Groupe de travail Réseau
Request for Comments : 2008
BCP : 7
Catégorie : Bonnes practiques actuelles

Y. Rekhter & T. Li, Cisco Systems
octobre 1996

Traduction Claude Brière de L'Isle

Implications de diverses politiques d'allocation d'adresses pour l'acheminement Internet

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la Communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Note de l'IESG :
Les contraintes d'adressage décrites dans ce document sont largement le résultat de l'interaction de la technologie existante pour les routeurs, de l'allocation des adresses, et de l'histoire de l'architecture. Après un examen et des discussions extensives, les auteurs de ce document, le groupe de travail de l'IETF qui l'a relu, et l'IESG sont arrivés à la conclusion qu'il n'y a aucune autre technologie disponible actuellement déployée pour surmonter ces limitations. Dans le cas où une technologie d'acheminement ou de routeur se développerait au point qu'une agrégation d'acheminement adéquate puisse être réalisée par d'autres moyens ou que les routeurs puissent traiter de plus grands tableaux d'acheminement plus dynamiques, il pourrait être approprié de réviser ces contraintes.

Table des matières

1 Résumé

L'allocation et la gestion des adresses IP en envoi individuel sont des fonctions opérationnelles essentielles pour l'Internet public. Les politiques exactes d'allocation et de gestion des adresses IP en envoi individuel continuent de faire l'objet de nombreuses discussions. De telles discussions ne peuvent se poursuivre dans le vide - les participants doivent comprendre les questions techniques et les implications des diverses politiques d'allocation et de gestion des adresses.

L'objet du présent document est d'articuler certaines questions techniques fondamentales pertinentes qui doivent être prises en considération dans la formulation des politiques d'allocation et de gestion des adresses IP en envoi individuel pour l'Internet public, et de faire des recommandations par rapport à ces politiques.

Le présent document se concentre sur deux politiques possibles, la "propriété de l'adresse" et le "prêt d'adresse," et sur les implications techniques de ces politiques pour l'Internet public. Pour les organisations qui pourraient fournir l'accessibilité à une fraction suffisamment large des destinations totales dans l'Internet, et pourraient exprimer une telle accessibilité à travers un seul préfixe d'adresse IP, le document suggère d'utiliser la politique de "propriété de l'adresse". Cependant, appliquer la politique de "propriété de l'adresse" à tous les sites ou organisations individuels qui se connectent à l'Internet résulterait en un acheminement non adaptable.

Par conséquent, le présent document recommande aussi que la politique du "prêt d'adresse" soit formellement ajoutée à

l'ensemble des politiques d'allocation d'adresse de l'Internet public. Le document recommande aussi que les organisations qui ne fournissent pas un degré suffisant d'agrégation d'informations d'acheminement, mais souhaitent obtenir l'accès aux services d'acheminement de l'Internet soient vivement encouragées à utiliser cette politique pour obtenir l'accès aux services.

2. Valeur intrinsèque des adresses IP

Syntaxiquement, l'ensemble des adresses IPv4 d'envoi individuel est l'ensemble (fini) des entiers dans la gamme de 0x00000000 à 0xDFFFFFFF. Les adresses IP sont utilisées pour l'acheminement de couche réseau (IP). Une adresse IP est le seul élément d'information sur le nœud injecté dans le système d'acheminement.

La sémantique remarquable d'une adresse IP d'envoi individuel est sa capacité à interagir avec le service d'acheminement de l'Internet public et par là d'échanger des données avec le reste de l'Internet. En d'autre termes, pour l'Internet public, c'est l'accessibilité d'une adresse IP qui lui donne une valeur intrinsèque. Observer, cependant, que les adresses IP sont utilisées en dehors de l'Internet public. Le présent document ne traite pas de la valeur des adresses dans d'autres contextes que celui de l'Internet public.

Ceci implique que l'Internet public est l'environnement de service (l'Internet) et son fonctionnement continu, y compris son système d'acheminement, qui donne à une adresse IP sa valeur intrinsèque, plutôt que l'inverse. Par conséquent, si le système d'acheminement de l'Internet public cesse d'être opérationnel, le service disparaît, et les adresses cessent d'avoir une valeur fonctionnelle dans l'Internet. À ce point, pour l'Internet public, toutes les politiques d'allocation et de gestion des adresses, y compris les politiques existantes, perdent leur signification.

3 L'acheminement hiérarchique et ses implications sur l'allocation d'adresse

L'acheminement hiérarchique [Kleinrock 77] est un mécanisme qui améliore les propriétés d'adaptation d'un système d'acheminement. C'est le seul mécanisme démontré pour l'adaptation de l'acheminement à la taille actuelle de l'Internet.

L'acheminement hiérarchique exige que les adresses soient allouées de façon à refléter la topologie réelle du réseau. L'acheminement hiérarchique fonctionne en prenant l'ensemble des adresses couvertes par une portion de la topologie, et en générant une seule annonce de chemin (de route) pour l'ensemble entier. De plus, l'acheminement hiérarchique permet que ce soit fait de façon récurrente : plusieurs annonces (de chemins) peuvent être combinées en une seule annonce (de chemin). En effectuant cette récurrence, la quantité d'informations nécessaires pour fournir l'acheminement peut être substantiellement diminuée.

Un exemple courant d'acheminement hiérarchique est le réseau téléphonique, où les codes de pays, les codes de zone, les commutateurs, et finalement les lignes d'abonné sont les différent niveaux de la hiérarchie. Dans le réseau téléphonique, un commutateur n'a pas besoin de conserver les informations d'acheminement détaillées sur tous les abonnés possibles dans un code de zone distante. Le commutateur connaît plutôt une entrée d'acheminement pour l'ensemble du code de zone.

On remarquera que l'effet sur l'adaptation est considérable. Si on regarde la complexité spatiale des différents schémas, le commutateur qui sait tout sur tous les abonnés dans le monde a besoin de l'espace O(n) pour n abonnés dans le monde entier. Considérons maintenant le cas de l'acheminement hiérarchique. On peut scinder n en nombre d'abonnés dans la zone locale (l), en nombre des autres commutateurs dans le code de zone (e), les autres codes de zone dans le code de pays local (a) et en autres codes de pays (c). En utilisant cette notation, l'acheminement hiérarchique a la complexité spatiale O(l + e + a + c). que chacun de ces facteurs est très, très inférieur à n, et croît très lentement, si il croît. Cela implique qu'un commutateur téléphonique peut aujourd'hui être construit avec quelque espoir qu'il ne soit pas trop petit le jour de sa mise en service.

La propriété fondamentale de l'acheminement hiérarchique qui rend son adaptation possible est la capacité à former des abstractions : ici, la capacité à grouper les abonnés dans les centraux, dans les codes de zone et les codes de pays. De plus, de telles abstractions doivent fournir des informations utiles pour la capacité à effectuer l'acheminement. Certaines abstractions, telles que le groupe des usagers avec des téléphones verts, ne sont pas utiles en matière d'acheminement des appels.

Comme l'information dont le système d'acheminement a réellement besoin est la localisation de l'adresse au sein de la topologie, pour l'acheminement hiérarchique, l'abstraction utile doit capturer la localisation topologique d'une adresse au sein du réseau. En principe, cela pourrait se réaliser de deux façons. Soit (a) contraindre la topologie (et admettre des changements topologiques) pour correspondre aux allocations d'adresses. Soit (b) éviter les contraintes sur la topologie (et les changements topologiques) mais exiger que lorsque la topologie change, l'adresse d'une entité change aussi. Le processus de changement de l'adresse d'une entité s'appelle un "dénumérotage".

4 Adaptation du système d'acheminement de l'Internet

L'énorme croissance de l'Internet public fait peser une lourde charge sur le système d'acheminement de l'Internet. Avant l'introduction de CIDR, le taux de croissance avait en gros fait doubler la taille du tableau d'acheminement tous les neuf mois. La capacité des ordinateurs double en gros tous les 24 mois. Même si on pouvait doubler la capacité des routeurs dans l'Internet tous les 24 mois, la taille des tableaux d'acheminement va inévitablement excéder la limite de celle des routeurs. Donc, pour préserver sans interruption la croissance continue de l'Internet public, il est essentiel de développer des mécanismes qui contiennent le taux de croissance des informations d'acheminement.

En l'absence de mécanismes capables de contenir le taux de croissance des informations d'acheminement, la croissance de l'Internet devrait être limitée ou gelée, ou le système d'acheminement de l'Internet deviendrait surchargé. Le résultat de la surcharge de l'acheminement est que le sous-système d'acheminement va être défaillant : soit les équipements (routeurs) ne pourront plus entretenir suffisamment de chemins pour assurer la connexité mondiale, soit les fournisseurs vont simplement exclure certains chemins pour assurer que d'autres chemins peuvent fournir la connexité à des sites particuliers. Le présent document suppose qu'aucun des résultats mentionnés dans ce paragraphe n'est acceptable.

L'acheminement inter domaine sans classe (CIDR, *Classless Inter-Domain Routing*) [RFC1518], [RFC1519] a été développé depuis la fin 1992 dans l'Internet public comme mécanisme principal pour contenir le taux de croissance des informations d'acheminement - sans CIDR, le système d'acheminement de l'Internet aurait déjà rendu l'âme. Par exemple, en octobre 1995, au sein de AlterNet (un des fournisseurs de service Internet majeurs) il y avait 3194 routes. Grâce à l'agrégation, AlterNet annonce seulement 799 routes pour le reste de l'Internet – une économie de 2395 routes (75 %) [Partan 95]. En octobre 1995, le registre d'acheminement de l'Internet (IRR, *Internet Routing Registry*) contenait une liste de 61 430 préfixes uniques, non compris les préfixes marqués comme retirés (ou 65 191 préfixes avec les préfixes marqués retirés). C'est en gros une borne inférieure car de nombreux préfixes ne sont pas enregistrés dans l'IRR. L'agrégation du CIDR a résulté en ce qu'il y ait moins de 30 000 routes dans la partie non par défaut du système d'acheminement de l'Internet [Villamizar 95].

CIDR est un exemple de l'application de l'acheminement hiérarchique dans l'Internet public, où les sous-réseaux, les abonnés, et finalement les fournisseurs sont des niveaux possibles de la hiérarchie. Par exemple, un routeur au sein d'un site n'a pas besoin de conserver des informations d'acheminement détaillées sur tous les hôtes possibles dans ce site. À la place de cela, le routeur conserve les informations d'acheminement sur la base du sous-réseau. De même, un routeur au sein d'un fournisseur n'a pas besoin de conserver des informations d'acheminement détaillées sur les sous-réseaux individuels chez ses abonnés. Le routeur va plutôt conserver les informations d'acheminement sur la base de l'abonné. De plus, un routeur au sein d'un fournisseur n'a pas besoin de garder des informations d'acheminement détaillées sur les abonnées de bout de réseau (les abonnés résidentiels) des autres fournisseurs mais va garder les informations d'acheminement sur la base du fournisseur.

À cause de l'allocation d'adresse pré CIDR, de nombreuses routes de l'Internet ne conviennent pas pour une agrégation hiérarchique. De plus, il existe des sites non connectés avec des allocations d'adresse pré CIDR. Si ces sites se connectent à l'Internet à l'avenir, les chemins vers ces sites ne vont vraisemblablement pas convenir pour une agrégation hiérarchique. Aussi, lorsque un site utilise des adresses obtenues de son fournisseur, mais ensuite passe à un fournisseur différent (tout en continuant d'utiliser la même adresse) le chemin pour le site peut ne plus convenir pour l'agrégation hiérarchique.

L'acheminement hiérarchique exige que les frontières d'agrégation pour les informations d'adressage soient formées selon une certaine hiérarchie. Il en résulte que de nombreuses exceptions vont à l'avenir être injectées dans le système d'acheminement, en plus des exceptions qui existent actuellement. Chaque exception ajoutée au système d'acheminement détériore l'adaptabilité du système d'acheminement. Le nombre exact d'exceptions qui peut être toléré dépend de la technologie utilisée pour prendre en charge l'acheminement. Une croissance débridée du nombre de telles exceptions causerait la mort du système d'acheminement.

5. Allocation d'adresse et politiques de gestion

La politique d'allocation et de gestion des adresses IP est une question complexe, qui présente de multiples facettes. Cela couvre une large gamme de questions, telles que qui formule la politique ? qui exécute la politique ? quel est le rôle des divers registres ? quel est le rôle des diverses organisations ? (par exemple, l'ISOC, l'IAB, l'IESG, l'IETF, l'IEPG, les divers organes gouvernementaux, etc.), quelle participation pour l'utilisateur final dans la demande d'adresse ? et ainsi de suite. L'allocation et la gestion d'adresse et l'adaptabilité du système d'acheminement sont en relations mutuelles - seules certaines politiques d'allocation et de gestion d'adresses donnent un acheminement adaptable. Le système d'acheminement de l'Internet est soumis à la fois à des contraintes technologiques et fondamentales. Ces contraintes restreignent le choix des politiques d'allocation d'adresse praticables.

5.1 La politique d'allocation "d'adresses propriétaires" et ses implications sur l'Internet public

La "propriété de l'adresse" est une des politiques possibles d'allocation et de gestion des adresses. La politique de "l'adresse propriétaire" signifie qu'une partie de l'espace des adresses, une fois alloué à une organisation, reste alloué à l'organisation aussi longtemps que le veut cette organisation. De plus, cette portion de l'espace d'adresses ne sera alloué à aucune autre organisation. Souvent, de telles adresses sont appelées "portables". Il a été supposé que si une organisation acquiert ses adresses via la politique de la "propriété de l'adresse", l'organisation sera capable d'utiliser ces adresses pour obtenir l'accès aux services d'acheminement de l'Internet, sans considération de l'endroit où l'organisation se connecte à l'Internet.

Bien qu'il n'ait jamais été explicitement déclaré que divers registres de l'Internet utilisent la politique d'allocation de "l'adresse propriétaire", elle a toujours été supposée (et pratiquée).

Pour comprendre les implications de la politique de la "propriété d'adresse" (adresse "portable") sur l'adaptabilité du systèmes d'acheminement de l'Internet, on doit observer que :

(a) par définition, la propriété de l'adresse suppose que les adresses, une fois allouées, tombent sous le contrôle de celui auquel elles sont allouées. C'est lui qui décide quand il renonce à la propriété (bien que la décision puisse être influencée par divers facteurs). Précisément, l'allocataire n'est pas obligé (mais il peut y être conduit) à renoncer à la propriété lorsque change la connexité de l'allocataire à l'Internet.

(b) par définition, l'acheminement hiérarchique suppose que les adresses reflètent autant que possible la topologie du réseau.

Donc, la seule pratique présentement connue pour satisfaire à la fois l'adaptabilité de l'acheminement hiérarchique et la propriété de l'adresse pour tous est de supposer que la topologie (ou au moins certains de ses éléments) sera fixée de façon permanente. Étant donnée la nature répartie, décentralisée, largement non réglementée, et mondiale (internationale) de l'Internet, contraindre la topologie de l'Internet (ou simplement de certaines de ses parties) peut avoir de vastes implications techniques, sociales, économiques, et politiques. On ne sait aujourd'hui pas grand chose de ce que sont ces implications ; on sait encore moins si ces implications seraient acceptables (faisables) en pratique. Donc, au moins pour l'instant, nous devons accepter un Internet avec une topologie sans contraintes (et des changements topologiques sans contraintes).

Comme l'Internet n'impose pas de contraintes à sa topologie (ou permet les changements de topologie) on peut avoir soit la propriété de l'adresse pour tous, soit un acheminement Internet, mais pas les deux, ou bien il faudra alors développer et déployer de nouveaux mécanismes (par exemple, en découplant l'adresse possédée par les utilisateurs finaux de celle utilisée par l'acheminement Internet, et prévoir des mécanismes de traduction entre les deux). En l'absence de nouveaux mécanismes, si nous avons la propriété de l'adresse (des adresses "portables") pour chacun, la surcharge de l'acheminement va conduire à une crise du système d'acheminement résultant en une fragmentation de l'Internet (une partition). Autrement, on peut avoir un acheminement Internet, mais sans la propriété des adresses (les adresses "portables") pour chacun.

5.2 La politique d'allocation "de prêt d'adresses" et ses implications sur l'Internet public

Récemment, en particulier depuis l'arrivée de CIDR, certains abonnées et fournisseurs ont suivi un modèle dans lequel l'espace des adresses n'est pas possédé (adresses non portables), mais est lié à la topologie. Ce modèle suggère une politique d'allocation et de gestion d'adresses qui diffère de la politique de "propriété de l'adresse". Ci-après est décrite une politique, appelée de "prêt d'adresse", qui fournit une meilleure correspondance (par rapport à la politique de "propriété de l'adresse") avec le modèle.

Une politique de "prêt d'adresse" signifie qu'une organisation obtient ses adresses sur la base d'un "prêt". Pour la durée du prêt, le prêteur ne peut pas laisser l'utilisation des adresses à un autre emprunteur. Les affectations et allocations effectuées sur la base de la politique de "prêt d'adresse" devraient explicitement inclure les conditions du prêt. De telles conditions doivent spécifier que les allocations sont rendues si l'emprunteur n'est plus lié contractuellement au prêteur, et le prêteur ne peut plus fournir d'agrégation pour l'allocation. Si un prêt se termine, l'organisation ne peut plus utiliser les adresses empruntées, et doit donc obtenir de nouvelles adresses et subir un dénumérotage pour les utiliser. La politique de "prêt d'adresse" n'exerce pas de contrainte sur la façon dont les nouvelles adresses sont acquises.

Le présent document prévoit que la politique de "prêt d'adresse" sera principalement utilisée par les registraires Internet associés aux fournisseurs *(d'accès Internet, les FAI)* ; cependant, le présent document n'interdit pas l'usage de la politique de "prêt d'adresse" par un registraire Internet qui ne serait pas associé à un fournisseur.

Le présent document prévoit que lorsque la politique de "prêt d'adresse" est utilisée par un registraire Internet associé à un FAI, le FAI est responsable de l'arrangement de l'agrégation de ces adresses à un degré suffisant pour réaliser la connexité IP avec l'ensemble de l'Internet.

Le présent document prévoit que lorsque la politique de "prêt d'adresse" est utilisée par un registraire Internet associé à un FAI, les termes et conditions du prêt seront couplés à un accord de service entre le FAI et les abonnés. C'est à dire que si l'abonné passe chez un autre FAI, le prêt sera annulé.

Pour réduire les interruptions lorsque qu'un abonné change de fournisseur, le présent document recommande fortement que les termes et conditions du prêt comportent des dispositions sur une période de grâce. Cette disposition permettrait à l'abonné qui se déconnecte de son fournisseur une certaine période de grâce après la déconnexion. Durant cette période de grâce, l'emprunteur (l'abonné) peut continuer d'utiliser les adresses obtenues au cours du prêt. Le présent document recommande une période de grâce d'au moins 30 jours. De plus, pour contenir la surcharge des informations d'acheminement, le présent document suggère qu'une période de grâce ne dépasse pas six mois.

Pour comprendre les implications sur l'adaptabilité de la politique de "prêt d'adresse", observons que si un abonné emprunte ses adresses au bloc de son fournisseur, le fournisseur peut alors annoncer un seul préfixe d'adresses. Cela réduit le volume des informations d'acheminement qui doivent être portées par le système d'acheminement de l'Internet (voir des informations complémentaires au paragraphe 5.3.1 de la RFC1518). Lorsque l'abonné change de fournisseur, le prêt de l'ancien fournisseur devrait être restitué, et le prêt du nouveau fournisseur devrait être établi. Il en résulte que l'abonné devrait être renuméroté à la nouvelle adresse. Une fois que l'abonné est renuméroté dans les blocs existants du nouveau fournisseur, aucune nouvelle route n'a besoin d'être introduite dans le système d'acheminement.

Donc, la politique de "prêt d'adresse", si elle est appliquée correctement, est cohérente avec les contraintes imposées aux politiques d'allocation d'adresse par l'acheminement hiérarchique, et promeut donc un système d'acheminement adaptable. Par conséquent, si la politique de "prêt d'adresse" est appliquée de façon appropriée, elle pourrait jouer un rôle important dans la poursuite ininterrompue de la croissance de l'Internet.

Pour être capable d'adapter l'acheminement dans les autres parties de la hiérarchie, la politique de "prêt" peut aussi être appliquée de façon hiérarchique, de sorte que les adresses puissent à leur tour être prêtées à d'autres organisations. Cela implique ici que la fin d'un seul prêt peut avoir des effets sur des organisations qui ont emprunté de façon répétée des parties de l'espace d'adresses à partir de l'allocation principale. Dans ce cas, les effets exacts sont difficiles à déterminer à priori.

5.3 En l'absence d'une politique explicite de "prêt d'adresses"

Les organisations qui se connectent à l'Internet devraient être conscientes que même si leur fournisseur actuel, et le fournisseur auquel elles passeront à l'avenir n'exigent pas la dénumérotation, celle-ci peut quand même être nécessaire pour réaliser une connexité IP à l'échelle de l'Internet. Par exemple, une organisation peut recevoir maintenant le service Internet d'un certain fournisseur et avoir ses adresses allouées à partir du bloc CIDR associé à ce fournisseur. Ultérieurement, l'organisation va passer à un autre fournisseur. Le fournisseur précédent peut être d'accord pour permettre à l'organisation de conserver une partie du bloc CIDR du fournisseur, et accepter un préfixe plus spécifique pour cette organisation de la part du nouveau fournisseur. De même, le nouveau fournisseur peut accepter cette organisation sans dénumérotage et annoncer le préfixe plus spécifique (qui couvre les destinations au sein de l'organisation) pour le reste de l'Internet. Cependant, si il existe un ou plusieurs autres fournisseurs qui ne sont pas d'accord ou pas capables d'accepter le préfixe plus long annoncé par le nouveau fournisseur, l'organisation n'aurait alors pas de connexité IP avec une partie de l'Internet. Parmi les solutions possibles ouvertes à l'organisation il y a le dénumérotage, ou l'acquisition de la connexité avec les fournisseurs qui veulent et sont capables d'accepter le préfixe.

Voilà qui montre qu'en l'absence d'une politique explicite de "prêt d'adresse" de la part d'un fournisseur actuel il n'est absolument pas garanti qu'il ne sera pas exigé à l'avenir qu'un changement de fournisseur s'accompagne d'un dénumérotage. Les organisations devraient être conscientes de ce fait si elle devaient rencontrer un fournisseur qui revendique le contraire.

6. Recommandations

On observe que le but de l'acheminement hiérarchique dans l'Internet n'est pas de réduire la quantité totale d'informations d'acheminement dans l'Internet au minimum théorique possible, mais juste de contenir le volume des informations d'acheminement dans les limites rendues possibles par la technologie, le rapport prix/performances, et les facteurs humains. Donc, les organisations qui pourraient fournir l'accessibilité à une fraction suffisamment large des destinations totales dans l'Internet et pourraient exprimer une telle accessibilité à travers un seul préfixe d'adresse IP pourraient s'attendre à ce qu'un

chemin possédant ce préfixe se conserve à travers la partie non par défaut du système d'acheminement de l'Internet, sans considération de l'endroit où elles se connectent à l'Internet. Donc, utiliser la politique de "propriété de l'adresse" lors de l'allocation des adresses à de telles organisations est un choix raisonnable. Le présent document suggère qu'au sein de ces organisations on utilise la politique du "prêt d'adresse".

Pour toutes les autres organisations qui attendent une connexité IP sur l'ensemble de l'Internet, les informations d'accessibilité qu'elles injectent dans le système d'acheminement de l'Internet devraient être soumises à une agrégation hiérarchique. Pour de telles organisations, l'allocation d'adresses sur la base de la politique de "propriété de l'adresse" rend difficile, sinon impossible, l'agrégation hiérarchique. Ceci a à son tour un effet très négatif sur le système d'acheminement de l'Internet. Pour empêcher l'écroulement du système d'acheminement de l'Internet, le présent document recommande d'utiliser, pour de telles organisations, la politique du "prêt d'adresse". Par conséquent, quand une telle organisation se connecte pour la première fois à l'Internet public ou change son rattachement topologique à l'Internet public, l'organisation peut éventuellement devoir être dénumérotée. La dénumérotation permet à l'organisation de supprimer tous les préfixes exceptionnels qu'elle devrait autrement injecter dans le système d'acheminement de l'Internet. Cela s'applique au cas où l'organisation tire ses adresses du bloc de son fournisseur direct et où l'organisation change de fournisseur direct. Cela peut aussi s'appliquer au cas où l'organisation tire ses adresses du bloc de son fournisseur indirect, et où l'organisation change de fournisseur indirect, ou où le fournisseur direct de l'organisation change de fournisseur.

Le transport des informations d'acheminement a un coût associé. Ce coût, dans une certaine mesure, peut être complètement répercuté sur les organisations qui injectent les informations d'acheminement. L'agrégation des informations d'adressage (via CIDR) pourrait réduire le coût, car elle permet une augmentation du nombre de destinations couvertes par un seul chemin. Les organisations dont les adresses sont allouées sur la base de la politique de la "propriété de l'adresse" (et peuvent n'être pas susceptibles d'agrégation) devraient être prêtes à supporter complètement leurs propres coûts.

On observera que ni la politique de la "propriété de l'adresse", ni celle du "prêt d'adresse" ne sont par elles-mêmes suffisantes pour garantir la connexité IP à l'échelle de l'Internet. Nous recommandons donc que les sites qui ont des adresses allouées sur la base de l'une ou l'autre politique consultent leurs fournisseurs sur la portée de l'accessibilité qui pourrait être réalisée avec ces adresses, et sur les coûts associés qui résultent de l'utilisation de ces adresses.

Si une organisation n'a pas besoin de la connexité IP sur l'ensemble de l'Internet, l'allocation d'adresses pour l'organisation pourrait alors se faire sur la base de la politique de la "propriété de l'adresse". L'organisation peut là encore conserver une connexité IP limitée (par exemple, avec tous les abonnés de son fournisseur direct) en limitant la portée de distribution de ses informations d'acheminement à son fournisseur direct. La connexité avec le reste de l'Internet peut être traitée par des passerelles de médiation (par exemple, des passerelles de couche application, des traducteurs d'adresse réseau (NAT, *Network Address Translators*)). Noter que l'utilisation de passerelles de médiation élimine le besoin de dénumérotage, et évite de surcharger le système d'acheminement de l'Internet avec des informations d'acheminement non agrégeables ; cependant, elles ont d'autres inconvénients qui peuvent se révéler étranges dans certaines situations.

Le dénumérotage (dû à la politique de "prêt d'adresse") les informations d'acheminement non agrégées (dues à la politique de la "propriété de l'adresse") comme l'utilisation de passerelles de médiation résultent en des coûts. Donc, une organisation doit analyser attentivement ses propres exigences de connexité et comparer les compromis associés aux adresses acquises via l'une et l'autre politique par rapport à la connexité via des passerelles de médiation (éventuellement augmentée par une connexité IP limitée) en utilisant des adresses acquises via la "propriété de l'adresse". Pour réduire le coût du dénumérotage, les organisations devraient vivement encourager le déploiement d'outils qui simplifient le dénumérotage (par exemple, le protocole de configuration dynamique d'hôte [RFC1541]). L'utilisation du DNS devrait être fortement encouragée.

7. Résumé

Toute politique d'allocation et de gestion d'adresses pour les adresses IP utilisées pour la connexité de l'Internet doit prendre en compte son impact sur la capacité d'adaptation du système d'acheminement de l'Internet public. Parmi toutes les politiques possibles d'allocation et de gestion d'adresse, seules celles qui donnent un système d'acheminement adaptable sont praticables. Toutes les autres politiques sont auto destructrices par nature, car elle conduisent à l'effondrement du système d'acheminement de l'Internet, et donc à la fragmentation (la partition) de l'Internet public.

Dans le contexte de l'Internet public actuel, les politiques d'allocation et de gestion d'adresses qui supposent une propriété sans restriction de l'adresse ont un impact extrêmement négatif sur l'adaptabilité du système d'acheminement de l'Internet. De telles politiques vont presque certainement épuiser la capacité d'adaptation du système d'acheminement de l'Internet bien avant que l'on s'approche de l'épuisement de l'espace d'adresses IPv4 et avant qu'on puisse faire un usage efficace de l'espace d'adresses IPv6. Étant donné le taux de croissance de l'Internet et les technologies en cours, l'idée que chacun puisse posséder son espace d'adresse et recevoir des services d'acheminement à l'échelle de l'Internet, quel que soit l'endroit

où il se connecte à l'Internet, est actuellement techniquement infaisable. Donc, le présent document fait deux recommandations. D'abord, que la politique de "prêt d'adresse" devrait être formellement ajoutée à l'ensemble des politiques d'allocation d'adresses dans l'Internet public. Ensuite, que les organisations qui ne présentent pas un degré suffisant d'agrégation d'informations d'acheminement pour obtenir l'accès aux services d'acheminement de l'Internet soient fortement encouragées à utiliser cette politique pour obtenir l'accès aux services.

Comme l'architecture actuelle d'allocation des adresses IPv6 se fonde sur CIDR, les recommandations présentées dans ce document s'appliquent aussi aux politiques d'allocation et de gestion des adresses IPv6s.

8. Considérations pour la sécurité

La dénumérotation d'un site a plusieurs implications possibles sur les politiques de sécurité à la fois du site lui-même et des sites qui communiquent régulièrement avec les sites dénumérotés.

De nombreux sites utilisent actuellement des systèmes de "pare-feu" pour fournir un contrôle d'accès grossier à ce qui vient des réseaux externes, tels que l'Internet, à leurs systèmes internes. De tels pare-feu peuvent comporter des décisions de contrôle d'accès fondées sur l'adresse de source revendiquée par les paquets qui arrivent sur de tels systèmes de pare-feu. Lorsque la politique du pare-feu se rapporte aux paquets qui arrivent sur le pare-feu en provenance de l'intérieur du site, le pare-feu devra alors être reconfiguré en même temps que le site est lui-même renuméroté. Lorsque la politique du pare-feu se rapporte aux paquets qui arrivent au pare-feu de l'extérieur du site, ces pare-feu doivent alors être reconfigurés chaque fois qu'est dénuméroté un site extérieur auquel l'accès à l'intérieur du site est accordé au travers du pare-feu.

Il est fortement conseillé de s'appuyer sur des adresses IP de source ou de destination authentifiées pour les décisions de politique de sécurité [Bellovin89]. Le déguisement d'adresses IP n'est pas difficile avec des systèmes largement disponibles, tels que les ordinateurs individuels. Une meilleure approche impliquerait probablement l'utilisation des techniques de sécurité IP, telles que l'en-tête d'authentification IP [RFC1826] ou l'encapsulation IP de charge utile de sécurité [RFC1827], au pare-feu, de sorte que le pare-feu puisse s'appuyer sur des techniques cryptographiques pour l'identification lors de la prise de ses décisions de politique de sécurité.

Il est extrêmement souhaitable que l'authentification soit présente dans tous les mécanismes utilisés pour dénuméroter les nœuds IP. Un mécanisme de dénumérotation qui n'aurait pas l'authentification pourrait être utilisé par un adversaire, par exemple pour dénuméroter des systèmes qui ne devraient pas l'être.

Il peut y avoir d'autre considérations pour la sécurité qui ne sont pas couvertes dans ce document.

9. Remerciements

Le présent document emprunte largement à divers envois sur plusieurs listes de diffusion. Des remerciements particuliers vont à Noel Chiappa, Dennis Ferguson, Eric Fleischman, Geoff Huston, et Jon Postel dont les envois ont été utilisés dans ce document.

La plus grande partie du paragraphe 5.3 est la contribution de Curtis Villamizar. La section sur la sécurité est la contribution de Ran Atkinson.

Nos remerciements à Scott Bradner, Randy Bush, Brian Carpenter, Noel Chiappa, David Conrad, John Curran, Sean Doran, Dorian Kim, Thomas Narten, Andrew Partan, Dave Piscitello, Simon Poole, Curtis Villamizar, et Nicolas Williams pour leur relecture, leurs commentaires, et leurs contributions à ce document.

Enfin, nous tenons à remercier les membres du groupe de travail CIDR pour leur relecture et leurs commentaires.

9. Références

[Bellovin89] Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Vol. 19, n° 2, mars 1989.

[Kleinrock 77] Kleinrock, L., and K. Farouk, K., "Hierarchical Routing for Large Networks," Computer Networks 1 (1977), North-Holland Publishing Company.

[Partan 95] Partan, A., communications privées, octobre 1995.

[RFC1541] R. Droms, "Protocole de configuration dynamique d'hôte", octobre 1993. *(P.S., remplacée par la RFC2131)*

[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 RFC4632)*

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

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

[RFC1826] R. Atkinson, "En-tête d'authentification IP", août 1995. *(Rendue obsolète par la RFC2402)*

[RFC1827] R. Atkinson, "Encapsulation dans IP de charge utile de sécurité (ESP)", août 1995. *(Obsolète, voir RFC2406)*

[Villamizar 95] Villamizar, C., communications privées, octobre 1995.

10. Adresse des auteurs

Yakov Rekhter
cisco Systems, Inc.
170 Tasman Dr.
San Jose, CA 95134
téléphone : (914) 528-0090
mél : yakov@cisco.com

Tony Li
cisco Systems, Inc.
170 Tasman Dr.
San Jose, CA 95134
téléphone : (408) 526-8186
mél : tli@cisco.com