Groupe de travail Réseau
Request for Comments : 3879
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

C. Huitema, Microsoft
B. Carpenter, IBM
septembre 2004

Les adresses IPv6 de site local en envoi individuel sont déconseillées

Résumé
Le présent document décrit les questions qui tournent autour de l'utilisation des adresses IPv6 de site local en envoi individuel dans leur forme originale, et les déconseille formellement. Ce désaveu n'empêche pas la poursuite de leur utilisation jusqu'à ce qu'une solution de remplacement ait été normalisée et mise en œuvre.

1. Introduction

Le groupe de travail IPv6 a passé un certain temps à débattre d'un ensemble de questions tournant autour de l'utilisation d'adresses de "site local". À sa réunion de mars 2003, le groupe a trouvé un terme d'accord sur le fait que ces questions étaient assez sérieuses pour qu'on garantisse un remplacement des adresses de site local sous leur forme originale. Bien que le consensus soit loin d'être unanime, le groupe de travail a confirmé à sa réunion de juillet 2003 la nécessité de documenter ces questions et la décision qui en découle de déconseiller les adresses IPv6 de site local en envoi individuel.

Les adresses de site local sont définies dans l'architecture d'adressage IPv6 [RFC3513], en particulier au paragraphe 2.5.6.

Le reste du présent document décrit les effets néfastes des adresses de site local selon la définition ci-dessus, et les déconseille formellement.

Des documents d'accompagnement vont décrire les buts d'une solution de remplacement et spécifier une solution de remplacement. Cependant, le désaveu formel permet que se poursuive l'usage existant des adresses de site local jusqu'à ce que la solution de remplacement soit normalisée et mise en œuvre.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC 2119].

2. Effets néfastes des adresses de site locales

Les discussions au sein du groupe de travail IPv6 ont souligné plusieurs défauts de la portée de l'adressage de site local actuel. Ces défauts entrent dans deux grandes catégories : ambiguïté des adresses, et définition floue des sites.

Comme elles sont actuellement définies, les adresses de site sont ambiguës : une adresse comme FEC0::1 peut être présente dans plusieurs sites, et l'adresse elle-même ne contient aucune indication du site auquel elle appartient. Cela crée des difficultés aux développeurs d'applications, aux concepteurs de routeurs et aux gestionnaires de réseaux. Ces difficultés découlent de la nature floue du concept de site. On développera la nature spécifique de ces difficultés dans les paragraphes suivants.

2.1 Difficulté pour le développeur, les identifiants de portée

Les retours de la part des développeurs indiquent que les adresses de site local sont difficiles à utiliser correctement dans une application. Ceci est particulièrement vrai pour les hôtes multi-rattachement, qui peuvent être simultanément connectés

à plusieurs sites, et pour les hôtes mobiles, qui peuvent être successivement connectés à plusieurs sites.

Les applications devraient apprendre ou se souvenir que l'adresse d'un certain correspondent était "FEC0::1234:5678:9ABC", elles vont essayer de rentrer l'adresse dans une structure de prise d'adresse et de produire une commande de connexion, et l'appel va échouer parce qu'elles n'auront pas rempli la variable "identifiant de site", comme dans "FEC0::1234:5678:9ABC%1". (L'utilisation du caractère % comme délimiteur pour les identifiants de zone est spécifié dans la [RFC4007].) Le problème est compliqué par le fait que l'identifiant de site varie avec l'instance d'hôte, par exemple, parfois %1 et parfois %2, et donc par le fait que l'identifiant d'hôte ne peut pas être mémorisé ou appris d'un serveur de noms.

En bref, le souci du développeur est causé par l'ambiguïté des adresses locales de site. Comme les adresses locales de site sont ambiguës, les développeurs d'applications doivent gérer les "identifiants de site" qui qualifient les adresses des hôtes. Cette gestion des identifiants s'est révélée difficile à comprendre pour les développeurs, et aussi dure à exécuter par les développeurs qui comprennent le concept.

2.2 Difficulté pour le développeur, les adresses locales

Les applications simples de client serveur qui partagent des adresses IP à la couche application sont rendues plus complexes par l'adressage IPv6 de site local. Ces applications ont besoin de prendre des décisions intelligentes sur les adresses qui devraient être ou non passées à travers les frontières de site. Ces décisions, en pratique, requièrent que les applications acquièrent une certaine connaissance de la topologie du réseau. Les adresses de site local peuvent être utilisées lorsque client et serveur sont dans le même site, mais essayer de les utiliser lorsque client et serveur sont dans des sites différents peut résulter en erreurs inattendues (c'est-à-dire, la connexion réinitialisée par l'homologue) ou l'établissement de connexions avec un mauvais nœud. Les implications pour la robustesse et la sécurité de l'envoi de paquets à un point d'extrémité inattendu vont différer d'une application à l'autre.

Les applications multi parties qui passent des adresses IP à la couche application présentent un défi particulier. Même si un nœud peut correctement déterminer si un seul nœud distant appartient ou non au site local, il n'aura aucun moyen de savoir où ces adresses peuvent finalement être envoyées. La meilleure ligne d'action pour ces applications pourrait être de n'utiliser que des adresses mondiales. Cependant, cela empêcherait l'utilisation de ces applications sur des réseaux isolés ou connectés de façon intermittente qui pourraient n'avoir de disponibles que des adresses de site local, et pourrait être incompatible avec l'utilisation d'adresses de site local pour le contrôle d'accès dans certains cas.

En résumé, l'ambiguïté des adresses de site local conduit à un comportement d'application inattendu lorsque les charges utiles d'application portent ces adresses en dehors du site local.

2.3 Difficultés pour le gestionnaire, les fuites

La gestion des adresses de site local IPv6 est de nombreuses façons similaire à la gestion des adresses de la [RFC1918] dans certains réseaux IPv4. En théorie, les adresses privées définies dans la RFC1918 ne devraient être utilisée qu'en local, et ne devraient jamais apparaître dans l'Internet. En pratique, ces adresses "fuitent". La conjonction des fuites et de l'ambiguïté conduit à causer des problèmes de gestion.

Les noms et les adresses littérales des hôtes "privés" fuitent dans les messages électroniques, les pages de la Toile, ou des fichiers. Les adresses privées finissent par être utilisées comme source ou destination de demandes TCP ou de messages UDP, par exemple dans le DNS ou des demandes trace-route, causant l'échec de la demande, ou l'arrivée de la réponse chez des hôtes inattendus.

L'expérience des adresses de la RFC1918 montre aussi des fuites non triviales, au delà du placement de ces adresses dans des en-têtes IP. Les adresses privées finissent aussi par être utilisées comme cibles d'interrogations inverses du DNS pour la RFC1918, surchargeant inutilement l'infrastructure du DNS. En général, de nombreuses applications qui utilisent directement les adresses IP finissent par passer les adresses de la RFC1918 dans des charges utiles d'application, créant de la confusion et des échecs.

La question des fuites est largement inévitable. Bien que certaines applications aient intrinsèquement une portée définie (par exemple, les annonces de routeur, la découverte de voisin) la plupart des applications n'ont pas de concept de portée, et aucun moyen d'exprimer une portée. Il en résulte des "fuites de matériel à travers les frontières". Comme les adresses sont ambiguës, les gestionnaires de réseau ne peuvent pas facilement découvrir "qui l'a fait". Les fuites ne sont pas difficiles à réparer, ce qui génère une certaine frustration.

2.4 Une complexité accrue pour les routeurs

L'ambiguïté des adresses de site local crée aussi des complications pour les routeurs. En théorie, les adresses de site local ne sont utilisées que au sein d'un site contigu, et tous les routeurs sur ce site peuvent les traiter comme si elles n'étaient pas ambiguës. En pratique, des mécanismes spéciaux sont nécessaires lorsque les sites sont disjoints, ou lorsque les routeurs ont plusieurs sites à gérer.

En théorie, les sites ne devraient jamais être disjoints. En pratique, si l'adressage de site local est utilisé sur un grand réseau, certains éléments du site ne seront pas directement connectés, par exemple à cause de partitions du réseau. Cela va créer une demande pour acheminer les paquets de site local à travers un réseau intermédiaire (comme la zone de cœur de réseau) qui ne peut pas être dédiée à un site spécifique. En pratique, cela conduit à une utilisation intensive des techniques de tunnelage, ou à l'utilisation de routeurs multi-sites, ou les deux.

Les adresses ambiguës ont des conséquences évidentes sur les routeurs multi sites. Dans l'architecture de routeur classique, l'interface de sortie est une fonction directe de l'adresse de destination, comme spécifiée par un seul tableau d'acheminement. Cependant, si un routeur est connecté à plusieurs sites, l'acheminement des paquets de site local dépend de l'interface sur laquelle le paquet est arrivé. Les interfaces doivent être associées aux sites, et les entrées d'acheminement pour les adresses de site local dépendent du site. Prendre cela en charge exige des dispositions spéciales dans les protocoles d'acheminement et des techniques de virtualisation de tableau d'acheminement et de transmission qui sont normalement utilisées pour les VPN. Cela contribue à une complexité supplémentaire des mises en œuvre et de la gestion du routeur.

La complexité de la gestion du réseau est aussi accrue par le fait que bien que des sites pourraient être pris en charge en utilisant les constructions d'acheminement existantes – comme les domaines et les zones – les facteurs qui conduisent la création et l'établissement des frontières des sites sont différents des facteurs qui conduisent celles des zones et domaines.

Dans les routeurs multi rattachements, comme par exemple des routeurs de bordure de site, le processus de transmission devrait être complété par un processus de filtrage, pour garantir que les paquets générés avec une adresse de site local ne quittent jamais le site. Ce processus de filtrage va à son tout interagir avec la transmission des paquets, par exemple si les défauts de la mise en œuvre causent l'abandon de paquets envoyés à une adresse mondiale, même si cette adresse mondiale se trouve appartenir au site cible.

En résumé, l'ambiguïté des adresses de site local les rend difficiles à gérer dans les routeurs multi sites, tandis que l'exigence de prendre en charge des sites disjoints et les constructions existantes de protocole d'acheminement créent une demande pour de tels routeurs.

2.5 Le concept de site est mal défini

La définition actuelle des portées suit un modèle idéalisé de "portées concentriques". Les hôtes sont supposés être rattachés à une liaison, qui appartient à un site, qui appartient à l'Internet. Les paquets pourraient être envoyés à la même liaison, au même site, ou en dehors de ce site. Cependant, les experts ont disputé sur la définition des sites pendant des années et ne sont arrivé à aucun consensus. Cela suggère qu'il n'y a en fait aucun consensus à atteindre.

À part la liaison locale, les frontières de portées sont mal définies. Qu'est ce qu'un site ? Est ce que la totalité d'un réseau d'entreprise est un site, ou les sites sont-ils limités à une seule localisation géographique ? De nombreux réseaux sont aujourd'hui partagés entre une zone interne et un extérieur qui fait face à une "DMZ", séparés par un pare-feu. Les serveurs dans la DMZ sont supposés être accessibles aussi bien par les hôtes internes que les hôtes externes sur l'Internet. La DMZ appartient elle au même site que l'hôte interne ?

Selon celui qu'on interroge, la définition de la portée du site varie. Elle peut représenter des limites de sécurité, des limites d'accessibilité, des frontières d'acheminement, des limites de qualité de service, des frontières administratives, des limites de tarification, d'autres sortes de frontières, ou une combinaison de tout cela. Il n'est pas très clair qu'une seule portée puisse satisfaire toutes ces exigences.

Il y a des phénomènes importants et bien connus de rupture de portée, comme des réseaux à connexion intermittente, des nœuds mobiles, des réseaux mobiles, des VPN inter-domaines, des réseaux hébergés, des fusions et des partages de réseau, etc. Précisément, cela signifie qu'une portée *ne peut pas* être transposée dans des cercles concentriques comme un modèle naïf liaison/local/mondial. Les portées se chevauchent et s'étendent les unes dans les autres. La relation de portée entre deux hôtes peut même être différente pour des protocoles différents.

En résumé, le concept actuel de site est naïf, et ne satisfait aux exigences opérationnelles.

3. Développement d'une meilleure solution de remplacement

La section précédente passait en revue les arguments contre les adresses de site local. Visiblement, les sites locaux ont aussi quelques avantages, sans lesquels ils auraient été retirés depuis longtemps de la spécification. L'avantage apparent du site local est qu'il est simple, stable, et privé. Cependant, il apparaît que ces avantages peuvent être aussi obtenus avec une autre architecture, par exemple celle de la [RFC4193], dans laquelle les adresses ne sont pas ambiguës et n'ont pas une portée explicite simple.

Avoir une adresse non ambiguë résout une grande partie du souci du développeur, car cela supprime le besoin de gérer des identifiants de site. L'application peut utiliser les adresses comme si elles étaient des adresses mondiales régulières, et la pile de protocole sera capable d'utiliser des techniques standard pour découvrir quelle interface devrait être utilisée. Quelques soucis vont subsister cependant, car ces adresses ne seront pas toujours accessibles ; les applications peuvent s'accommoder des problèmes de non accessibilité en essayant les connexions un peu plus tard, ou avec une adresse différente. On peut espérer qu'un mécanisme de portée plus sophistiqué pourrait être introduit ultérieurement.

Avoir des adresses non ambiguës n'éliminera pas les fuites qui causent les difficultés de gestion. Cependant, comme les adresses ne sont pas ambiguës, le débogage de ces fuites sera beaucoup plus simple.

Avoir des adresses non ambiguës résoudra une large part des problèmes de routeur : comme les adresses ne sont pas ambiguës, les routeurs seront capables d'utiliser les techniques d'acheminement standard, et n'auront pas besoin de tableaux d'acheminement différents pour chaque interface. Certains des soucis vont subsister aux routeurs frontières, qui devront filtrer les paquets provenant de certaines gammes d'adresses de source ; ceci est cependant une fonction très courante.

Éviter la déclaration explicite de portée va supprimer les problèmes liés à l'ambiguïté du concept de site. La non accessibilité peut être obtenue en utilisant des "pare-feu" lorsque approprié. Les règles du pare-feu peuvent explicitement s'accommoder de diverses configurations de réseau, en acceptant ou refusant le trafic de ou vers des gammes des nouvelles adresses non ambiguës.

Une question demeure, l'adressage à la cantonade. Les adresses à la cantonade sont ambiguës par construction, car elles se réfèrent par définition à tout hôte à qui a été allouée une certaine adresse d'envoi à la cantonade. Les adresses d'envoi à la cantonade de liaison locale ou mondiales peuvent être "incorporées dans le code". Des études complémentaires sont nécessaires sur le besoin d'adresses d'envoi à la cantonade avec une portée entre liaison locale et mondial.

4. Désapprobation

Le présent document déconseille formellement le préfixe d'envoi individuel IPv6 de site local défini dans la [RFC3513], c'est-à-dire, 1111111011 en binaire ou FEC0::/10. Le comportement particulier de ce préfixe NE DOIT PAS être pris en charge dans les nouvelles mises en œuvre. Le préfixe NE DOIT PAS être réalloué pour d'autres usages excepté par une future action de normalisation de l'IETF. Les futures versions de l'architecture d'adressage [RFC3513] incluront cette information.

Cependant, les mises en œuvre de routeurs DEVRAIENT être configurées par défaut pour empêcher l'acheminement de ce préfixe.

Les références aux adresses de site local devraient être retirées aussitôt que possible en pratique de la révision du protocole Internet de sélection d'adresse par défaut, version 6 [RFC3484], de la révision des extensions d'interface de prise de base pour IPv6 [RFC3493], et de la révision de l'architecture d'adressage du protocole Internet version 6 (IPv6) [RFC3513]. Les références incidentes aux adresses de site local devraient être retirées de tous les autres documents de l'IETF si et quand ils seront mis à jour. Ces documents incluent les [RFC2772], [RFC2894], [RFC3082], [RFC3111], [RFC3142], [RFC3177], et [RFC3316].

Les mises en œuvre et déploiements existants PEUVENT continuer à utiliser ce préfixé.

5. Considérations pour la sécurité

L'utilisation d'adresses de site local ambiguës a un potentiel d'effet nuisible sur la sécurité du réseau par des fuites, des ambiguïtés et de mauvais acheminements potentiels, comme exposé à la Section 2. Déconseiller l'utilisation d'adresses ambiguës aide à résoudre beaucoup de ces problèmes.

Le préfixe d'envoi individuel de site local permet certaines actions de blocage des règles de pare-feu et des règles de sélection d'adresse, qui sont généralement vues comme un dispositif de sécurité car elles empêchent les paquets de franchir les frontières administratives. De telles règles de blocage peuvent être configurées pour tout préfixe, y compris le remplacement futur attendu du préfixe de site local. Si ces règles de blocage sont bien mises en application, l'avis défavorable émis sur l'utilisation du préfixe de site local ne met pas en danger la sécurité.

6. Considérations relatives à l'IANA

Il est demandé à l'IANA de marquer le préfixe FEC0::/10 comme "déconseillé", en pointant sur le présent document. La réallocation du préfixe pour tout usage exige des justifications via une action de normalisation de l'IETF [RFC2434].

7. Remerciements

Les auteurs tiennent à remercier Fred Templin, Peter Bieringer, Chirayu Patel, Pekka Savola, et Alain Baudot de leur relecture de la version initiale de ce document. Le texte du paragraphe 2.2 inclut deux paragraphes tirés d'une version de Margaret Wasserman qui décrit l'impact de l'adressage de site local. Alain Durand a souligné la nécessité de réviser les RFC existantes qui font référence aux adresses de site local.

8. Références

8.1 Références normatives

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226*)*

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

8.2 Références pour information

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

[RFC2772] R. Rockell, R. Fink, "Lignes directrices pour l'acheminement 6Bone", février 2000. (*MàJ par* RFC3152) *(Information)*

[RFC2894] M. Crawford, "Dénumérotage de routeurs pour IPv6", août 2000. *(P.S.)*

[RFC3082] J. Kempf, J. Goldschmidt, "Notification et souscription pour SLP", mars 2001. *(Expérimentale)*

[RFC3111] E. Gutman, "Modifications au protocole de localisation de service pour IPv6", mai 2001.

[RFC3142] J. Hagino, K. Yamamoto, "Traducteur de relais de transport IPv6 à IPv4", juin 2001. *(Information)*

[RFC3177] IAB, IESG, "Recommandations IAB/IESG sur l'allocation des adresses IPv6 aux sites", septembre 2001. *(Information)*

[RFC3316] J. Arkko et autres, "Protocole Internet version 6 (IPv6) pour hôtes cellulaires de 2ème et 3ème génération", avril 2003. *(Information) (Remplacée par* RFC7066)

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

[RFC3493] R. Gilligan et autres, "Extensions d'interface de prise de base pour IPv6", février 2003. *(Information)*

[RFC4007] S. Deering et autres, "Architecture d'adresse IPv6 calibrée", mars 2005. *(P.S.) (MàJ par* RFC 7346)

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

9. Adresse des auteurs

Christian Huitema
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA
mél : huitema@microsoft.com

Brian Carpenter
IBM Corporation
Sauemerstrasse 4
8803 Rueschlikon
Confédération Helvétique
mél : brc@zurich.ibm.com

10. Déclaration complète de droits de reproduction

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