Groupe de travail Réseau
Request for Comments : 4632
BCP : 122
RRC rendue obsolète : 1519
Catégorie : Bonnes pratiques actuelles

V. Fuller, Cisco Systems
T. Li, Tropos Networks
août 2006

Traduction Claude Brière de L'Isle

Acheminement inter domaine sans classe (CIDR) : Plan d'allocation et d'agrégation des adresses Internet

Résumé
Le présent mémoire expose la stratégie pour l'allocation d'adresse de l'espace d'adresses IPv4 à 32 bits existant en vue de conserver l'espace d'adresses et de limiter le taux de croissance de l'état d'acheminement global. Le présent document rend obsolète la spécification originale d'acheminement inter domaine sans classe (CIDR, *Classless Inter-domain Routing*) de la RFC 1519, avec des changements apportés à la fois pour préciser les concepts introduits, et après plus de douze ans, de mettre à jour les informations de la communauté de l'Internet sur les résultats du déploiement de la technologie décrite.

Table des Matières

1. Introduction

Le présent mémoire expose la stratégie d'allocation des adresses de l'espace d'adresses IPv4 de 32 bits existant en vue de conserver l'espace d'adresses et limiter le taux de croissance de l'état d'acheminement. Le présent document rend obsolète la spécification CIDR d'origine [RFC1519], avec les changements faits à la fois pour préciser les concepts qu'elle

introduisait et, après plus de douze années, d'informer la communauté de l'Internet sur les résultat du déploiement de la technologie décrite.

2. Histoire et description du problème

Ce qui est connu aujourd'hui comme l'Internet a commencé par un projet de recherche dans les années 1970 pour concevoir et développer un ensemble de protocoles qui pourraient être utilisés avec de nombreuses technologies de réseau différentes pour fournir une facilité de bout en bout sans interruption pour interconnecter un ensemble divers de systèmes d'extrémité. Lorsque on a déterminé comment l'espace d'adresses de 32 bits serait utilisé, certaines hypothèses ont été faites sur le nombre d'organisations à connecter, sur le nombre de systèmes d'extrémité par organisation, et le nombre total de systèmes d'extrémité du réseau. Le résultat final a été l'établissement (voir la [RFC0791]) de trois classes de réseaux : Classe A (avec les bits de poids fort de l'adresse à '00'), avec 128 réseaux possibles chacun et 16 777 216 systèmes d'extrémité (moins les valeurs de bit spéciales réservées pour les adresses de réseau/diffusion) ; Classe B (MSB '10') avec 16 384 réseaux possibles chacune avec 65 536 systèmes d'extrémité (moins les valeurs réservées) et Classe C (MSB '110'), et 2 097 152 réseaux possibles chacun et 254 systèmes d'extrémité (256 combinaisons binaires moins les schémas réservés tout à zéro et tout à un). L'ensemble des adresses avec le MSB '111' était réservé pour des utilisations futures ; des parties en ont finalement été définies (MSB '1110') pour l'utilisation de la diffusion groupée IPv4 et d'autres parties sont toujours réservées au moment de la rédaction du présent document.

À la fin des années 1980, l'expansion et la commercialisation de l'ancien réseau de recherche résultait en la connexion de nombreuses nouvelles organisations à l'Internet en croissance rapide, et chaque nouvelle organisation exigeait une adresse allouée dans le plan d'adressage de classes A/B/C. Comme la demande de nouveaux numéros de réseau (en particulier dans l'espace de classe B) prenait ce qui paraissait un taux de croissance exponentiel, certains membres de la communauté du fonctionnement et de l'ingénierie ont déclaré avoir des soucis avec les propriétés d'adaptation à long terme du système de classes A/B/C et ont commencé à réfléchir à la façon de modifier la politique d'allocation des numéros de réseau et les protocoles d'acheminement pour s'accommoder de la croissance. En novembre 1991, l'équipe d'ingénierie de l'Internet (IETF, *Internet Engineering Task Force*) a créé le groupe acheminement et adressage (ROAD, *Routing and Addressing*) pour examiner la situation. Ce groupe s'est réuni en janvier 1992 et a identifié trois problèmes majeurs :

1. Épuisement de l'espace d'adresses réseau de classe B. Une cause fondamentale de ce problème est le manque d'une classe de réseau d'une taille appropriée pour les organisations de taille moyenne. La classe C, avec un maximum de 254 adresses d'hôtes, est trop petite, tandis que la classe B, qui permet jusqu'à 65 534 adresses d'hôtes, est trop grande pour la plupart des organisations mais était la meilleure disponible pour l'utilisation avec le sous réseautage.

2. La croissance des tableaux d'acheminement dans les routeurs de l'Internet au delà de la capacité des logiciels, matériels et personnels actuels, et au delà de ce qu'il est possible de gérer efficacement.

3. L'épuisement éventuel de l'espace d'adresses IPv4 de 32 bits.
   Il était clair que les taux de croissance de l'Internet d'alors allaient donner aux deux premiers problèmes un caractère critique quelque part entre 1993 et 1995. Les travaux déjà engagés sur l'allocation topologique de l'adressage pour le service réseau sans connexion (CLNS, *Connectionless Network Service*) qui a été présenté à la communauté à la réunion de Boulder de l'IETF en décembre 1990, ont conduit à réfléchir sur la façon de restructurer l'espace d'adresses IPv4 de 32 bits pour accroître sa durée de vie. Les travaux du groupe ROAD ont suivi et ont finalement résulté en la publication de la [RFC1338], et ensuite de la [RFC1519].

La conception et le déploiement de CIDR étaient destinés à résoudre ces problèmes en fournissant un mécanisme pour ralentir la croissance des tableaux d'acheminement mondial et réduire le taux de consommation de l'espace d'adresses IPv4. Ils ne tentaient pas de résoudre le troisième problème, qui est à plus long terme par nature ; à la place, ils s'efforçaient de faciliter suffisamment les difficultés à court et moyen terme pour permettre à l'Internet de continuer à fonctionner efficacement pendant que des progrès seraient faits sur une solution à plus long terme.

On trouvera plus de détails sur les fondements historiques de cet effort et sur le groupe ROAD dans la [RFC1380] et dans [LWRD].

3. La solution de l'adressage sans classe

La solution que la communauté a créée était de déconseiller le système d'allocation d'adresses réseau de classes A/B/C en faveur de l'utilisation de blocs hiérarchiques "sans classes" d'adresses IP (en s'y référant comme à des préfixes). L'allocation des préfixes est destinée à suivre en gros la topologie sous-jacente de l'Internet afin que l'agrégation puisse être utilisée pour faciliter l'adaptation du système d'acheminement mondial. Une implication de cette stratégie est que

l'allocation et l'agrégation de préfixes sont généralement faites suivant les relations fournisseur-abonné, car c'est ainsi que la topologie de l'Internet est déterminée.

Lorsque il fut à l'origine proposé dans les [RFC1338] et [RFC1519], ce plan d'adressage était destiné à être une réponse à relativement court terme, durant approximativement trois ou cinq ans, pendant lesquels une architecture plus permanente d'adressage et d'acheminement serait conçue et mise en œuvre. Comme on peut le déduire des dates des documents d'origine, CIDR a de beaucoup dépassé sa durée de vie prévue et est devenu la solution à moyen terme aux problèmes décrits plus haut.

Noter que dans le texte qui suit, on décrit les politiques et procédures actuelles qui ont été mises en place pour mettre en œuvre l'architecture d'allocation qu'on expose ici. Cette description n'est pas destinée à être interprétée comme des directives à l'IANA.

Couplé avec les stratégies de gestion des adresses mises en œuvre par les registraires régionaux de l'Internet (voir [NRO] pour les détails) le déploiement de l'adressage de style CIDR a aussi réduit le taux de consommation de l'espace d'adresses IPv4, fournissant ainsi un répit à court et moyen terme au problème n° 3, décrit plus haut.

Noter que comme on l'a défini, ce plan n'exige ni ne suppose la réallocation des parties du vieil espace de "classe C" qui n'étaient pas amendables pour l'agrégation (parfois appelé "le marais"). Faire ainsi devrait quelque peu réduire les tailles de tableau d'acheminement (les estimations courantes disent que "le marais" contient approximativement 15 000 entrées) bien qu'à un coût significatif de dénumérotage. De même, il n'y a pas d'exigence forte qu'aucun site d'extrémité soit dénuméroté lorsque il change de fournisseur de service de transit, mais les sites d'extrémité sont invités à le faire pour éliminer le besoin d'une annonce explicite de leurs préfixes dans le système d'acheminement mondial.

3.1 Concept de base et notation de préfixe

Au sens le plus simple, le changement des numéros de réseau en classes A/B/C aux préfixes sans classe est de rendre explicite quels bits dans une adresse IPv4 de 32 bits sont interprétés comme le numéro (ou préfixe) de réseau associé à un site et lesquels sont utilisés pour numéroter les systèmes d'extrémité individuels au sein du site. Dans la notation CIDR, un préfixe se présente comme une quantité de quatre octets, tout comme une adresse IPv4 traditionnelle ou un numéro de réseau, suivi par le caractère "/" (barre oblique) suivi par une valeur décimale entre 0 et 32 qui décrit le nombre de bits significatifs. Par exemple, le réseau traditionnel de "classe B" 172.16.0.0, avec un gabarit de réseau implicite de 255.255.0.0, est défini comme le préfixe 172.16.0.0/16, le "/16" indiquant que le gabarit pour extraire la portion réseau du préfixe est une valeur de 32 bits où les 16 bits de poids fort sont des uns et les 16 bits de moindre poids sont des zéros. De même, le numéro de réseau traditionnel de "classe C" 192.168.99.0 est défini comme le préfixe 192.168.99.0/24 ; les 24 bits de poids fort sont des uns et les 8 bits de moindre poids sont des zéros.

L'utilisation des préfixes sans classe avec des longueurs explicites de préfixe permet une correspondance plus souple des blocs de l'espace d'adresse avec les besoins réels. Alors qu'auparavant seules trois tailles de réseau étaient disponibles, des préfixes peuvent être définis pour décrire un bloc d'une taille de toute puissance de deux entre une et 2^32 adresses de système d'extrémité. En pratique, le réservoir d'adresses non allouées est administré par l'autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) [IANA]. L'IANA fait les allocations à partir de ce réservoir aux registraires régionaux de l'Internet, comme nécessaire. Ces allocations sont faites en blocs contigus alignés sur le bit de 2^24 adresses (autrement dit des préfixes /8). Les registraires régionaux de l'Internet (RIR, *Regional Internet Registries*) allouent à leur tour ou affectent de plus petits blocs d'adresses aux registraires locaux de l'Internet (LIR, *Local Internet Registry*) ou aux fournisseurs d'accès Internet (FAI). Ces entités peuvent faire un usage direct de l'allocation (comme ce sera couramment le cas pour un FAI) ou faire des sous allocations des adresses à leurs abonnés. Ces allocations d'adresses aux RIR varient selon les besoins de chaque FAI ou LIR. Par exemple, un grand FAI peut se voir allouer un bloc d'adresses de 2^17 adresses (un préfixe /15) tandis qu'un plus petit FAI va recevoir un bloc d'adresses de 2^11 adresses (un préfixe / 21).

Noter que les termes "allouer" et "affecter" ont une signification spécifique dans le système des registres d'adresse de l'Internet ; "allouer" se réfère à la délégation d'un espace de blocs d'adresses à une organisation qui est supposée effectuer ensuite des sous délégations, et "affecter" est utilisé pour les sites qui utilisent directement (c'est-à-dire, numérotent des hôtes individuels) le bloc d'adresses reçu.

Le tableau qui suit donne un raccourci pratique de toutes les tailles de préfixe CIDR, et montre le nombre d'adresses possibles dans chaque préfixe et le nombre de préfixes de cette taille qui peuvent être numérotés dans l'espace d'adresses IPv4 à 32 bits:

notation	adresse/bloc	nombre de blocs	
n.n.n.n/32	1	4 294 967 296	"chemin d'hôte"
n.n.n.x/31	2	2 147 483 648	"liaison d'homologue à homologue"
n.n.n.x/30	4	1 073 741 824	
n.n.n.x/29	8	536 870 912	
n.n.n.x/28	16	268 435 456	
n.n.n.x/27	32	134 217 728	
n.n.n.x/26	64	67 108 864	
n.n.n.x/25	128	33 554 432	
n.n.n.0/24	256	16 777 216	"Classe C" traditionnelle
n.n.x.0/23	512	8 388 608	
n.n.x.0/22	1024	4 194 304	
n.n.x.0/21	2048	2 097 152	
n.n.x.0/20	4096	1 048 576	
n.n.x.0/19	8192	524 288	
n.n.x.0/18	16 384	262 144	
n.n.x.0/17	32 768	131 072	
n.n.0.0/16	65 536	65 536	"Classe B" traditionnelle
n.x.0.0/15	131 072	32 768	
n.x.0.0/14	262 144	16 384	
n.x.0.0/13	524 288	8 192	
n.x.0.0/12	1 048 576	4 096	
n.x.0.0/11	2 097 152	2 048	
n.x.0.0/10	4 194 304	1 024	
n.x.0.0/9	8 388 608	512	
n.0.0.0/8	16 777 216	256	"Classe A" traditionnelle
x.0.0.0/7	33 554 432	128	
x.0.0.0/6	67 108 864	64	
x.0.0.0/5	134 217 728	32	
x.0.0.0/4	268 435 456	16	
x.0.0.0/3	536 870 912	8	
x.0.0.0/2	1 073 741 824	4	
x.0.0.0/1	2 147 483 648	2	
0.0.0.0/0	4294967296	1	"chemin par défaut"

n est une valeur d'octet décimale de huit bits. Les liaisons point à point sont discutées plus en détails dans la [RFC3021].

x est une valeur de 1 à 7 bits, selon la longueur de préfixe, qui se glisse dans les bits de poids fort de l'octet et est convertie en forme décimale ; les bits de moindre poids de l'octet sont des zéros.

En pratique, les préfixes de longueur inférieure à 8 n'ont pas été alloués ou affectés à ce jour, bien que des chemins pour des préfixes aussi courts puissent exister dans les tableaux d'acheminement si ou lorsque une agrégation agressive est effectuée. Au moment de la rédaction du présent document, aucun de ces chemins n'apparaît dans le système d'acheminement mondial, mais des erreurs d'opérateur et d'autres événements ont causé l'observation de certains d'entre eux (c'est-à-dire, 128.0.0.0/1 et 192.0.0.0/2) dans certains réseaux à une certaine époque.

4. Allocation d'adresse et agrégation d'acheminement

L'adressage et l'acheminement sans classe a été développé initialement pour améliorer les propriétés d'adaptabilité de l'acheminement sur l'Internet mondial. Parce que l'adaptabilité de l'acheminement est très étroitement liée à la façon dont les adresses sont utilisées, le déploiement de CIDR a des implications sur la façon dont les adresses sont affectées.

4.1 Efficacité et limitations de l'agrégation

La seule méthode couramment comprise pour réduire l'état d'acheminement sur un réseau à commutation par paquets est par l'agrégation des informations. Pour que CIDR réussisse à réduire la taille et le taux de croissance du système d'acheminement mondial, le processus d'affectation des adresses IPv4 avait besoin d'être changé pour rendre possible l'agrégation des informations d'acheminement le long des lignes topologiques. Comme, en général, la topologie du réseau est déterminée par les fournisseurs d'accès qui l'ont construit, des affectations d'adresses topologiquement significatives sont nécessairement centrées sur les fournisseurs d'accès.

L'agrégation est simple pour un site d'extrémité qui est connecté à un fournisseur d'accès : il utilise l'espace d'adresses affecté par son fournisseur d'accès, et cet espace d'adresses est une petite pièce d'un plus gros bloc alloué au fournisseur d'accès. Aucun chemin explicite n'est nécessaire pour le site d'extrémité ; le fournisseur d'accès annonce un seul chemin agrégé pour le plus grand bloc. Cette annonce assure l'accessibilité et la capacité à acheminer pour tous les abonnés numérotés dans le bloc.

Il y a deux situations, plus complexes, qui réduisent l'efficacité de l'agrégation :

- Une organisation qui est multi rattachements. Parce qu'une organisation multi rattachements doit être annoncée dans le système par chacun de ses fournisseurs d'accès, il n'est souvent pas possible d'agréger ses informations d'acheminement dans l'espace d'adresses d'aucun de ces fournisseurs. Noter que l'organisation reçoit quand même son affectation d'adresse dans l'espace d'adresses d'un fournisseur d'accès (ce qui a d'autres avantages) mais qu'un chemin vers le préfixe de l'organisation est, dans le cas le plus général, explicitement annoncé par tous ses fournisseurs d'accès. Pour cette raison, le coût de l'acheminement mondial pour une organisation multi rattachements est généralement le même qu'il était avant l'adoption du CIDR. On trouvera un examen plus détaillé des pratiques du multi rattachement dans la [RFC4116].

- Une organisation qui change de fournisseur d'accès mais n'est pas dénumérotée. Ceci a pour effet de "creuser un trou" dans une des annonces des chemins agrégés du fournisseur d'accès original. Le CIDR traite cette situation en exigeant que le nouveau fournisseur d'accès fasse une annonce spécifique pour l'organisation qui a le nouveau rattachement ; cette annonce est préférée aux agrégats de fournisseur parce que c'est une correspondance plus longue. Pour conserver l'efficacité de l'agrégation, il est recommandé qu'une organisation qui change de fournisseur d'accès prévoit éventuellement de migrer son réseau dans un préfixe affecté à partir de l'espace d'adresses de son nouveau fournisseur. À cette fin, il est recommandé que soient déployés des mécanismes pour faciliter une telle migration, comme une allocation dynamique d'adresse d'hôte qui utilise la [RFC2131]) chaque fois que possible, et qu'un travail supplémentaire sur le protocole soit fait pour développer une technologie améliorée pour la dénumérotation.

Noter qu'un gain d'efficacité d'agrégation peut quand même être obtenu pour les sites multi rattachements (et, en général, pour tout site composé de plusieurs réseaux logiques IPv4) en allouant au site un espace d'adresses d'un bloc d'une puissance de deux contiguës (par opposition à plusieurs préfixes indépendants) les informations d'acheminement du site peuvent être agrégées en un seul préfixe. Aussi, comme le coût d'acheminement associé à l'affectation à un site multi rattachements à partir de l'espace d'adresses d'un fournisseur d'accès n'est pas supérieur à celui de la vieille méthode d'affectation de numéros qui se suivent par une autorité centrale, il y a du sens à affecter tout l'espace d'adresses des sites d'extrémité à partir des blocs alloués aux fournisseurs d'accès.

Il vaut aussi la peine de mentionner que comme l'agrégation peut survenir à de multiples niveaux dans le système, il est encore possible d'agréger ces chemins atypiques à des niveaux plus élevés de toute hiérarchie qui pourrait être présente. Par exemple, si un site est multi rattachements sur deux fournisseurs relativement petits qui obtiennent tous deux la connexité et l'espace d'adresses du même grand fournisseur, l'agrégation par le grand fournisseur des chemins partant des plus petits réseaux va alors inclure tous les chemins vers le site multi rattachements. La faisabilité de cette sorte d'agrégation de second niveau dépend de l'existence d'une hiérarchie topologique parmi un site, de ses fournisseurs directement connectés, et des autres fournisseurs auxquels ils sont connectés ; cela peut être pratique dans certaines régions de l'Internet mondial mais pas dans d'autres.

Note : Dans la discussion et les exemples qui suivent, la notation de préfixes est utilisée pour représenter les destinations d'acheminement. C'est utilisé seulement à des fins d'illustration et n'exige pas que les protocoles d'acheminement utilisent cette représentation dans leurs mises à jour.

4.2 Allocation répartie de l'espace d'adresse

Dans les premiers jours de l'Internet, l'allocation de l'espace d'adresses IPv4 était effectuée par le centre d'informations central du réseau (NIC, *Network Information Center*). Les numéros de réseau de classe A/B/C étaient affectés dans un ordre essentiellement arbitraire, en gros , selon la taille de l'organisation qui les demandait. Toutes les affectations étaient enregistrées centralement, et rien n'était tenté pour affecter les numéros de réseau d'une manière qui pourrait permettre une agrégation de l'acheminement.

Lorsque le CIDR a été déployé à l'origine, l'autorité d'affectation centrale a continué d'exister mais a changé ses procédures pour affecter de larges blocs de numéros de réseau de "classe C" à chaque fournisseur d'accès. Ceux-ci à leur tour affectent des sous ensembles fondés sur le gabarit binaire de leur espace d'adresses à chaque abonné. Cela a fonctionné raisonnablement bien, tant que le nombre des fournisseurs d'accès était relativement faible et constant, mais cela ne s'est

pas bien adapté lorsque le nombre des fournisseurs d'accès s'est mis à augmenter rapidement.

Lorsque l'Internet s'est mis à s'étendre rapidement dans les années 1990, il est devenu clair qu'une seule autorité centralisée d'allocation des adresses était un problème. Cette fonction a commencé à être décentralisée lorsque l'allocation d'espace d'adresses pour les sites Internet européens fut déléguée en blocs en alignement binaire de 16 777 216 d'adresses (ce que CIDR définira plus tard comme un /8) au NCC RIPE ([RIPE]), en faisant effectivement le premier des RIR. Depuis lors, l'affectation d'adresse a été formellement répartie comme une fonction hiérarchique avec l'IANA, les RIR, et les fournisseurs d'accès. En retirant le goulot d'étranglement d'une seule organisation avec la responsabilité de l'espace d'adresses Internet mondial, on a grandement amélioré l'efficacité et le temps de réponse pour les nouvelles affectations.

La délégation hiérarchique des adresses de cette manière implique que les sites avec des adresses affectées à partir d'un certain fournisseur d'accès sont, pour les besoins de l'acheminement, incorporés dans ce fournisseur d'accès et seront acheminés via son infrastructure. Cela implique que les informations d'acheminement sur les organisations multi rattachements (c'est-à-dire, les organisations connectées à plus d'un fournisseur d'accès) vont toujours avoir besoin d'être connues par les niveaux supérieurs de la hiérarchie.

Une perspective historique ce ces questions est décrite dans la [RFC1518]. On pourra aussi trouver un exposé supplémentaire dans la [RFC3221].

5. Considérations sur la mise en œuvre de l'acheminement

Avec le changement des numéros de réseau à classes aux numéros à préfixes sans classes, il n'est plus possible de déduire le gabarit de réseau du schéma binaire initial d'une adresse IPv4. Cela a des implications sur la façon dont les informations d'acheminement sont mémorisées et propagées. Les gabarits de réseau ou les longueurs de préfixe doivent être explicitement portés dans les protocoles d'acheminement. Les protocoles d'acheminement intérieurs, comme OSPF [RFC2328], système intermédiaire à système intermédiaire (IS-IS) [RFC1195], RIPv2 [RFC2453], et protocole amélioré d'acheminement de passerelle intérieure (EIGRP) de Cisco, et le protocole d'acheminement extérieur BGP4 [RFC4271], prennent tous en charge cette fonctionnalité, ayant été développés ou modifiés au titre du déploiement de l'acheminement inter domaines sans classe durant les années 1990.

Les protocoles d'acheminement intérieur plus anciens comme RIP [RFC1058], HELLO, et le protocole d'acheminement de passerelle intérieure (IGRP) de Cisco, et de plus anciens protocoles d'acheminement extérieur, comme le protocole de passerelle extérieure (EGP) [RFC904], ne prennent pas en charge le portage explicite de la longueur/gabarit de préfixe et donc ne peuvent pas être effectivement utilisés sur l'Internet autrement que dans des configurations de bout très limitées. Bien que leur usage puisse être approprié dans des configurations de site d'extrémité traditionnelles, ils sont considérés comme obsolètes et NE DEVRAIENT PAS être utilisés dans les réseaux de transit connectés à l'Internet mondial.

De même, les tableaux d'acheminement et de transmission dans les équipements de réseau de couche 3 doivent être organisés pour mémoriser à la fois le préfixe et la longueur ou gabarit de préfixe. L'équipement qui organise ses informations d'acheminement/transmission conformément aux conventions traditionnelles de réseau/sous-réseau de classes A/B/C ne peut pas être supposé fonctionner correctement sur les réseaux connectés à l'Internet mondial ; l'utilisation de tels équipements n'est pas recommandée. Heureusement, très peu de ces équipements sont utilisés aujourd'hui.

5.1 Règles pour l'annonce d'acheminement

1. Dans l'Internet la transmission est faite sur la base de la plus longue correspondance. Cela implique que les destinations qui sont multi rattachement par rapport à un domaine d'acheminement doivent toujours être annoncées explicitement dans ce domaine d'acheminement (c'est-à-dire, elles ne peuvent pas être résumées). Si un réseau est multi rattachements, tous ses chemins dans un domaine d'acheminement qui sont "plus haut" dans la hiérarchie des réseaux doivent être connus du réseau "plus haut").

2. Un routeur qui génère un chemin agrégé pour plusieurs chemins plus spécifiques doit éliminer les paquets qui correspondent au chemin agrégé, mais à aucun des chemins plus spécifiques. En d'autre termes, le "prochain bond" pour le chemin agrégé devrait être la destination nulle. Ceci est nécessaire pour empêcher les transmissions en boucle lorsque certaines adresses couvertes par l'agrégat ne sont pas joignables.

Noter que durant une défaillance, un acheminement partiel du trafic pour un site qui tire son espace d'adresse d'un fournisseur d'accès mais qui n'est en fait joignable que par un autre (c'est-à-dire, le cas d'un site qui a changé de fournisseur d'accès) peut survenir parce qu'un tel trafic sera transmis le long du chemin annoncé par le chemin agrégé. La règle n° 2 va empêcher la mauvaise livraison du paquet en causant l'élimination d'un tel trafic par l'annonceur du chemin

agrégé, mais le résultat de "traceroute" et autres outils similaires va suggérer qu'un problème existe au sein de ce réseau plutôt que dans le réseau qui n'annonce plus le préfixe le plus spécifique. Ceci peut être une source de confusion pour ceux qui essayent de diagnostiquer les problèmes de connexité ; voir les détails dans l'exemple du paragraphe 6.2. Une solution à ce "problème" perçu sort du domaine d'application du présent document ; elle tient à une meilleure éducation de la communauté des usagers/opérateurs, et non dans la technologie de l'acheminement.

Une mise en œuvre qui suit ces règles devrait aussi être généralisée, afin qu'un numéro et un gabarit de réseau arbitraire soient acceptée pour toutes les destinations d'acheminement. La seule contrainte en suspens est que le gabarit doit rester contigu. Noter que le chemin factice au préfixe 0.0.0.0/0 est utilisé comme chemin par défaut et DOIT être accepté par toutes les mises en œuvre. De plus, pour protéger contre les annonces accidentelles de ce chemin via le protocole inter-domaines, ce chemin ne devrait être annoncé à un autre domaine d'acheminement que lorsque un routeur est explicitement configuré à le faire, et jamais comme une option par défaut non configurée.

5.2 Comment fonctionne la règle

La règle n° 1 garantit que l'algorithme de transmission utilisé est cohérent à travers les protocoles et mises en œuvre d'acheminement. Les réseaux multi rattachements sont toujours annoncés explicitement par tous les fournisseurs d'accès à travers lesquels ils sont acheminés, même si ce sont des sous ensembles spécifiques de l'agrégat d'un fournisseur d'accès (si ils ne le sont pas, il est clair qu'ils doivent être annoncés explicitement). Cela pourrait sembler être comme si le fournisseur d'accès "principal" pouvait annoncer implicitement le site multi rattachement au titre de son agrégat, mais la transmission à la plus longue correspondance ne permet pas que cela fonctionne. On trouvera plus de détails dans la [RFC4116].

La règle n° 2 garantit qu'aucune boucle d'acheminement ne se forme à cause de l'agrégation. Considérons un site à qui l'adresse 192.168.64/19 a été affectée par son fournisseur "parent", qui a 192.168.0.0/16. Le réseau "parent" va annoncer 192.168.0.0/16 au réseau "fils". Si le réseau "fils" devait perdre la connexité au 192.168.65.0/24 (qui fait partie de son agrégat) le trafic du "parent" au "fils" destiné au 192.168.65.1 va suivre le chemin annoncé par le "fils". Lorsque ce trafic arrive cependant chez le "fils", celui-ci NE DOIT PAS suivre le chemin 192.168.0.0/16 en retour jusqu'au "parent", car il en résulterait une boucle d'acheminement. La règle n° 2 dit que le "fils" n'a pas le droit de suivre un chemin moins spécifique pour une destination qui correspond à un de ses propres chemins agrégés (normalement, ceci est mis en œuvre en installant un chemin "d'élimination" ou "nul" pour tous les préfixes agrégés qu'un réseau annonce à un autre). Noter que le traitement du chemin "par défaut" (0.0.0.0/0) est un cas particulier de cette règle ; un réseau ne doit pas suivre le chemin par défaut pour des destinations qui font partie d'une de ses annonces agrégées.

5.3 Note sur les formats de filtre de préfixe

Les systèmes qui traitent les annonces de chemins doivent être capables de vérifier que les informations qu'ils reçoivent sont acceptables selon les règles de politique. Les mises en œuvre qui filtrent les annonces de chemins doivent permettre des longueurs de gabarit ou de préfixe dans les éléments de filtre. Donc, les éléments de filtre qui étaient anciennement spécifiés comme

```
accepter 172.16.0.0
accepter 172.25.120.0.0
accepter 172.31.0.0
refuser 10.2.0.0
accepter 10.0.0.0
```

ressemblent maintenant à quelque chose comme :

```
accepter 172.16.0.0/16
accepter 172.25.0.0/16
accepter 172.31.0.0/16
refuser 10.2.0.0/16
accepter 10.0.0.0/8
```

Cela rend simplement explicite le gabarit de réseau qui était implicite dans la classification des numéros de réseau de classes A/B/C. Il est aussi utile d'améliorer la capacité de filtrage pour permettre la correspondance d'un préfixe et de tous les préfixes plus spécifiques avec le même schéma binaire ; heureusement, cette fonctionnalité a été mise en œuvre par la plupart des fabricants d'équipements utilisés sur l'Internet.

5.4 Responsabilité de la configuration de l'agrégation

Dans des circonstances normales, un domaine d'acheminement (ou "système autonome", (AS)) à qui a été alloué ou affecté un ensemble de préfixes a seul la responsabilité d'agréger ces préfixes. Dans le cas usuel, l'AS va installer la configuration dans un ou plusieurs de ses routeurs pour générer les chemins agrégés sur la base des chemins les plus spécifiques connus de son système d'acheminement interne. Ces chemins agrégés sont annoncés dans le système d'acheminement mondial par les routeurs bordure pour le domaine d'acheminement. Les chemins internes les plus spécifiques qui se chevauchent avec les chemins agrégés ne devraient pas être annoncés mondialement. Dans certains cas, un AS peut souhaiter déléguer la responsabilité de l'agrégation à un autre AS (par exemple, un abonné peut souhaiter que son fournisseur d'accès génère des informations d'acheminement agrégé en son nom) ; dans ce cas, l'agrégation est effectuée par un routeur dans le second AS selon les chemins qu'il reçoit du premier, combinés avec les informations de politique configurées qui décrivent comment ces chemins devraient être agrégés.

Noter qu'un fournisseur peut choisir d'effectuer l'agrégation sur les chemins qu'il reçoit d'un autre sans accord explicite ; c'est ce qu'on appelle une "agrégation de mandataire". Cela peut être un outil utile pour réduire la quantité d'état d'acheminement qu'un AS doit porter et propager à ses abonnés et voisins. Cependant, l'agrégation de mandataire peut aussi créer des conséquences imprévues dans l'ingénierie du trafic. Considérons ce qui arrive si les AS 2 et 3 reçoivent tous deux des chemins de AS 1 mais AS 2 effectue une agrégation de mandataire tandis que AS 3 ne le fait pas. Les autres AS qui reçoivent les informations d'acheminement de transit de AS 2 et AS 3 vont voir une incohérence des informations d'acheminement générées par AS 1. Cela peut causer un glissement inattendu du trafic vers AS 1 à travers AS 3 pour les abonnés de AS 3 et tous les autres qui reçoivent du trafic en transit de AS 3. Parce que l'agrégation de mandataire peut causer des conséquences imprévues pour des parties de l'Internet qui n'ont pas de relations avec, soit la source des chemins agrégés, soit la partie qui fournit l'agrégation, elle devrait être utilisée avec une extrême prudence.

La configuration des chemins à combiner dans les agrégats est une mise en œuvre de la politique d'acheminement et exige un entretien manuel des informations. En plus de l'entretien des informations pour un ensemble de préfixes acheminables, la configuration d'agrégation est normalement juste une ligne ou deux qui définissent la gamme du bloc d'adresses IPv4 à agréger. Un site qui effectue sa propre agrégation le fait pour des blocs d'adresses qui lui sont affectés ; un site qui effectue l'agrégation au nom d'un autre connaît ces informations à cause d'un accord de délégation de l'agrégation. En supposant que la meilleure pratique courante pour les administrateurs de réseau est d'échanger les listes de préfixes à accepter les uns des autres, la configuration des informations d'agrégation n'introduit pas de surcharge administrative supplémentaire significative.

La génération d'un chemin agrégé est normalement spécifiée soit statiquement, soit en réponse à l'apprentissage d'un chemin dynamique actif pour un préfixe contenu dans le chemin agrégé. Si une annonce d'un tel chemin agrégé dynamique est faite, il faut veiller à ce que les chemins ne s'ajoutent ou se soustraient pas de façon excessive (ce qu'on appelle la "fluctuation de chemin"). En général, une annonce d'agrégat de chemin dynamique est ajoutée lorsque au moins un composant de l'agrégat devient accessible, et n'est retirée que lorsque tous les composants deviennent inaccessibles. Les chemins agrégés configurés correctement sont plus stables que les chemins non agrégés et améliorent donc la stabilité globale de l'acheminement.

Note pour la mise en œuvre : l'agrégation de l'espace d'adresse de "classe D" (diffusion groupée) sort du domaine d'application du présent document.

5.5 Considérations sur la propagation de chemin et le protocole d'acheminement

Avant le déploiement original de CIDR, la pratique courante était de propager les chemins appris via des protocoles d'acheminement extérieurs (c'est-à-dire, EGP ou BGP) par l'intermédiaire du protocole d'acheminement intérieur d'un site (normalement, OSPF, IS-IS, ou RIP). On faisait cela pour assurer que des points de sortie cohérents et corrects étaient choisis pour le trafic à envoyer à une destination apprise par l'intermédiaire de ces protocole. Quatre effets d'évolution – l'avènement de CIDR, la croissance explosive de l'état d'acheminement mondial, l'adoption largement répandue de BGP4, et une exigence de propager les informations de chemin complètes – se sont combinés pour faire déconseiller cette pratique. Pour assurer une propagation appropriée du chemin et empêcher des incohérences d'acheminement inter AS (le mécanisme de détection/prévention de boucles d'acheminement de BGP4 exige la propagation du chemin complet) les réseaux de transit doivent utiliser BGP interne (iBGP) pour porter les chemins appris des autres fournisseurs aussi bien au sein qu'à travers leurs réseaux.

6. Exemple de la nouvelle allocation d'adresse et l'acheminement

6.1 Délégation d'adresse

Considérons le bloc de 524 288 (2^19) adresses, commençant par 10.24.0.0 et se terminant par 10.31.255.255, allouées à un seul opérateur, "PA". Ceci est équivalent en taille à un bloc de 2048 numéros de réseau de "classe C" traditionnelle (ou / 24). Un chemin sans classes vers ce bloc serait décrit comme 10.24.0.0 avec un gabarit de 255.248.0.0 et le préfixe 10.24.0.0/13.

Supposons que cet opérateur connecte six sites dans l'ordre suivant (significatif parce qu'il montre comment des "trous" temporaires peuvent se former dans l'espace d'adresses du fournisseur d'accès) :

- "C1", exigeant moins de 2048 adresses (/21 ou 8 x /24)
- "C2", exigeant moins de 4096 adresses (/20 ou 16 x /24)
- "C3", exigeant moins de 1024 adresses (/22 ou 4 x /24)
- "C4", exigeant moins de 1024 adresses (/22 ou 4 x /24)
- "C5", exigeant moins de 512 adresses (/23 ou 2 x /24)
- "C6", exigeant moins de 512 adresses (/23 ou 2 x /24)

Dans tous les cas, le nombre d'adresses IPv4 "exigé" par chaque site est supposé permettre une croissance significative. Le fournisseur d'accès délègue son espace d'adresses comme suit :

- C1 affecte de 10.24.0 à 10.24.7. Ce bloc de réseaux est décrit par le chemin 10.24.0.0/21 (gabarit 255.255.248.0).
- C2 affecte de 10.24.16 à 10.24.31. Ce bloc est décrit par le chemin 10.24.16.0/20 (gabarit 255.255.240.0).
- C3 affecte de 10.24.8 à 10.24.11. Ce bloc est décrit par le chemin 10.24.8.0/22 (gabarit 255.255.252.0).
- C4 affecte de 10.24.12 à 10.24.15. Ce bloc est décrit par le chemin 10.24.12.0/22 (gabarit 255.255.252.0).
- C5 affecte 10.24.32 et 10.24.33. Ce bloc est décrit par le chemin 10.24.32.0/23 (gabarit 255.255.254.0).
- C6 affecte 10.24.34 et 10.24.35. Ce bloc est décrit par le chemin 10.24.34.0/23 (gabarit 255.255.254.0).

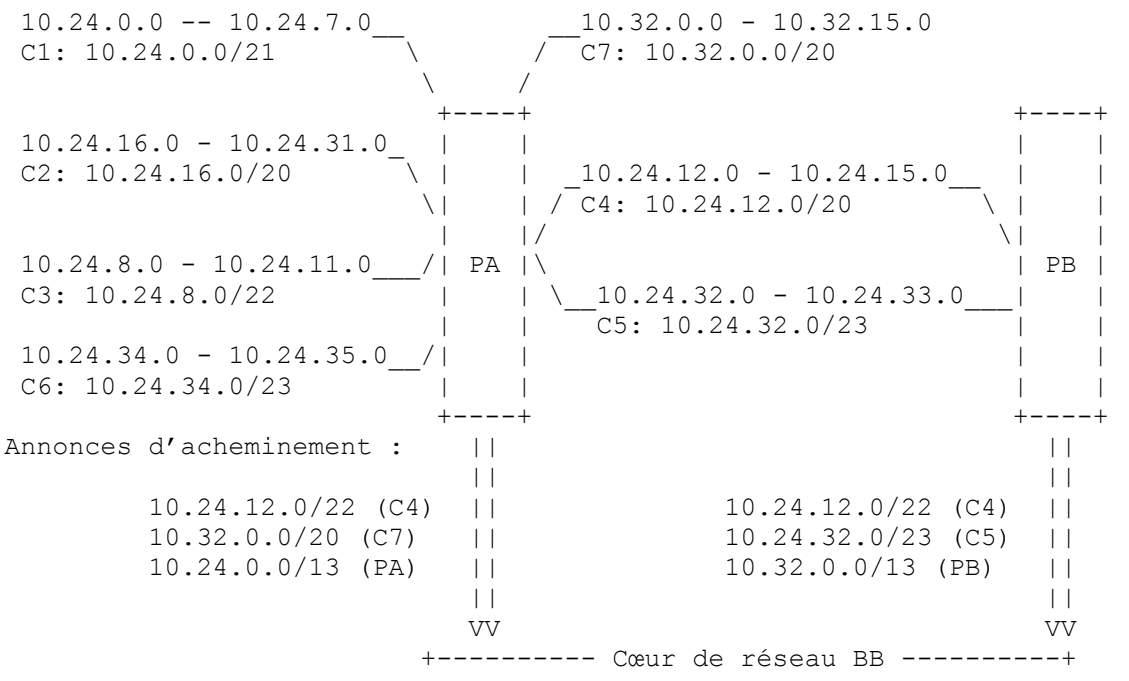
Ces six sites devraient être représentés comme six préfixes de diverses tailles au sein de l'IGP du fournisseur. Si pour une raison, le fournisseur utilise un IGP obsolète qui ne prend pas en charge l'acheminement sans classes ni les sous réseaux de longueur variable, des chemins explicites pour toutes les /24 devront être portés.

Pour rendre cet exemple plus réaliste, supposons que C4 et C5 soient multi rattachements à travers un autre fournisseur d'accès, "PB". Supposons de plus l'existence d'un site, "C7", qui était à l'origine connecté à "RB" mais qui est passé à "PA". Pour cette raison, il a un bloc de numéros de réseau qui sont affectés à partir du bloc de PB du prochain 2048 x /24.

- C7 affecte de 10.32.0 à 10.32.15. Ce bloc est décrit par le chemin 10.32.0.0/20 (gabarit 255.255.240.0).

Pour les sites multi rattachements, supposons que C4 soit annoncé comme principal via "RA" et secondaire via "RB"; que C5 soit principal via "RB" et secondaire via "RA". De plus, supposons que "RA" et "RB" sont tous deux connectées au même fournisseur d'accès de transit, "BB".

Graphiquement, cette topologie ressemble à quelque chose comme :



6.2 Annonces d'acheminement

Pour suivre la règle n° 1, PA va avoir besoin d'annoncer le bloc d'adresses qui a été donné et C7. Comme C4 est multi rattachements principal à travers PA, il doit aussi être annoncé. C5 est multi rattachements et principal à travers PB. En principe (et dans l'exemple ci-dessus) il n'a pas besoin d'être annoncé, car la plus longue correspondance par PB va automatiquement choisir PB comme principal et l'annonce de l'agrégat de PA sera utilisée comme secondaire. Dans la pratique réelle, C5 va normalement être annoncé via les deux fournisseurs.

Les annonces de "PA" à "BB" seront :
10.24.12.0/22 principal (annonce à C4)
10.32.0.0/20 principal (annonce à C7)
10.24.0.0/13 principal (reste des annonces de PA)

Pour PB, les annonces doivent aussi inclure C4 et C5, ainsi que son bloc d'adresses.

Les annonces de "PB" à "BB" seront :
10.24.12.0/22 secondaire (annonce à C4)
10.24.32.0/23 principal (annonce à C5)
10.32.0.0/13 principal (annonce le reste de RB)

Pour illustrer la question du diagnostic des problèmes mentionnée au paragraphe 5.1, considérons ce qui arrive si PA perd la connexité avec C7 (le site qui a son affectation dans l'espace de PB). Dans un protocole à états pleins, PA va annoncer à BB que 10.32.0.0/20 est devenu injoignable. Maintenant, lorsque BB purge ces informations de son tableau d'acheminement, tout le futur trafic envoyé à travers lui pour cette destination sera transmis à PB (où il sera éliminé conformément à la règle n° 2) en vertu de la correspondance moins spécifique de PB, 10.32.0.0/13. Bien que cela ne cause pas de problème de fonctionnement (C7 est injoignable dans tous les cas) cela crée un trafic supplémentaire à travers "BB" (et peut aussi créer de la confusion chez ceux qui essayent de déboguer la panne avec "traceroute"). Un mécanisme pour mettre en antémémoire un tel état injoignable serait utile, mais cela sort du domaine d'application du présent document.

7. Considérations sur le service des noms de domaine

Un aspect des services Internet qui a été affecté de façon notable par le passage à CIDR a été le mécanisme utilisé pour la traduction d'adresse en nom : la zone IN-ADDR.ARPA du système des domaines. Parce que cette zone est déléguée uniquement aux limites d'octet, le passage à un plan d'affectation d'adresses qui utilise un adressage fondé sur le gabarit binaire a causé une augmentation du travail pour ceux qui font la maintenance des parties de la zone IN-ADDR.ARPA.

Une description des techniques pour remplir la zone IN-ADDR.ARPA lorsque on utilise des adresses dont les blocs ne s'alignent pas sur les limites d'octet est décrite dans la [RFC2317].

8. Transition vers une solution à long terme

CIDR a été conçu comme une solution à court terme aux problèmes de l'état d'acheminement et de l'épuisement des adresses sur l'Internet IPv4. Il ne change pas l'architecture fondamentale d'acheminement ou d'adressage de l'Internet. On ne s'attend pas à ce qu'il affecte les plans de transition vers une solution à plus long terme, excepté peut-être, en retardant l'urgence du développement d'une telle solution.

9. Analyse de l'effet de CIDR sur l'état d'acheminement global

Lorsque CIDR a été proposé au début des années 1990, les auteurs d'origine ont fait des observations sur le taux de croissance de l'état d'acheminement global et ont proposé des projections sur la façon dont on pouvait espérer que le déploiement de CIDR réduirait ce qui apparaissait comme une croissance exponentielle à un rythme plus raisonnable. Depuis ce déploiement, des travaux menés sous le nom de "rapport CIDR" [CRPT], ont tenté de quantifier et restituer ce taux de croissance. On donne ci-après un bref résumé du rapport CIDR de mars 2005, en tentant d'expliquer les divers schémas et les changements du taux de croissance qui se sont produits depuis ces mesures de la taille de l'état d'acheminement global commencées en 1988.

Lorsque on examine la courbe des "entrées actives du tableau de BGP " [CBGP], il apparaît qu'il y a plusieurs tendances de croissance différentes avec des point d'inflexion distincts qui reflètent les changements des politiques et des pratiques. Les tendances et les événements dont on pense qu'ils les ont causées étaient les suivantes :

1. Une croissance exponentielle à l'extrême gauche de la courbe. Cela représente la période de la première expansion et la commercialisation de l'ancien réseau de recherche, depuis la fin des années 1980 jusqu'à approximativement 1994. Le pilote majeur de cette croissance était une absence de capacité d'agrégation pour les fournisseurs de transit, et l'utilisation largement répandue des allocations des classes C traditionnelles aux sites d'extrémité. Chaque fois qu'un nouveau site était connecté à l'Internet mondial, une ou plusieurs entrées d'acheminement étaient générées.

2. Une accélération de la tendance exponentielle fin 1993 et début 1994 lorsque les blocs de "super réseau" CIDR ont commencé d'être affectés par le NIC et acheminés comme des réseaux séparés de classe C traditionnelle par les fournisseurs d'accès.

3. Une forte chute en 1994 lorsque le déploiement de BGP4 par les fournisseurs permettait l'agrégation des blocs du "super réseau". Noter que les périodes de plus grand déclin du nombre d'entrées de tableau d'acheminement correspondent normalement aux semaines qui suivent chaque réunion du groupe de travail Déploiement de CIDR de l'IETF.

4. Une croissance en gros linéaire depuis la mi-1994 au début 1999 lorsque les affectations d'adresses fondées sur CIDR ont été faites et que les chemins agrégés ont été ajoutés partout dans le réseau.

5. Une nouvelle période de croissance exponentielle revient du début 1999 jusqu'à 2001 lorsque la "bulle des nouvelles technologies" alimente à la fois la rapide expansion de l'Internet et une grosse augmentation d'annonces de chemins plus spécifiques pour les multi rattachements et l'ingénierie du trafic.

6. Un écrasement de la croissance en 2001 causé par la combinaison de "l'explosion point-com", qui a causé l'arrêt des activités de nombreuses organisations, et un effort de "police de CIDR" [CPOL] qui visait à améliorer l'efficacité de l'agrégation.

7. Une croissance à peu près linéaire en 2002 et 2003. Cela représente très probablement une reprise du taux de croissance "normal" observé avant la "bulle", ainsi que la fin de la "police de CIDR".

8. Une tendance plus récente de croissance exponentielle a commencé en 2004. La meilleure explication semble être une amélioration de l'économie mondiale conduisant à une expansion accrue de l'Internet et l'absence d'effort de "police de CIDR", qui avait précédemment servi d'outil d'éducation pour les nouveaux fournisseurs pour améliorer l'efficacité de l'agrégation. Il y a eu aussi des cas où les fournisseurs de service ont délibérément désagrégé des préfixes pour tenter d'atténuer les problèmes de sécurité causés par des annonces de chemin contradictoires (voir la Section 12). Bien que ce comportement puisse résoudre les problèmes à court terme rencontrés par de tels fournisseurs, il est fondamentalement non adaptable et assez préjudiciable à la communauté toute entière. De plus, il apparaît que de nombreux fournisseurs annoncent à la fois les préfixes qui leur sont alloués et tous leurs composants /24, probablement à cause d'un manque d'informations cohérentes actuelles sur la configuration d'acheminement recommandée.

10. Conclusions et recommandations

En 1992, au début du développement de CIDR, il y avait de sérieux problèmes face à la croissance continuelle de l'Internet. La croissante de la complexité de l'état d'acheminement et l'augmentation rapide de la consommation de l'espace d'adresses laissaient penser qu'un problème, ou les deux, allaient empêcher la poursuite de la croissance de l'Internet dans les quelques années à venir.

Le déploiement de CIDR, combiné avec la prise en charge par BGP4 du transport des chemins à préfixes sans classes a atténué la crise à court terme. C'est seulement par un effort concerté des fabricants d'équipements et de la communauté des opérateurs que ceci a été réalisé. La menace (et peut-être dans certains cas, la mise en œuvre réelle) d'une taxation des réseaux pour les annonces de préfixes peut avoir offert une incitation supplémentaire à partager l'espace d'adresses, et donc les coûts associés d'annoncer les chemins aux fournisseurs d'accès.

L'architecture du système d'acheminement IPv4 porte les informations de topologie sur la base des annonces d'adresse agrégées et d'une collection d'annonces plus spécifiques qui sont associées à l'ingénierie du trafic, au multi rattachement, et à la configuration locale. En mars 2005, la charge de base de l'agrégation d'adresse dans le système d'acheminement est estimée a environ 75 000 entrés.

Approximativement 85 000 entrées supplémentaires sont les entrées plus spécifiques de cette collection "racine" de base. Il y a des raisons de penser que beaucoup de ces entrées supplémentaires existent pour résoudre des problèmes de portée régionale ou même locale qui ne devraient pas avoir besoin d'une propagation mondiale.

Une question évidente à poser est celle de la poursuite de CIDR comme approche viable pour garder la croissance globale de l'état d'acheminement et la diminution de l'espace d'adresses à des taux soutenables. Des mesures récentes indiquent que la croissance exponentielle a repris, mais une analyse plus approfondie suggère que cette tendance peut être atténuée par un effort plus actif pour éduquer les fournisseurs d'accès aux stratégies efficaces d'agrégation et une configuration d'équipement appropriée. Si on regarde plus loin vers l'avenir, il y a un clair besoin d'une meilleure technologie de multi rattachement qui n'ait pas besoin de l'état d'acheminement mondial pour chaque site et de méthodes d'équilibrage de la charge de trafic qui n'exigent pas d'ajouter encore plus d'état. Sans de tels développements et en l'absence de changement architectural majeur, l'agrégation est le seul outil disponible pour adapter l'acheminement dans l'Internet mondial.

11. Mises à jour de l'état des documents CIDR

Le présent mémoire rend obsolètes les RFC suivantes qui décrivent l'utilisation et le déploiement de CIDR, et demande leur reclassification comme "Historiques" :

- RFC 1467 : État du déploiement de CIDR dans l'Internet
  Cette RFC pour information décrivait l'état du déploiement de CIDR en 1993. En 2005, CIDR a été complètement déployé, de sorte que cette note sur l'état ne fournit qu'un point de données historique.

- RFC 1481 : Recommandation de l'IAB pour une stratégie intermédiaire pour régler le problème de l'adaptation
  Cette très courte RFC pour information décrivait l'approbation par l'IAB de l'utilisation de CIDR pour régler les problèmes d'adaptation. Comme le but de la RFC 1481 a été atteint, elle n'a plus maintenant qu'une valeur historique.

- RFC 1482 : Prise en charge de l'agrégation dans la base de données d'acheminement fondé sur la politique de NSFNET
  Cette RFC pour information décrit les plans de prise en charge de l'agrégation de chemins, comme spécifié par CIDR, sur le NSFNET. Comme le NSFNET a depuis longtemps cessé d'exister et que CIDR a été déployé partout, la RFC 1482 n'a plus maintenant qu'un intérêt historique.

- RFC 1517 : Déclaration d'applicabilité pour la mise en œuvre de l'acheminement inter domaines sans classes (CIDR)
  Cette RFC sur la voie de la normalisation décrivait où CIDR devait être exigé et où il était (fortement) recommandé. Avec le déploiement complet de CIDR sur l'Internet, les situations où CIDR n'est pas exigé n'ont un intérêt qu'historique.

- RFC 1518 : Architecture de l'allocation des adresses IP avec CIDR
  Cette RFC sur la voie de la normalisation discutait en détails les considérations d'acheminement et d'agrégation d'adresse. Certaines de ces questions sont résumées dans le présent document au paragraphe 3.1. Parce que les politiques et procédures d'affectation d'adresse sont maintenant principalement entre les mains des RIR, il n'est plus approprié d'essayer de documenter ces pratiques dans une RFC sur la voie de la normalisation. De plus, la [RFC3221] décrit aussi beaucoup des mêmes questions du point de vue du système d'acheminement.

- RFC 1520 : Exchange des informations d'acheminement à travers les frontières de fournisseur d'accès dans l'environnement de CIDR
  Cette RFC pour information décrivait les scénarios de transition là où CIDR n'était pas totalement pris en charge pour échanger les informations d'acheminement entre les fournisseurs d'accès. Avec le déploiement complet de CIDR sur l'Internet, de tels scénarios n'ont plus de pertinence opérationnelle.

- RFC 1817: CIDR et classes d'acheminement
  Cette RFC pour information décrivait les implications du déploiement de CIDR en 1995 ; elle note que les adresses anciennement en classes sont maintenant allouées en utilisant les mécanismes de CIDR et elle décrit l'utilisation d'un chemin par défaut pour les sites sans capacité CIDR. Avec le déploiement complet de CIDR sur l'Internet, de tels scénarios n'ont plus de pertinence opérationnelle.

- RFC 1878: "Tableau de sous-réseau de longueur variable pour IPv4"
  Cette RFC pour information fournissait un tableau des gabarits pré calculés de sous-réseaux et de comptes d'adresse pour chaque taille de sous-réseau. Avec l'incorporation d'un tableau similaire dans le présent document (au paragraphe 3.1) il n'est plus nécessaire de le documenter dans une RFC séparée.

- RFC 2036: "Observations sur l'utilisation des composants de l'espace d'adresse de classe A au sein de l'Internet"
  Cette RFC pour information décrit plusieurs questions de fonctionnement associées à l'allocation des préfixes sans classes à partir de l'espace d'adresse anciennement en classes. Avec le déploiement complet de CIDR dans l'Internet et plus de six années d'expérience d'allocation de préfixes sans classes à partir de l'espace d'adresse historique de la "classe A", cette RFC n'a plus maintenant qu'une valeur historique.

12. Considérations sur la sécurité

L'introduction de protocoles d'acheminement qui prennent en charge les préfixes sans classes et passent à un modèle de transmission qui rend obligatoire que les chemins les plus spécifiques (plus longue correspondance) soient préférés lorsque ils se chevauchement avec des chemins pour des préfixes moins spécifiques soulève au moins deux problèmes pour la sécurité.

1. Le trafic peut être capturé en annonçant pour une certaine destination un préfixe qui est plus spécifique que l'agrégat qui est normalement annoncé pour cette destination. Par exemple, supposons qu'un système d'extrémité populaire qui a l'adresse 192.168.17.100 soit connecté à un fournisseur d'accès qui annonce 192.168.16.0/20. Un opérateur de réseau malveillant qui souhaite intercepter le trafic pour ce site peut annoncer, ou au moins tenter d'annoncer, 192.168.17.0/24 dans le système d'acheminement mondial. Parce que ce préfixe est plus spécifique que le préfixe "normal", le trafic va être détourné du système d'extrémité légitime vers le réseau de l'opérateur malveillant. Avant l'arrivée de CIDR, il était possible d'induire du trafic de certaines parties du réseau à suivre une fausse annonce qui correspondait exactement à un numéro de réseau particulier ; CIDR rend ce problème encore pire car l'acheminement selon la plus longue correspondance fait généralement que tout le trafic préfère le chemin le plus spécifique à celui qui l'est moins. Le remède à l'attaque fondée sur CIDR est le même que pour celle fondée sur le système pré-CIDR : l'établissement de relations de confiance entre les fournisseurs, couplé avec de forts filtres de politique d'acheminement aux frontières du fournisseur. Malheureusement, la mise en œuvre de tels filtres est difficile dans l'Internet très décentralisé. Comme moyen de contournement, de nombreux fournisseurs mettent en œuvre des filtres génériques qui fixent des limites supérieures, dérivées des lignes directrices aux RIR pour la taille des blocs qu'ils allouent, sur la longueur des préfixes qui sont acceptés des autres fournisseurs. Noter que les "envoyeurs de pourriels" utilisent cette sorte d'attaque pour capturer temporairement un espace d'adresses afin de cacher l'origine du trafic (des messages électroniques non désirés "spam") qu'ils génèrent.

2. Des attaques de déni de service peuvent être lancées contre de nombreuses parties de l'infrastructure de l'Internet par l'annonce d'un grand nombre de chemins dans le système. Une telle attaque est destinée à causer des défaillances de routeur par la submersion des tableaux d'acheminement et de transmission. Un bon exemple d'un incident non malveillant qui a causé cette sorte de défaillance était le tristement célèbre événement "AS 7007" [7007], où une mauvaise configuration d'un routeur par un opérateur a causé la propagation d'un énorme nombre de chemins invalides à travers le système d'acheminement mondial. Là encore, cette sorte d'attaque n'est pas réellement nouvelle avec CIDR ; en utilisant les chemins traditionnels de classes A/B/C, il était possible d'annoncer un maximum de 16 843 008 numéros de réseau uniques dans le système d'acheminement mondial, nombre qui est suffisant pour causer des problèmes même aux équipement d'acheminement les plus modernes fabriqués en 2005. Ce qui est différent est que la complexité modérée d'une configuration correcte des routeurs en présence de CIDR tend à rendre plus probables des "attaques" accidentelles de cette sorte. Les mesures pour prévenir cette sorte d'attaques sont très semblables à celle décrites ci-dessus pour la capture de trafic, en ajoutant que la meilleure pratique actuelle est aussi de configurer un nombre maximum raisonnable de préfixes qu'un routeur frontière va accepter de ses voisins.

Noter que ceci n'est pas destiné à constituer une analyse exhaustive des sortes d'attaques que CIDR rend plus faciles ; une analyse plus complète des vulnérabilités de la sécurité dans les système d'acheminement mondial sort du domaine d'application du présent document.

13. Remerciements

Les auteurs souhaitent exprimer leur gratitude aux autres auteurs originaux de la RFC 1519 (Kannan Varadhan, Jessica Yu), au groupe ROAD duquel de nombreuses idées de CIDR ont été inspirées et développées, aux premiers relecteurs de cette version revisitée du document (Barry Greene, Danny McPherson, Dave Meyer, Eliot Lear, Bill Norton, Ted Seely, Philip Smith, Pekka Savola) dont les commentaires, corrections, et suggestions ont été sans prix. Nous tenons tout spécialement à remercier Geoff Huston pour ses contributions bien au dessus et au delà de ce à quoi il était obligé.

14. Références

14.1 Référence normative

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

14.2 Références pour information

[7007] "NANOG mailing list discussion of the "AS 7007" incident", < http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html >.

[CBGP] "Graph: Active BGP Table Entries, 1988 to Present", < http://bgp.potaroo.net/as4637/ >.

[CPOL] "CIDR Police - Please Pull Over and Show Us Your BGP", < http://www.nanog.org/mtg-0302/cidr.html >.

[CRPT] "The CIDR Report", < http://www.cidr-report.org/ >.

[IANA] "Internet Assigned Numbers Authority", < http://www.iana.org >.

[LWRD] "The Long and Winding Road", < http://rms46.vlsm.org/1/42.html >.

[NRO] "Number Resource Organization", < http://www.nro.net >.

[RFC0904] D. Mills, "Spécification formelle du protocole de passerelle extérieure", avril 1984. *(Historique)*

[RFC1058] C. Hedrick, "Protocole d'informations d'acheminement", juin 1988. *(Historique)*

[RFC1195] R. Callon, "Utilisation de l'IS-IS OSI pour l'acheminement dans les environnements TCP/IP et duels", décembre 1990. *(Mise à jour par les* RFC 1349, 5302, 5304*)*

[RFC1338] V. Fuller et autres, "Super-réseautage : une stratégie d'allocation et d'agrégation d'adresses", juin 1992. *(obsolète, voir*1519*)*

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

[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)

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849*)*

[RFC2317] H. Eidnes, G. de Groot et P. Vixie, "Délégation IN-ADDR.ARPA sans classe", BCP 20, mars 1998.

[RFC2328] J. Moy, "OSPF version 2", STD 54, avril 1998. *(MàJ par la* RFC6549)

[RFC2453] G. Malkin, "RIP version 2", STD 56, novembre 1998. *(Mise à jour par la RFC 4822)*

[RFC3021] A. Retana et autres, "Utilisation de préfixes à 31 bits sur les liaisons point à point IPv4", décembre 2000. *(P.S.)*

[RFC3021] A. Retana et autres, "Utilisation de préfixes à 31 bits sur les liaisons point à point IPv4", décembre 2000. *(P.S.)*

[RFC4116] J. Abley et autres, "Pratiques et limitations du rattachement multiple en IPv4", juillet 2005. *(Information)*

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608)

[RIPE] "RIPE Network Coordination Centre", < http://www.ripe.net >.

Adresses des auteurs

Vince Fuller
170 W. Tasman Drive
San Jose, CA 95134
USA
mél : vaf@cisco.com

Tony Li
555 Del Rey Avenue
Sunnyvale, CA 94085
USA
mél : tli@tropos.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’édition des RFC est actuellement fourni par l’activité de soutien administratif (IASA) de l’IETF.