse IPv4 de liaison locale de 169.254/16 comme adresse de source lorsque ils communiquent avec des hôtes qui ne sont pas sur la liaison locale. Windows 98/98SE ne prend pas en charge la sollicitation/annonce de routeur. Les systèmes Windows 98/98SE ne vont pas découvrir automatiquement une passerelle par défaut lorsque ils sont en mode autoconfiguré.

A.4 Windows XP, 2000, et ME

Le comportement d'autoconfiguration des systèmes Windows XP, Windows 2000, et Windows ME est identique à celui de Windows 98/98SE sauf sur les points suivants :
Détection du support
Découverte du routeur
Protocole d'informations d'adressage (RIP, *routing information protocol*) silencieux

Windows XP, 2000, et ME mettent en œuvre la détection du support. Sitôt que la connexité réseau est détectée, une DHCP REQUEST ou DHCP DISCOVER va être envoyée sur l'interface. Cela signifie que les systèmes vont immédiatement sortir du mode autoconfiguré aussitôt que la connexité est restaurée.

Windows XP, 2000, et ME prennent aussi en charge la découverte de routeur, bien qu'elle soit désactivée par défaut. Windows XP et 2000 prennent aussi en charge l'écoute RIP. Cela signifie qu'ils peuvent découvrir par inadvertance une passerelle par défaut lorsque ils sont en mode autoconfiguré.

ICS sur Windows XP/2000/ME se comporte de façon identique à celle de Windows 98SE à l'égard de l'allocation d'adresse et de la traduction d'adresse réseau (NAT) des préfixes de liaison locale.

Adresse des auteurs

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

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

Erik Guttman
Sun Microsystems
Eichhoelzelstr. 7
74915 Waibstadt Germany
téléphone : +49 7263 911 701
mél : erik@spybeam.org

Déclaration de droits de reproduction

Copyright (C) The Internet Society (2005).

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

Le présent document et les informations qui y sont contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faits au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

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