Groupe de travail Réseau
Request for Comments : 5220
Catégorie : Information
Traduction Claude Brière de L'Isle

A. Matsumoto, NTT
T. Fujisaki, NTT
R. Hiromi, Intec Netcore
K. Kanayama, INTEC Systems
juillet 2008

Position du problème du choix d'adresse par défaut dans les environnements multi préfixes : questions de fonctionnement des règles par défaut de la RFC 3484

Résumé
Une seule liaison physique peut avoir plusieurs préfixes qui lui sont alloués. Dans un tel environenment, les hôtes d'extrémité pourraient avoir plusieurs adresses IP et être obligés de les utiliser de façon sélective. La RFC 3484 définit des règles de choix d'adresse de source et de destination par défaut et est mise en œuvre dans divers systèmes d'exploitation. Mais, il a été trop difficile de l'utiliser pour plusieurs raisons. Dans certains environnements où plusieurs préfixes sont alloués sur une seule liaison physique, l'hôte qui utilise les règles de choix d'adresse par défaut va subir des problèmes dans la communication. Le présent document décrit les problèmes possibles que les hôtes d'extrémité pourraient rencontrer dans un environnement avec plusieurs préfixes.

Table des Matières

1. Introduction

Dans IPv6, une seule liaison physique peut avoir plusieurs préfixes alloués. Dans ce cas, un hôte d'extrémité peut avoir plusieurs adresses IP allouées à une interface sur cette liaison. Dans l'environnement de double pile IPv4-IPv6 ou dans un site connecté à la fois à une adresse locale unique (ULA, *Unique Local Address*) [RFC4193] et à des réseaux acheminables mondialement, un hôte d'extrémité a normalement plusieurs adresses IP. Ce sont des exemples de réseaux sur lesquels se concentre le présent document. Dans un tel environnement, un hôte d'extrémité peut rencontrer des problèmes de communication.

Un choix inapproprié de l'adresse de source chez l'hôte d'extrémité cause un acheminement asymétrique inattendu, le filtrage par un routeur, ou l'élimination de paquets parce qu'il n'y a pas de chemin vers l'hôte.

Quand on considère un environnement multi préfixes, le choix de l'adresse de destination est aussi important pour un établissement correct ou meilleur de la communication.

La [RFC3484] définit les algorithmes de choix d'adresse de source et de destination par défaut et est mise en œuvre dans divers systèmes d'exploitation. Mais, elle a été trop difficile à utiliser en pratique pour plusieurs raisons, comme l'absence d'une méthode d'autoconfiguration. Il y a des cas problématiques où les hôtes qui utilisent les règles de choix d'adresse par défaut rencontrent des problèmes de communication.

Le présent document décrit les possibilités de choix incorrect d'adresse qui conduisent à l'élimination de paquets et à des échecs de communication.

1.1 Portée du document

Comme d'autres mécanismes existent déjà, les techniques de multi rattachements pour réaliser la redondance sortent naturellement du domaine d'application de ce document.

On se concentre sur un environnement de réseau de site d'extrémité et des hôtes non gérés dans un tel environnement. C'est parce que le comportement de choix d'adresse chez ce type d'hôtes est difficile à manipuler, du fait du manque de connaissance des utilisateurs, de la localisation des hôtes, ou de leur grand nombre.

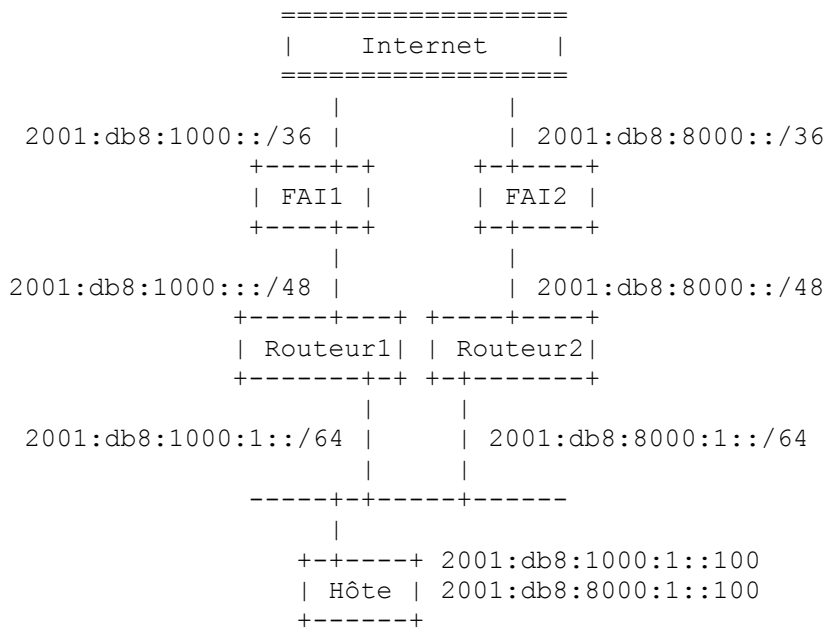
Le but du présent document est de trier les cas problématiques relatifs au choix d'adresses. Il inclut les problèmes qui peuvent êtte résolus dans le cadre de la RFC 3484 et ceux qui ne le peuvent pas. Pour les premiers, la RFC 3484 pourrait être modifiée pour staisfaire leurs besoins, ou une autre solution de choix d'adresses pourrait être nécessaire. Pour les autres, un mécanisme supplémentaire qui atténue la difficulté de fonctionnement pourrait être nécessaire.

Le présent document inclut aussi une analyse des solutions simples pour chaque cas problématique. Cette analyse se concentre essentiellement sur si le cas peut ou non être résolu dans le cadre de la RFC 3484. Sinon, des solutions possibles sont décrites. Même si un cas peut être résolu dans le cadre de la RFC 3484, comme mentionné ci-dessus, cela ne veut pas nécessairement dire qu'il n'y a pas de difficulté de fonctionnement. Par exemple, dans l'environnement mentionné ci-dessus, ce n'est pas une solution faisable de configurer chaque tableau de politique d'hôte à la main. Donc, pour une telle solution, la difficulté de configuration est encore un autre problème commun.

2. Position du problème

2.1 Choix de l'adresse de source

2.1.1 Plusieurs routeurs sur une seule interface



(FAI, fournisseur d'accès Internet)

Figure 1

D'une façon générale, il n'y a pas d'interaction entre la détermination du prochain bond et le choix de l'adresse. Dans cet exemple, quand un hôte commence une nouvelle connexion et envoie un paquet via le Routeur1, l'hôte ne choisit pas nécessairement l'adresse 2001:db8:1000:1::100 donnée par le Routeur1 comme adresse de source. Cela pose le même problème que celui décrit au paragraphe suivant, "Problème du filtrage à l'entrée".

Analyse de la solution : comme ce cas dépend du choix du prochain bond, contrôler le comportement de choix d'adresse chez l'hôte seul ne résoud pas tout le problème. Une solution possible pour ce cas est d'adopter l'acheminement fondé sur l'adresse de source au Routeur1 et au Routeur2. Une autre solution peut être d'utiliser un acheminement statique à Routeur1, Routeur2, et chez l'Hôte, et d'utiliser la politique de choix d'adresse statique correspondante chez l'hôte.

2.1.2 Problème du filtrage à l'entrée

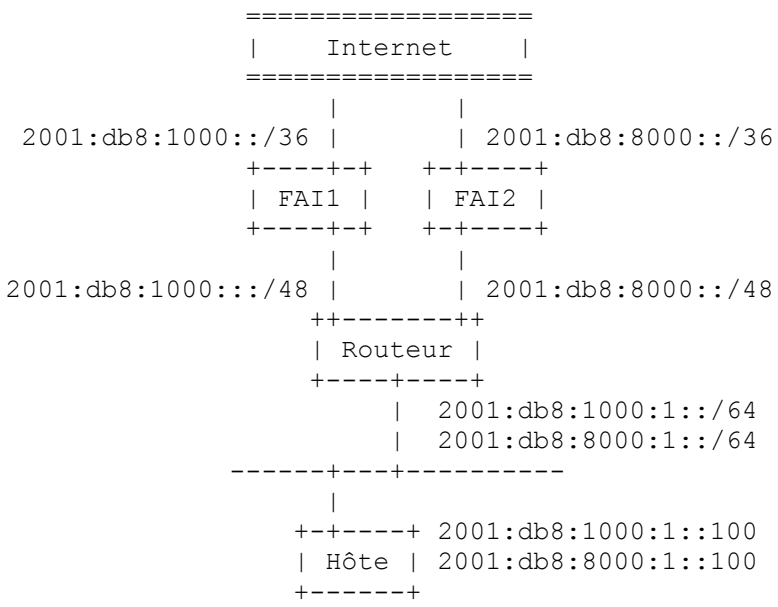


Figure 2

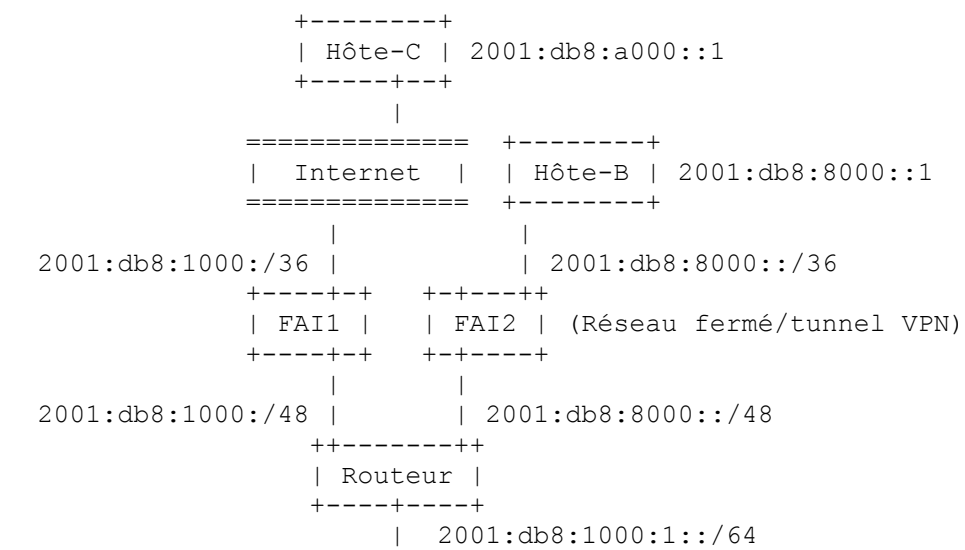
Quand un site relativement petit, qu'on appelle un "réseau consomnateur", est rattaché à deux FAI en amont, chaque FAI délègue un bloc d'adresses réseau, qui est généralement /48, et un hôte a plusieurs adresses IPv6.

Quand l'adresse de source d'un paquet sortant n'est pas celle qui a été déléguée par un FAI en amont, il y a une possibilité que le paquet soit éliminé au filtre d'entrée du FAI. Le filtrage d'entrée devient très populaire chez les FAI pour contrer les dommages des attaques de déni de service (DoS). Dans cet exemple, quand le routeur choisit le chemin par défaut pour le FAI2 et que l'hôte choisit 2001:db8:1000:1::100 comme adresse de source pour les paquets envoyés à l'hôte (2001:db8:2000::1) quelque part sur l'Internet, les paquets peuvent être éliminés chez le FAI2 à cause du filtrage d'entrée.

Analyse de la solution : Une solution possible de ce cas est d'adopter l'acheminement fondé sur l'adresse de source chez le routeur. Une autre solution peut être d'utiliser un acheminement statique au routeur, et d'utiliser la politique de choix d'adresse statique correspondante chez l'hôte.

2.1.3 Problème du réseau mi clos

On peut voir un second problème typique de choix d'adresse de source dans un site multi rattachements avec une connexité semi fermée globale, comme montré dans la figure ci-dessous. Dans ce cas, l'hôte-A est dans un réseau multi rattachements et a deux adresses IPv6, une déléguée de chaque FAI en amont. Noter que le FAI2 est un réseau fermé et n'a pas de connexité à l'Internet.



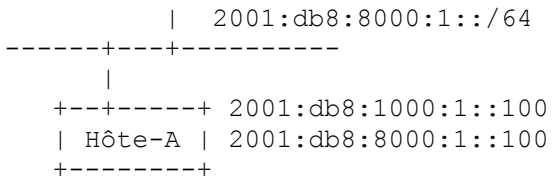


Figure 3

On n'a pas besoin ici de connexions de réseau physique. La connexion du routeur au FAI2 peut être une liaison logique entre le FAI1 et l'Internet.

Quand l'Hôte-A commence la connexion à l'Hôte-B dans le FAI2, l'adresse de source d'un paquet envoyé va être une adresse déléguée du FAI2 (c'est-à-dire, 2001:db8:8000:1::100) à cause de la règle 8 (plus long préfixe correspondant) dans la RFC 3484.

L'Hôte-C est situé quelque part sur l'Internet et a l'adresse IPv6 2001:db8:a000::1. Quand l'Hôte-A envoie un paquet à l'Hôte-C, l'algorithme de plus longue correspondance choisit 2001:db8:8000:1::100 pour l'adresse de source. Dans ce cas, le paquet passe à travers FAI1 et peut être filtré par le filtre d'entrée de FAI1. Même si le paquet n'est pas filtré par FAI1, un paquet de retour provenant de l'Hôte-C ne peut pas être livré à l'Hôte-A parce que le paquet de retour est destiné à 2001:db8:8000:1::100, qui est fermé à l'Internet.

Le point important est que chaque hôte choisisse une adresse de source correcte pour une certaine adresse de destination. Pour résoudre cette sorte de problème de choix d'adresse fondé sur la politique du réseau, il est probable que la livraison d'informations supplémentaires à un nœud donne une meilleure solution que d'utiliser des algorithmes locaux à ce nœud.

Analyse de la solution : ce problème peut être résolu dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresse dans le tableau de politiques de la RFC 3484 de l'Hôte-A peut résoudre ce problème.

2.1.4 Utilisation combinée de d'adresse mondiale et d'ULA

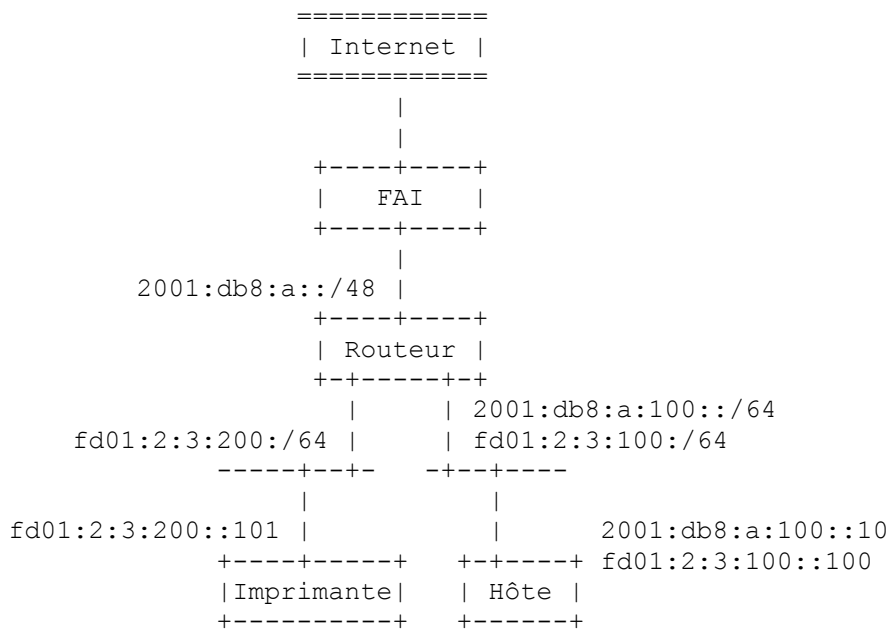


Figure 4

Comme le décrit la [RFC4864], utiliser une ULA peut être avantageux dans certains scénarios. Si l'ULA est utilisée pour la communication interne, les paquets avec l'ULA doivent être filtrés au routeur.

Ce cas ne crée pas actuellement de problème de choix d'adresse à cause de la dissemblance entre l'ULA et l'adresse mondiale d'envoi individuel. La règle de plus longue correspondance de la RFC 3484 choisit l'adresse correcte pour la communication intra-site aussi bien que extra-site .

À l'avenir, cependant, il y a une possibilité que la règle de la plus longue correspondance ne soit plus capable de choisir l'adresse correcte. C'est le moment où commence l'allocation de ces adresses mondiales d'envoi individuel, où le premier bit est 1. Dans la [RFC4291], presque tous les espaces d'adresses de IPv6, incluant ceux dont le premier bit est 1, sont alloués comme adresses mondiales d'envoi individuel.

À savoir que quand on commece à allouer une partie du bloc d'adresses 8000::/1 comme adresse mondiale en envoi individuel et que cette partie est utilisée quelque part dans l'Internet, la règle de plus longue correspondance cesse de fonctionner de façon appropriée pour les gens qui essayent de se connecter aux serveurs avec ces adresses.

Par exemple, quand l'hôte de destination a une adresse IPv6 de 8000::1, et que l'hôte d'origine a 2001:db8:a:100::100 et fd01:2:3:100::100, l'adresse de source va être fd01:2:3:100::100, parce que la plus longue séquence binaire correspondante est 0 pour 2001:db8:a:100::100 et 1 pour fd01:2:3:100::100, respectivement.

Analyse de la solution : ce problème peut être résolu dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte peut résoudre ce problème. Une autre solution est de modifier la RFC 3484 et de définir des portées d'ULA plus petites que la portée mondiale.

2.1.5 Renumérotation de site

La [RFC4192] décrit une procédure recommandée pour renuméroter un réseau d'un préfixe à un autre. Une adresse autoconfigurée a une durée de vie, de sorte qu'en cessant d'annoncer l'ancien préfixe, l'adresse autoconfigurée est finalement invalidée.

Cependant, invalider le vieux préfixe prend longtemps. On ne peut pas cesser d'acheminer sur le vieux préfixe tant qu'il n'est pas supprimé de l'hôte. Cela peut être un gros problème pour les administrateurs de réseau du FAI.

Il y a une technique pour annoncer le préfixe avec la durée de vie préférée de zéro ; cependant, le paragraphe 5.5.4 de la [RFC4862] n'interdit absolument pas l'utilisation d'une adresse déconseillée pour une nouvelle connexion sortante à cause des limitations des capacités des applications.

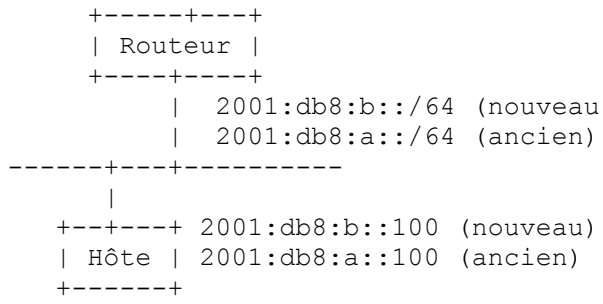


Figure 5

Analyse de la solution : ce problème peut être atténué dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte peut résoudre ce problème.

2.1.6 Choix d'adresse de source de diffusion groupée

Ce cas est un exemple de priorité d'envoi individuel de site local ou mondial. Quand on envoie un paquet en diffusion groupée à travers les frontières du site, l'adresse de source du paquet en diffusion groupée devrait être une adresse d'acheminement mondial. Cependant l'algorithme de plus longue correspondance choisit une ULA si l'hôte envoyeur a à la fois une ULA et une adresse d'envoi individuel mondiale.

Analyse de la solution : ce problème peut être résolu dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte envoyeur peut résoudre ce problème.

2.1.7 Choix d'adresse temporaire

La [RFC3041] définit une adresse temporaire. L'usage d'une adresse temporaire a des avantages et des inconvénients. Elle est bonne pour voir des pages de la Toile ou pour communiquer avec le public en général, mais elle n'est pas bonne pour un service qui utilise l'authentification fondée sur l'adresse ou pour les besoins de connexion.

Si on peut activer et désactiver l'adresse temporaire, ce serait parfait. Si on peut activer son usage par service (adresse de destination) ce serait aussi parfait. La même situation peut se trouver quand on utilise une adresse de rattachement et une adresse d'entretien dans un réseau IPv6 mobile [RFC3775].

La Section 6 ("Travaux futurs") de la RFC 3041 discute d'une extension d'API qui pourrait être nécessaire pour réaliser un meilleur mécanisme de choix d'adresse avec une granularité plus fine.

Analyse de la solution : ce problème ne peut pas être résolu dans le cadre de la RFC 3484. Une solution possible est de faire que les applications choisissent les adresses désirables en utilisant l'API de prise IPv6 pour le choix d'adresse de source définie dans la [RFC5014].

2.2 Choix d'adresse de destination

2.2.1 Priorité IPv4 ou IPv6

Le tableau de politique par défaut donne aux adresses IPv6 une préséance supérieure aux adresses IPv4. Il semble cependant qu'il y ait de nombreux cas où les administrateurs de réseau veulent contrôler la politique de choix d'adresse des hôtes d'extrémité de façon que ce soit le contraire.

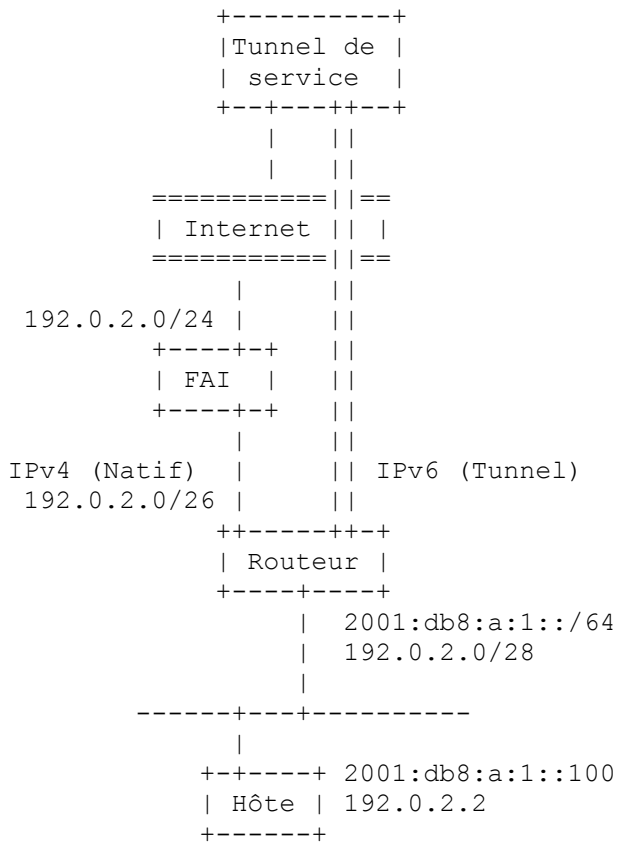


Figure 6

Dans la figure ci-dessus, un site a IPv4 natif etIPv4 la connexité IPv6 tunnelée. Donc, l'administrateur peut vouloir établir une priorité supérieure pour l'utilisation de IPv4 que de IPv6 parce que la qualité du réseau tunnel semble être pire que celle du transport natif.

Analyse de la solution : ce problème peut être atténué dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte peut résoudre ce problème.

2.2.2 Environnement de double pile ULA et IPv4

C'est une forme particulière de priorité IPv4 et IPv6. Quand une entreprise a la connexité Internet IPv4 mais n'a pas encore la connexité Internet IPv6, et que l'entreprise veut fournir la connexité IPv6 de site local, une ULA est le meilleur choix

pour la connexité IPv6 de site local. Chaque hôte employé va avoir à la fois une adresse IPv4 mondiale ou privée et une ULA. Ici, quand cet hôte essaye de se connecter à l'Hôte-B qui a été enregistré avec des enregistrements A et AAAA dans le DNS, l'hôte va choisir AAAA comme adresse de destination et la ULA pour l'adresse de source. Cela va clairement résulter en un échec de connexion.

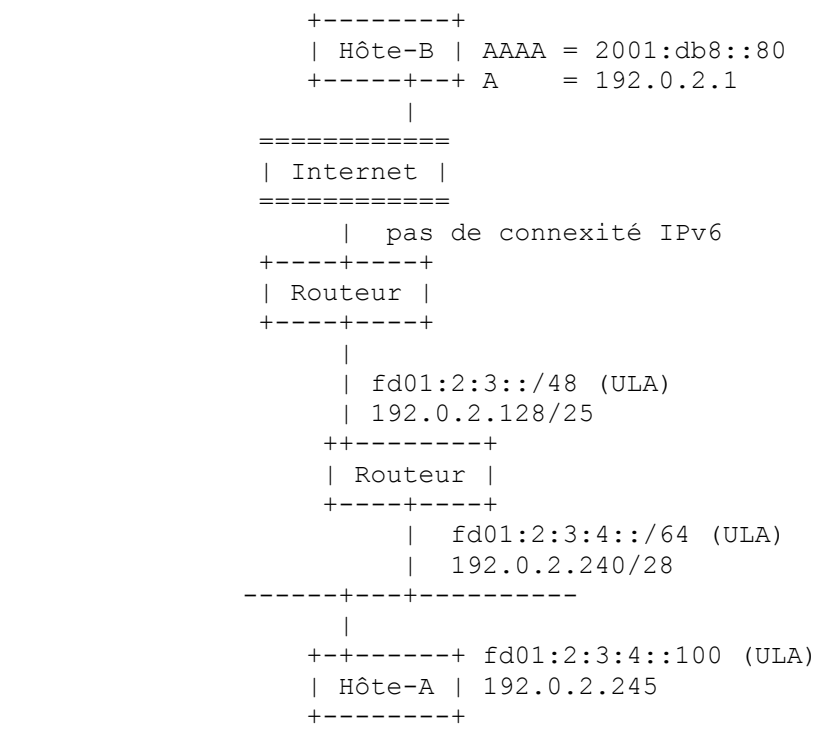


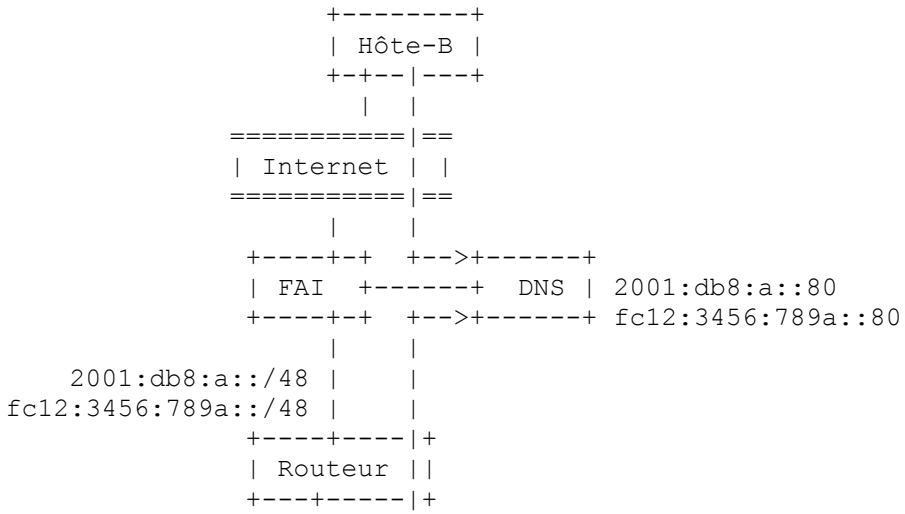
Figure 7

Analyse de la solution : ce problème peut être atténué dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte peut résoudre ce problème.

2.2.3 ULA ou prioritisation globale

Différencier les services par l'adresse de source du client est très courant. L'authentification fondée sur l'adresse esr un exemple typique de cela. Un autre exemple typique est un service de la Toile qui a des pages pour le public et des pages internes pour les employés ou les parties impliquées. Encore un autre exemple est le partage de zone du DNS.

Cependant, une ULA et une adresse mondiale IPv6 ont toutes deux une portée mondiale, et les règles par défaut de la RFC 3484 ne spécifient pas quelle adresse devrait avoir la priorité. Ce point rend un peu plus difficile la mise en œuvre de la différenciation de service IPv6 fondée sur l'adresse .



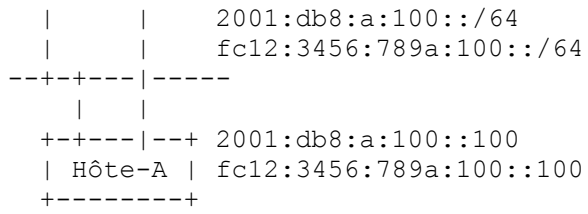


Figure 8

Analyse de la solution : ce problème peut être atténué dans le cadre de la RFC 3484. Par exemple, configurer des politiques de choix d'adresses dans le tableau des politiques de la RFC 3484 de l'hôte peut résoudre ce problème.

3. Conclusion

On a traité les problèmes relatifs au choix d'adresse de destination ou de source. Ces problèmes ont leurs racines dans la situation où les hôtes d'extrémité ont plusieurs adresses IP. Dans cette situation, chaque hôte d'extrémité doit choisir une adresse appropriée de destination et de source ; ce choix ne peut pas être réalisé seulement par les routeurs.

On devrait noter que les hôtes d'extrémité doivent être informés des politiques d'acheminement de leurs réseaux en amont pour un choix approprié d'adresse. Un administrateur de site doit considérer chaque problème possible de choix de fausse adresse et prendre à l'avance des contre mesures.

4. Considérations sur la sécurité

Quand un routeur intermédiaire effectue un acheminement de politique (par exemple un acheminement fondé sur l'adresse de source) un choix d'adresse inapproprié cause un acheminement inattendu. Par exemple, dans le réseau décrit au paragraphe 2.1.3, quand l'Hôte-A utilise une politique de choix d'adresse par défaut et choisit une adresse inappropriée, un paquet envoyé à un VPN peut être livré à une localisation via l'Internet. Ce problème peut conduire à l'espionnnage des paquets ou à la capture de session. Cependant, renvoyer le paquet au nœud sur le chemin correct à partir de l'attaquant n'est pas facile, de sorte que ces deux risques ne sont pas sérieux.

Comme expliqué dans la section des considérations sur la sécurité de la RFC 3484, les algorithmes de choix d'adresse exposent à un risque potentiel pour la confidentialité. Quand un hôte malveillant peut amener un hôte cible à effectuer un choix d'adresse (par exemple, en envoyant un paquet en envoi à la cantonnade ou en diffusion groupée) l'hôte malveillant peut obtenir la connaissance de plusieurs adresses rattachées à l'hôte cible. Dans un cas comme celui du paragraphe 2.1.4, si un attaquant peut obliger l'hôte à envoyer un paquet en diffusion groupée et si l'hôte effectue l'algorithme de choix d'adresse par défaut, l'attaquant peut être capable de déterminer les ULA rattachées à l'hôte.

Ces risques pour la sécurité ont leurs racines dans le choix d'adresses inappropriées. Donc, si des contre-mesures sont prises, et si les hôtes choisissent toujours une adresse appropriée qui convient à la structure de réseau et à l'acheminement d'un site, ces risques peuvent être évités.

5. Références normatives

[RFC3041] T. Narten, R. Draves, " pour l'auto-configuration d'adresse sans état dans IPv6", janvier 2001. (*P.S., ; obsolète, voir* RFC4941 *; remplacée par* RFC8981)

[RFC3484] R. Draves, "Choix d'adresse par défaut pour le protocole Internet version 6 (IPv6)", février 2003. (*Remplacée par la* RFC6724) *(P.S.)*

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC4192] F. Baker et autres, "Procédures de renumérotage Extensions de confidentialitéd'un réseau IPv6 sans utiliser un 'jour J'", septembre 2005. *(Info.)*

[RFC4193] R. Hinden, B. Haberman, "Adresses IPv6 en envoi individuel uniques localement", octobre 2005. *(P.S.)*

[RFC4292] B. Haberman, "MIB de tableau de transmission IP", avril 2006. (*Remplace* RFC2096) *(P.S.)*

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007. (*Remplace* RFC2462) *(D.S.)*

[RFC4864] G. Van de Velde et autres, "Protection de réseau local pour IPv6", mai 2007. *(Information)*

[RFC5014] E. Nordmark et autres, "API de prises IPv6 pour la sélection d'adresse de source", septembre 2007. *(Information)*

Adresse des auteurs

Arifumi Matsumoto
NTT PF Lab
Midori-Cho 3-9-11
Musashino-shi, Tokyo 180-8585
Japan
téléphone : +81 422 59 3334
mél : arifumi@nttv6.net

Tomohiro Fujisaki
NTT PF Lab
Midori-Cho 3-9-11
Musashino-shi, Tokyo 180-8585
Japan
téléphone : +81 422 59 7351
mél : fujisaki@nttv6.net

Ruri Hiromi
Intec Netcore, Inc.
Shinsuna 1-3-3
Koto-ku, Tokyo 136-0075
Japan
téléphone : +81 3 5665 5069
mél : hiromi@inetcore.com

Ken-ichi Kanayama
INTEC Systems Institute, Inc.
Shimoshin-machi 5-33
Toyama-shi, Toyama 930-0804
Japan
téléphone : +81 76 444 8088
mél : kanayama_kenichi@intec-si.co.jp

Déclaration complète de droits de reproduction