Groupe de travail Réseau
Request for Comments : 3056
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Carpenter
K. Moore
février 2001

Connexion des domaines IPv6 via des nuages IPv4

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire spécifie un mécanisme intérimaire facultatif pour que les sites IPv6 communiquent les uns avec les autres sur le réseau IPv4 sans établissement explicite de tunnel, et pour qu'ils communiquent avec les domaines IPv6 natifs via des routeurs relais. Il traite en fait les réseaux IPv4 de large zone comme une couche de liaison en point à point en envoi individuel. Le mécanisme est destiné à être un outil de démarrage de la transition durant la période de coexistence de IPv4 et IPv6. Il n'est pas destiné à être une solution permanente.
Le document définit une méthode pour allouer un préfixe d'adresse IPv6 intérimaire unique à tout site qui a actuellement au moins une adresse IPv4 unique au monde, et spécifie un mécanisme d'encapsulation pour transmettre les paquets IPv6 en utilisant un tel préfixe sur le réseau IPv4 mondial.

Les motivations de cette méthode sont de permettre aux domaines ou hôtes IPv6, rattachés à un réseau IPv4 qui n'a pas de prise en charge native d'IPv6, de communiquer avec d'autres domaines ou hôtes IPv6 dans la même situation avec une configuration manuelle minimale, avant qu'ils puissent obtenir une connexité IPv6 naturelle. Il fournit incidemment un préfixe d'adresse IPv6 intérimaire unique au monde à tout site qui a au moins une adresse IPv4 unique au monde, même si elle est combinée à un traducteur d'adresse réseau (NAT, *Network Address Translator*) IPv4.

Table des Matières

1. Introduction

Le présent mémoire spécifie un mécanisme intérimaire facultatif pour que les sites IPv6 communiquent les uns avec les autres sur le réseau IPv4 sans établissement explicite de tunnel, et pour qu'ils communiquent avec les domaines IPv6 natifs via des routeurs relais. Il traite en fait les réseaux IPv4 de large zone comme une couche liaison point à point en envoi individuel. Le mécanisme est destiné à être un outil de démarrage de transition durant la période de coexistence de IPv4 et IPv6. Il n'est pas destiné à être une solution permanente.

Le document définit une méthode pour allouer un préfixe d'adresse IPv6 unique intérimaire à tout site qui a actuellement au moins une adresse IPv4 unique au monde, et spécifie un mécanisme d'encapsulation pour transmettre des paquets IPv6 en utilisant un tel préfixe sur le réseau IPv4 mondial. Il décrit aussi des scénarios pour l'utilisation de tels préfixes durant la phase de coexistence de la transition de IPv4 à IPv6. Noter que ces scénarios sont seulement une partie de l'image totale de la transition vers IPv6. Noter aussi que ceci est considéré comme étant une solution intérimaire et que les sites devraient migrer dès que possible vers les préfixes IPv6 natifs et la connexité IPv6 native. Cela sera possible dès que le FAI du site offrira la connexité IPv6 native.

Le mécanisme de base décrit dans le présent document, qui s'applique aux sites plutôt qu'aux hôtes individuels, va s'adapter indéfiniment en limitant le nombre de sites desservis par un routeur relais particulier (voir au paragraphe 5.2). Il va introduire de nouvelles entrées dans les tableaux d'acheminement IPv4, et exactement une nouvelle entrée dans le tableau d'acheminement IPv6 natif (voir au paragraphe 5.10).

Bien que le mécanisme soit spécifié pour un site IPv6, il peut également s'appliquer à un hôte IPv6 individuel ou à un très petit site, pour autant qu'il ait au moins une adresse IPv4 unique au monde. Cependant, ce dernier cas soulève de sérieux problèmes d'adaptation qui feront l'objet d'études complémentaires [SCALE].

Les motivations de cette méthode sont de permettre à des sites ou hôtes IPv6 isolés, rattachés à un réseau de zone large qui n'a pas de prise en charge d'IPv6 natif de communiquer avec les autres domaines ou hôtes IPv6 qui sont dans la même situation avec le minimum de configuration manuelle.

Les sites ou hôtes IPv6 connectés en utilisant cette méthode n'exigent pas d'adresses IPv6 compatibles IPv4 de la [RFC2893] ou de tunnels configurés. De cette façon, IPv6 gagne une considérable indépendance à l'égard du réseau de large zone sous-jacent et peut passer par dessus beaucoup de bonds des sous réseaux IPv4. Le nom abrégé de ce mécanisme est 6-4 (pour ne pas le confondre avec celui de la [RFC2529]). Le mécanisme 6-4 est normalement mis en œuvre presque entièrement dans les routeurs frontières, sans modification spécifique des hôtes à part une sélection d'adresse par défaut suggérée. Une modeste quantité de configuration de routeur est seulement exigée.

Les Sections 2 à 4 du présent document spécifient le schéma technique de 6-4. La Section 5 discute certains, mais pas tous, des scénarios d'usage, y compris les aspects d'acheminement, pour les sites 6-4. Les scénarios pour les hôtes 6-4 isolés ne sont pas exposés dans le présent document. Les Sections 6 à 9 discutent des autres considérations générales.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

1.1 Terminologie

La terminologie de la [RFC2460] s'applique au présent document.

pseudo-interface 6-4 :
L'encapsulation 6-4 de paquets IPv6 à l'intérieur de paquets IPv4 survient à un point qui est logiquement équivalent à une interface IPv6, la couche de liaison étant le réseau IPv4 d'envoi individuel. Ce point est référencé comme une pseudo-interface. Certaines mises en œuvre peuvent la traiter exactement comme toute autre interface et d'autres peuvent la traiter comme un point d'extrémité de tunnel.

préfixe 6-4 : C'est un préfixe IPv6 construit conformément aux règles de la Section 2 ci-dessous.

adresse 6-4 : C'est une adresse IPv6 construite en utilisant un préfixe 6-4.

adresse IPv6 native : C'est une adresse IPv6 construite en utilisant un autre type de préfixe que 6-4.

routeur 6-4 (ou routeur frontière 6-4) : C'est un routeur IPv6 qui prend en charge une pseudo-interface 6-4. C'est normalement le routeur frontière entre un site IPv6 et un réseau IPv4 de large zone.

hôte 6-4 : C'est un hôte IPv6 qui se trouve avoir au moins une adresse 6-4. Sous tous autres aspects c'est un hôte IPv6 standard.

Note : Un nœud IPv6 peut dans certains cas utiliser une adresse 6-4 pour un tunnel configuré. Un tel nœud peut fonctionner comme un hôte IPv6 en utilisant une adresse 6-4 sur son interface de tunnel configuré, et il peut aussi servir de routeur IPv6 pour d'autres hôtes via une pseudo-interface 6-4, mais ce sont des fonctions distinctes.

site 6-4 : C'est un site qui fonctionne avec IPv6 en interne en utilisant des adresses 6-4, contenant donc au moins un hôte 6-4 et au moins un routeur 6-4.

Routeur relais : C'est un routeur 6-4 configuré pour prendre en charge l'acheminement de transit entre des adresses 6-4 et des adresses IPv6 natives.

domaine d'acheminement extérieur 6-4 : C'est un domaine qui interconnecte un ensemble de routeurs 6-4 et de routeurs relais. Il est distinct d'un domaine d'acheminement intérieur d'un site IPv6, et distinct de tous les domaines d'acheminement extérieurs IPv6 natifs.

2. Allocation d'un préfixe IPv6

Supposons qu'un site d'abonné ait au moins une adresse IPv4 valide à 32 bits unique au monde, qu'on appellera dans le présent document "V4ADDR". Cette adresse DOIT être dûment allouée au site par un registraire d'adresses (éventuellement via un fournisseur d'accès) et elle NE DOIT PAS être une adresse privée [RFC1918].

L'IANA a alloué de façon permanente un identifiant d'agrégateur de niveau supérieur (TLA, *Top Level Aggregator*) IPv6 de 13 bits IPv6 sous le préfixe de format IPv6 001 [RFC2373], [RFC2374] pour le schéma 6-4. Sa valeur numérique est 0x0002, c'est-à-dire que c'est 2002::/16 quand il est exprimé comme un préfixe d'adresse IPv6.

Le site d'abonné est alors réputé avoir le préfixe d'adresse IPv6 suivant, sans qu'aucune autre procédure d'allocation soit nécessaire :

Longueur de préfixe : 48 bits
Format du préfixe : 001
Valeur du TLA : 0x0002
Valeur du NLA : V4ADDR

Qui est illustré comme suit :

```
| 3 |  13  |    32     |   16   |          64 bits               |
+---+------+-----------+--------+--------------------------------+
|FP | TLA  | V4ADDR    | SLA ID |   Identifiant d'interface      |
|001|0x0002|           |        |                                |
+---+------+-----------+--------+--------------------------------+
```

Donc, ce préfixe a exactement le même format que les préfixes /48 normaux alloués conformément à la [RFC2374]. Il peut être abrégé en 2002:V4ADDR::/48. Au sein du site d'abonné, il peut être utilisés exactement comme n'importe quel autre préfixe IPv6 valide, par exemple, pour une allocation et découverte automatisée d'adresse selon les mécanismes normaux comme les [RFC2462], [RFC2461], pour l'acheminement IPv6 natif, ou pour le mécanisme "6sur4" de la [RFC2529].

Noter que si l'adresse IPv4 est allouée de façon dynamique, le préfixe IPv6 correspondant va aussi être dynamique par nature, avec la même durée de vie.

2.1 Sélection d'adresse

Pour assurer le fonctionnement correct de 6-4 dans des topologies complexes, la sélection d'adresse de source et de destination doit être mise en œuvre de façon appropriée. Si l'hôte IPv6 de source qui envoie un paquet a au moins une adresse 2002:: qui lui est allouée, et si l'ensemble des adresses IPv6 retourné par le DNS pour l'hôte de destination contient au moins une adresse 2002::, l'hôte de source doit faire un choix approprié des adresses de source et de destination à utiliser. Les mécanismes pour la sélection d'adresse en général sont à l'étude au moment de cette publication [RFC3484]. Sous réserve de ces mécanismes généraux, le principe qui va normalement permettre un fonctionnement correct du 6-4 est celui-ci :

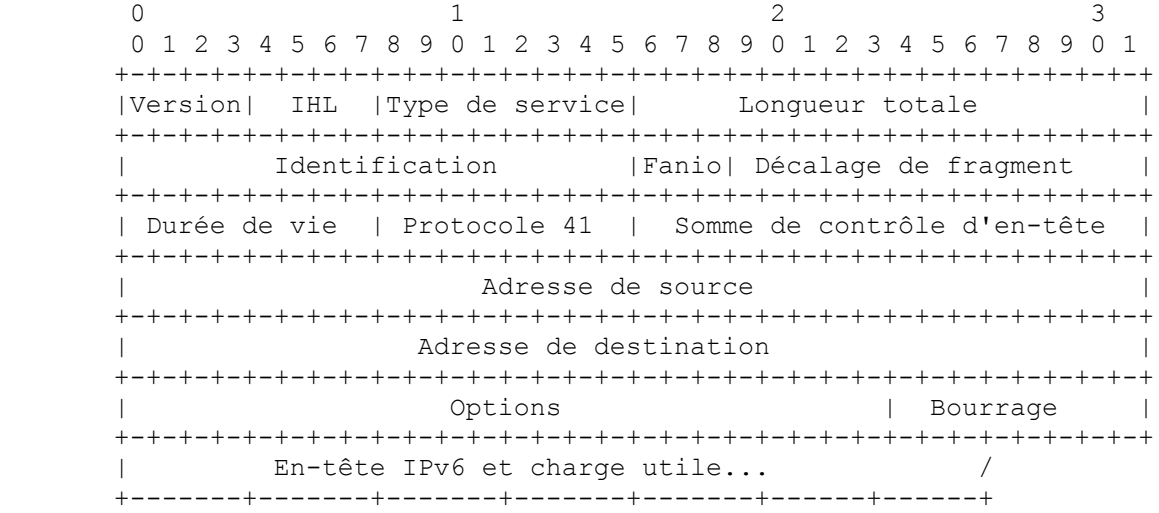
Si un hôte a seulement une adresse 6-4, et si l'autre a à la fois une adresse 6-4 et une adresse IPv6 native, l'adresse 6-4 devrait alors être utilisée pour les deux.

Si les deux hôtes ont une adresse 6-4 et une adresse IPv6 native, ils devraient utiliser l'adresse 6-4 pour les deux, ou l'adresse IPv6 native pour les deux. Le choix devrait être configurable. La configuration par défaut devrait être IPv6 natif pour les deux.

3. Encapsulation dans IPv4

Les paquets IPv6 provenant d'un site 6-4 sont encapsulés dans un paquet IPv4 lorsque ils quittent le site via sa connexion IPv4 externe. Noter que l'interface IPv4 qui porte le trafic 6-4 est une notion équivalente à une interface IPv6, mais on l'appelle ci-dessous une pseudo-interface, bien que cette expression ne soit pas destinée à définir une technique de mise en œuvre. Une V4ADDR DOIT être configurée sur l'interface IPv4.

Les paquets IPv6 sont transmis dans les paquets IPv4 [RFC0791] avec un type de protocole IPv4 de 41, le même que celui alloué par la [RFC2893] pour les paquets IPv6 qui sont tunnelés à l'intérieur de trames IPv4. L'en-tête IPv4 contient les adresses IPv4 de destination et de source. Une d'elles ou les deux seront identiques au champ V4ADDR d'un préfixe IPv6 formé comme spécifié ci-dessus (voir les précisions à la section 5). Le corps du paquet IPv4 contient l'en-tête IPv6 et la charge utile.



La durée de vie IPv4 sera réglée normalement selon la [RFC0791], comme le sera la limite de bonds IPv6 encapsulée [RFC2460]. Les autres considérations sont comme décrit au paragraphe 4.1.2 de la [RFC2893].

3.1 Adresse et NUD de liaison locale

L'adresse de liaison locale d'une pseudo-interface 6-4 effectuant l'encapsulation 6-4 serait, si nécessaire, formée comme décrit au paragraphe 3.7 de la [RFC2893]. Cependant, aucun scénario n'est connu où une telle adresse serait utile, car une passerelle 6-4 homologue ne peut pas déterminer l'adresse de couche liaison appropriée (IPv4) à laquelle envoyer.

La détection d'inaccessibilité du voisin (NUD, *Neighbor Unreachability Detection*) est traitée comme décrit au paragraphe 3.8 de la [RFC2893].

4. Unité de transmission maximum

Les questions de taille d'unité de transmission maximum (MTU) sont celles décrites pour les tunnels dans la [RFC2893].

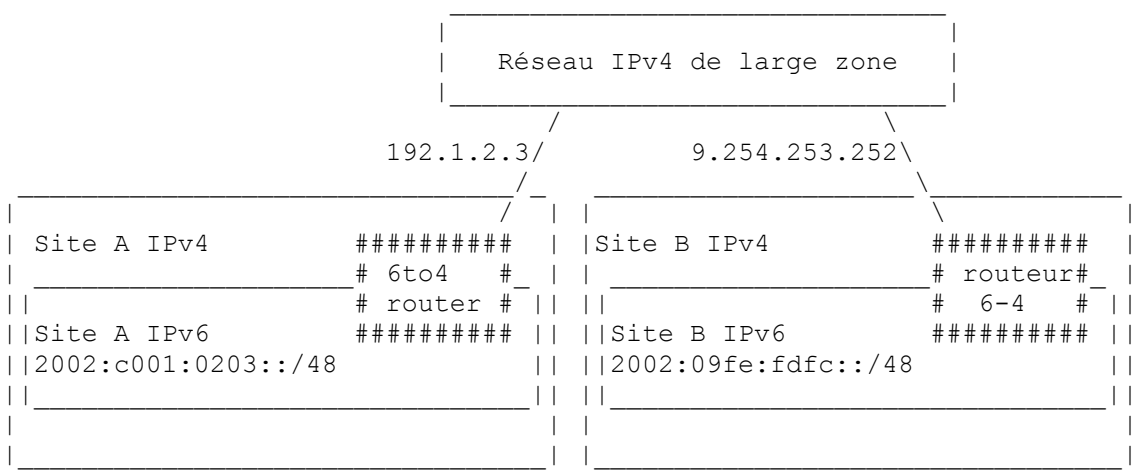
Si la taille de la MTU IPv6 se révèle être trop grande pour certains réseaux IPv4 intermédiaires, la fragmentation IPv4 va intervenir. Bien qu'indésirable, ce n'est pas nécessairement un désastre, sauf si les fragments sont livrés à des destinations IPv4 différentes à cause de certaines formes d'envoi à la cantonade IPv4. Le bit IPv4 "Ne pas fragmenter" NE DEVRAIT PAS être établi dans l'en-tête IPv4 d'encapsulation.

5. Scénarios d'envoi individuel, échelonnement, et transition aux préfixes normaux

5.1 Scénario simple – tous les sites font la même chose

Le plus simple scénario de déploiement pour 6-4 est de l'utiliser entre un certain nombre de sites, dont chacun a au moins une connexion à un Internet IPv4 partagé. Cela peut être l'Internet mondial, ou cela peut être un réseau IP d'entreprise. Dans le cas de l'Internet mondial, il n'est pas exigé que les sites soient tous connectés au même fournisseur d'accès Internet. La seule exigence est que tous les sites soient capables d'envoyer des paquets IPv4 avec le type de protocole 41 à n'importe lequel des autres. Par définition, chaque site a un préfixe IPv6 du format défini à la Section 2. Il va donc créer des enregistrements DNS pour ces adresses. Par exemple, le site A qui possède l'adresse IPv4 192.1.2.3 va créer des enregistrements DNS avec le préfixe IPv6 {FP=001,TLA=0x0002,NLA=192.1.2.3}/48 (c'est-à-dire, 2002:c001:0203::/48). Le site B qui possède l'adresse 9.254.253.252 va créer des enregistrements DNS avec le préfixe IPv6 {FP=001,TLA=0x0002,NLA=9.254.253.252}/48 (c'est-à-dire, 2002:09fe:fdfc::/48).

Lorsque un hôte IPv6 sur le site B interroge une entrée du DNS sur un hôte sur le site A, ou obtient autrement son adresse, il obtient une adresse avec le préfixe {FP=001,TLA=0x0002,NLA=192.1.2.3}/48 et le SLA et l'identifiant d'interface qui s'appliquent. L'inverse s'applique quand un hôte sur le site A interroge le DNS sur un hôte sur le site B. Les paquets IPv6 sont formés et transmis de la façon normale au sein des deux sites.



Au sein d'un site 6-4, les adresses avec le préfixe 2002::/16, à part celles qui ont le préfixe local 2002:V4ADDR::/48, vont être traitées comme toute autre adresse IPv6 non locale, c'est-à-dire, par un chemin explicite ou par défaut vers le routeur frontière 6-4.

Lorsque un paquet sortant atteint le routeur 6-4, il est encapsulé comme défini à la Section 3, conformément à la règle d'envoi supplémentaire définie au paragraphe 5.3. Les paquets entrants sont désencapsulés conformément à la règle de désencapsulation supplémentaire définie au paragraphe 5.3. Les règles supplémentaires d'envoi et de désencapsulation sont les seuls changements à la transmission IPv6, et elles n'interviennent qu'aux routeurs frontières. Aucune information d'acheminement IPv4 n'est importée dans l'acheminement IPv6 (ni vice versa).

Dans ce scénario, tous les ensembles de sites 6-4 peuvent interopérer sans configuration de tunnel, et aucune exigence particulière de la part du service IPv4. Tout ce qui est exigé sont les entrées appropriées du DNS et les règles supplémentaires d'envoi et de désencapsulation configurées dans le routeur 6-4. Ce routeur DEVRAIT aussi générer les annonces de préfixe IPv6 appropriées [RFC2462], [RFC2461].

Bien que le site A et le site B aient chacun besoin de faire fonctionner l'acheminement IPv6 en interne, ils n'ont pas besoin de faire fonctionner un protocole d'acheminement IPv6 extérieur dans ce scénario simple ; l'acheminement IPv4 extérieur fait le travail pour eux.

Il est RECOMMANDÉ que dans tous les cas, chaque site n'utilise qu'une seule adresse IPv4 par routeur 6-4, et ce devrait être l'adresse allouée à l'interface externe du routeur 6-4. Les sites à rattachement unique DEVRAIENT donc n'utiliser qu'une adresse IPv4 pour l'acheminement 6-4. Les sites multi rattachements sont discutés brièvement au paragraphe 5.6.

Grâce à l'absence de configuration, et au caractère réparti du modèle de déploiement, on pense qu'il n'y a pas de problème particulier d'adaptation avec le mécanisme 6-4 de base à part la redondance de l'encapsulation. Précisément, il n'introduit pas de nouvelle entrée dans les tableaux d'acheminement IPv4.

5.2 Scénario mixte avec relais vers l'IPv6 natif

Durant la transition vers IPv6, on peut s'attendre à ce que certains sites s'ajustent au modèle qu'on vient juste de décrire (sites isolés dont la seule connexité est avec l'Internet IPv4) tandis que d'autres feront partie de plus grandes îles d'IPv6 natif ou tunnelés qui utilisent l'espace d'adresse de TLA IPv6 normal. Les sites 6-4 auront besoin de la connexité avec ces îles d'IPv6 natif et vice versa. Dans le modèle 6-4, cette connexité est accomplie par les routeurs IPv6 qui possèdent à la fois des adresses 6-4 et IPv6 natif. Bien qu'ils se comportent essentiellement comme des routeurs IPv6 standard, pour les besoins du présent document, on les appelle des routeurs relais pour les distinguer des routeurs qui ne prennent en charge que l'IPv6 natif.

Il doit y avoir au moins un routeur qui agit comme relais entre le domaine 6-4 et un domaine IPv6 natif donné. Il n'y a rien de particulier à en dire, c'est simplement un routeur normal qui se trouve avoir au moins une pseudo-interface 6-4 logique et au moins une autre interface IPv6. Comme c'est un routeur 6-4, il met en œuvre les règles supplémentaires d'envoi et de désencapsulation définies au paragraphe 5.3.

Nous avons maintenant trois classes distinctes de domaine d'acheminement à considérer :

1. le domaine d'acheminement IPv6 interne de chaque site 6-4 :
2. un domaine d'acheminement IPv6 extérieur qui interconnecte un ensemble donné de routeurs frontières 6-4, incluant parmi eux des routeurs relais, c'est-à-dire, un domaine d'acheminement 6-4 extérieur ;
3. le domaine d'acheminement IPv6 extérieur IPv6 de chaque île d'IPv6 natif.

1. Le domaine d'acheminement interne d'un site 6-4 se comporte comme décrit au paragraphe 5.1.

2. Il y a deux options de déploiement pour un domaine d'acheminement 6-4 extérieur :

   2.1 Aucun protocole d'acheminement IPv6 extérieur n'est utilisé. Les routeurs 6-4 qui utilisent un routeur relais donné ont chacun un chemin IPv6 par défaut qui pointe sur le routeur relais. Le routeur relais PEUT appliquer des filtres fondés sur l'adresse de source pour n'accepter le trafic que de routeurs 6-4 spécifiques.

   2.2 Un protocole d'acheminement IPv6 extérieur est utilisé. L'ensemble des routeurs 6-4 qui utilisent un routeur relais donné obtient des chemins IPv6 natifs du routeur relais en utilisant un protocole d'acheminement tel que BGP4+ [RFC2283], [RFC2545]. Le routeur relais va annoncer chaque préfixe d'acheminement IPv6 natif approprié sur sa pseudo-interface 6-4. Ces préfixes vont indiquer les régions de topologie IPv6 natif auxquelles le routeur relais veut relayer. Leur choix est une affaire de politique d'acheminement. Il est nécessaire que les opérateurs de réseau étudient avec soin les schémas et topologies de trafic qu'ils désirent lorsque ils choisissent la portée de telles annonces d'acheminement. Le routeur relais ne va établir un échange de trafic BGP qu'avec des routeurs 6-4 spécifiques dont il est prêt à accepter le trafic.

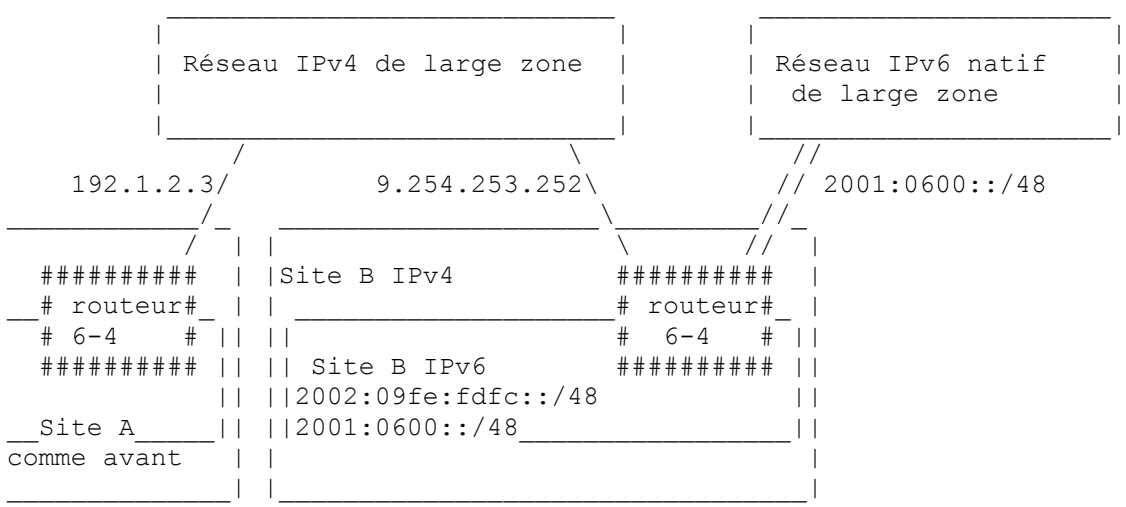
   Bien que cette solution soit plus complexe, elle donne un contrôle de politique effectif, c'est-à-dire que BGP4 plus la politique déterminent quels routeurs 6-4 sont capables d'utiliser quel routeur relais.

3. Un routeur relais DOIT annoncer un chemin pour 2002::/16 dans le domaine d'acheminement extérieur IPv6 natif. La profondeur de la propagation de cette annonce d'acheminement de 2002::/16 est une affaire de politique d'acheminement. Comme il y aura en général plusieurs routeurs relais qui l'annoncent, les opérateurs de réseau vont exiger de le filtrer de façon contrôlable. Une politique incorrecte dans ce domaine conduira à une inaccessibilité potentielle ou à des schémas de trafic pervers.

Les préfixes 6-4 plus spécifiques que 2002::/16 ne doivent pas être propagés dans un acheminement IPv6 natif, pour empêcher la pollution du tableau d'acheminement IPv6 par des éléments du tableau d'acheminement IPv4. Donc, un site 6-4 qui a aussi une connexion IPv6 native NE DOIT PAS annoncer son préfixe d'acheminement 2002::/48 sur cette connexion, et tous les opérateurs de réseau IPv6 natif DOIVENT filtrer en sortie et éliminer toute annonce de préfixe d'acheminement 2002:: plus long que /16.

Les sites qui ont au moins une connexion IPv6 native, en plus d'une connexion 6-4, vont donc avoir au moins un préfixe IPv6 qui n'est pas un préfixe 2002::. Les entrées du DNS de tels sites vont refléter cela et les recherches sur le DNS vont retourner plusieurs adresses. Si deux de ces sites ont besoin d'interopérer, si le chemin 6-4 ou le chemin natif est utilisé dépend du choix de l'adresse IPv6 par les hôtes individuels (ou même des applications).

Considérons maintenant l'exemple du paragraphe précédent. Supposons qu'un hôte IPv6 du site B interroge une entrée du DNS sur un hôte du site A, et que le DNS retourne plusieurs adresses IPv6 avec des préfixes différents.



Si l'hôte prend le préfixe 6-4 selon des règles qui concernent les préfixes multiples il va simplement envoyer les paquets à une adresse IPv6 formée avec le préfixe {FP=001,TLA=0x0002,NLA=192.1.2.3}/48. Il est essentiel qu'ils aient pour source le préfixe {FP=001,TLA=0x0002,NLA=9.254.253.252}/48 pour que la connexité bidirectionnelle soit possible. Le mécanisme de sélection d'adresse du paragraphe 2.1 va le garantir.

5.2.1 Variante du scénario avec FAI relais

Le scénario précédent suppose que le routeur relais est fourni par un site d'usager 6-4 coopératif. Il en est une variante pour un fournisseur d'accès Internet qui offre déjà la connexité IPv6 native, pour faire fonctionner un routeur relais. Techniquement, il n'y a pas de différence avec le scénario précédent ; le site B est simplement un site 6-4 interne du FAI, contenant éventuellement un seul système, c'est-à-dire, le routeur relais lui-même.

5.2.2 Résumé de la configuration de routeur relais

Un routeur relais participe aux protocoles d'acheminement IPv6 en envoi individuel sur son interface IPv6 native et peut le faire sur sa pseudo-interface 6-4, mais ce sont des domaines d'acheminement indépendants avec des politiques distinctes, même si le même protocole, probablement BGP4+, est utilisé dans les deux cas.

Un routeur relais participe aussi aux protocoles d'acheminement d'envoi individuel IPv4 sur son interface IPv4 utilisée pour prendre en charge 6-4, mais on n'en discutera pas plus ici.

Sur son interface IPv6 native, le routeur relais DOIT annoncer un chemin pour 2002::/16. Il NE DOIT PAS annoncer un préfixe d'acheminement 2002:: plus long sur cette interface. Les politiques d'acheminement au sein du domaine d'acheminement IPv6 natif déterminent la portée de cette annonce, limitant par là la visibilité du routeur relais dans ce domaine.

Les paquets IPv6 reçus par le routeur relais dont l'adresse IPv6 de prochain bond correspond à 2002::/16 seront acheminés à sa pseudo-interface 6-4 et traités conformément à la règle d'envoi du paragraphe 5.1.

5.2.2.1 BGP4+ non utilisé

Si BGP4+ n'est pas déployé dans le domaine d'acheminement 6-4 extérieur (option 2.1 du paragraphe 5.2) le routeur relais va être configuré pour accepter et relayer tout le trafic IPv6 mais seulement provenant de ses sites 6-4 clients. Chaque routeur 6-4 desservi par le routeur relais sera configuré avec un chemin IPv6 par défaut pour le routeur relais (par exemple, le chemin IPv6 par défaut du site A ::/0 va pointer sur l'adresse du routeur relais sous le préfixe 2002:09fe:fdfc::/48).

5.2.2.2 BGP4+ utilisé

Si BGP4+ est déployé dans le domaine d'acheminement extérieur 6-4 (option 2.2 du paragraphe 5.2) le routeur relais annonce des préfixes d'acheminement IPv6 natif sur sa pseudo-interface 6-4, n'échangeant du trafic qu'avec les routeurs 6-4 qu'il dessert. (Une solution de remplacement est que ces chemins pourraient être annoncés avec les chemins IPv4 qui utilisent BGP4 sur IPv4, plutôt qu'en faisant tourner une session BGP4+ distincte.) Les chemins spécifiques annoncés dépendent de la politique d'acheminement applicables, mais ils doivent être choisis parmi ceux qui sont accessibles à travers l'interface IPv6 natif du routeur relais. Dans le cas le plus simple, un chemin par défaut pour la totalité de l'espace d'adresse IPv6 pourrait être annoncé. Lorsque plusieurs routeurs relais sont utilisés, des préfixes d'acheminement plus spécifiques seraient annoncés conformément à la politique d'acheminement désirée. L'usage de BGP4+ est complètement normalisé de sorte qu'on en parlera pas plus dans ce document.

5.2.2.3 Adaptation des routeurs relais

Les routeurs relais introduisent des problèmes potentiels d'adaptation. En général un routeur relais ne devrait pas tenter de desservir plus de sites qu'un autre routeur de transit, pour tenir compte de la redondance d'encapsulation.

5.2.3 Réticents au relais

Il peut survenir qu'un site ait un routeur avec à la fois des pseudo-interfaces 6-4 et des interfaces IPv6 natif, mais qu'il ne veuille pas agir comme routeur relais. Un tel site NE DOIT PAS annoncer de préfixe d'acheminement 2002:: dans le domaine IPv6 natif et NE DOIT PAS annoncer de préfixe d'acheminement IPv6 natif ou un chemin IPv6 par défaut dans le domaine 6-4. Au sein du domaine 6-4, il doit se comporter exactement comme dans le scénario 6-4 de base du paragraphe 5.1.

5.3 Règles d'envoi et de désencapsulation

Le seul changement à la transmission IPv6 standard est que chaque routeur 6-4 (et seulement les routeurs 6-4) DOIT mettre en œuvre les règles supplémentaires suivantes d'envoi et de désencapsulation.

Dans la règle d'envoi, "prochain bond" se réfère au prochain nœud IPv6 auquel le paquet sera envoyé, qui n'est pas nécessairement la destination finale mais plutôt le prochain voisin IPv6 indiqué par les mécanismes d'acheminement IPv6 normaux. Si la destination finale est une adresse 6-4, elle sera considérée comme le prochain bon pour les besoins de cette règle. Si la destination finale n'est pas une adresse 6-4, et si elle n'est pas locale, le prochain bond indiqué par l'acheminement sera l'adresse 6-4 d'un routeur relais.

Règle d'envoi supplémentaire pour les routeurs 6-4

si l'adresse de prochain bond IPv6 pour un paquet IPv6 ne correspond pas au préfixe 2002::/16, et
ne correspond à aucun préfixe du site local
alors
appliquer toutes les vérifications de sécurité (voir la Section 8) ;
encapsuler le paquet dans IPv4 comme spécifié à la Section 3,
avec l'adresse de destination IPv4 = la valeur de NLA V4ADDR extraite de l'adresse IPv6 du prochain bond ;
mettre le paquet en file d'attente pour la transmission IPv4.

Une règle simple de désencapsulation pour les paquets IPv4 entrants avec le type de protocole 41 DOIT être mise en œuvre :

Règle de désencapsulation supplémentaire pour les routeurs 6-4

appliquer toutes les vérifications de sécurité (voir la Section 8) ;
retirer l'en-tête IPv4 ;
soumettre le paquet à l'acheminement IPv6 local.

5.4 Variante du scénario avec tunnel vers l'espace IPv6

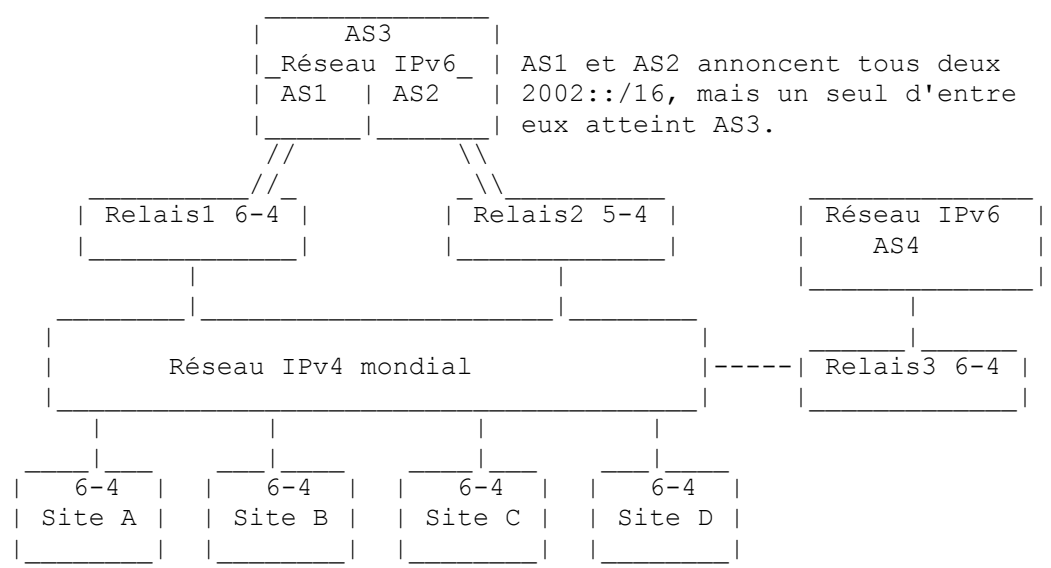
Un site 6-4 qui n'a pas de connexions IPv6 à l'Internet IPv6 "natif" peut acquérir une connexité effective avec l'Internet v6 via un "tunnel configuré" (en utilisant la terminologie de la [RFC2893]) vers un routeur coopérant qui a bien l'accès IPv6, mais qui n' pas besoin d'être un routeur 6-4. De tels tunnels pourraient être autoconfigurés en utilisant une adresse IPv4 d'envoi à la cantonade, mais ceci sort du domaine d'application de ce document. Autrement, on peut utiliser un courtier en tunnel. Ce scénario conviendrait pour un petit site géré par l'utilisateur.

Ces mécanismes ne sont pas décrits en détails dans le présent document.

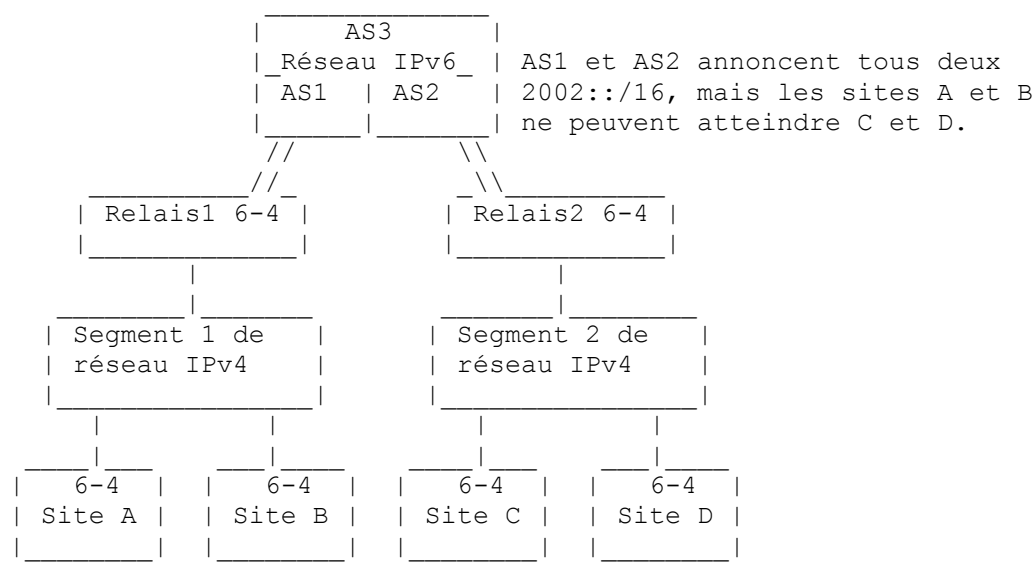
5.5 Scénarios fragmentés

Si il y a plusieurs routeurs relais entre l'IPv6 natif et le monde 6-4, les différentes parties du monde 6-4 seront desservies par des relais différents. La seule complexité que cela introduit est dans l'établissement de la portée des annonces d'acheminement 2002::/16 au sein du monde IPv6 natif. Comme toutes annonces BGP4+, leur portée doit être correctement définie par la politique d'acheminement pour s'assurer que le trafic pour 2002::/16 suit les chemins prévus.

Si il y a plusieurs bouts de réseau IPv6 qui sont tous interconnectés par 6-4 à travers l'Internet IPv4 mondial, c'est une simple généralisation des scénarios de base des paragraphes 5.1 et 5.2 et aucun nouveau problème ne surgit. C'est ce que montre la figure suivante. Sous réserve d'une configuration cohérente des annonces d'acheminement, il n'y a pas de problème connu avec ce scénario.



Si plusieurs bouts IPv6 sont interconnectés à travers plusieurs réseaux IPv4 disjoints (c'est-à-dire, un monde IPv4 fragmenté) le monde 6-4 est alors aussi fragmenté ; c'est le seul scénario qui doit être évité. C'est illustré ci-dessous pour montrer pourquoi cela ne marche pas, car les annonces 2002::/16 provenant du Relais1 seront invisibles au Relais2, et vice versa. Les sites A et B n'ont donc pas de connexité avec les sites C et D.



5.6 Multi rattachement

Les sites qui sont multi rattachements sur IPv4 PEUVENT étendre le scénario 6-4 en utilisant un préfixe 2002:: pour chaque routeur frontière IPv4, obtenant par là une forme simple de multi rattachement IPv6 par l'utilisation de plusieurs préfixes IPv6 simultanés et plusieurs routeurs relais simultanés.

5.7 Considérations sur la transition

Si les règles ci-dessus pour les annonces d'acheminement et la sélection d'adresse sont suivies, un site peut alors migrer de l'utilisation de 6-4 à l'utilisation de connexions IPv6 natives sur une longue période de coexistence, sans qu'il soit besoin d'arrêter 6-4 jusqu'à ce qu'il cesse d'être utilisé. Les étapes impliquées sont :

1. De faire fonctionner IPv6 sur le site en utilisant toute mise en œuvre convenable. Le vrai IPv6 natif de la [RFC2529], ou les tunnels sont tous acceptables.
2. Configurer un routeur frontière (ou un routeur plus un NAT IPv4) connecté au réseau IPv4 externe pour prendre en charge 6-4, y compris les annonces en local du préfixe d'acheminement 2002:: approprié. Configurer les entrées de DNS IPv6 en utilisant ce préfixe. À ce point, le mécanisme 6-4 est automatiquement disponible, et le site a obtenu un préfixe IPv6 "libre".

3. Identifier un routeur relais 6-4 qui veut relayer le trafic du site jusqu'au monde IPv6 natif. Cela pourrait être un autre site 6-4 coopérant, ou un service d'un FAI. Si aucun protocole d'acheminement extérieur n'est en usage dans le domaine d'acheminement extérieur 6-4, le routeur 6-4 du site sera configuré avec un chemin IPv6 par défaut pointant sur l'adresse 6-4 de ce routeur relais. Si un protocole d'acheminement extérieur tel que BGP4+ est utilisé, le routeur 6-4 du site sera configuré pour établir les échanges de trafic BGP appropriés.

4. Lorsque la connexité IPv6 externe native devient disponible, ajouter un second préfixe IPv6 (natif) à la fois à la configuration du routeur frontière et à la configuration DNS. À ce point, une règle de sélection d'adresse va déterminer quand 6-4 et quand IPv6 natif seront utilisés.

5. Lorsque l'usage 6-4 est déterminé comme ayant cessé (ce qui peut être des années plus tard) retirer la configuration 6-4.

5.8 Coexistence avec les pare-feu, les NAT ou RSIP

Le mécanisme 6-4 paraît ne pas être affecté par la présence d'un pare-feu au routeur frontière.

Si le site concerné a un espace très limité d'adresses IPv4 mondiales, et s'il fait fonctionner un traducteur d'adresse réseau (NAT), tous les mécanismes ci-dessus restent valides. La boîte de NAT doit aussi contenir un routeur IPv6 à pleines fonctionnalités incluant le mécanisme 6-4. L'adresse utilisée pour V4ADDR va simplement être une adresse IPv4 unique au monde allouée à ce NAT. Dans l'exemple du paragraphe 5.1 ci-dessus, les routeurs 6-4 seraient aussi les NAT IPv4 des sites, et possèderaient les adresses IPv4 uniques au monde 192.1.2.3 et 9.254.253.252.

Combiner de cette façon un routeur 6-4 avec un NAT IPv4 offre automatiquement au site concerné un préfixe IPv6 /48 unique au monde, derrière l'adresse IPv4 du NAT. Donc chaque hôte derrière le NAT peut devenir un hôte IPv6 sans qu'il soit besoin d'une allocation d'espace d'adresse supplémentaire, ni d'intervention du fournisseur d'accès Internet. Aucune traduction d'adresse n'est nécessaire par ces hôtes IPv6.

Une situation plus complexe survient si un hôte est éloigné de plus d'un bond de l'espace d'adresse IPv4 unique au monde, car seul le NAT le plus externe a une adresse IPv4 unique au monde. Tous les hôtes IPv6 dans cette situation doivent utiliser les adresses déduites du préfixe 2002: construit à partir de l'adresse IPv4 mondiale du NAT le plus externe. Les adresses IPv4 des NAT internes ne sont pas uniques au monde et ne jouent aucun rôle dans le mécanisme 6-4, et l'encapsulation et la désencapsulation 6-4 peuvent seulement avoir lieu au NAT le plus externe.

Le mécanisme d'IP spécifique du domaine (RSIP, *Realm-Specific IP*) [RFC3103] peut aussi coexister avec 6-4. Si un routeur frontière 6-4 est combiné avec un routeur frontière RSIP, il peut prendre en charge des hôtes IPv6 en utilisant des adresses 6-4, les hôtes IPv4 utilisant RSIP, ou les hôtes à double pile utilisant les deux. La fonction RSIP fournit la gestion fine de l'allocation dynamique d'adresses IPv4 mondiales et la fonction 6-4 fournit une adresse IPv6 mondiale stable à chaque hôte. Comme avec le NAT, l'adresse IPv4 utilisée pour construire le préfixe 2002: du site sera une des adresses mondiales du routeur frontière RSIP.

5.9 Usage au sein des intranets

Rien ne peut empêcher le scénario présenté ci-dessus d'être déployé dans un réseau privé d'entreprise au titre de sa transition interne vers IPv6 ; le cœur de réseau IPv4 du réseau d'entreprise va servir de couche liaison virtuelle pour les sites individuels de l'entreprise en utilisant des préfixes 2002::. Le V4ADDR DOIT être une adresse IPv4 mondiale dûment allouée, qui DOIT être unique au sein du réseau privé. L'intranet obtient ainsi des adresses IPv6 uniques au monde même si il utilise en interne des adresses IPv4 privées de la [RFC1918].

5.10 Résumé de l'impact sur l'acheminement

L'acheminement IGP (de site) va traiter le préfixe 2002::/48 du site local exactement comme un préfixe de site IPv6 natif alloué au site local. Il y aura aussi un chemin IGP vers le préfixe 2002::/16 générique qui sera un chemin vers le routeur 6-4 du site, sauf si cela est traité comme un chemin par défaut.

L'acheminement EGP (c'est-à-dire, BGP) va comporter des annonces pour le préfixe 2002::/16 provenant des routeurs relais dans le domaine IPv6 natif, dont la portée est limitée par la politique d'acheminement. C'est le seul préfixe IPv6 non natif annoncé par BGP.

Il sera nécessaire aux routeurs 6-4 d'obtenir des chemins vers les routeurs relais afin d'accéder au domaine IPv6 natif. Dans le cas le plus simple, il y a un chemin IPv6 par défaut configuré manuellement vers l'adresse d'un routeur relais sous le préfixe {FP=001,TLA=0x0002,NLA=V4ADDR}/48, où V4ADDR est l'adresse IPv4 du routeur relais. Un tel chemin pourrait être utilisé pour établir une session BGP pour l'échange de chemins IPv6 supplémentaires.

Par construction, le trafic IPv6 en envoi individuel au sein d'un domaine 6-4 va suivre exactement le même chemin que le trafic IPv4 en envoi individuel.

5.11 Prévention de l'acheminement en boucle

Comme 6-4 n'a pas d'impact sur l'acheminement IPv4, il ne peut pas induire de boucle d'acheminement dans IPv4. Comme les préfixes 2002: se comportent exactement comme des préfixes IPv6 standard, ils ne vont pas créer de nouveau mécanisme d'acheminement en boucle dans IPv6 sauf s'ils sont mal configurés. Une mauvaise configuration très dangereuse serait une annonce du préfixe 2002::/16 dans un domaine d'acheminement 6-4 extérieur, car cela attirerait tout le trafic 6-4 dans le site qui fait l'annonce. Son routeur 6-4 renverrait alors le trafic 6-4 non local à l'extérieur, formant une boucle.

Le préfixe d'acheminement 2002::/16 peut être légitimement annoncé dans le domaine d'acheminement IPv6 natif par un routeur relais, et dans le domaine IPv6 local d'un site IPv6 ; il y a donc un risque qu'une mauvaise configuration cause son annonce dans un domaine d'acheminement 6-4 extérieur.

Pour résumer, le préfixe 2002::/16 NE DOIT PAS être annoncé à un domaine d'acheminement 6-4 extérieur.

6. Diffusion groupée et envoi à la cantonade

Il n'est pas possible de supposer la disponibilité générale de la diffusion groupée IPv4 de large zone, aussi (à la différence de la [RFC2529]) le mécanisme 6-4 ne doit supposer que la seule capacité d'envoi individuel dans son réseau transporteur IPv4. Un protocole d'acheminement de diffusion groupée IPv6 est nécessaire [MULTI].

L'espace d'adresses d'envoi à la cantonade alloué [RFC2526] est compatible avec les préfixes 2002::, c'est-à-dire que les adresses d'envoi à la cantonade formées avec de tels préfixes peuvent être utilisées au sein d'un site 6-4.

7. Messages ICMP

Les messages ICMP "injoignable" et autres retournés par le système d'acheminement IPv6 seront retournés au routeur 6-4 qui a généré un paquet 2002:: encapsulé. Cependant, ce routeur va souvent être incapable de retourner un message ICMPv6 au nœud IPv6 d'origine, dû au manque d'informations suffisantes dans le message "injoignable". Cela signifie que le réseau IPv4 va apparaître comme une couche liaison sur laquelle on ne peut pas faire de diagnostics pour les besoins du fonctionnement d'IPv6. Les autres considérations sont décrites au paragraphe 4.1.3 de la [RFC2893].

8. Considérations relatives à l'IANA

Aucune allocation par l'IANA n'est exigée au delà de la valeur particulière de TLA de 0x0002 déjà allouée.

9. Considérations pour la sécurité

Les personnes chargées de la mise en œuvre devraient être conscientes de ce qu'en plus des attaques possibles contre IPv6, les attaques contre la sécurité d'IPv4 doivent aussi être considérées. L'utilisation de la sécurité IP aux deux niveaux, IPv4 et IPv6, ne devrait néanmoins pas être évitée, pour des raisons d'efficacité. Par exemple, si IPv6 fonctionne chiffré, le chiffrement de IPv4 sera redondant sauf si on redoute l'analyse de trafic. Si IPv6 fonctionne sous authentification, l'authentification de IPv4 ajoutera peu. À l'inverse, la sécurité IPv4 ne va pas protéger le trafic IPv6 une fois qu'il aura quitté le domaine 6-4. Donc, la mise en œuvre de la sécurité IPv6 est nécessaire même si la sécurité IPv4 est disponible.

Par défaut, le trafic 6-4 sera accepté et désencapsulé provenant de toute source de laquelle du trafic IPv4 régulier est accepté. Si pour quelque raison que ce soit, ceci est perçu comme présentant un risque pour la sécurité (par exemple, si l'usurpation d'identité en IPv6 est perçue comme plus probable que dans IPv4) un filtrage supplémentaire de paquet fondé sur l'adresse de source pourrait être appliqué. Un contrôle possible de plausibilité est de voir si l'encapsulation de l'adresse IPv4 est cohérente avec l'adresse 2002:: encapsulée. Si on applique cette vérification, des exceptions doivent être configurées pour admettre le trafic provenant des routeurs relais (Section 5). Le trafic 2002:: doit aussi être excepté des vérifications appliquées pour empêcher l'usurpation d'identité dans le trafic de "6 sur 4" [RFC2529].

Dans tous les cas, tout trafic 6-4 dont l'adresse de source ou de destination incorpore une V4ADDR qui n'est pas dans le format d'une adresse d'envoi individuel mondiale DOIT être éliminé en silence par les deux encapsulateurs et désencapsulateurs. Précisément, cela signifie que les adresses IPv4 définies dans la [RFC1918], les adresses de diffusion, les adresses de sous réseau de diffusion, de diffusion groupée et de rebouclage sont inacceptables.

Remerciements

L'idée de base présentée ci-dessus n'est probablement pas originale, et nous avons eu des commentaires précieux de Magnus Ahltorp, Harald Alvestrand, Jim Bound, Scott Bradner, Randy Bush, Matt Crawford, Richard Draves, Jun-ichiro Itojun Hagino, Joel Halpern, Tony Hain, Andy Hazeltine, Bob Hinden, Geoff Huston, Perry Metzger, Thomas Narten, Erik Nordmark, Markku Savela, Ole Troan, Sowmini Varadhan, membres de l'équipe d'ingénierie IPv6 de Compaq, et des autres membres du groupe de travail NGTRANS. Une partie du texte a été copiée de la [RFC2529]. George Tsirtsis a eu la gentillesse de faire deux des diagrammes.

Références

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

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2283] T. Bates, R. Chandra, D. Katz, Y. Rekhter, "Extensions multiprotocoles pour BGP-4", février 1998. (*Obsolète, voir* RFC2858) *(P.S.)*

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. *(Obsolète, voir* RFC3513*) (P.S.)*

[RFC2374] R. Hinden, M. O'Dell, S. Deering, "Format mondial d'adresse d'envoi individuel IPv6 agrégeable", juillet 1998. (*Obsolète, voir* RFC3587) *(Historique)*

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par 5095, D.S)*

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2462] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", décembre 1998. *(Obsolète, voir* RFC4862*) (D.S.)*

[RFC2526] D. Johnson, S. Deering, "Adresses réservées d'envoi à la cantonade de sous-réseau IPv6", mars 1999. *(P.S.)*

[RFC2529] B. Carpenter, C. Jung, "Transmission d'IPv6 sur des domaines IPv4 sans tunnels explicites", mars 1999. *(P.S.)*

[RFC2545] P. Marques, F. Dupont, "Utilisation des extensions multi protocoles de BGP-4 pour l'acheminement inter-domaine IPv6", mars 1999. *(P.S.)*

[RFC2553] R. Gilligan, S. Thomson, J. Bound, W. Stevens, "Extensions de base d'interface de prise pour IPv6", mars 1999. *(Obsolète, voir* RFC3493) (*MàJ par* RFC3152) *(Information)*

[RFC2893] R. Gilligan, E. Nordmark, "Mécanismes de transition pour les hôtes et routeurs IPv6", août 2000. *(Obsolète, voir* RFC4213)

[RFC3103] M. Borella et autres, "IP spécifique de domaine : Spécification du protocole (RSIP)", octobre 2001. *(Expér.)*

[RFC3484] R. Draves, "Choix d'adresse par défaut pour le protocole Internet version 6 (IPv6)", février 2003. *(P.S.)*

[MULTI] Thaler, D., "Support for Multicast over 6to4 Networks", Travail en cours.

[SCALE] Hain, T., "6to4-relay discovery and scaling", Travail en cours.

Adresse des auteurs

Brian E. Carpenter
IBM
iCAIR, Suite 150
1890 Maple Avenue
Evanston IL 60201, USA
EMail: brian@icair.org

Keith Moore
UT Computer Science Department
1122 Volunteer Blvd, Ste 203
Knoxville, TN 37996-3450
USA
EMail: moore@cs.utk.edu

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Déclaration de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.