Groupe de travail Réseau
Request for Comments : 1918
BCP : 5
RFC rendues obsolètes : 1627, 1597
Catégorie : Bonnes pratiques actuelles
Traduction Thomas PEDOUSSAUT / Ingénieur EISTI / octobre 1998

Y. Rekhter, Cisco Systems
B. Moskowitz, Chrysler Corp.
D. Karrenberg, RIPE NCC
G. J. de Groot, RIPE NCC
E. Lear, Silicon Graphics, Inc.
février 1996

Allocation d'adresse pour Internets privés

Statut de ce mémoire
Ce document spécifie les bonnes pratiques actuelles sur l'Internet pour la communauté de l'Internet, et demande des discussions et suggestions pour son amélioration. La diffusion de ce mémoire est libre.

1. Introduction

Pour le contexte de ce document, une entreprise est une entité autonome, exploitant un réseau utilisant TCP/IP et en particulier définissant un plan d'adressage et assignant ces adresses sur ce réseau.

Ce document décrit l'allocation d'adresses pour des réseaux privés. Cette allocation permet une connexité de toutes les couches réseau entre toutes les machines à l'intérieur de l'entreprise ainsi que vers des machines publiques de différentes entreprises. Le coût d'utilisation d'adresses dans des plages publiques est égal au coût potentiel de renumérotation des machines et des réseaux entre le public et le privé.

2. Motivation

Avec la prolifération de la technologie TCP/IP à travers le monde, même en dehors de l'Internet lui même, un nombre croissant d'entreprises non connectées utilisent cette technologie et ses capacités d'adressage pour des besoins de communication uniquement intra-entreprise, sans jamais l'intention de se connecter à d'autres entreprises ni à l'Internet lui-même.

L'Internet a crû au delà de toutes les prévisions. Cette croissance exponentielle constante amène de nouveaux défis. Un de ceux-ci concerne toute la communauté informatique : l'attribution intégrale de cet espace d'adressage unique.

Un autre défi un peu différent est la charge des tables de routage qui croit au delà des possibilités des Fournisseurs d'Accès à l'Internet (FAI). Des efforts sont faits par la communauté internaute pour trouver des solutions à long terme pour ces deux problèmes. De toutes façons, il est nécessaire de revoir les procédures d'allocation d'adresses et leur impact sur le système de routage d'Internet.

Pour contenir la croissance des tables de routage, un fournisseur d'accès demande un bloc d'adresses à un organisme d'enregistrement, et en réattribue à l'intérieur de ce bloc, selon les besoins de ses clients. Le résultat est que les routes vers plusieurs clients peuvent être agrégées ensemble et apparaîtront pour les autres fournisseurs comme une seule route [RFC1518], [RFC1519]. Pour que l'agrégation des routes soit efficace, les FAI (Fournisseurs d'accès Internet) encouragent leurs clients qui rejoignent leur réseaux d'utiliser une plage du bloc du FAI, et par là-même renuméroter leurs machines. De tels encouragements peuvent devenir des obligations dans le futur.

Avec la taille actuelle de l'Internet et son rythme de croissance, il n'est plus réaliste de croire que grâce aux vertus de l'obtention d'adresses IP uniques de la part d'un organisme d'enregistrement, une organisation qui acquiert de telles adresses pourra avoir une connexité IP sur tout l'Internet lorsque cette organisation sera elle-même connectée à Internet. Au contraire, il est plus probable que lorsque l'organisation se connectera à l'Internet pour réaliser la connexité IP sur tout l'Internet, l'organisation devra changer d'adresse IP (renuméroter) toutes ses machines publiques (qui ont besoin de se connecter à l'Internet) en fonction de l'unicité globale ou non des adresses utilisées initialement par l'organisation.

Il a été typique d'assigner des adresses globalement uniques à toutes les machines qui utilisent TCP/IP. Pour pouvoir étendre la durée de vie de l'adressage IPv4, les organismes d'enregistrement demandent beaucoup plus de justifications qu'auparavant, rendant la tâche plus difficile à des organisations pour acquérir un espace d'adressage supplémentaire [RFC1466].

Les machines de l'entreprise qui utilisent TCP/IP peuvent être divisées en 3 catégories :

Catégorie 1 :
les machines qui n'ont pas besoin d'accéder à des machines d'autres entreprises ou à l'Internet dans son ensemble. Les

machines de cette catégorie peuvent utiliser des adresses IP qui sont uniques dans l'entreprise, mais qui peuvent être ambiguës entre différentes entreprises.

Catégorie 2 :
les machines qui ont besoin d'accéder à un nombre limité de services extérieurs (ex: E-Mail, WWW, FTP, remote login) qui peuvent être servis par des passerelles applicatives. Pour beaucoup de machines dans cette catégorie, un accès non restreint (fourni par la connexité IP) n'est pas forcément nécessaire et même quelque fois non désiré pour des raisons de sécurité. Pour les mêmes raisons que pour les machines de la première catégorie, de telles machines peuvent utiliser des adresses IP uniques dans l'entreprise, mais qui peuvent être ambiguës entre différentes entreprises.

Catégorie 3 :
les machines qui ont besoin d'un accès réseau à l'extérieur de l'entreprise (fourni par la connexité IP). Les machines de cette dernière catégorie ont besoin d'une adresse unique sur tout l'Internet.

Nous parlerons des machines des catégories 1 et 2 comme de machines "privées", et de celles de la 3eme catégorie comme de machines "publiques".

Beaucoup d'applications n'ont besoin de connectivité qu'à l'intérieur de l'entreprise et n'ont pas besoin de connexité extérieure (à l'entreprise). Dans de grandes entreprises, il est souvent facile d'identifier un nombre important de machines utilisant TCP/IP qui n'ont pas besoin de connexité à l'extérieur de l'entreprise.

Quelques exemples, où la connexité extérieure n'est pas obligatoire :

Un grand aéroport qui possède des écrans d'affichage d'Arrivée/Départ utilisant TCP/IP. Il n'est absolument pas souhaitable que ces écrans soient accessibles directement depuis d'autres réseaux.

De grandes organisations comme des banques ou des chaines de location de voitures basculent vers TCP/IP pour leur communication. Un grand nombre de stations de travail comme des caisses automatiques, des distributeurs de billets, ou des postes de courtage ont rarement besoin d'une telle connexité.

Pour des raisons de sécurité, beaucoup d'entreprises utilisent des passerelles applicatives pour connecter leur réseau interne à l'Internet. Le réseau interne n'a souvent aucun accès direct à l'Internet, c'est pourquoi seulement une ou plusieurs passerelles sont visibles depuis l'Internet. Dans ce cas, le réseau interne peu utiliser des adresses IP non globales.

Les interfaces des routeurs sur un réseau interne n'ont souvent pas besoin d'être directement accessibles depuis l'extérieur de l'entreprise.

3. Espace d'adresses privées

L'Autorité d'Affectation de Numéros sur Internet (IANA) a réservé les 3 blocs suivants dans l'espace d'adressage pour des réseaux internes :

10.0.0.0 - 10.255.255.255 (préfixe 10/8)

172.16.0.0 - 172.31.255.255 (préfixe 172.16/12)

192.168.0.0 - 192.168.255.255 (préfixe 192.168/16)

Nous parlerons du premier bloc comme le bloc de 24 bits, le second comme celui de 20 bits, et du troisième comme le bloc de 16 bits. Notez (en notation pré-CIDR) que le premier bloc n'est rien d'autre qu'une classe A, le second, un ensemble de 16 classes B contiguës et le troisième, un ensemble de 256 classes C contiguës.

Une entreprise qui décide d'utiliser des adresses à l'intérieur des plages spécifiées dans ce document peut le faire sans en référer à l'IANA ni à un organisme d'enregistrement. L'espace ainsi défini peut être simultanément utilisé par de nombreuses entreprises. Les adresses dans ces plages ne seront uniques qu'à l'intérieur de l'entreprise, ou du groupe d'entreprises qui décident de se mettre d'accord sur cet espace d'adressage pour être capables de communiquer ensemble dans leur propre inter-réseau.

Comme précédemment, toute entreprise qui a besoin de plages d'adresses mondialement uniques doit en faire la demande auprès des organismes d'enregistrement. Une entreprise qui demande des adresses pour sa connexité externe ne se les verra jamais attribuer dans les plages ci-dessus.

Pour pouvoir utiliser les plages d'adresses privées, une entreprise doit déterminer quelles machines n'ont pas, et n'auront pas dans un futur proche, besoin d'une connexité à l'extérieur de l'entreprise et pourront être qualifiées de privées. De telles machines utiliseront l'espace d'adressage ci-dessus. Les machines privées peuvent communiquer avec toutes les autres machines de l'entreprise, à la fois publiques et privées. Néanmoins, elles ne peuvent avoir de connexité IP avec une machine à l'extérieur de l'entreprise. Même si elles n'ont pas de connexité IP vers l'extérieur, les machines privées peuvent toutefois avoir accès à des services extérieurs grâce à des passerelles (ex passerelles applicatives).

Toutes les autres machines seront publiques et utiliseront l'espace d'adressage unique global assigné par un service

d'enregistrement. Les machines publiques peuvent communiquer avec d'autres machines privées ou publiques à l'intérieur de l'entreprise et possèdent une connexité IP avec les machines publiques extérieures à l'entreprise. Les machines publiques n'ont pas de connexité avec des machines privées d'autres entreprises.

Passer une machine du statut privé au public ou vice-versa implique le changement de l'adresse IP, de l'entrée correspondante dans les DNS et des fichiers de configuration des différentes machines accédant à celle ci par adresse IP.

Comme les adresses privées n'ont aucune signification globale, les informations de routage ne doivent pas être propagées sur des liens inter-entreprises, et les paquets ayant de telles adresses source ou destination ne doivent pas être envoyés sur de tels liens. Les routeurs sur des réseaux n'utilisant pas d'espace d'adressage privé, plus spécialement ceux des FAI, doivent être configurés pour rejeter (filtre sortant) les informations de routage concernant les réseaux privés. Si un routeur de la sorte reçoit un tel paquet, il ne doit être traité comme une erreur de protocole de routage.

Des références indirectes à de telles adresses doivent être maintenues à l'intérieur de l'entreprise. Des exemples typiques sont les enregistrements DNS ou d'autres informations se référant aux adresses privées internes. En particulier, les FAI doivent prendre des mesures pour éviter de telles fuites.

4. Avantages et inconvénients de l'utilisation d'espace d'adressage privé

L'avantage évident de l'adressage privé pour l'Internet est la protection conservatoire de l'espace d'adressage global en ne l'utilisant pas là où l'unicité globale n'est pas requise.

Les entreprises elles mêmes se réjouissent des nombreux avantages de l'utilisation d'espace d'adressage privé. Elles gagnent en flexibilité dans l'architecture du réseau en ayant un espace d'adressage à leur disposition plus grand que celui qu'elles auraient pu obtenir par une plage unique. Cela permet des schémas d'adressage conformes aux préoccupations administratives et opérationnelles ainsi qu'une croissance plus facile des zones.

Pour différentes raisons, l'Internet a déjà été confronté à des situations où une entreprise qui n'a pas été connectée à l'Internet utilisait un espace d'adressage IP pour ses machines sans que celui-ci lui ait été assigné par l'IANA. Dans quelques cas, cet espace avait déjà été assigné à une autre entreprise. Si une telle entreprise veut plus tard se connecter à l'Internet, cela peut créer de sérieux problèmes, car le routage IP ne peut fonctionner correctement en présence d'adresses ambiguës. De toute façon, en principe, les FAI se prémunissent de telles erreurs en mettant en œuvre des filtres sur les routes, même si cela n'est pas toujours le cas dans la pratique. L'utilisation d'espaces d'adressage privés est un choix sécurisant pour de telles entreprises, empêchant les problèmes une fois que la connexité externe devient nécessaire.

Un principal inconvénient dans l'utilisation de l'adressage privé est la réduction de la flexibilité dans l'accès de l'entreprise à l'Internet.

Une fois validée l'utilisation d'adresses privées, c'est la renumérotation d'une partie ou la totalité de l'entreprise qui est validée si l'on décide de fournir la connexité IP entre cette partie (ou toute l'entreprise) et l'Internet. Habituellement, le coût de la renumérotation peut être mesuré par le nombre de machines devant passer du domaine privé au public. Néanmoins, comme nous en avons discuté précédemment, même si un réseau utilise des adresses uniques globales, il faudra de toute façon renuméroter pour obtenir la connexité IP sur tout l'Internet.

Un autre inconvénient à l'utilisation d'espace d'adressage privé apparait lorsque l'entreprise connecte son réseau avec ceux d'autres entreprises en un seul inter-réseau. Il y a alors le risque d'avoir à renuméroter. En regardant les exemples que nous avons vus en section 2, les entreprises tendent à fusionner. Si, avant la fusion, ces entreprises entretenaient une certaine cohérence en utilisant des espaces d'adressage privés, et veulent après la fusion combiner leurs réseaux en un seul inter-réseau, certaines adresses dans ces réseaux risquent de ne plus être uniques. Le résultat est l'obligation de renuméroter ces machines.

Le coût de la renumérotation peut être atténué par le développement et l'utilisation d'outils qui facilitent la renumérotation (par exemple, Dynamic Host Configuration Protocol (DHCP)). Lors de la décision d'utiliser des classes d'adresses privées, nous recommandons d'interroger les vendeurs de matériel et de logiciel sur la disponibilité de tels outils. Un groupe de l'IETF (groupe de travail PIER) produit une documentation sur les prérequis et les procédures pour la renumérotation.

5. Considérations opératoires

Une stratégie possible est de concevoir la partie privée du réseau en premier et d'utiliser l'adressage privé pour tous les liens internes. Ensuite, planifier les sous-réseaux publics là où cela est requis et concevoir la connexité externe.

Cette conception n'a pas besoin d'être fixée une fois pour toutes. Si un groupe de machine doit changer de statut (de privé vers public ou vice-versa) par la suite, cela peut être fait en ne renumérotant que les machines impliquées et en changeant la

connexité si besoin est. Dans les endroits où de tels changements sont à prévoir (salles machines) il est conseillé de prévoir des médiums physiques séparés pour les réseaux publiques et privés afin de faciliter l'opération. Pour éviter d'importantes interruptions du réseau, il est conseillé de grouper sur un même brin des machines ayant le même profil de connexité.

Si un plan de découpage en sous-réseaux acceptable peut être conçu et supporté par le matériel, il est conseillé d'utiliser le bloc de 24 bits (classe A) de l'espace d'adressage privé et de faire un plan d'adressage avec une bonne capacité d'évolution. Si le découpage en sous réseaux est un problème, le bloc de 16 bits (réseaux de classe C) ou celui de 20 bits (réseaux de classe B) peut aussi être utilisé pour l'adressage.

On peut être tenté d'avoir à la fois des adresses publiques et privées sur le même médium physique. Bien que cela soit possible, il y a des limitations à une telle architecture (notez que les limitations n'ont rien à voir avec les adresses privées, mais sont dues à la présence de plusieurs sous-réseaux IP sur le même brin physique). Nous vous conseillons la prudence en procédant de la sorte.

Il est fortement recommandé que les routeurs connectant l'entreprise aux réseaux extérieurs soient configurés avec des filtres appropriés sur les paquets et le routage aux deux extrémités afin de se prémunir contre la fuite de paquets et de routes. Une entreprise doit aussi filtrer les informations de routage entrantes concernant des réseaux privés pour se protéger elle-même de situations de routage ambiguës qui peuvent survenir lorsque des routes vers l'espace d'adressage privé pointent vers l'extérieur de l'entreprise.

Il est possible pour deux sites qui coordonnent leur espace privé d'adressage de communiquer ensemble au travers d'un réseau public. Pour ce faire, ils doivent utiliser une méthode d'encapsulation à leur frontière avec le réseau public, pour préserver leurs adresses privées.

Si deux (ou plus) organisations suivent les plans d'adressage spécifiés ci-dessus et veulent par la suite établir une connexité IP les unes avec les autres, il y a un risque d'ambiguïté dans les adresses. Pour minimiser le risque, il est fortement conseillé qu'une organisation utilisant l'adressage privé choisisse une plage aléatoire dans cet espace, lorsqu'elle alloue des sous-blocs.

Si une entreprise utilise l'espace d'adressage privé, ou un mélange privé/public, alors les DNS secondaires, à l'extérieur de l'entreprise, ne doivent pas voir d'adresses appartenant à l'adressage privé car celles-ci sont ambiguës (ou ont quelques chances de l'être). Une façon de s'assurer de cela est de faire tourner deux serveurs de noms de domaines "autorisés" pour chaque zone contenant des adresses publiques et privées. Un serveur, visible depuis l'extérieur et ne servant que les adresses joignables depuis l'extérieur. Le deuxième, uniquement accessible depuis l'intérieur et servant la totalité des données, y compris les adresses privées et les adresses publiques accessibles depuis le réseau privé. Pour assurer la cohérence, les deux serveurs doivent être configurés à partir des mêmes données. Ces possibilités ajoutent un certain degré de complexité.

6. Considérations de sécurité

Les fonctions de sécurité ne sont pas traitées dans ce mémoire.

7. Conclusion

Selon le schéma expliqué ci-dessus, de grandes entreprises n'ont besoin finalement que d'un relativement petit bloc d'adresses publiques issues de l'espace d'adressage global. L'Internet dans son ensemble bénéficie de la préservation de l'espace d'adressage global qui permet d'accroître la durée de vie d'IPv4. L'entreprise bénéficie d'une flexibilité plus grande apportée par l'espace d'adressage relativement grand des plages d'adresses privées. Néanmoins, l'utilisation de l'adressage privé requiert que l'organisation change une partie de son adressage lorsque ses besoins de connexion changent.

8. Remerciements

Nous voulons remercier Tony Bates (MCI), Jordan Becker (ANS), Hans-WernerBraun (SDSC), Ross Callon (BayNetworks), John Curran (BBN Planet), Vince Fuller(BBN Planet), Tony Li (cisco Systems), Anne Lord (RIPE NCC), Milo Medin (NSI),Marten Terpstra (BayNetworks), Geza Turchanyi (RIPE NCC), Christophe Wolfhugel(Pasteur Institute), Andy Linton (connect.com.au), Brian Carpenter (CERN),Randy Bush (PSG), Erik Fair (Apple Computer), Dave Crocker (BrandenburgConsulting), Tom Kessler (SGI), Dave Piscitello (Core Competence), MattCrawford (FNAL), Michael Patton (BBN), et Paul Vixie (Internet SoftwareConsortium) pour leur relecture et commentaires constructifs.

9. Références

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

[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 RFC4632)*

10. Adresses des auteurs

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

Robert G Moskowitz
Chrysler Corporation
CIMS: 424-73-00
25999 Lawrence Ave
Center Line, MI 48015
téléphone : +1 810 758 8212
Fax: +1 810 758 8173
mél : rgm3@is.chrysler.com

Daniel Karrenberg
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam,
the Netherlands
téléphone : +31 20 592 5065
Fax: +31 20 592 5090
mél : Daniel.Karrenberg@ripe.net

Geert Jan de Groot
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam,
the Netherlands
téléphone : +31 20 592 5065
Fax: +31 20 592 5090
mél : GeertJan.deGroot@ripe.net

Eliot Lear
Mail Stop 15-730
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA 94043-1389
téléphone : +1 415 960 1980
Fax : +1 415 961 9584
mél : lear@sgi.com