Groupe de travail Réseau	B. Carpenter
Request for Comments : 2101	J. Crowcroft
Catégorie : Information	Y. Rekhter
	IAB
Traduction Claude Brière de L'Isle	février 1997

Comportement actuel des adresses IPv4

Résumé
Le principal objet de la présente note est de préciser l'interprétation actuelle de l'espace d'adresse d'IP version 4 à 32 bits, dont la signification a changé substantiellement depuis sa définition d'origine. Une brève section sur les adresses IPv6 mentionne les principaux points de similitude et de différence avec IPv4.

Table des matières

1. Introduction

Le principal objet de cette note est de préciser l'interprétation actuelle de l'espace d'adresse IP à 32 bits, dont la signification a changé substantiellement depuis sa définition originale de 1981 dans la [RFC0791].

Cette clarification est destinée à aider les concepteurs de protocoles, les mises en œuvres de produits, les fournisseurs de service Internet, et les sites d'usagers. Elle vise à éviter sur les adresses IP des incompréhensions qui pourraient résulter des changements substantiels qui sont survenus dans les dernières années, par suite de la croissance exponentielle de l'Internet.

Une brève section sur les adresses IPv6 mentionne les principaux points de similitudes et de différence avec IPv4.

2. Terminologie

Il est bien compris que dans les réseaux informatiques, les concepts de répertoires, noms, adresses réseau, et de chemin sont distincts et doivent être analysés séparément [RFC1498]. Cependant, il est aussi nécessaire de subdiviser le concept d'adresse réseau (abrégé à partir d'ici en "adresse") en au moins deux notions, à savoir "identifiant" et "localisateur". Cela était peut-être moins bien compris lors de la rédaction de la RFC 791.

Dans le présent document, le terme "hôte" se réfère à tout système qui génère et/ou termine les paquets IPv4, et "routeur" se réfère à tout système qui transmet des paquets IPv4 d'un hôte ou routeur à un autre hôte ou routeur.

Pour les besoins de ce document, un "identifiant" est une chaîne binaire qui est utilisée durant toute la durée de vie d'une session de communication entre deux hôtes, pour identifier un des hôtes pour autant que l'autre est concerné. Un tel

identifiant est utilisé pour vérifier la source des paquets entrants comme étant vraiment l'autre extrémité de la communication concernée, par exemple dans le pseudo en-tête TCP [RFC0793] ou dans une association de sécurité IP [RFC1825]. Traditionnellement, l'adresse IPv4 de source dans chaque paquet est utilisée pour cela.

Noter que d'autres définitions de "identifiant" sont parfois utilisées ; le présent document ne discutera pas du problème général de la sémantique des identifiants de points d'extrémité.

Pour les besoins de ce document, un "localisateur" est une chaîne binaire qui est utilisée pour identifier où doit être livré un paquet particulier, c'est-à-dire, il sert à localiser l'endroit de la topologie de l'Internet où est rattaché l'hôte de destination. Traditionnellement, l'adresse IPv4 de destination dans chaque paquet est utilisée pour cela. Les protocoles d'acheminement IP interprètent les adresses IPv4 comme des localisateurs et construisent des tableaux d'acheminement sur la base des routeurs (qui ont leurs propres localisateurs) qui revendiquent la connaissance du chemin vers les localisateurs d'hôtes particuliers.

Les identifiants et les localisateurs ont tous deux des exigences d'unicité, mais ces exigences sont différentes. Les identifiants doivent être uniques par rapport à chaque ensemble d'hôtes inter communicants. Les localisateurs doivent être uniques par rapport à chaque ensemble de routeurs inter communicants (qu'on appellera un "domaine" d'acheminement). Bien que les localisateurs doivent être uniques au sein d'un domaine d'acheminement donné, cette unicité (mais pas la capacité d'acheminement) pourrait s'étendre à plus d'un domaine. Donc nous pouvons encore distinguer entre un ensemble de domaines avec des localisateurs uniques opposés à un ensemble de domaines avec des localisateurs non uniques (qui se chevauchent).

Les identifiants et les localisateurs ont tous deux des exigences de durée de vie, mais ces exigences sont différentes. Les identifiants doivent être valides pour au moins la durée de vie maximum d'une communication entre deux hôtes. Les localisateurs ne doivent être valides qu'autant que l'exigent les mécanismes d'acheminement (qui pourraient être plus courts ou plus longs que la durée de vie d'une communication).

On notera que c'est par un hasard de l'histoire que le même espace d'adresse et les mêmes champs dans l'en-tête IP (adresses de source et de destination) sont utilisés par la RFC 791 et la RFC 793 à la fois pour les identifiants et pour les localisateurs, et que dans l'Internet traditionnel un identifiant d'hôte est identique à son localisateur, tout en étant unique dans l'espace (non ambigu) et unique dans le temps (constant).

Ces conditions d'unicité ont un certain nombre de conséquences pour les hypothèses de conception de l'acheminement (l'infrastructure que les localisateurs IPv4 rendent possible) et de protocoles de transport (ceux qui dépendent de la connexité IP). L'unicité spatiale d'une adresse signifie qu'elle serve à la fois comme identifiant d'interface et comme identifiant d'un hôte, ainsi que de clé pour le tableau d'acheminement. L'unicité temporelle d'une adresse signifie qu'il n'est pas besoin que les mises en œuvre de TCP maintiennent d'état en ce qui concerne l'identité de l'extrémité distante, autre que l'adresse IP. Donc, les adresses IP pourraient être utilisées à la fois pour la sécurité IP de bout en bout et pour lier les sessions de couche supérieure.

D'une façon générale, l'utilisation des adresses IPv4 comme localisateurs a été considérée comme plus importante que leur utilisation comme identifiants, et chaque fois qu'il y a eu un conflit entre les deux utilisations, l'utilisation d'un localisateur a prévalu. C'est à dire qu'il a été considéré plus utile de livrer le paquet puis de se soucier de la façon d'identifier les points d'extrémité, que de fournir l'identité dans un paquet qui ne peut pas être livré. En d'autres termes, il y eu un travail intense sur les protocoles d'acheminement et peu de travail concret sur les autres aspects de l'utilisation de l'adresse.

3. Propriétés idéales

Quelles que soient les contraintes mentionnées ci-dessus, il est facile de voir les propriétés idéales des identifiants et des localisateurs. Les identifiants devraient être alloués à la naissance, ne jamais changer, et ne jamais être réutilisés. Les localisateurs devraient décrire la position de l'hôte dans la topologie du réseau, et devraient changer chaque fois que change la topologie.

Malheureusement, aucun de ces idéaux n'est satisfait par les adresses IPv4. Le reste de ce document est destiné à présenter une photographie de la situation réelle actuelle.

4. Survol de la situation actuelle des adresses IPv4

Il est un fait que les adresses IPv4 ne sont plus uniques au monde et n'ont plus des durées de vie infinies.

4.1 Les adresses ne sont plus des localisateurs uniques au monde

La [RFC1918] montre comment les réseaux d'entreprise, autrement dit, les intranets, peuvent si nécessaire légitimement réutiliser un sous-ensemble de l'espace d'adresses IPv4, formant plusieurs domaines d'acheminement. À la frontière entre deux (ou plus) domaines d'acheminement, on peut trouver un ensemble d'appareils qui permettent la communication entre les domaines.

À une extrémité de cet ensemble se trouve une passerelle de couche application (ALG, *Application Layer Gateway*). Un tel appareil agit comme un point de terminaison pour le flux de données de couche application, et il est visible à l'utilisateur final. Par exemple, lorsque un utilisateur final Ua dans un domaine d'acheminement A veut communiquer avec un utilisateur final Ub dans le domaine d'acheminement B, Ua doit d'abord établir explicitement la communication avec l'ALG qui interconnecte A et B, et c'est seulement via cette ALG que Ua établit la communication avec Ub. On appelle une telle passerelle une ALG "non transparente".

Une autre forme d'ALG rend la communication à travers elle transparente à l'utilisateur final. En utilisant l'exemple précédent, avec une ALG "transparente", Ua ne serait pas obligé d'établir d'abord une connexité explicite avec l'ALG, avant de commencer à communiquer avec Ub. Une telle connexité sera établie de façon transparente avec Ua, de sorte que Ua ne verra que la connexité avec Ub.

Pour être complet, on notera qu'il n'est pas nécessaire que la communication via une ALG implique des changements dans l'en-tête de réseau. Une ALG pourrait n'être utilisée qu'au début d'une session pour les besoins de l'authentification, après quoi l'ALG s'en va et la communication continue normalement.

Il est demandé (par définition) aux ALG aussi bien non transparentes que transparentes de comprendre la syntaxe et la sémantique du flux des données d'application. Les ALG sont très simples du point de vue de l'architecture de couche réseau car elles apparaissent comme des hôtes Internet dans chaque domaine, c'est à dire qu'elle agissent comme point d'origine et de terminaison pour la communication.

À l'autre extrémité du spectre se trouve un traducteur d'adresse réseau (NAT, *Network Address Translator*) [RFC1631]. Dans le contexte du présent document on définit un NAT comme un appareil qui modifie juste les en-têtes de couche réseau et transport, mais ne comprend pas la syntaxe/sémantique du flux de données de couche application (en utilisant notre terminologie, ce qui est décrit dans la RFC1631 est un appareil qui a les deux fonctionnalités de NAT et d'ALG).

Dans le cas standard d'un NAT placé entre un réseau d'entreprise qui utilise des adresses privées [RFC1918] et l'Internet public, ce NAT change l'adresse IPv4 de source dans les paquets qui vont vers l'Internet, et change l'adresse IPv4 de destination dans les paquets qui viennent de l'Internet. Lorsque un NAT est utilisé pour interconnecter les domaines d'acheminement avec des adresses qui se chevauchent , telles qu'une connexion directe entre deux intranets, le NAT peut modifier les deux adresses dans l'en-tête IP. Comme le NAT modifie la ou les adresses dans l'en-tête IP, le NAT a aussi à modifier la somme de contrôle du pseudo en-tête de transport (par exemple, TCP, UDP). Après un peu d'introspection, on pourra observer que lorsque on interconnecte des domaines d'acheminement qui ont des adresses qui se chevauchent, l'ensemble des opérations effectuées par un NAT sur l'en-tête réseau et transport forme un sous-ensemble (approprié) de l'ensemble des opérations effectuées par une ALG transparente sur la couche réseau et transport.

Par définition, un NAT ne comprend pas la syntaxe et la sémantique d'un flux de données d'application. Donc, un NAT ne peut pas prendre en charge des applications qui portent des adresses IP à la couche application (par exemple, FTP avec la commande PORT ou PASV [RFC0959]). D'un autre côté, un NAT peut prendre en charge toute application, pour autant qu'elle ne porte pas d'adresses IP à la couche application. C'est une différence avec une ALG qui ne peut prendre en charge que les applications codées dans l'ALG.

On peut en conclure que les NAT et les ALG ont tous deux leurs propres limitations, qui pourraient restreindre leur utilité. La combinaison de la fonctionnalité de NAT et d'ALG en un seul appareil pourrait être utilisée pour surmonter certaines, mais pas toutes, de ces limitations. Un tel appareil utiliserait la fonctionnalité de NAT pour les applications qui ne portent pas d'adresses IP, et s'en remettrait à la fonctionnalité d'ALG pour traiter avec les applications qui portent des adresses IP. Par exemple, un tel appareil pourrait utiliser la fonctionnalité de NAT pour traiter la connexion de données FTP, mais utiliserait la fonctionnalité d'ALG pour traiter de la connexion de contrôle FTP. Cependant, un tel appareil échouera complètement à traiter une application qui porte des adresses IP, lorsque l'appareil ne prend pas en charge l'application via la fonctionnalité d'ALG, mais la traite plutôt via la fonctionnalité de NAT.

La communication à travers des ALG ou des NAT implique des changements à l'en-tête de réseau (et en particulier aux adresses de source et de destination) et à l'en-tête de transport. Comme les en-tête d'authentification de sécurité IP (IPsec) supposent que les adresses dans l'en-tête réseau sont préservées de bout en bout, on ne voit pas bien comment on peut prendre en charge l'authentification fondée sur IPsec entre une paire d'hôtes qui communiquent à travers une ALG ou un

NAT. Comme la sécurité IP, lorsque elle est utilisée pour la confidentialité, chiffre la totalité de la couche transport de bout en bout, on ne voit pas comment une ALG ou un NAT pourrait modifier les paquets chiffrés comme elle l'exige. En d'autres termes, les ALG et les NAT sont vraisemblablement tous deux obligés de forcer une frontière entre deux domaines de sécurité IP distincts, à la fois pour l'authentification et pour la confidentialité, à moins que des améliorations spécifiques à la sécurité IP ne soient conçues à cette fin.

L'interconnexion de domaines d'acheminement via des ALG ou des NAT s'appuie sur le DNS [RFC1035]. Précisément, pour un ensemble donné de domaines d'acheminement (interconnectés) même si les adresses de couche réseau ne sont plus uniques au sein de l'ensemble, les noms de domaine pleinement qualifiés devraient être uniques dans cet ensemble. Cependant, un site qui utilise un NAT ou une ALG a probablement besoin d'avoir deux serveurs DNS, un à l'intérieur, et un à l'extérieur du NAT ou ALG, donnant des réponses différentes à des interrogations identiques. Ceci est exposé plus en détails dans la [RFC2182]. La sécurité du DNS [RFC2065] et certaines mises à jour dynamiques du DNS [RFC2136] ne seront vraisemblablement pas valides à travers une frontière de NAT/ALG, de sorte qu'on doit supposer que le serveur DNS externe acquiert au moins une partie de ses tableaux par quelque autre mécanisme.

Pour résumer, depuis la RFC 1918, nous n'avons pas réellement changé l'unicité spatiale d'une adresse, tout en reconnaissant qu'il y a plusieurs espaces. c'est à dire que chaque espace est encore un domaine d'acheminement tel qu'un intranet, éventuellement connecté à d'autres intranets, ou à l'Internet, par des NAT ou des ALG (voir l'exposé ci-dessus). L'unicité temporelle d'une adresse n'est pas changée par la RFC 1918.

4.2 Les adresses ne sont plus toutes temporellement uniques

Noter qu'aussitôt que la signification d'une adresse change quelque part dans l'espace d'adresses, elle a dans un certain sens changé partout. Cela est en fait déjà arrivé.

Les blocs d'adresses IPv4 ont été pendant de longues années alloués de façon chronologique, c'est à dire, en fait de façon aléatoire par rapport à la topologie du réseau. Cela a conduit à la croissance constante des tableaux d'acheminement ; cela ne se sent pas. Aujourd'hui, l'acheminement hiérarchique (CIDR [RFC1518], [RFC1519]) est utilisé comme mécanisme pour améliorer le dimensionnement de l'acheminement au sein d'un domaine d'acheminement; et en particulier au sein de l'Internet (l'Annexe est plus détaillée sur CIDR).

Les capacités de dimensionnement de CIDR se fondent sur l'hypothèse que l'allocation des adresses reflète la topologie du réseau autant que possible, et il n'est pas obligé que les frontières pour l'agrégation des informations d'adressage soient entièrement contenues dans une seule organisation – elles peuvent s'étendre sur plusieurs organisations (par exemple, un fournisseur avec ses abonnés). Donc, si un abonné change de fournisseur, pour éviter alors d'injecter de la redondance supplémentaire dans le système d'acheminement de l'Internet, l'abonné peut avoir besoin d'un dénumérotage.

Le changement de fournisseur est juste une des raisons possibles de dénumérotage. Le document d'information [RFC1900] montre pourquoi la dénumérotation est devenue un événement de plus en plus fréquent. DHCP [RFC1541] et PPP [RFC1661] promeuvent tous deux l'utilisation de l'allocation dynamique des adresses.

Pour résumer, depuis le développement et le déploiement de DHCP et de PPP, et comme on s'attend à ce que les dénumérotages deviennent vraisemblablement un événement courant, la signification de l'adresse IP a bien sûr changé. L'unicité spatiale devrait être la même, de sorte que les adresses sont encore des localisateurs efficaces. L'unicité temporelle n'est plus assurée. Elle peut être assez brève, éventuellement plus brève que la durée d'une connexion TCP. Dans un tel cas, une adresse IP n'est plus un bon identifiant. Cela a un certain impact sur la sécurité de bout en bout, et casse TCP sous sa forme actuelle.

4.3 Envoi en diffusion groupée et envoi à la cantonade

Depuis que nous avons déployé la diffusion groupée [RFC1112], nous devons séparer le débat sur la signification des adresses IP en signification des adresses de source et signification des adresses de destination. Une adresse de destination de diffusion groupée (c'est à dire un localisateur d'un groupe d'hôtes topologiquement dispersés) peut traverser un NAT, et n'est pas nécessairement restreint à un intranet (ou à l'Internet public). Sa durée de vie peut elle aussi être brève.

Le concept d'adresse à la cantonade est celui d'une adresse qui localise sémantiquement tout système d'un groupe de systèmes qui effectuent des fonctions équivalentes. Il n'y a aucun moyen qu'une telle adresse puisse être autre chose qu'un localisateur ; elle ne peut jamais servir d'identifiant comme défini dans le présent document, car elle n'identifie pas de façon univoque un hôte. Dans ce cas, l'unicité temporelle effective, ou la durée de vie utile d'une adresse IP peut être inférieure au temps que prend l'établissement d'une connexion TCP.

Ici, nous avons utilisé TCP simplement pour illustrer l'idée d'une association – beaucoup d'applications fondées sur UDP (ou d'autres systèmes sur la couche IP) allouent un état après la réception ou l'envoi d'un premier paquet, sur la base de la source et/ou de la destination. Toutes sont affectées par l'absence de l'unicité temporelle tandis que seule l'infrastructure d'acheminement est affectée par les changements d'unicité spatiale.

4.4 Résumé

Du fait de l'allocation dynamique d'adresse et du dénumérotage réseau de plus en plus fréquent, l'unicité temporelle des adresses IPv4 n'est plus garantie au niveau mondial, ce qui remet sévèrement en question leur utilisation comme identifiants. Du fait de la prolifération des intranets, l'unicité spatiale n'est elle non plus pas garantie à travers les domaines d'acheminement ; l'interconnexion des domaines d'acheminement pourrait être accomplie via des ALG ou des NAT. En principe une telle interconnexion aura des fonctionnalités inférieures à celles où les intranets sont connectés directement. En pratique, la différence de fonctionnalités peut avoir ou non de l'importance, selon les circonstances.

5. Considérations pour IPv6

Pour autant qu'est concernée l'unicité temporelle (comportement de type identifiant), le modèle IPv6 [RFC1884] est très similaire à l'état actuel du modèle IPv4, seulement plus encore. IPv6 va fournir des mécanismes pour auto configurer les adresses IPv6 sur des hôtes IPv6. Les changements de préfixes, qui exigent le changement des adresses IPv6 globales de tous les hôtes derrière un préfixe donné, sont à prévoir. Donc, IPv6 va amplifier le problème existant de trouver des identifiants stables à utiliser pour la sécurité de bout en bout et pour les liaisons de session telles que l'état TCP.

L'IAB estime que ceci est regrettable, et que la transition vers IPv6 serait une occasion idéale pour fournir des protocoles de bout en bout de couche supérieure avec des identifiants uniques dans le temps. La nature exacte de ces identifiants exige des études complémentaires.

Pour autant qu'est concernée l'unicité spatiale (le comportement de type localisateur) l'espace d'adresse IPv6 est tellement grand qu'un manque d'adresses, exigeant une approche comme celle de la RFC1918 et une traduction d'adresse, est difficilement concevable. Bien qu'il n'y ait pas de manque d'adresses IPv6, il y a aussi un mécanisme bien connu pour obtenir des adresses de liaison locale et de site local dans IPv6 [RFC1884, paragraphe 2.4.8]. Ces propriétés de IPv6 n'empêchent pas des domaines d'acheminement séparés pour IPv6, si on le désire (résultant aussi en plusieurs domaines de sécurité). Alors que pour l'instant on ne peut pas identifier un cas dans lequel plusieurs domaines d'acheminement IPv6 seraient exigés, il est aussi difficile de donner une réponse définitive à la question de savoir si il y aura seulement un, ou plusieurs domaines d'acheminement IPv6. Si on fait l'hypothèse qu'il y aura plus d'un domaine d'acheminement IPv6, de tels domaines pourraient alors être interconnectés ensemble via des ALG et des NAT. Les considérations pour de telles ALG et de tels NAT paraissent être identiques à celles pour IPv4.

ANNEXE Pratiques actuelles pour l'allocation et l'acheminement des adresses IPv4

Au départ, la structure d'adresse IP et l'acheminement IP étaient conçus autour de la notion de classes de numéros de réseau (réseaux de classes A/B/C) [RFC0790]. Au début des années 90 la croissance de l'Internet demandait des améliorations significatives à la fois dans la capacité d'adaptation du système d'acheminement de l'Internet et dans l'utilisation de l'espace d'adresse IP. La structure de classes de l'espace d'adresse IP associée à son acheminement par classes s'est révélée inadéquate à satisfaire les demandes, de sorte que durant la période 1992 – 1993, l'Internet a adopté l'acheminement inter domaine sans classe (CIDR, *Classless Inter-Domain Routing*) [RFC1380], [RFC1518], [RFC1519]. CIDR renferme une nouvelle architecture d'allocation d'adresses, de nouveaux protocoles d'acheminement, et une nouvelle structure des adresses IP.

CIDR améliore la capacité d'adaptation du système d'acheminement de l'Internet en étendant la notion d'acheminement hiérarchique au delà du niveau des sous-réseaux et réseaux individuels, pour permettre l'agrégation des informations non seulement au niveau des sous-réseaux et réseaux individuels, mais aussi au niveau des sites individuels, ainsi qu'au niveau des fournisseurs de service Internet. Donc une organisation (un site) peut agir comme agrégateur pour toutes les destinations au sein de l'organisation. De même, un fournisseur peut agir comme agrégateur pour toutes les destinations parmi ses abonnés (organisations directement connectées au fournisseur).

Étendre la notion d'acheminement hiérarchique au niveau des sites et fournisseurs individuels, et permettre aux sites et fournisseurs d'agir comme agrégateurs d'informations d'acheminement exigeait des changements aussi bien aux procédures

d'allocation d'adresses qu'aux protocoles d'acheminement. Alors que dans les temps précédant le CIDR, l'allocation des adresses aux sites était faite sans prendre en considération le besoin d'agréger les informations d'adressage au-dessus du niveau des numéros de réseau individuel, l'allocation fondée sur CIDR recommande que l'allocation d'adresse soit faite d'une façon qui permette aux sites et fournisseurs d'agir comme agrégateurs des informations d'adressage – une telle allocation est dite "fondée sur l'agrégateur". Pour bénéficier de l'allocation d'adresse "fondée sur l'agrégateur", CIDR introduit un protocole d'acheminement inter domaine (BGP-4) [RFC1771], [RFC1772] qui apporte des capacités d'agrégation des informations d'acheminement au niveau des sites et fournisseurs individuels.
CIDR améliore l'utilisation de l'espace d'adresse en éliminant la notion de classes de réseau, et en la remplaçant par la notion de blocs d'adresse de taille variable contigus (puissance de 2). Cela permet une meilleure correspondance entre la quantité d'espace d'adresse demandé et la quantité d'espace d'adresse alloué [RFC1466]. Cela facilite aussi l'allocation d'adresse "fondée sur l'agrégateur". En éliminant la notion de classes de réseau, on a besoin de nouvelles capacités dans les protocoles d'acheminement (à la fois en intra et en inter domaine) et dans la transmission IP. Précisément, les protocoles à capacité CIDR doivent traiter les informations d'accessibilité (adressage) exprimées en termes de préfixes d'adresse de longueur variable, et la transmission doit mettre en œuvre l'algorithme de la "plus longue correspondance". Les implications de CIDR sur les protocoles d'acheminement sont décrites dans la [RFC1817].

Les capacités d'adaptation de CIDR se fondent sur l'hypothèse que l'allocation d'adresse reflète la topologie du réseau autant qu'il est possible, en particulier au niveau des sites, et leur interconnexion avec les fournisseurs, pour permettre aux sites et aux fournisseurs d'agir comme agrégateurs. Si un site change de fournisseur, pour éviter alors d'injecter de la redondance supplémentaire dans le système d'acheminement de l'Internet, le site peut avoir besoin d'un dénumérotage. Alors que CIDR n'exige pas que chaque site qui change de fournisseur soit dé numéroté, il est important de souligner que si aucun des sites qui change de fournisseur n'est dénuméroté, le système d'acheminement de l'Internet pourrait être défaillant à cause de la quantité excessive d'informations d'acheminement qu'il devrait traiter.

Le maintien de l'allocation d'adresse "fondée sur l'agrégateur" (pour promouvoir l'adaptabilité de l'acheminement) et le besoin de prendre en charge la capacité des sites à changer de fournisseurs (pour promouvoir la concurrence) demande des solutions pratiques pour les sites dénumérotés. La nécessité de contenir la redondance dans un système d'acheminement Internet en croissance rapide rendra vraisemblablement la dénumérotation de plus en plus fréquente [RFC1900].

La nécessité d'adapter le système d'acheminement de l'Internet, et l'utilisation de CIDR comme principal mécanisme d'adaptation, résultent en l'évolution des politiques d'allocation et de gestion d'adresses pour l'Internet. Cette évolution résulte en l'ajout de politiques de "prêt d'adresse" comme solution de remplacement à la politique de "propriété de l'adresse" de la [RFC2008].

L'adressage et l'acheminement IP ont été en constante évolution depuis que IP a été spécifié pour la première fois par la [RFC0791]. Certains des principes d'adressage et d'acheminement ont été déconseillés, et certains des principes ont été préservés, alors que de nouveaux principes ont été introduits. L'acheminement et les adresses Internet actuels (fondés sur CIDR) sont une étape de l'évolution qui étend l'utilisation d'une hiérarchie pour maintenir la possibilité d'un acheminement mondial sur l'Internet.

Considérations pour la sécurité

L'impact du modèle d'adressage IP sur la sécurité est discuté dans les sections 4.1 et 5 de ce document.

Remerciements

Le présent document a été développé au sein de l'IAB. Des commentaires constructifs ont été reçus de Ran Atkinson, Jim Bound, Matt Crawford, Tony Li, Michael A. Patton, Jeff Schiller. Des communications privées de Noel Chiappa ont aidé à préciser les concepts de localisateurs et d'identifiants.

Références

(Les liens sur le numéro pointent sur la versionanglaise, ceux du titre sur la traduction française)

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0790] J. Postel, "Numéros alloués", septembre 1981.

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

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987.

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989.

[RFC1380] P. Gross et P. Almquist, "Délibérations de l'IESG sur l'acheminement et l'adressage", novembre 1992. *(Info)*

[RFC1466] E. Gericht, "Lignes directrices pour la gestion de l'espace adresse IP", mai 1993. *(Info, rempl. par 2050)*

[RFC1498] J. Saltzer, "Sur la dénomination et la liaison des destinations réseau", août 1993. *(Information)*

[RFC1518] Y. Rekhter et T. Li, "Architecture pour l'allocation d'adresses IP avec CIDR", septembre 1993. *(Historique)*

[RFC1519] V. Fuller, T. Li, J. Yu et K. Varadhan, "Acheminement inter domaine sans classe (CIDR) : stratégie d'allocation et d'agrégation d'adresses", septembre 1993. *(D.S., rendue obsolète par la RFC 4632)*

[RFC1541] R. Droms, "Protocole de configuration dynamique d'hôte", octobre 1993. *(P.S., remplacé par 2131)*

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la RFC 2153)*

[RFC1771] Y. Rekhter, T. Li , "Protocole de routeur frontière v. 4 (BGP-4)", mars 1995. *(Obsolète, voir RFC4271) (D.S.)*

[RFC1772] Y. Rekhter, P. Gross, "Application du protocole de routeur frontière dans l'Internet", mars 1995. *(D.S.)*

[RFC1817] Y. Rekhter, "CIDR et acheminement avec classes", août 1995. *(Historique)*

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC 1825, août 1995. *(Rendue obsolète par la RFC2401)*

[RFC1900] B. Carpenter, Y. Rekhter, "Un dénumérotage représente du travail", février 1996. *(Information)*

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

[RFC1933] R. Gilligan, E. Nordmark, "Mécanismes de transition pour hôtes et routeurs IPv6", avril 1996. (*Obs., voir* RFC2893) *(P.S.)*

[RFC2008] Y. Rekhter, T. Li, "Implications des diverses politiques d'allocation d'adresse pour l'acheminement Internet", octobre 1996. (BCP0007)

[RFC2065] D. Eastlake 3rd, C. Kaufman, "Extensions de sécurité du système de noms de domaines", janvier 1997. (*Obsolète, voir* RFC2535) (MàJ RFC1034, RFC1035) *(P.S.)*

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

[RFC2182] R. Elz et autres, "Sélection et fonctionnement des serveurs secondaires du DNS", juillet 1997. (BCP0016)

Adresse des auteurs

Brian E. Carpenter
Computing and Networks Division
CERN
European Laboratory for Particle Physics
1211 Geneva 23, Switzerland
mél : brian@dxcoms.cern.ch

Jon Crowcroft
Dept. of Computer Science
University College London
London WC1E 6BT, UK
mél : j.crowcroft@cs.ucl.ac.uk

Yakov Rekhter
Cisco systems
170 West Tasman Drive
San Jose, CA, USA
téléphone : +1 914 528 0090
Fax: +1 408 526-4952
mél : yakov@cisco.com