Groupe de travail Réseau
Request for Comments : 1887
Catégorie : Information
Traduction Claude Brière de L'Isle

Y. Rekhter, éditeur, cisco Systems
T. Li, éditeur, cisco Systems
décembre 1995

Architecture d'allocation d'adresse d'envoi individuel pour IPv6

Résumé
Le présent document présente une architecture pour l'allocation des adresses d'envoi individuel IPv6 [RFC1883] dans l'Internet. L'architecture globale d'adressage IPv6 est définie dans la [RFC1884]. Le présent document ne rentre pas dans les détails d'un plan d'adressage.

Table des matières

1. Domaine d'application

L'internet global peut être modélisé comme une collection d'hôtes interconnectés via des facilités de transmission et de commutation. Le contrôle sur la collection des hôtes et les facilités de transmission et de commutation qui composent les ressources de réseautage de l'internet global n'est pas homogène, mais est réparti parmi plusieurs autorités administratives. Les ressources sous le contrôle d'une seule administration au sein d'un segment contigu de topologie de réseau forment un domaine. Dans la suite de cet article, "domaine" et "domaine d'acheminement" sont utilisés de façon interchangeable.

Les domaines qui partagent leurs ressources avec d'autres domaines sont appelés des fournisseurs de service réseau (ou juste fournisseurs). Les domaines qui utilisent les ressources d'autres domaines sont appelés des abonnés de service réseau (ou juste des abonnés). Un certain domaine peut agir simultanément comme fournisseur et abonné.

Deux aspects sont à prendre en compte quand on discute de l'allocation d'adresse IPv6 en envoi individuel au sein de l'Internet. Le premier est l'ensemble des exigences administratives pour obtenir et allouer les adresses IPv6 ; le second est l'aspect technique de telles allocations, qui a largement à voir avec l'acheminement, à la fois au sein d'un domaine d'acheminement (acheminement intra domaine) et entre les domaines d'acheminement (acheminement inter domaines). Le présent document se concentre sur les questions techniques.

Dans l'Internet actuel, de nombreux domaines d'acheminement (comme des réseaux d'entreprise et de campus) se rattachent à des réseaux de transit (comme des réseaux régionaux) en un seul ou en un petit nombre de points d'accès soigneusement contrôlés. Les premiers agissent comme des abonnés, tandis que ces derniers agissent comme des fournisseurs.

Les solutions d'adressage qui exigent des changements ou contraintes substantielles sur la topologie courante ne sont pas examinées.

L'architecture et les recommandations du présent document sont orientées principalement vers la division à grande échelle de l'allocation d'adresses IPv6 dans l'Internet. Les sujets couverts incluent :
- les avantages du codage de certaines informations topologiques dans les adresses IPv6 pour réduire significativement les frais généraux de protocole d'acheminement ;
- le besoin prévu de niveaux supplémentaires de hiérarchie dans l'adressage de l'Internet pour prendre en charge la croissance du réseau ;
- la transposition recommandée entre les entités topologiques de l'Internet (c'est-à-dire, les fournisseurs de service, et les abonnés au service) et les composants d'adressage et d'acheminement IPv6 ;
- la division recommandée de l'allocation d'adresse IPv6 parmi les fournisseurs de service (par exemple, les cœurs de réseau, les réseaux régionaux) et les abonnés au service (par exemple, les sites) ;
- l'allocation des adresses IPv6 par le registre de l'Internet ;
- le choix de la portion de poids fort des adresses IPv6 dans les domaines d'acheminement d'extrémité qui sont connectés à plus d'un fournisseur de service (par exemple, à un cœur de réseau ou à un réseau régional).

On notera que d'autres aspects de l'allocation d'adresse IPv6, techniques et administratifs, ne sont pas traités dans cet article. Les sujets non couverts ou mentionnés seulement de façon superficielle incluent :
- un plan spécifique pour l'allocation d'adresses ;
- incorporer des espaces d'adresses provenant d'autres protocoles de couche réseau (incluant IPv4) dans l'espace d'adresses IPv6 et l'architecture d'adressage pour de telles adresses incorporées ;
- l'adressage de diffusion groupée ;
- l'allocation d'adresse pour les hôtes mobiles ;
- l'identification de domaines administratifs spécifiques dans l'Internet ;
- la politique ou les mécanismes pour faire connaître aux tiers les informations enregistrées (comme l'entité à laquelle a été allouée une adresse IPv6 spécifique ou une potion de l'espace d'adresses IPv6) ;
- comment un domaine d'acheminement (en particulier un site) devrait organiser sa topologie interne ou allouer des portions de son espace d'adresses IPv6 ; les relations entre topologie et adresses sont discutées, mais la méthode de décision sur une topologie particulière ou plan d'adressage interne ne l'est pas ;
- les procédures pour allouer les adresses IPv6 des hôtes.

2. Fondements

Quelques informations de base sont fournies dans cette section pour aider à comprendre les questions impliquées par l'allocation d'adresses IPv6. Une brève discussion de l'acheminement IPv6 est fournie.

IPv6 partage le problème de l'acheminement en trois parties :
- les échanges d'acheminement entre les systèmes d'extrémité et les routeurs,
- les échanges d'acheminement entre routeurs dans le même domaine d'acheminement, et,
- l'acheminement entre les domaines d'acheminement.

3. Adresses IPv6 et acheminement

Pour les besoins du présent document, un préfixe d'adresse IPv6 est défini comme une adresse IPv6 et des indications des bits de plus fort poids contigus les plus à gauche au sein de cette portion d'adresse. Dans le présent document, les préfixes d'adresses IPv6 vont être représentés par X/Y, où X est un préfixe d'une adresse IPv6 de longueur supérieure ou égale à ce qui est spécifié par Y, et Y est le nombre (décimal) des bits de plus fort poids contigus les plus à gauche au sein de cette adresse. Dans la notation, X, le préfixe d'une adresse IPv6 [RFC1884] va avoir les chiffres non significatifs de fin qui sont supprimés. Donc, un préfixe IPv6 peut apparaître comme 43DC:0A21:76/40.

Quand on détermine une politique administrative pour l'allocation d'adresses IPv6, il est important de comprendre les

conséquences techniques. Les objectifs derrière l'utilisation de l'acheminement hiérarchique sont de réaliser un certain niveau d'abstraction des données d'acheminement, ou de résumé, pour réduire la cpu, la mémoire, et la bande passante de transmission consommés par l'acheminement.

Bien que la notion d'abstraction des données d'acheminement puisse être appliquée à divers types d'informations d'acheminement, le présent mémoire se concentre sur un type particulier, à savoir les informations d'accessibilité. Les informations d'accessibilité décrivent l'ensemble des destinations accessibles. L'abstraction des informations d'accessibilité dicte que les adresses IPv6 sont allouées selon les structures topologiques d'acheminement. Cependant en pratique, l'allocation administrative suit les limites des organisations ou politiques. Ceci peut n'être pas congruent aux limites topologiques et donc les exigences des deux peuvent être contradictoires. Il est nécessaire de trouver un équilibre entre ces deux besoins.

L'abstraction des informations d'accessibilité se produit à la frontière entre les structures d'acheminement arrangées hiérarchiquement. Un élément plus bas dans la hiérarchie rapporte des informations d'accessibilité résumées à son ou ses parents.

Aux frontières de domaine d'acheminement, les informations d'adresse IPv6 sont échangées (de façon statique ou dynamique) avec les autres domaines d'acheminement. Si les adresses IPv6 au sein d'un domaine d'acheminement sont toutes tirées d'espaces non contigus d'adresses IPv6 (ne permettant pas d'abstraction) alors les informations d'adresses échangées à la frontière consistent en une liste énumérant toutes les adresses IPv6.

Autrement, si le domaine d'acheminement devait tirer les adresses IPv6 pour tous les hôtes au sein du domaine d'un seul préfixe d'adresses IPv6, les informations d'acheminement de frontière pourraient être résumées en le seul préfixe d'adresses IPv6. Cela permet une réduction substantielle de données et permet une meilleurs adaptabilité (comparée à l'adressage non coordonné discuté au paragraphe précédent).

Si les domaines d'acheminement sont interconnectés de façon plus ou moins aléatoire (c'est-à-dire, non hiérarchique) il est très probable qu'aucune autre abstraction des données d'acheminement ne peut se produire. Comme les domaines d'acheminement n'auraient pas de relations hiérarchiques définies, les administrateurs ne seraient pas capables d'allouer des adresses IPv6 au sein des domaines à partir d'un préfixe commun pour les besoins de l'abstraction de données. Le résultat seraient un acheminement inter domaines plat ; tous les domaines d'acheminement auraient besoin de connaître explicitement tous les autres domaines d'acheminement auxquels ils acheminent. Ceci peut bien fonctionner dans des internets de taille petite et moyenne. Cependant, ceci ne s'adapte pas pour les très grands internets. Par exemple, on s'attend à ce que IPv6 englobe des centaines de milliers de domaines d'acheminement dans la seule Amérique du Nord. Ceci exige un haut degré d'abstraction des informations d'accessibilité au delà de ce qui peut être réalisé au niveau du domaine d'acheminement.

Dans l'Internet, il devrait être possible de réduire significativement le volume et la complexité des informations d'acheminement en tirant parti de l'inter connexité hiérarchique existante. Ceci est discuté plus en détails à la Section 5. Donc, il y a une opportunité pour qu'un groupe de domaines d'acheminement ait chacun alloué un préfixe d'adresses à partir d'un préfixe plus court alloué à un autre domaine d'acheminement dont la fonction est d'interconnecter le groupe de domaines d'acheminement. Chaque membre du groupe de domaines d'acheminement a maintenant son propre préfixe (un peu plus long) à partir duquel il alloue ses adresses.

Le cas le plus direct de cette situation se produit quand il y a un ensemble de domaines d'acheminement qui sont tous rattachés à un seul domaine de fournisseur de service (par exemple, un réseau régional) et qui utilise le fournisseur pour tout le trafic externe (inter domaines). Un préfixe court peut être donné au fournisseur, qui va alors donner des préfixes légèrement plus longs (sur la base du préfixe du fournisseur) à chaque domaine d'acheminement qu'il interconnecte. Cela permet au fournisseur, quand il informe les autres domaines d'acheminement des adresses qu'ils peuvent atteindre, d'abstraire les informations d'accessibilité pour un grand nombre de domaines d'acheminement dans un seul préfixe. Cette approche peut donc permettre une grosse réduction des informations d'acheminement, et par là largement améliorer l'adaptabilité de l'acheminement inter domaines.

Il est clair que cette approche est récurrente et peut être portée à travers plusieurs itérations. Les domaines d'acheminement à tout "niveau" de la hiérarchie peuvent utiliser leur préfixe comme base de sous allocations suivantes, en supposant que les adresses IPv6 restent au sein de la longueur globale et des contraintes de structure.

À ce point, on observe que le nombre de nœuds à chaque niveau inférieur d'une hiérarchie tend à croître exponentiellement. Donc les plus grands gains dans l'abstraction d'informations d'accessibilité (pour le bénéfice de tous les niveaux supérieurs de la hiérarchie) se produisent quand l'agrégation des informations d'accessibilité se fait près des extrémités de la hiérarchie ; les gains chutent significativement à chaque niveau supérieur. Donc, la loi des rendements décroissants suggère qu'à un

certain point l'abstraction des données cesse de produire des avantages significatifs. La détermination du point auquel cette abstraction de données cesse d'être avantageuse exige une considération attentive du nombre de domaines d'acheminement qui sont supposés apparaître à chaque niveau de la hiérarchie (sur une certaine période) comparé au nombre de domaines d'acheminement et préfixes d'adresses qui peuvent être pratiquement et efficacement traités via des protocoles d'acheminement dynamiques inter domaines.

3.1 Efficacité contre contrôle décentralisé

Si l'Internet prévoit de prendre en charge une administration décentralisée des adresses, il faut alors rechercher un équilibre entre les exigences d'un acheminement efficace des adresses IPv6 et le besoin d'une administration décentralisée des adresses. Un plan d'adressage cohérent à tous les niveaux au sein de l'Internet doit porter une considération attentive à cette alternative.

Comme exemple de décentralisation administrative, supposons que le préfixe d'adresse IPv6 43/8 identifie une partie de l'espace d'adresses IPv6 alloué à l'Amérique du Nord. Toutes les adresses au sein de ce préfixe peuvent être allouées le long de frontières topologiques au profit d'une abstraction de données accrue. Au sein de ce préfixe, les adresses peuvent être allouées par fournisseur, sur la base de la géographie ou selon quelque autre critère topologique significatif. Pour les besoins de cet exemple, supposons que ce préfixe soit alloué par fournisseur. Les abonnés d'Amérique du Nord utilisent des parties de l'espace d'adresses qui sont en dessous de l'espace d'adresses IPv6 de leurs fournisseur de services. Au sein d'un domaine d'acheminement les adresses pour les sous réseaux et hôtes sont allouées à partir de l'unique préfixe IPv6 alloué au domaine conformément au plan d'adressage pour ce domaine.

4. Administration et acheminement d'adresse IPv6 dans l'Internet

Les composants de l'acheminement Internet – fournisseurs de service (par exemple, cœurs de réseau, réseaux régionaux) et les abonnés aux services (par exemple, les sites ou les campus) -- sont arrangés hiérarchiquement pour la plus grande partie. Une transposition naturelle de ces composants en composants d'acheminement IPv6 est que fournisseurs et abonnés agissent comme des domaines d'acheminement.

Autrement, un abonné (par exemple, un site) peut choisir d'opérer comme partie d'un domaine formé par un fournisseur de service. On suppose que certains, sinon la plupart, des sites vont préférer opérer au titre du domaine d'acheminement de leur fournisseur, échangeant les informations d'acheminement directement avec le fournisseur. Un préfixe est quand même alloué au site dans l'espace d'adresses du fournisseur, et le fournisseur va annoncer son propre préfixe dans l'acheminement inter domaines.

Étant donnée une telle transposition, où devraient être effectuées l'administration et l'allocation d'adresses pour satisfaire à la fois la décentralisation administrative et l'abstraction des données ? les possibilités suivantes sont considérées :
1) à une certaine partie au sein d'un domaine d'acheminement,
2) au domaine d'acheminement d'extrémité,
3) au domaine d'acheminement de transit (TRD, *Transit Routing Domain*) et
4) à une autre frontière, plus générale, comme la frontière d'un continent.

Une partie au sein d'un domaine d'acheminement correspond à tout ensemble arbitraire connecté de sous réseaux. Si un domaine est composé de plusieurs sous réseaux, ils sont interconnectés via des routeurs. Les domaines d'acheminement d'extrémité correspondent aux sites, où le principal objet est de fournir des services d'acheminement intra domaine. Les domaines d'acheminement de transit sont déployés pour porter le trafic de transit (c'est-à-dire, inter domaines) ; les cœurs de réseau et les fournisseurs sont des TRD. Des frontières plus générales peuvent être vues comme des collections topologiquement significatives de TRD.

La plus grosse charge de la transmission et du traitement des informations d'accessibilité est au sommet de la hiérarchie d'acheminement, où les informations d'accessibilité tendent à s'accumuler. Dans l'Internet, par exemple, les fournisseurs doivent gérer les informations d'accessibilité pour tous les abonnés directement connectés au fournisseur. Le trafic destiné aux autres fournisseurs est généralement acheminé aux cœurs de réseau (qui agissent aussi comme fournisseurs). Les cœurs de réseau doivent cependant être conscients des informations d'accessibilité pour tous les fournisseurs rattachés et leurs abonnés associés.

En général, l'avantage de l'abstraction des informations d'acheminement à un certain niveau de la hiérarchie d'acheminement est supérieur à celui des niveaux supérieurs de la hiérarchie. Il y a relativement peu d'avantage direct pour

l'administration qui effectue l'abstraction, car elle doit conserver individuellement les informations d'acheminement sur chaque structure d'acheminement rattachée topologiquement.

Par exemple, supposons qu'un certain site essaye de décider si il va obtenir un préfixe d'adresse IPv6 directement de l'espace d'adresses IPv6 alloué pour l'Amérique du Nord, ou de l'espace d'adresses IPv6 alloué à son fournisseur de services. Si on considère seulement leur intérêt propre, le site lui-même et le fournisseur qui le rattache ont peu de raisons de choisir une approche plutôt que l'autre. Le site doit utiliser un préfixe ou l'autre ; la source du préfixe a peu d'effet sur l'efficacité de l'acheminement au sein du site. Le fournisseur doit conserver les informations sur chaque site rattaché afin d'acheminer, sans considération de normalisation des préfixes des sites.

Cependant, il y a une différence quand le fournisseur distribue les informations d'acheminement à d'autres fournisseurs (par exemple, des cœurs de réseau ou des TRD). dans le premier cas, le fournisseur ne peut pas agréger l'adresse du site dans son propre préfixe ; l'adresse doit être explicitement mentionnée dans les échanges d'acheminement, ce qui résulte en une charge supplémentaire pour les autres fournisseurs qui doivent échanger et conserver ces informations.

Dans le second cas, chaque autre fournisseur (par exemple, un cœur de réseau ou un TRD) voit un seul préfixe d'adresse pour le fournisseur, qui englobe le nouveau site. Cela évite l'échange d'informations d'acheminement supplémentaires pour identifier le préfixe d'adresse du nouveau site. Donc, les avantages reviennent principalement aux autres fournisseurs qui conservent les informations d'acheminement sur ce site et ce fournisseur.

On peut appliquer un modèle de fournisseur/consommateur à ce problème : le niveau supérieur (par exemple, un cœur de réseau) est un fournisseur de services d'acheminement, tandis que le niveau inférieur (par exemple, un TRD) est le consommateur de ces services. Le prix facturé pour les services est fondé sur le coût de leur fourniture. Les frais généraux de la gestion d'un grand tableau d'adresses pour l'acheminement à une entité rattachée topologiquement contribuent à ce coût.

À présent, l'Internet n'est cependant pas une économie de marché. L'efficacité du fonctionnement est plutôt fondée sur la coopération. Les recommandations discutées ci-dessous décrivent des façons simples et maniables de gérer l'espace d'adresses IPv6 qui bénéficient à la communauté entière.

4.1 Administration des adresses IPv6 au sein d'un domaine

Si des hôtes individuels prennent leurs adresses IPv6 à partir d'une myriade d'espaces d'adresses IPv6 sans relations, il n'y aura effectivement aucune abstraction des données au delà de ce qui est construit dans les protocoles d'acheminement intra domaine existants. Par exemple, si on suppose qu'au sein d'un domaine d'acheminement on utilise trois préfixes indépendants alloués à partir de trois espaces différents d'adresses IPv6 associés à trois fournisseurs rattachés différents.

Ceci a un effet négatif sur l'acheminement inter domaines, en particulier sur les autres domaines qui ont besoin de conserver les chemins vers ce domaine. Il n'y a pas de préfixe commun qui puisse être utilisé pour représenter ces adresses IPv6 et donc aucun résumé ne peut avoir lieu à la frontière du domaine d'acheminement. Quand les adresses sont annoncées par ce domaine d'acheminement aux autres domaines d'acheminement, une énumération des trois préfixes individuels doit être utilisée.

Le nombre de préfixes IPv6 que les domaines d'acheminement d'extrémité vont annoncer est de l'ordre du nombre de préfixes alloués au domaine ; le nombre de préfixes du domaine d'acheminement qu'un fournisseur va annoncer est approximativement le nombre de préfixes rattachés aux domaines d'acheminement des clients d'extrémité ; et pour un cœur de réseau, cela va être additionné sur tous les fournisseurs rattachés. Cette situation n'est acceptable que dans l'Internet actuel, et n'est pas maniable pour l'Internet IPv6. Un plus haut degré de réduction des informations hiérarchiques est nécessaire pour permettre la poursuite de la croissance de l'Internet.

4.2 Administration au domaine d'acheminement d'extrémité

Comme on l'a mentionné précédemment, le plus haut degré d'abstraction des données vient aux plus bas niveaux de la hiérarchie. Fournir à chaque domaine d'acheminement d'extrémité (c'est-à-dire, un site) un bloc contigu d'adresses provenant du bloc d'adresse de son fournisseur résulte en la plus grosse augmentation d'abstraction. De l'extérieur, le domaine d'acheminement d'extrémité, l'ensemble de toutes les adresses accessibles dans le domaine peut alors être représenté par un seul préfixe. De plus, toutes les destinations accessibles au sein du préfixe du fournisseur peuvent être représentées par un seul préfixe.

Par exemple, considérons un seul campus qui est un domaine d'acheminement d'extrémité qui exigerait actuellement quatre préfixes IPv6 différents. À la place, on peut lui donner un seul préfixe qui fournit le même nombre d'adresses de destination. De plus, comme le préfixe est un sous ensemble du préfixe du fournisseur, cela n'impose pas de charge supplémentaire aux niveaux supérieurs de la hiérarchie d'acheminement.

Il y a une relation étroite entre les hôtes et les domaines d'acheminement. Le domaine d'acheminement représente le seul chemin entre un hôte et le reste de l'inter réseau. Il est raisonnable que cette relation s'étende aussi à inclure un espace d'adressage IPv6 commun. Donc, les hôtes au sein du domaine d'acheminement d'extrémité devraient prendre leurs adresses IPv6 dans le préfixe alloué au domaine d'acheminement d'extrémité.

4.3 Administration au domaine d'acheminement de transit

Deux sortes de domaines d'acheminement de transit sont considérés, les fournisseurs directs et les fournisseurs indirects. La plupart des abonnés à un fournisseur direct sont des domaines qui agissent seulement comme abonnés au service (ils ne portent pas de trafic de transit). La plupart des abonnés à un fournisseur indirect sont des domaines qui, eux-mêmes, agissent comme fournisseurs de services. Dans la terminologie actuelle, un cœur de réseau est un fournisseur indirect, tandis qu'un NSFnet régional est un exemple de fournisseur direct. Chaque cas est discuté séparément ci-dessous

4.3.1 Fournisseur de service direct

Dans un plan d'adressage fondé sur le fournisseur, les fournisseurs de services directs devraient utiliser leur espace d'adresses IPv6 pour allouer des adresses IPv6 à partir d'un unique préfixe aux domaines d'acheminement d'extrémité qu'ils desservent. Les avantages découlant de l'abstraction des données sont supérieurs à ceux du cas des domaines d'acheminement d'extrémité, et le degré supplémentaire d'abstraction des données fourni peut être nécessaire à court terme.

Pour illustrer cela, considérons un exemple d'un fournisseur direct qui dessert 100 clients. Si chaque client prend ses adresses de 4 espaces d'adresse indépendants, le nombre total d'entrées nécessaires pour traiter l'acheminement de ces clients est 400 (100 clients fois 4 fournisseurs). Si chaque client prend ses adresses d'un seul espace d'adresses, le nombre total d'entrées va être seulement 100. Finalement, si tous les clients prennent leur adresses du même espace d'adresses, le nombre total des entrées va être seulement 1.

On s'attend qu'à très court terme le nombre de domaines d'acheminement dans l'Internet va croître au point qu'il va être infaisable d'acheminer sur la base d'un champ plat des domaines d'acheminement. Il va donc être essentiel de fournir un plus grand degré d'abstraction des informations avec IPv6.

Les fournisseurs directs peuvent donner une partie de leur espace d'adresses (les préfixes) aux domaines d'extrémité, sur la base d'un préfixe d'adresse donné au fournisseur. Il en résulterait que les fournisseurs directs annoncent aux autres fournisseurs une petite fraction du nombre de préfixes d'adresses qui serait nécessaire si ils énuméraient les préfixes individuels des domaines d'acheminement d'extrémité. Cela représente une économie significative étant donnée l'étendue prévue de l'interfonctionnement global.

L'efficacité gagnée dans l'acheminement inter domaines garantit clairement l'adoption des préfixes d'adresse IPv6 déduits de l'espace d'adresses IPv6 des fournisseurs.

Le mécanisme de ce scénario est direct. Chaque fournisseur direct reçoit un unique petit ensemble de préfixes d'adresses IPv6, à partir desquels ses domaines d'acheminement d'extrémité rattachés peuvent allouer des préfixes légèrement plus longs d'adresse IPv6. Par exemple, en supposant que NIST soit un domaine d'acheminement d'extrémité dont la liaison inter domaines est via SURANet. Si un unique préfixe d'adresse IPv6 43DC:0A21/32 est alloué à SURANet, NIST pourrait utiliser un unique préfixe IPv6 de 43DC:0A21:7652:34/56.

Si un fournisseur de service direct est connecté à un autre fournisseur (direct ou indirect) via plusieurs points de rattachement, alors dans certains cas il peut être avantageux pour le fournisseur direct d'exercer un certain degré de contrôle sur le couplage entre les points de rattachement et les flux de trafic destinés à un abonné particulier. Un tel contrôle peut être facilité d'abord en partageant tous les abonnés en groupes, de façon à ce que le trafic destiné à tous les abonnés au sein d'un groupe doive s'écouler à travers un point de rattachement particulier. Une fois le partitionnement effectué, l'espace d'adresses du fournisseur est subdivisé selon les frontières de groupes. Un domaine d'acheminement d'extrémité qui veut accepter les préfixes dérivés de son fournisseur direct obtient un préfixe provenant de la subdivision de l'espace d'adresses du fournisseur associée au groupe auquel appartient le domaine.

Au point de rattachement (entre les fournisseurs direct et indirect) le fournisseur direct annonce à la fois un préfixe d'adresse qui correspond à l'espace d'adresses du fournisseur, et un ou plusieurs préfixes d'adresse qui correspondent à l'espace d'adresses associé à chaque subdivision. Ces derniers préfixes correspondent au premier préfixe, mais sont plus longs que celui-ci. L'utilisation de l'algorithme de transmission de "plus longue correspondance" par les receveurs de ces préfixes (par exemple, un routeur au sein du fournisseur indirect) revient à forcer le flux de trafic pour les destinations décrites par les plus longs préfixes d'adresse à passer à travers le point de rattachement où ces préfixes sont annoncés au fournisseur.

Par exemple, supposons que SURANet est connecté à un autre fournisseur régional, NEARNet, à deux points de rattachement, A1 et A2. Un unique préfixe d'adresse IPv6 43DC:0A21/32 est alloué a SURANet. Pour exercer son contrôle sur le flux de trafic destiné à un abonné particulier au sein de SURANet, SURANet peut subdiviser l'espace d'adresses qui lui est alloué en deux groupes, 43DC:0A21:8/34 et 43DC:0A21:C/34. Le premier groupe peut être utilisé pour les sites rattachés à SURANet qui sont plus proches (comme déterminé par la topologie au sein de SURANet) de A1, tandis que le dernier groupe peut être utilisé pour les sites qui sont plus proches de A2. Le routeur SURANet à A1 annonce les deux préfixes d'adresse 43DC:0A21/32 et 43DC:0A21:8/34 au routeur dans NEARNet. De même, le routeur SURANet à A2 annonce les deux préfixes d'adresse 43DC:0A21/32 et 43DC:0A21:C/34 au routeur dans NEARNet. Le trafic qui s'écoule à travers NEARNet pour les destinations qui correspondent au préfixe d'adresse 43DC:0A21:8/34 va entrer dans SURANet à A1, tandis que le trafic pour les destinations qui correspondent au préfixe d'adresse 43DC:0A21:C/34 va entrer dans SURANet en A2.

Noter que l'annonce par le fournisseur direct des informations d'acheminement associées à chaque subdivision doit être faite avec soin pour s'assurer qu'une telle annonce ne va pas résulter en une distribution globale des informations d'accessibilité séparées associées à chaque subdivision, sauf si il est garanti qu'une telle distribution est pour un autre objet (par exemple, de prendre en charge certains aspects d'acheminement fondé sur la politique).

4.3.2 Fournisseurs indirects (cœurs de réseau)

Il n'apparaît pas qu'il y ait à présent de cas où des fournisseurs directs tirent leurs espaces d'adresses de l'espace IPv6 d'un fournisseur indirect (par exemple, un cœur de réseau). Le bénéfice en termes d'abstraction des données d'acheminement est relativement faible. Le nombre de fournisseurs directs aujourd'hui est en dizaines et une croissance de l'ordre de grandeur ne causerait pas une surcharge indue sur les cœurs de réseau. Aussi, on peut s'attendre qu'au fil du temps il y aura une augmentation de l'interconnexion directe des fournisseurs directs, des domaines d'acheminement d'extrémité directement rattachés aux cœurs de réseau, et de liaisons internationales directement rattachées aux fournisseurs. Dans ces circonstances, la distinction entre fournisseurs directs et indirects peut s'estomper.

Un facteur supplémentaire qui détourne l'allocation des adresses IPv6 d'un préfixe de cœur de réseau est que les cœurs de réseau et leurs fournisseurs rattachés sont perçus comme étant indépendants. Les fournisseurs peuvent prendre leur service à longue portée sur plusieurs cœurs de réseau, ou peuvent changer de cœur de réseau si un service moins coûteux devait être fourni ailleurs. Avoir les adresses IPv6 déduites d'un cœur de réseau n'est pas cohérent avec la nature de la relation.

4.4 Domaines d'acheminement multi rattachements

Les discussions du paragraphe 4.3 suggèrent des méthodes pour allouer les adresses IPv6 sur la base de la connexité au fournisseur direct ou indirect. Cela permet de réaliser une grande réduction des informations pour les domaines d'acheminement qui sont rattachés à un seul TRD. En particulier, de tels domaines d'acheminement peuvent choisir leurs adresses IPv6 dans un espace qui leur est délégué par le fournisseur direct. Cela permet au fournisseur, quand il annonce les adresses qu'il peut atteindre aux autres fournisseurs, d'utiliser un seul préfixe d'adresse pour décrire un grand nombre d'adresses IPv6 correspondant à plusieurs domaines d'acheminement.

Cependant, il y a des considérations supplémentaires pour les domaines d'acheminement qui sont rattachés à plusieurs fournisseurs. De tels domaines d'acheminement multi rattachements peuvent, par exemple, consister en des campus et entreprises sur un seul site qui sont rattachés à plusieurs cœurs de réseau, de grandes organisations qui sont rattachées à différents fournisseurs à différentes localisations dans le même pays, ou des organisations multinationales qui sont rattachées à des cœurs de réseau dans divers pays à travers le monde. Il y a un certain nombre de façons possibles de traiter ces domaines d'acheminement multi rattachements.

4.4.1 Solution 1

Une solution possible est que chaque organisation multi rattachements obtienne son espace d'adresses IPv6

indépendamment des fournisseurs auxquels elle est rattachée. Cela permet à chaque organisation multi rattachements de fonder ses allocations IPv6 sur un seul préfixe, et par là de rassembler l'ensemble de toutes les adresses IPv6 accessibles au sein de cette organisation via un seul préfixe. L'inconvénient de cette approche est que comme l'adresse IPv6 pour cette organisation n'a pas de relation avec les adresses d'un TRD particulier, les TRD auxquels cette organisation est rattachée vont avoir besoin d'annoncer le préfixe pour cette organisation aux autres fournisseurs. Les autres fournisseurs (potentiellement dans le monde entier) vont devoir maintenir une entrée explicite pour cette organisation dans leurs tableaux d'acheminement.

Par exemple, supposons qu'une très grosse compagnie nord américaine "Mega Big International Incorporated" (MBII) ait un réseau interne pleinement interconnecté et qu'il lui soit alloué un seul préfixe au titre du préfixe nord américain. Il est probable qu'en dehors de l'Amérique du Nord, une seule entrée peut être maintenue dans les tableaux d'acheminement pour toutes les destinations d'Amérique du Nord. Cependant, au sein de l'Amérique du Nord, chaque fournisseur va avoir besoin de conserver une entrée d'adresse séparée pour MBII. Si MBII est en fait une organisation internationale, il peut alors être nécessaire que chaque fournisseur dans le monde entier conserve une entrée séparée pour MBII (incluant les cœurs de réseau auxquels MBII n'est pas rattaché). Ceci peut clairement être acceptable si il y a un petit nombre de tels domaines d'acheminement multi rattachements, mais ferait peser une charge inacceptable sur les routeurs au sein des cœurs de réseau si toutes les organisations devaient choisir de telles allocations d'adresses. Cette solution ne peut pas s'adapter aux internets où il y a des centaines de milliers d'organisations multi rattachements.

4.4.2 Solution 2

Une seconde approche possible serait que les organisations multi rattachements se voient allouer un espace d'adresses IPv6 séparé pour chaque connexion à un TRD, et d'allouer un seul préfixe à certains sous réseaux de son ou ses domaines sur la base du point d'interconnexion le plus proche. Par exemple, si MBII a des connexions à deux fournisseurs aux U.S.A (un côte Est, et un côte Ouest) ainsi que trois connexions aux cœurs de réseaux nationaux en Europe, et un en extrême Orient, MBII peut alors utiliser six différents préfixes d'adresse. Chaque partie de MBII se verrait allouer un seul préfixe d'adresse sur la base de la connexion la plus proche.

Pour les besoins de l'acheminement externe du trafic provenant de l'extérieur de MBII pour une destination à l'intérieur de MBII, cette approche fonctionne comme si on traitait MBII comme six organisations séparées. Pour les besoins de l'acheminement interne, ou pour l'acheminement du trafic de l'intérieur de MBII à une destination extérieure à MBII, cette approche fonctionne comme la première solution.

Si on suppose que le trafic entrant (venant de l'extérieur de MBII, avec une destination au sein de MBII) va toujours entrer via le point le plus proche de la destination, alors chaque TRD qui a une connexion à MBII a besoin d'annoncer aux autres TRD la capacité d'atteindre seulement les parties de MBII dont l'adresse est prise dans son propre espace d'adresses. Cela implique qu'aucune information d'acheminement supplémentaire n'a besoin d'être échangée entre les TRD, ce qui résulte en une plus petite charge sur les tableaux d'acheminement inter domaines tenus par les TRD comparée à la première solution. Cette solution s'adapte donc mieux aux internets extrêmement grands qui contiennent de très grands nombres d'organisations multi rattachements.

Un problème de cette seconde solution est que les chemins de sauvegarde pour les organisations multi rattachements ne sont pas automatiquement maintenus. Avec la première solution, chaque TRD, en annonçant la capacité de joindre MBII, spécifie qu'il est capable de joindre tous les hôtes au sein de MBII. Avec la seconde solution, chaque TRD annonce qu'il peut joindre tous les hôtes sur la base de son propre préfixe d'adresse, qui n'inclut que certains des hôtes au sein de MBII. Si la connexion entre MBII et un TRD particulier TRD est en panne, alors les hôtes au sein de MBII qui ont des adresses fondées sur ce TRD vont devenir injoignables via l'acheminement inter domaines. L'impact de ce problème peut être un peu réduit par la maintenance d'informations supplémentaires au sein des tableaux d'acheminement, mais cela réduit l'avantage d'adaptabilité de la seconde approche.

La seconde solution exige aussi que quand la connexité externe change, les adresses internes changent aussi.

On note aussi que cette approche et la précédente vont tendre à faire prendre aux paquets des chemins différents. Avec la première approche, les paquets venant de l'extérieur de MBII destinés au sein de MBII vont tendre à entrer via le point qui est le plus proche de la source (ce qui va donc tendre à maximiser la charge sur les réseaux internes à MBII). Avec la seconde solution, les paquets provenant de l'extérieur destinés à MBII vont tendre à entrer via le point qui est le plus proche de la destination (ce qui va tendre à minimiser la charge sur les réseaux au sein de MBII, et la maximiser sur les TRD).

Ces solutions ont aussi des effets différents sur les politiques. Par exemple, supposons que le pays `X' ait une loi disant que le trafic provenant d'une source au sein du pays X pour une destination au sein du pays X doit toujours rester entièrement

au sein du pays. Avec la première solution, il n'est pas possible de déterminer à partir de l'adresse de destination si la destination est ou non au sein du pays. Avec la seconde solution, une adresse séparée peut être allouée aux hôtes qui sont au sein du pays X, permettant ainsi que les politiques d'acheminement soient suivies. De même, supposons que `Little Small Company' (LSC) ait pour politique que ses paquets ne peuvent jamais être envoyés à une destination qui est au sein de MBII. Avec l'une et l'autre solution, les routeurs au sein de LSC peuvent être configurés à éliminer tout trafic qui a une destination au sein de l'espace d'adresses de MBII. Cependant, avec la première solution cela n'exige qu'une entrée ; avec la seconde cela exige de nombreuses entrées et peut être impossible en pratique.

4.4.3 Solution 3

Il y a aussi d'autres solutions possibles. Une troisième approche est d'allouer à chaque organisation multi rattachements un seul préfixe d'adresse, sur la base d'une de ses connexions à un TRD. Les autres TRD auxquels l'organisation multi rattachements est rattachée tiennent une entrée de tableau d'acheminement pour l'organisation, mais sont extrêmement sélectifs en termes de quels autres TRD sont informés de cette route. Cette approche va produire une seule entrée d'acheminement par défaut dont tous les TRD vont connaître comment l'atteindre (parce que on peut supposer que tous les TRD tiennent des chemins avec chaque autre) tout en fournissant un acheminement plus direct dans certains cas.

Il y a au moins une situation dans laquelle cette troisième approche est particulièrement appropriée. Supposons qu'un groupe d'organisations d'intérêt particulier ait déployé son propre fournisseur. Par exemple, supposons que les fabricants et chercheurs nationaux U.S. de gadgets ait constitué un fournisseur à l'échelle des USA, qui est utilisé par les entreprises qui fabriquent des gadgets, et certaines universités qui sont connues pour leurs efforts de recherches sur les gadgets. On peut s'attendre à ce que les diverses organisations qui sont dans le groupe gadget vont faire fonctionner leurs réseaux internes comme des domaines d'acheminement séparés, et que la plupart d'entre elles vont aussi être rattachées à d'autres TRD (car la plupart des organisations impliquées dans la fabrication et la recherche de gadgets vont aussi être impliquées dans d'autres activités). On peut donc s'attendre à ce que beaucoup ou la plupart des organisations du groupe gadget soient à double rattachement, avec un rattachement pour les communications associées au gadget et l'autre rattachement pour les autres types de communications. Supposons aussi que le nombre total d'organisations impliquées dans le groupe gadget soit assez petit pour qu'il soit raisonnable de tenir un tableau d'acheminement contenant une entrée par organisation, mais qu'elles soient réparties dans un plus grand internet avec de nombreux millions de domaines d'acheminement (pour la plupart non associés au gadget).

Avec la troisième approche, chaque organisation multi rattachements du groupe gadget va utiliser une allocation d'adresse fondée sur son ou ses autres rattachements aux TRD (les rattachements non associés au groupe gadget). Le fournisseur gadget va devoir tenir des chemins pour les domaines d'acheminement associés aux diverses organisations membres. de même, tous les membres du groupe gadget vont devoir tenir un tableau des chemins pour les autres membres via le fournisseur gadget. Cependant, comme le fournisseur gadget n'informe pas les autres TRD généraux du monde entier de quelles adresses il peut joindre car ce fournisseur n'est pas destiné à l'utilisation par d'autres organisations extérieures) l'ensemble relativement grand de préfixes d'acheminement ne doit être tenu que dans un nombre d'endroits limité. Les adresses allouées aux diverses organisations qui sont membres du groupe gadget vont fournir un "chemin par défaut" via les autres rattachements aux TRD de chaque membre, tout en permettant que les communications au sein du groupe gadget utilisent le chemin préféré.

4.4.4 Solution 4

Une quatrième solution impliquant l'allocation d'un préfixe d'adresse particulier pour les domaines d'acheminement qui sont rattachés à précisément deux (ou plus) domaines d'acheminement spécifiques. Par exemple, supposons qu'il y ait deux fournisseurs `SouthNorthNet' et `NorthSouthNet' qui ont un très grand nombre d'abonnés en commun (c'est-à-dire, il y a un grand nombre de domaines d'acheminement qui sont rattachés au deux). Plutôt que d'obtenir deux préfixes d'adresse, ces organisations pourraient en obtenir trois. Les domaines d'acheminement qui sont rattachés à NorthSouthNet mais pas à SouthNorthNet obtiennent une allocation d'adresse sur la base d'un des préfixes. Les domaines d'acheminement qui sont rattachés à SouthNorthNet mais pas à NorthSouthNet vont obtenir une adresse fondée sur le second préfixe. Finalement, les domaines d'acheminement qui sont multi rattachement aux deux réseaux vont obtenir une adresse sur la base du troisième préfixe. Chacun de ces deux TRD va alors annoncer deux préfixes aux autres TRD, un préfixe pour les domaines d'acheminement d'extrémité qui lui sont rattachés seulement, et un préfixe pour les domaines d'acheminement d'extrémité rattachés au deux.

Cette quatrième solution sera probablement importante quand l'utilisation de réseaux de données publics deviendra plus courante. En particulier, il est probable qu'à un moment futur un pourcentage substantiel de tous les domaines d'acheminement va être rattaché aux réseaux de données publics. Dans ce cas, presque tous les réseaux financés par les

gouvernements (comme certains réseaux régionaux actuels) pourront avoir un ensemble d'abonnés qui se chevauchent substantiellement avec les réseaux publics.

4.4.5 Résumé

Il y a donc un certain nombre de solutions possibles au problème de l'allocation des adresses IPv6 aux domaines d'acheminement multi rattachements. Chacune de ces solutions a des avantages et inconvénients très différents. Chaque solution fait peser un coût réel (c'est-à-dire, financier) différent sur les organisations multi rattachements, et sur les TRD (y compris ceux auxquels les organisations multi rattachements ne sont pas rattachées).

De plus, la plupart des solutions décrites soulignent aussi le besoin que chaque TRD développe une politique sur si et sous quelles conditions accepter des adresses qui ne sont pas fondées sur son propre préfixe d'adresse, et comment des telles adresses non locales vont être traitées. Par exemple, une politique un peu prudente pourrait être que les préfixes d'adresse IPv6 non locales vont être acceptés de tout domaine d'acheminement d'extrémité rattaché, mais non annoncés aux autres TRD. Dans une politique moins prudente, un TRD pourrait accepter de tels préfixes non locaux et accepter de les échanger avec un ensemble défini d'autres TRD (cet ensemble pourrait être un groupe a priori de TRD qui ont quelque chose en commun comme une localisation géographique, ou le résultat d'un accord spécifique du domaine d'acheminement d'extrémité demandeur). Diverses politiques impliquent des coûts réels pour les TRD, qui peuvent être reflétés dans ces politiques.

4.5 Liaisons privées

La discussion jusqu'à ce point s'est concentrée sur les relations entre adresses IPv6 et acheminement entre divers domaines d'acheminement sur des domaines d'acheminement de transit, où chaque domaine d'acheminement de transit s'interconnecte à un grand nombre de domaines d'acheminement et offre un service plus ou moins public.

Cependant, il peut aussi exister un certain nombre de liaisons qui interconnectent deux domaines d'acheminement de cette façon, et l'usage de ces liaisons peut être limité à porter le trafic seulement entre les deux domaines d'acheminement. On appelle de telles liaisons des liaisons "privées".

Par exemple, supposons que que la corporation XYZ fasse des affaires avec MBII. Dans ce cas, XYZ et MBII peuvent faire un contrat avec un transporteur pour fournir une liaison privée entre les deux corporations, où cette liaison peut seulement être utilisée pour des paquets dont la source est au sein d'une des deux corporations, et dont la destination est au sein de l'autre corporation. Finalement, supposons que la liaison point à point est connectée entre un seul routeur (routeur X) au sein de la corporation XYZ et un seul routeur (routeur M) au sein de MBII. Il est donc nécessaire de configurer le routeur à savoir quelles adresses peuvent être jointes sur cette liaison (spécifiquement, toutes les adresses accessibles dans MBII). De même, il est nécessaire de configurer le routeur M à savoir quelles adresses peuvent être atteintes sur cette liaison (en l'occurrence, toutes les adresses accessibles dans la corporation XYZ).

L'observation importante à faire ici est que la connectivité supplémentaire due à de telles liaisons privées peut être ignorée pour les besoins de l'allocation d'adresses IPv6 et ne pose pas de problème d'acheminement à une plus grande échelle. C'est parce que les informations d'acheminement associées à une telle connectivité ne sont pas propagées à travers l'internet, et donc n'ont pas besoin d'être collectées dans un préfixe de TRD.

Dans notre exemple, supposons que la corporation XYZ a une seule connexion à un fournisseur régional, et a donc à utiliser l'espace d'adresses IPv6 provenant de l'espace donné à ce fournisseur régional. De même, supposons que MBII, comme corporation internationale avec des connexions à six différents fournisseurs, a choisi la seconde solution du paragraphe 4.4, et donc a obtenu six allocations d'adresses différentes. Dans ce cas, toutes les adresses accessibles dans la corporation XYZ peuvent être décrites par un seul préfixe d'adresse (impliquant que le routeur M a seulement besoin d'être configuré avec un seul préfixe d'adresse pour représenter les adresses accessibles sur cette liaison). Toutes les adresses accessibles dans MBII peuvent être décrites par six préfixes d'adresse (ce qui implique que le routeur X doit être configuré avec six préfixes d'adresse pour représenter les adresses accessibles sur la liaison).

Dans certains cas, de telles liaisons privées peuvent permettre de transmettre du trafic pour un petit nombre d'autres domaines d'acheminement, comme d'organisations étroitement affiliées. Cela va augmenter légèrement les exigences de configuration. Cependant, pourvu que le nombre d'organisations qui utilisent la liaison soit relativement faible, cela ne représente pas un problème significatif.

Noter que les relations entre l'acheminement et l'adressage IPv6 décrites dans les autres sections de ce document concernent

les problèmes d'adaptabilité causés par les grands domaines d'acheminement de transit, essentiellement publics, qui interconnectent un grand nombre de domaines d'acheminement. Cependant, pour les besoins de l'allocation d'adresse IPv6, les liaisons privées qui interconnectent seulement un petit nombre de domaines d'acheminement privés ne posent pas de problème, et peuvent être ignorées. Par exemple, cela implique qu'un seul domaine d'acheminement d'extrémité qui a une seule connexion à un fournisseur "public" (par exemple, le Alternet) plus un certain nombre de liaisons privées avec d'autres domaines d'acheminement d'extrémité, peut être traité comme si c'était un seul rattachement au fournisseur pour les besoins de l'allocation d'adresse IPv6. On pense que c'est aussi une autre façon de traiter des domaines multi rattachements.

4.6 Domaines d'acheminement à rattachement zéro

Actuellement, un très grand nombre d'organisations ont des réseaux internes de communications qui ne sont pas connectés à un fournisseur de services. De telles organisations peuvent, cependant, avoir un certain nombre de liaisons privées qu'elles utilisent pour les communications avec d'autres organisations. Ces organisations ne participent pas à l'acheminement global, mais sont satisfaites de l'accessibilité aux organisations avec lesquelles elles ont établi des liaisons privées. On les appelle des domaines d'acheminement à rattachement zéro.

Les domaines d'acheminement à rattachement zéro peuvent être considérés comme une forme dégénérée de domaines d'acheminement avec des liaisons privées, comme exposé au paragraphe précédent, et ne posent pas de problème pour l'acheminement inter domaines. Comme ci-dessus, les informations d'acheminement échangées sur les liaisons privées ont une distribution très limitée, généralement seulement au domaine d'acheminement à l'autre extrémité de la liaison. Donc, il n'y a pas d'exigence d'abstraction d'adresses au delà de celles inhérentes aux préfixes d'adresses échangé à travers la liaison privée.

Cependant, il est important que les domaines d'acheminement à rattachement zéro utilisent des adresses IPv6 valides uniques au monde. Supposons que le domaine d'acheminement à rattachement zéro soit connecté à travers une liaison privée à un domaine d'acheminement. De plus, ce domaine d'acheminement participe à un internet qui souscrit au plan d'adressage global IPv6. Ce domaine doit être capable de distinguer entre les adresses IPv6 du domaine d'acheminement à rattachement zéro et toutes les autres adresses IPv6 auxquelles il peut devoir acheminer. La seule façon dont cela peut être garanti est que le domaine d'acheminement à rattachement zéro utilise des adresses IPv6 uniques au monde.

Alors que les adresses uniques au monde sont nécessaires pour différencier entre destinations dans l'Internet, les adresses uniques au monde peuvent n'être pas suffisantes pour garantir la connexité mondiale. Si un domaine d'acheminement à rattachement zéro est connecté à l'Internet, le bloc d'adresses utilisé au sein du domaine peut n'être pas en relation avec le bloc des adresses allouées au fournisseur direct du domaine. Afin de conserver les gains de l'acheminement hiérarchique et l'allocation d'adresses, le domaine à rattachement zéro devrait dans ces circonstances changer les adresses allouées aux systèmes au sein du domaine.

4.7 Agrégation continentale

Un autre niveau de hiérarchie peut aussi être utilisé dans ce schéma d'adressage pour réduire encore la quantité d'informations d'acheminement nécessaires pour l'acheminement global. L'agrégation continentale est utile parce que les limites de continent fournissent des barrières naturelles aux frontières de connexion topologiques et administratives. Donc, elle présente une frontière naturelle pour un autre niveau d'agrégation des informations d'acheminement inter domaines. Pour utiliser cela, il est nécessaire que chaque continent ait alloué un bloc d'adresses contiguës approprié. Les fournisseurs (directs et indirects) au sein de ce continent vont allouer leurs adresses à partir de cet espace. Noter qu'il y a de nombreuses exceptions à cela, dans lesquelles un fournisseur de services (direct ou indirect) s'étend à travers une division continentale. Ces exceptions peuvent être traitées d'une façon similaire aux domaines d'acheminement multi rattachement, comme discuté précédemment.

L'avantage de l'agrégation continentale est qu'elle aide à absorber l'entropie introduite au sein de l'acheminement continental causée par les cas où une organisation doit utiliser un préfixe d'adresse qui doit être annoncé au delà de son fournisseur direct. Dans ce cas, si l'adresse est prise dans le préfixe continental, le coût supplémentaire de la route n'est pas propagé au delà du point où l'agrégation continentale a lieu.

Noter que, à l'opposé du cas des fournisseurs, l'agrégation des informations d'acheminement continentales ne peut pas être faite sur le continent auquel le préfixe est alloué. Le coût des liaisons inter continentales (et en particulier transocéaniques) est très élevé. Si l'agrégation est effectuée sur le côté "proche" de la liaison, alors les informations d'acheminement sur des destinations injoignable au sein de ce continent peuvent seulement résider sur ce continent. Autrement, si l'agrégation continentale est faite sur le côté "distant" de la liaison inter continentale, l'extrémité "distante" peut effectuer l'agrégation et

l'injecter dans l'acheminement continental. Cela signifie que les destinations qui font partie de l'agrégation continentale, mais pour lesquelles il n'y a pas de préfixe correspondant plus spécifique peuvent être rejetées avant de quitter le continent d'où elle sont originaires.

Par exemple, supposons qu'un préfixe de 46/8 soit alloué à l'Europe, tel que l'acheminement européen contienne aussi les préfixes plus longs 46DC:0A01/32 et 46DC:0A02/32. Tous les plus longs préfixes européens peuvent être annoncés à travers une liaison transatlantique en Amérique du Nord. Le routeur en Amérique du Nord va alors agréger ces chemins, et annoncer seulement le préfixe 46/8 dans l'acheminement nord américain. Les paquets qui sont destinés à 46DC:0A01:1234:5678:ABCD:8765:4321:AABB vont traverser l'acheminement nord américain, mais vont rencontrer le routeur nord américain qui a effectué l'agrégation européenne. Si le préfixe 46DC:0A01/32 est injoignable, le routeur va éliminer le paquet et envoyer un message injoignable sans utiliser la liaison transatlantique.

4.8 Adresses privées (utilisation locale)

De nombreux domaines vont avoir des hôtes qui, pour une raison ou pour une autre, ne vont pas exiger d'adresse IPv6 unique au monde. Un domaine qui décide d'utiliser des adresses IPv6 tirées de l'espace d'adresses privé est capable de le faire sans allocation d'adresse par une autorité. À l'inverse, le préfixe d'adresse privée n'a pas besoin d'être annoncé dans la portion publique de l'Internet.

Afin d'utiliser l'espace d'adresses privé, un domaine a besoin de déterminer quels hôtes n'ont pas besoin de connexité de couche réseau en dehors du domaine dans le futur prévisible. De tels hôtes vont être appelés des hôtes privés, et peuvent utiliser les adresses privées décrites ci-dessus si cela est topologiquement convenable. Les hôtes privés peuvent communiquer avec tous les autres hôtes à l'intérieur du domaine, aussi bien publics que privés. Cependant, ils ne peuvent pas avoir de connexité IPv6 avec un hôte externe. Bien qu'il n'ait pas de connexité de couche réseau externe , un hôte privé peut quand même avoir accès aux services externes via des relais de couche application. Les hôtes publics n'ont pas de connexité aux hôtes privés en-dehors de leur propre domaine.

Parce que les adresses privées n'ont pas de signification mondiale, les informations d'accessibilité associées à l'espace d'adresses privé ne devront pas être propagées sur des liaisons inter domaines, et les paquets avec des adresses de source ou destination privées ne devrait pas être transmises sur de telles liaisons. Les routeurs dans les domaines qui n'utilisent pas d'espace d'adresses privées, en particulier ceux des fournisseurs de service Internet, sont supposés être configurés à rejeter (filtrer) les informations d'acheminement qui portent des informations d'accessibilité associées à des adresses privées. Si un tel routeur reçoit de telles informations, le rejet ne devra pas être traité comme une erreur de protocole d'acheminement.

De plus, des références indirectes aux adresses privées devraient être contenues au sein de l'entreprise qui utilise ces adresses. Un exemple évident de telles références est celui des enregistrements de ressource (RR) du DNS. Une approche possible pour éviter des fuites de RR du DNS est de faire fonctionner deux serveurs de noms, un serveur externe d'autorité pour toutes les adresses IP uniques au monde de l'entreprise et un serveur interne d'autorité pour toutes les adresses IP de l'entreprise, publiques et privées. Afin d'assurer la cohérence des deux serveurs, ils devraient être configurés à partir des mêmes données dont les serveur de noms externe reçoit seulement une version filtrée. Les résolveurs sur tous les hôtes internes, aussi bien publics que privés, interrogent seulement le serveur de noms interne. Le serveur externe résout les interrogations provenant de résolveurs en dehors de l'entreprise et est relié au DNS mondial. Le serveur interne transmet toutes les interrogations sur des informations en dehors de l'entreprise au serveur de noms externe, afin que tous les hôtes internes puissent accéder au DNS mondial. Cela assure que les informations sur les hôtes privés n'atteignent pas les résolveurs et serveurs de noms en dehors de l'entreprise.

4.9 Interaction avec la politique d'acheminement

On suppose que tout protocole d'acheminement inter domaines va avoir des difficultés à essayer d'agréger plusieurs destinations avec des politiques dissemblables. En même temps, la capacité d'agréger les informations d'acheminement sans violer les politiques d'acheminement est essentiel. Donc, on suggère que les autorités d'allocation d'adresses tentent d'allouer les adresses de telle sorte que les agrégats de destinations avec des politiques similaires puissent être facilement formés.

5. Recommandations

On prévoit que la croissance exponentielle actuelle de l'Internet va se continuer ou accélérer dans l'avenir prévisible. De plus, on prévoit une rapide internationalisation de l'Internet. La capacité de l'acheminement à s'adapter dépend de l'utilisation de l'abstraction des données sur la base de la hiérarchisation des adresses IPv6. Il est donc essentiel de choisir avec grand soin une structure hiérarchique des adresses IPv6.

Une grande attention doit être portée à la définition des structures d'adressage pour équilibrer les conflits d'objectifs entre :
- l'optimisation de chemin
- l'efficacité de l'algorithme d'acheminement
- la facilité et l'efficacité administrative de l'enregistrement d'adresse
- les considérations de quelles adresses sont allouées par quelle autorité d'adressage.

Il est de l'intérêt de la communauté de l'inter réseautage que les coûts de fonctionnement restent aussi faibles que possible. Dans le cas de l'allocation d'adresse IPv6 cela signifie encore que l'abstraction des données d'acheminement doit être encouragée.

Afin que l'abstraction des données soit possible, l'allocation des adresses IPv6 doit être réalisée en cohérence avec la topologie physique réelle de l'Internet. Par exemple, dans les cas où les frontières organisationnelles et administratives ne sont pas en rapport avec la topologie réelle de réseau, l'allocation d'adresses fondée sur de telles limites organisationnelles n'est pas recommandée.

Les protocoles d'acheminement intra domaine permettent de conserver une abstraction des informations au sein d'un domaine. Pour les domaines d'acheminement à rattachement zéro et à rattachement unique (qui sont supposés rester à rattachement zéro ou à rattachement unique) on recommande que les adresses IPv6 allouées au sein d'un seul domaine d'acheminement utilisent un seul préfixe d'adresse alloué à ce domaine. Précisément, cela permet que l'ensemble de toutes les adresses IPv6 accessibles au sein d'un seul domaine soit pleinement décrit via un seul préfixe.

On prévoit que le nombre total de domaines d'acheminement existants dans l'Internet mondial sera assez grand pour que des niveaux supplémentaires d'abstraction hiérarchique des données soient nécessaires au delà du niveau du domaine d'acheminement.

Dans la plupart des cas, la topologie de réseau va avoir une relation étroite avec les frontières nationales. Par exemple, le degré de connexité réseau sera souvent supérieur au sein d'un seul pays que entre les pays. Il est donc approprié de faire des recommandations spécifiques sur la base des frontières nationales, en comprenant qu'il peut y avoir des situations spécifiques où ces recommandations générales doivent être modifiées.

De plus, de l'expérience de IPv4, on sent que l'agrégation continentale est bénéfique et devrait être prise en charge lorsque possible comme moyen de limiter l'extension non garantie des exceptions d'acheminement.

5.1 Recommandations d'un plan d'allocation d'adresses

On prévoit que l'inter connectivité publique entre domaines d'acheminement privés va être fournie par un ensemble divers de TRD, incluant (mais sans s'y limiter nécessairement) :
- les cœurs de réseaux ;
- un certain nombre de réseaux régionaux ou nationaux ;
- un certain nombre de réseaux commerciaux publics de données.

Ces réseaux ne vont pas être interconnectés d'une manière strictement hiérarchique (par exemple, il est supposé y avoir une connexité directe entre les réseaux régionaux, et tous ces types de réseaux peuvent avoir des connexions internationales directes). Ces TRD vont être utilisés pour interconnecter une grande variété de domaines d'acheminement, chacun pouvant comprendre une seule corporation, une partie d'une corporation, un campus universitaire, une agence gouvernementale, ou une autre unité organisationnelle.

De plus, on peut s'attendre à ce que certaines corporations privées utilisent des TRD privés dédiés pour les communications au sein de leur propre corporation.

On prévoit que la grande majorité des domaines d'acheminement va être rattachée à seulement un des TRD. Cela va permettre une agrégation hiérarchique d'adresse sur la base du TRD. On recommande donc fortement que les adresses

soient allouées de façon hiérarchique, sur la base des préfixes d'adresses alloués aux TRD individuels.

Pour prendre en charge l'agrégation continentale des chemins, on recommande que toutes les adresses pour les TRD qui sont entièrement au sein d'un continent soient prises sur le préfixe continental.

Pour le schéma d'allocation d'adresses proposé, cela implique que des portions de l'espace d'adresses IPv6 devraient être allouées à chaque TRD (en incluant explicitement les cœurs de réseau et les réseaux régionaux). Pour les domaines d'acheminement d'extrémité qui sont connectés à un seul TRD, il devrait leur être alloué une valeur de préfixe dans l'espace d'adresses alloué à ce TRD.

Pour les domaines d'acheminement qui ne sont pas rattachés à un TRD publiquement disponible, il n'y a pas le même besoin urgent d'agrégation hiérarchique d'adresses. On ne fait donc pas de recommandations supplémentaires pour de tels domaines d'acheminement "isolés". Lorsque de tels domaines sont connectés aux autres domaines par des liaisons point à point privées, et lorsque de telles liaisons sont utilisées seulement pour l'acheminement entre deux domaines qu'elles interconnectent, là encore aucun problème technique supplémentaire relatif à l'abréviation d'adresse n'est causé par une telle liaison, et aucune recommandation spécifique supplémentaire n'est nécessaire. On recommande que comme ces domaines peuvent souhaiter utiliser un espace d'adresses privé, que le plan d'adressage spécifie un préfixe spécifique pour l'adressage privé.

De plus, afin de permettre l'agrégation des adresses IPv6 aux frontières nationales et continentales en aussi peu de préfixes que possible, on recommande que les adresses IPv6 allouées aux domaines d'acheminement devraient être allouées sur la base de la connexité de chaque domaine d'acheminement aux cœurs de réseau nationaux et continentaux de l'Internet.

5.2 Recommandations de domaines d'acheminement multi rattachements

Certains domaines d'acheminement vont être rattachés à plusieurs TRD au sein du même pays, ou à des TRD au sein de plusieurs pays différents. On les appelle des domaines d'acheminement "multi rattachements". Il est clair que le strict modèle hiérarchique discuté ci-dessus ne s'adapte pas nettement à de tels domaines d'acheminement.

Il y a plusieurs façons possibles de traiter ces domaines d'acheminement multi rattachements, comme décrit au paragraphe 4.4. Chacune de ces méthodes varie eu égard à la quantité des informations qui doivent être conservées pour l'acheminement inter domaines et aussi à l'égard des chemins inter domaines. De plus, l'organisation qui va supporter la charge de ce coût varie selon les solutions possibles. Par exemple, les solutions varient en fonction :
- des ressources utilisées au sein des routeurs dans les TRD ;
- des coûts administratifs du personnel du TRD ;
- de la difficulté de configuration des informations d'acheminement inter domaines fondé sur la politique au sein des domaines d'acheminement d'extrémité.

Aussi, la solution utilisée peut affecter les chemins réels que suivent les paquets, et peut affecter la disponibilité de chemins de secours en cas de défaillance du chemin principal.

Pour ces raisons il n'est pas possible de rendre obligatoire une seule solution pour toutes les situations. Des considérations économiques vont plutôt exiger diverses solutions pour les différents domaines d'acheminement, fournisseurs de services, et cœurs de réseau.

6. Considérations sur la sécurité

Les questions de sécurité ne sont pas abordées dans le présent document.

7. Remerciements

Le présent document s'appuie largement sur la RFC 1518. La Section sur les adresses privées a beaucoup emprunté à la RFC 1597.

Nous souhaitons remercier Havard Eidnes, Bill Manning, Roger Fajman de leur relecture et leurs commentaires constructifs.

Références

[RFC1883] S. Deering, R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1995. *(Rendue obsolète par la* RFC2460) *(P.S.)*

[RFC1884] R. Hinden, S. Deering, éditeurs, "Architecture d'adressage d'IP version 6", décembre 1995. (*Rendue obsolète par la* RFC2373) *(Historique)*

Adresse des auteurs

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

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