Groupe de travail Réseau
Request for Comments : 4007
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle
mars 2005

S. Deering, Cisco Systems
B. Haberman, Johns Hopkins Univ
T. Jinmei, Toshiba
E. Nordmark, Sun Microsystems
B. Zill, Microsoft

Architecture d'adresse IPv6 calibrée

Résumé
Le présent document spécifie les caractéristiques architecturales, le comportement espéré, la représentation textuelle et l'usage des adresses IPv6 de différentes portées. Conformément à une décision du groupe de travail IPv6, le présent document évite intentionnellement la syntaxe et l'usage des adresses de site local en envoi individuel

Table des Matières

1. Introduction

La version 6 du protocole Internet comporte la prise en charge des adresses de différentes "portées" ; c'est-à-dire des adresses aussi bien mondiales que non mondiales (par exemple, de liaison locale). Bien que l'adressage non mondial ait été introduit opérationnellement dans l'Internet IPv4, à la fois dans l'utilisation d'espace d'adresses privé ("net 10", etc.) et avec des adresses de diffusion groupée à portée réduite administrativement, la conception de IPv6 incorpore formellement la notion de portée d'adresses dans son architecture de base. Le présent document spécifie les caractéristiques architecturales, le comportement attendu, la représentation textuelle, et l'usage des adresses IPv6 de portées différentes.

Bien que la spécification actuelle de l'architecture d'adresses [RFC3513] définisse les adresses en envoi individuel de site local, le groupe de travail IPv6 a décidé d'en déconseiller la syntaxe et l'usage [RFC3879] et explore maintenant d'autres formes d'adressage IPv6 local. L'usage de toutes nouvelles formes d'adresses locales sera documenté ailleurs à l'avenir. Donc, le présent document se concentre intentionnellement seulement sur la liaison locale et la diffusion groupée.

2. Définitions

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].

3. Terminologie de base

Les termes de liaison, interface, nœud, hôte, et routeur sont définis dans la [RFC2460]. Les définitions des portées d'adresse en envoi individuel (liaison locale et mondiale) et de portées d'adresse de diffusion groupée (interface locale, liaison locale, etc.) sont contenues dans la [RFC3513].

4. Portée d'adresse

Toute adresse IPv6 autre que l'adresse inspécifiée a une portée spécifique ; c'est-à-dire, une portée topologique au sein de laquelle l'adresse peut être utilisée comme un identifiant univoque pour une interface ou ensemble d'interfaces. La portée d'une adresse est codée au titre de l'adresse, comme spécifié dans la [RFC3513].

Pour les adresses d'envoi individuel, le présent document discute de deux portées définies :
- Portée de liaison locale, pour identifier de façon univoque les interfaces au sein (c'est-à-dire, rattachées à) d'une seule liaison.
- Portée mondiale, pour identifier de façon univoque les interfaces partout dans l'Internet.

L'adresse IPv6 de bouclage en envoi individuel, ::1, est traitée comme ayant une portée de liaison locale au sein d'une liaison imaginaire à laquelle une "interface de bouclage" virtuelle est rattachée.

L'adresse inspécifiée, ::, est un cas particulier. Elle n'a aucune portée parce qu'elle ne doit jamais être allouée à un nœud, conformément à la [RFC3513]. Noter cependant, qu'une mise en œuvre pourrait utiliser une sémantique propre pour l'adresse inspécifiée et pourrait vouloir allouer l'adresse inspécifiée pour avoir des portées spécifiques. Par exemple, les mises en œuvre utilisent souvent l'adresse inspécifiée pour représenter "toute" adresse dans les API. Dans ce cas, les mises en œuvre peuvent considérer l'adresse inspécifiée avec une portée particulière comme représentant la notion de "toute adresse dans la portée". Le présent document n'interdit pas un tel usage, pour autant qu'il soit limité à la mise en œuvre.

La [RFC3513] définit les adresses IPv6 avec des adresses IPv4 incorporées comme faisant partie des adresses mondiales. Donc, ces adresses ont une portée mondiale, par rapport à l'architecture d'adresse calibrée IPv6. Cependant, une mise en œuvre peut utiliser par convenance ces adresses comme si elles avaient d'autres portées. Par exemple, la [RFC3484] alloue une portée de liaison locale aux adresses IPv4 de liaison locale autoconfigurée (les adresses du préfixe 169.254.0.0/16 [RFC3927]) et convertit ces adresses en adresses IPv6 transposées en IPv4 afin d'effectuer le choix d'adresse de destination parmi les adresses IPv4 et IPv6. Cela voudrait implicitement dire que les adresses IPv6 transposées en IPv4 équivalentes à des adresses de liaison locale IPv4 à autoconfiguration ont une portée de liaison locale. Le présent document n'interdit pas un tel usage, pour autant qu'il soit limité à cette mise en œuvre.

Les adresses d'envoi à la cantonade [RFC3513] sont allouées à partir de l'espace d'adresses d'envoi individuel et ont les mêmes propriétés de portée que les adresses d'envoi individuel. Toutes les déclarations du présent document concernant l'envoi individuel s'appliquent également à l'envoi à la cantonade.

Pour les adresses de diffusion groupée, il y a quatorze portées possibles, allant de l'interface locale au mondial (en incluant la liaison locale). La portée d'interface locale couvre seulement une interface ; une adresse de diffusion groupée de portée interface locale n'est utile que pour la livraison en bouclage de diffusions groupées au sein d'un seul nœud ; par exemple, comme une forme de communication inter-procès au sein d'un ordinateur. À la différence de l'adresse de bouclage en envoi individuel, les adresses de diffusion groupée d'interface locale peuvent être allouées à toute interface.

Il y a une relation de taille entre les portées :
- Pour les portées d'envoi individuel, la liaison locale est une plus petite portée que mondial.
- Pour les portées de diffusion groupée, les portées avec des valeurs inférieures dans les sous-champ "scop" de l'adresse de diffusion groupée (paragraphe 2.7 de la [RFC3513]) sont plus petites que les portées avec de plus grandes valeurs, avec interface locale qui est le plus petit et mondial qui est le plus grand.

Cependant, deux portées de taille différente peuvent couvrir exactement la même région de topologie. Par exemple, un site (de

diffusion groupée) peut consister en une seule liaison, dans laquelle les portées liaison locale et site local couvrent effectivement la même zone topologique.

5. Zones de portée

Une zone de portée, ou simplement une zone, est une région connectée dont la topologie à une certaine portée. Par exemple, l'ensemble des liaisons connectées par des routeurs au sein d'un site particulier (en diffusion groupée) et les interfaces rattachées à ces liaisons, constitue une seule zone de portée de site local de diffusion groupée.

Noter qu'une zone est une instance particulière d'une région topologique (par exemple, le site d'Alice ou le site de Bob) tandis qu'une portée est la taille d'une région topologique (par exemple, un site ou une liaison). La zone à laquelle appartient une certaine adresse non mondiale n'est pas codée dans l'adresse elle-même mais est déterminée par le contexte, comme l'interface d'où elle est envoyée ou reçue. Donc, les adresses d'une certaine portée (non mondiale) peuvent être réutilisées dans des zones différentes de cette portée. Par exemple, deux liaisons physiques différentes peuvent chacune contenir un nœud avec l'adresse de liaison locale de fe80::1.

Les zones de portée différente sont instanciées comme suit :
- o Chaque interface sur un nœud comporte une seule zone de portée d'interface locale (seulement pour la diffusion groupée).
- o Chaque liaison et les interfaces rattachées à cette liaison comportent une seule zone de portée de liaison locale (pour l'envoi individuel et la diffusion groupée).
- o Il y a une seule zone de portée mondiale (pour l'envoi individuel et la diffusion groupée) qui comprend toutes les liaisons et interfaces de l'Internet.
- o Les frontières de zones d'une portée autre que d'interface locale, de liaison locale, et mondiale doivent être définies et configurées par les administrateurs de réseau.

Les frontières de zone sont des caractéristiques relativement statiques, qui ne changent pas en réponse aux changements à court terme de la topologie. Donc, l'exigence que la topologie au sein d'une zone soit "connectée" est destinée à inclure des liaisons et interfaces qui peuvent n'être qu'occasionnellement connectées. Par exemple, un nœud ou réseau résidentiel qui obtient l'accès Internet en appelant le site d'un employeur (en diffusion groupée) peut être traité comme faisant partie de la zone de site local de l'employeur (en diffusion groupée) lorsque la liaison de numérotation est déconnectée. De même, la défaillance d'un routeur, d'une interface, ou d'une liaison qui cause la partition d'une zone ne partage pas cette zone en plusieurs zones. Les différentes parties sont plutôt toujours considérées appartenir à la même zone résidentielle.

Les zones ont les propriétés supplémentaires suivantes :
- o Les frontières de zone coupent à travers les nœuds, pas des liaisons. (Noter que la zone mondiale n'a pas de frontière, et que la frontière d'une zone d'interface locale inclut juste une seule interface.)
- o Les zones de même portée ne peuvent pas se chevaucher ; c'est-à-dire qu'elles peuvent n'avoir pas de liaisons ou d'interfaces en commun.
- o Une zone d'une certaine portée (inférieure à mondiale) tombe complètement dans des zones de portée plus large. C'est-à-dire qu'une zone de portée plus petite ne peut pas inclure plus de topologie qu'une zone de portée plus large avec laquelle elle partagerait des liaisons ou de plus petites interfaces.
- o Chaque zone doit être "convexe" du point de vue de l'acheminement ; c'est-à-dire, les paquets envoyés d'une interface à toute autre dans la même zone ne sont jamais acheminés en dehors de la zone. Noter, cependant, que si une zone contient une liaison tunnelée (par exemple, un tunnel de liaison IPv6 sur IPv6 [RFC2473]) un réseau de couche inférieure du tunnel peut être situé en dehors de la zone sans violer la propriété de convexité.

Chaque interface appartient exactement à une zone de chaque portée possible. Noter que cela signifie qu'une interface appartient à une zone de portée sans considération de la sorte d'adresse en envoi individuel qu'a l'interface ou à quels groupes de diffusion groupée se joint le nœud sur l'interface.

6. Indices de zone

Comme la même adresse non mondiale peut être utilisée dans plus d'une zone de la même portée (par exemple, l'utilisation de l'adresse de liaison locale fe80::1 dans deux liaisons physiques séparées) et qu'un nœud peut avoir des interfaces rattachées à différentes zones de la même portée (par exemple, un routeur a normalement plusieurs interfaces rattachées à des liaisons différentes) un nœud a besoin d'un moyen interne pour identifier à quelle zone appartient une adresse non mondiale. Cela se fait en allouant, au sein du nœud, un "indice de zone" distinct pour chaque zone de la même portée à laquelle ce nœud est rattaché, et en permettant que toutes les utilisations internes d'une adresse soient qualifiées par un indice de zone.

L'allocation des indices de zone est illustrée dans l'exemple de la figure ci-dessous :

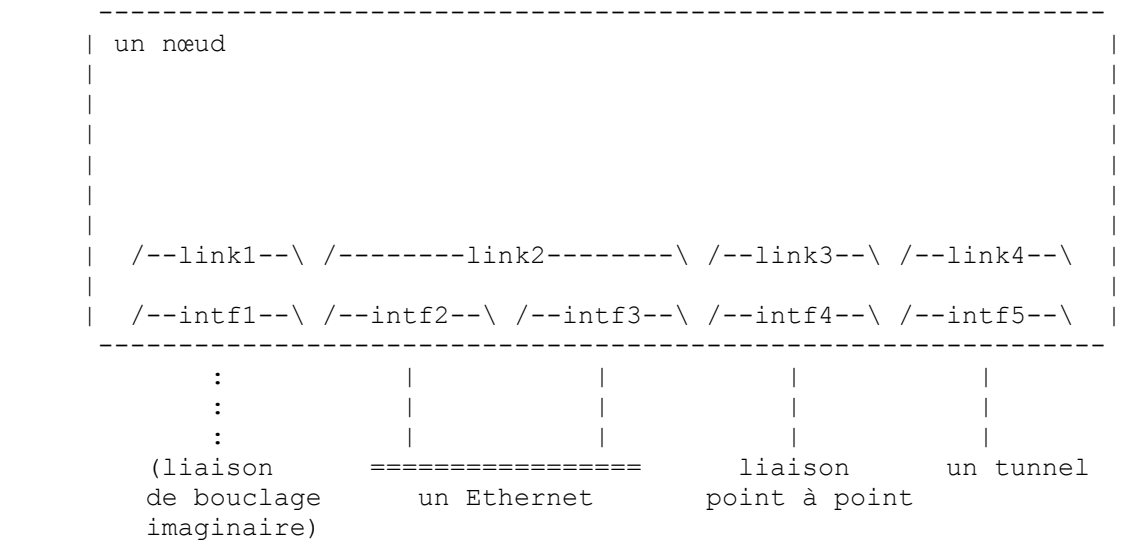

Figure 1 : Exemple d'indices de zone

Cet exemple de nœud a cinq interfaces :
une interface de bouclage à la liaison de bouclage imaginaire (une liaison fantôme qui ne va nulle part) ;
deux interfaces pour la même liaison Ethernet ;
une interface pour une liaison point à point ;
une interface tunnel (par exemple, le point d'extrémité abstrait d'un tunnel IPv6 sur IPv6 [RFC2473], vraisemblablement établi sur la liaison Ethernet ou celle point à point).

Il est donc rattaché à cinq zones d'interface locale, identifiées par les indices d'interface 1 à 5.

Parce que les deux interfaces Ethernet sont rattachées à la même liaison, le nœud est seulement rattaché à quatre zones de liaison locale, identifiée par les indices de liaison de 1 à 4. Noter aussi que même si l'interface de tunnel est établie sur l'Ethernet, la liaison tunnel obtient son propre indice de liaison, qui est différent de l'indice de la zone de liaison Ethernet.

Chaque indice de zone d'une portée particulière devrait contenir assez d'informations pour indiquer la portée, afin que tous les indices de toutes les portées soient uniques au sein des indices de nœud et que les indices de zone eux-mêmes puissent être utilisés dans un but déterminé. L'usage de l'indice pour identifier une entrée dans la base de données d'informations de gestion (MIB, *Management Information Base*) est un exemple de but déterminé. La représentation réelle pour coder la portée dépend de la mise en œuvre et sort du domaine d'application du présent document. Dans le présent document, les indices sont simplement représentés dans un format tel que "liaison indice 2" pour la lisibilité.

Les indices de zone sont strictement locaux pour le nœud. Par exemple, le nœud à l'autre extrémité de la liaison point à point peut fort bien utiliser une interface et des valeurs d'indice de liaison entièrement différentes pour cette liaison.

Une mise en œuvre devrait aussi prendre en charge le concept d'une zone "par défaut" pour chaque portée. Et, lorsque il est pris en charge, la valeur d'indice zéro à chaque portée DEVRAIT être réservée pour signifier "utiliser la zone par défaut". À la différence des autres indices de zone, l'indice par défaut ne contient aucune portée, et la portée est déterminée par l'adresse qu'accompagne l'indice par défaut. Une mise en œuvre peut en plus définir une zone par défaut séparée pour chaque portée. Ces indices par défaut peuvent aussi être utilisés comme le qualificatif de zone pour une adresse pour laquelle le nœud est rattaché à une seule zone ; par exemple, lorsque on utilise des adresses mondiales.

À présent, il n'y a aucun moyen pour qu'un nœud détermine automatiquement lesquelles de ses interfaces appartiennent aux mêmes zones ; par exemple, la même liaison ou la même zone de portée de diffusion groupée plus grande qu'une interface. À l'avenir, des protocoles pourront être développés pour déterminer ces informations. En l'absence de tels protocoles, une mise en œuvre doit fournir le moyen d'allouer et/ou réallouer des indices de zone. De plus, pour éviter d'effectuer dans la plupart des cas une configuration manuelle, une mise en œuvre devrait, par défaut, n'allouer initialement les indices de zone que comme suit :
- un unique indice d'interface pour chaque interface,
- un unique indice de liaison pour chaque interface.

La configuration manuelle serait alors seulement nécessaire pour les cas moins courants de nœuds avec des interfaces multiples avec une seule liaison ou celles avec des interfaces avec des zones de portées différentes (seulement de diffusion groupée).

Donc, les allocations d'indice de zone par défaut pour l'exemple de nœud de la Figure 1 seraient comme indiqué à la Figure 2, ci-dessous. La configuration manuelle serait alors nécessaire pour, par exemple, allouer le même indice de liaison à deux interfaces Ethernet, comme montré à la Figure 1.

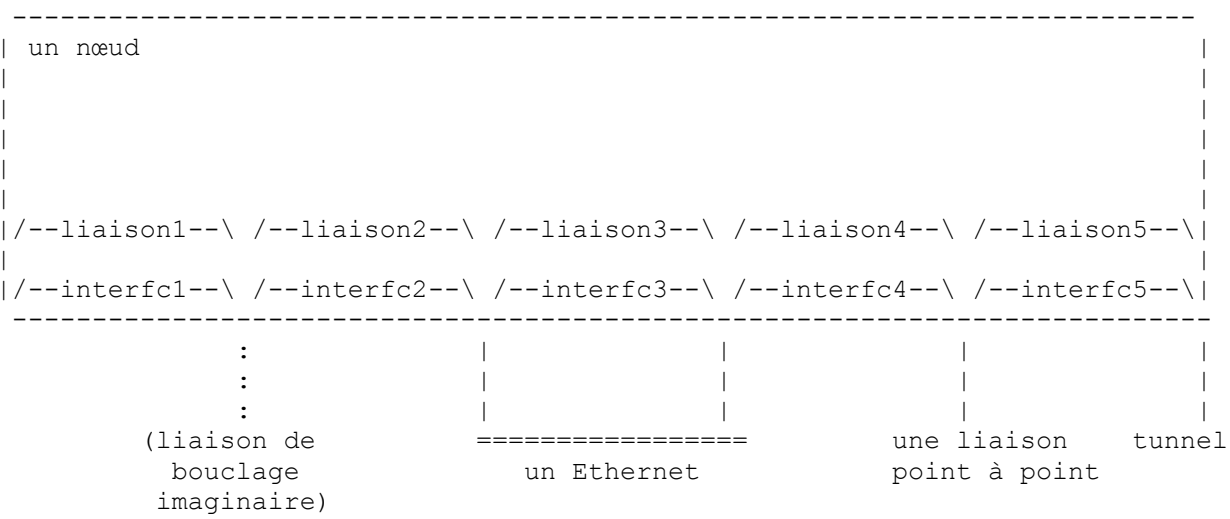

Figure 2 : Exemple d'indices de zone par défaut

En plus d'allouer initialement les indices de zone, comme spécifié ci-dessus, une mise en œuvre devrait automatiquement choisir une zone par défaut pour chaque portée pour laquelle il y a plus d'un choix, à utiliser chaque fois qu'une adresse est spécifiée sans indice de zone (ou avec un indice de zone de zéro). Par exemple, à la Figure 2, la mise en œuvre pourrait automatiquement choisir interfc2 et liaison2 comme zones par défaut pour chacune de ces deux portées. (Un algorithme de choix possible est de prendre la première zone qui inclut une interface autre que l'interface de bouclage comme défaut pour chaque portée.) Un moyen doit aussi être fourni pour allouer manuellement la zone par défaut, outrepassant toute allocation automatique.

L'adresse de bouclage en envoi individuel, ::1, ne peut pas être allouée à une interface autre que l'interface de bouclage. Il est donc recommandé que chaque fois que ::1 est spécifiée sans un indice de zone ou avec l'indice de zone par défaut, cela soit interprété comme appartenant à la zone locale de la liaison de bouclage, sans considération de la zone de liaison locale qui a été choisie comme zone par défaut. Si cela est fait, pour les nœuds avec une seule interface non de bouclage (par exemple, une seule interface Ethernet), le cas courant, les adresses de liaison locale n'ont pas besoin d'être qualifiées avec un indice de zone. L'adresse non qualifiée ::1 va toujours se référer à la zone de liaison locale contenant l'interface de bouclage. Toutes les autres adresses de liaison locale non qualifiée vont se référer à la zone de liaison locale qui contient l'interface de non bouclage (pour autant que la zone de liaison locale par défaut ait été réglée à être la zone contenant l'interface de non bouclage).

À cause de l'exigence qu'une zone d'une certaine portée entre entièrement dans des zones de plus large portée (voir la Section 5) deux interfaces allouées à des zones différentes de portée S doivent aussi être allouées à des zones différentes de toute portée plus petite que S. Donc, l'allocation manuelle d'indices de zone distincts pour une portée peut exiger l'allocation automatique d'indices de zone distincts pour des portées plus petites. Par exemple, supposons que les indices de site local de diffusion groupée distincts 1 et 2 soient manuellement alloués dans la Figure 1 et que site 1 contienne les liaisons 1, 2, et 3, mais que le site 2 contienne seulement la liaison 4. Cette configuration causerait la création automatique des indices 1 et 2 d'administration locale correspondante (c'est-à-dire, la valeur de diffusion groupée "scop" 4) parce que la portée administration locale est plus petite que la portée site local.

Avec les considérations ci-dessus, l'ensemble complet des indices de zone pour notre exemple de nœud de la Figure 1, avec les présente configurations supplémentaires, est montré à la Figure 3, ci-dessous.

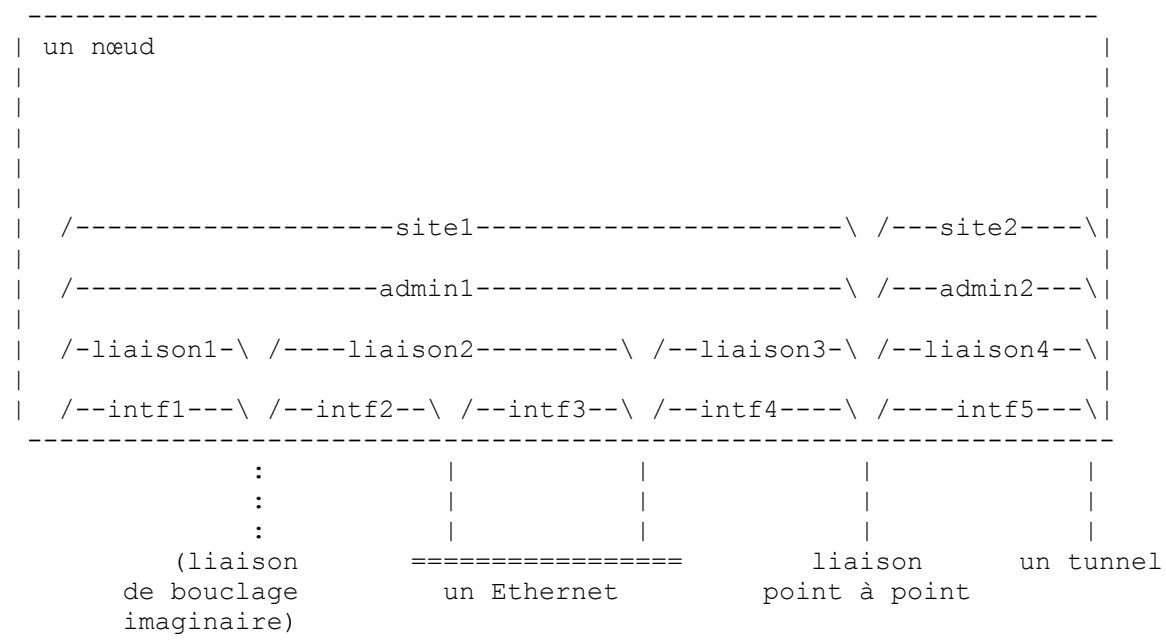

Figure 3 : Exemple complet d'indices de zone

Bien que les exemples ci-dessus montrent des zones auxquelles sont allouées des valeurs d'indice en séquence pour chaque portée, en commençant à un, les valeurs d'indice de zone sont arbitraires. Une mise en œuvre peut étiqueter une zone avec la valeur de son choix, pour autant que la valeur d'indice de chaque zone de toutes les portées soit unique pour le nœud. Zéro DEVRAIT être réservé pour représenter la zone par défaut. Les mises en œuvre qui choisissent de suivre l'API de base recommandée [RFC3493] voudront restreindre leur valeurs d'indice à celles qui peuvent être représentées par le champ sin6_scope_id dans la structure sockaddr_in6.

7. Envoi des paquets

Lorsque un protocole de couche supérieure envoie un paquet à une adresse de destination non mondiale, il doit avoir un moyen d'identifier la zone prévue à la couche IPv6 pour les cas dans lesquels le nœud est rattaché à plus d'une zone de la portée de l'adresse de destination.

Bien que l'identification d'une interface sortante soit suffisante pour identifier une zone de destination (parce que chaque interface n'est rattachée qu'à une seule zone de chaque portée) dans de nombreux cas, ceci est plus spécifique qu'il n'est désiré. Par exemple, lors de l'envoi à une adresse d'envoi individuel de liaison locale à partir d'un nœud qui a plus d'une interface avec la liaison désirée (une configuration non habituelle) le protocole de couche supérieure peut ne pas se soucier de l'interface utilisée pour la transmission. Il va plutôt laisser ce choix à la fonction d'acheminement à la couche IP. Donc, la couche supérieure exige la capacité de spécifier un indice de zone lors de l'envoi à une adresse de destination non mondiale qui n'est pas de bouclage.

8. Réception des paquets

Lorsque un protocole de couche supérieure reçoit un paquet qui contient une adresse de source ou de destination non mondiale, la zone à laquelle appartient cette adresse peut être déterminée à partir de l'interface d'arrivée, parce que l'interface d'arrivée peut seulement être rattachée à une seule zone de la même portée que celle de l'adresse considérée. Cependant, il est recommandé que la couche IP porte à la couche supérieure les indices de zone corrects pour les adresses de source et de destination d'arrivée, en plus de l'identifiant d'interface d'arrivée.

9. Transmission

Lorsque un routeur reçoit un paquet adressé à un nœud autre que lui-même, il doit prendre en compte comme suit la zone des adresses de destination et de source :

- La zone de l'adresse de destination est déterminée par la portée de l'adresse et l'interface d'arrivée du paquet. L'interface du prochain bond est choisie en cherchant l'adresse de destination dans un tableau d'acheminement (conceptuel) spécifique de cette zone (voir la Section 10). Ce tableau d'acheminement se restreint à la référence aux interfaces qui appartiennent à cette zone.

- Après le choix de l'interface de prochain bond, la zone de l'adresse de source est considérée. Comme avec l'adresse de destination, la zone de l'adresse de source est déterminée par la portée de l'adresse et l'interface d'arrivée du paquet. Si la transmission du paquet sur l'interface de prochain bond choisie ferait quitter la zone de l'adresse de source au paquet, c'est-à-dire, traverser une frontière de zone de la portée de l'adresse de source, le paquet est alors éliminé. De plus, si l'adresse de destination du paquet est une adresse d'envoi individuel, un message ICMP Destination injoignable [RFC2463] avec le code 2 ("au delà de la portée de l'adresse de source") est envoyé à la source du paquet d'origine. Noter que le code 2 est actuellement laissé non alloué dans la [RFC2463], mais l'IANA va réallouer la valeur pour ce nouvel objet, et la [RFC2463] sera révisée avec ce changement.

Noter que même si les adresses de site local en envoi individuel sont déconseillées, la procédure ci-dessus s'applique quand même aux adresses de site local. Donc, si un routeur reçoit un paquet avec une adresse de destination de liaison locale qui n'est pas une des propres adresses de liaison locale du routeur sur la liaison d'arrivée, le routeur est supposé essayer de transmettre le paquet à la destination sur cette liaison (sous réserve de la réussite de la détermination de l'adresse de couche liaison de la destination via le protocole de découverte de voisin [RFC2461]). Le paquet transmis peut être retransmis par l'interface d'arrivée, ou par toute autre interface rattachée à la même liaison.

Un nœud qui reçoit un paquet adressé à lui-même et qui contient un en-tête d'acheminement avec plus de zéro segments restants (paragraphe 4.4 de la [RFC2460]) vérifie d'abord la portée de la prochaine adresse dans l'en-tête Acheminement. Si la portée de la prochaine adresse est plus petite que la portée de l'adresse de destination originale, le nœud DOIT éliminer le paquet. Autrement, il change l'adresse de destination originale en la prochaine adresse dans l'en-tête Acheminement. Puis les règles de transmission ci-dessus s'appliquent comme suit :

- La zone de la nouvelle adresse de destination est déterminée par la portée de la prochaine adresse et de l'interface d'arrivée du paquet. L'interface de prochain bond est choisie selon le premier point des règles ci-dessus.

- Après le choix de l'interface de prochain bond, la zone de l'adresse de source est considérée selon le second point des règles ci-dessus.

Cette vérification de la portée de la prochaine adresse assure que lorsque un paquet arrive à sa destination finale, si cette destination est de liaison locale, le nœud receveur peut alors savoir que le paquet a été généré sur la liaison. Cela va aider le nœud receveur à envoyer un paquet de "réponse" avec la destination finale du paquet reçu comme adresse de source sans casser sa zone de source.

Noter qu'il est possible, bien que généralement déconseillé, d'utiliser un en-tête Acheminement pour porter une adresse non mondiale à travers sa frontière de zone associée dans le champ Prochaine adresse précédemment utilisé. Par exemple, considérons le cas dans lequel un nœud de liaison bordure (par exemple, un routeur) reçoit un paquet dont la destination est une adresse de liaison locale, et dont l'adresse de source est une adresse mondiale. Si le paquet contient un en-tête Acheminement dont la prochaine adresse est une adresse mondiale, l'interface de prochain bond pour l'adresse mondiale peut appartenir à une liaison différente de la destination d'origine. Ceci est permis parce que la portée de la prochaine adresse n'est pas plus petite que la portée de la destination originale.

10. Acheminement

Noter que comme les adresses de site local en envoi individuel sont déconseillées, et que les adresses de liaison locale n'ont pas besoin d'acheminement, l'exposé de cette section s'applique seulement à l'acheminement de diffusion groupée à portée limitée.

Lorsque un protocole d'acheminement détermine qu'il fonctionne dans une frontière de zone, il DOIT protéger l'intégrité inter-zone et conserver la connexité intra-zone.

Pour conserver la connexité, le protocole d'acheminement doit être capable de créer des informations de transmission pour les groupes globaux et pour tous les groupes à portée limitée pour chacune de ses zones rattachées. La façon la plus directe de faire cela est de créer des tableaux de transmission (conceptuels) pour chaque zone spécifique.

Pour protéger l'intégrité inter-zone, les routeurs doivent être sélectifs dans les informations de groupe partagées avec les routeurs du voisinage. Les routeurs échangent de façon habituelle des informations d'acheminement avec les routeurs du voisinage. Lorsque un routeur transmet ces informations d'acheminement, il ne doit pas inclure d'informations sur des zones

autres que les zones allouées à l'interface utilisée pour transmettre les informations.

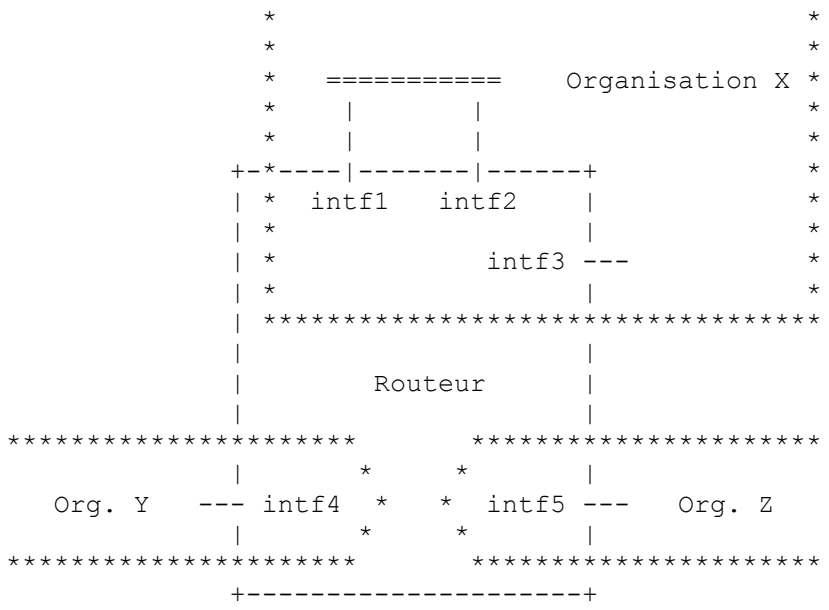

Figure 4 : Routeur de diffusion groupée multi organisations

Par exemple, le routeur de la Figure 4 doit échanger les informations d'acheminement sur cinq interfaces. Les informations échangées sont les suivantes (pour simplifier, les portées de diffusion groupée plus petites ou plus grandes que la portée d'organisation sauf mondiale ne sont pas considérées ici) :

- Interface 1
  - tous les groupes mondiaux
  - tous les groupes d'organisation appris des interfaces 1, 2, et 3

- Interface 2
  - tous les groupes mondiaux
  - tous les groupes d'organisation appris des interfaces 1, 2, et 3

- Interface 3
  - tous les groupes mondiaux
  - tous les groupes d'organisation appris des interfaces 1, 2, et 3

- Interface 4
  - tous les groupes mondiaux
  - tous les groupes d'organisation appris de l'interface 4

- Interface 5
  - tous les groupes mondiaux
  - tous les groupes d'organisation appris de l'interface 5

En imposant les règles d'échange, l'intégrité de zone est conservée en conservant toutes les informations d'acheminement spécifiques de la zone contenues dans la zone.

11. Représentation textuelle

Comme déjà mentionné, pour spécifier une adresse IPv6 non mondiale sans ambiguïté, une zone de portée prévue devrait aussi être spécifiée. Comme notation commune pour spécifier la zone de portée, une mise en œuvre DEVRAIT prendre en charge le format suivant :

<adresse>%<identifiant_de_zone>

où

<adresse> est une adresse IPv6 littérale,

<identifiant_de_zone> est une chaîne qui identifie la zone de l'adresse, et

'%' est un caractère délimiteur pour distinguer entre <adresse> et <identifiant_de_zone>.

Les paragraphes qui suivent décrivent les définitions détaillées, des exemples concrets, et des notes supplémentaires sur le format.

11.1 Adresses non mondiales

Le format s'applique à toutes les sortes d'adresses d'envoi individuel et de diffusion groupée de portée non mondiale excepté l'adresse inspécifiée, qui n'a pas de portée. Le format n'a pas de signification et ne devrait pas être utilisé pour les adresses mondiales. L'adresse de bouclage appartient à la liaison triviale ; c'est-à-dire, la liaison rattachée à l'interface de bouclage. Donc, le format ne devrait pas non plus être utilisé pour l'adresse de bouclage. Le présent document ne spécifie pas l'usage du format lorsque <adresse> est l'adresse inspécifiée, car l'adresse n'a pas de portée. Le présent document n'interdit cependant pas qu'une mise en œuvre utilise le format pour ces adresses spéciales pour des besoins dépendants de la mise en œuvre.

11.2 Partie <zone_id>

Dans la représentation textuelle, la partie <identifiant_de_zone> devrait être capable d'identifier une zone particulière de la portée de l'adresse. Bien qu'un indice de zone soit supposé contenir suffisamment d'informations pour déterminer la portée et soit unique parmi toutes les portées comme décrit à la Section 6, la partie <identifiant_de_zone> de ce format n'a pas à contenir la portée. Cela parce que la partie <adresse> devrait spécifier la portée appropriée. Cela signifie aussi que la partie <identifiant_de_zone> n'a pas à être unique entre toutes les portées.

Avec cette propriété plus lâche, une mise en œuvre peut utiliser une représentation pratique comme <identifiant_de_zone>. Par exemple, pour représenter l'indice de liaison 2, la mise en œuvre peut simplement utiliser "2" comme <identifiant_de_zone>, qui serait plus lisible que d'autres représentations qui contiennent la portée "liaison".

Lorsque une mise en œuvre interprète le format, elle devrait construire l'indice de zone "complet", qui contient la portée, à partir de la partie <identifiant_de_zone> et la portée spécifiée par la partie <adresse>. (Se rappeler qu'un indice de zone devrait lui-même contenir la portée, comme spécifié à la Section 6.)

Une mise en œuvre DEVRAIT prendre en charge au moins des indices numériques qui soient des entiers décimaux non négatifs comme <identifiants_de_zone>. L'indice de zone par défaut, qui devrait normalement être 0 (voir la Section 6) est inclus dans les entiers. Lorsque <identifiant_de_zone> est le défaut, les caractères délimiteurs "%" et <identifiant_de_zone> peuvent être omis. De façon similaire, si une représentation textuelle d'une adresse IPv6 est donnée sans un indice de zone, elle devrait être interprétée comme<adresse>%<Identifiant par défaut>, où <Identifiant par défaut> est l'indice de zone par défaut de la portée qu'a <adresse>.

Une mise en œuvre PEUT prendre en charge d'autres sortes de chaînes non nulles comme <identifiant_de_zone>. Cependant, les chaînes ne doivent pas entrer en conflit avec le caractère délimiteur. Le format et la sémantique précise des chaînes supplémentaires dépendent de la mise en œuvre.

Une chaîne candidate possible serait des noms d'interface, car les interfaces ôtent toute ambiguïté des portées. En particulier, les noms d'interface peuvent être utilisés comme des "identifiants par défaut" pour les interfaces et les liaisons, parce que par défaut il y a une transposition biunivoque entre les interfaces et chacune de ces portées comme décrit à la Section 6.

Une mise en œuvre pourrait aussi utiliser des noms d'interface comme <identifiant_de_zone> pour des portées plus grandes que la liaison, mais il pourrait y avoir un peu de confusion dans cette utilisation. Par exemple, lorsque plus d'une interface appartient au même site (de diffusion groupée) un utilisateur ne saurait pas quelle interface devrait être utilisée. Aussi, une fonction de transposition d'adresse en nom rencontrerait le même type de problème lorsque elle imprime une adresse avec un nom d'interface comme indice de zone. Le présent document ne spécifie pas comment ces cas devraient être traités et laisse cela à chaque mise en œuvre.

On ne peut pas supposer que les indices sont communs entre tous les nœuds d'une zone (voir la Section 6). Donc, le format DOIT être utilisé seulement au sein d'un nœud et NE DOIT PAS être envoyé sur le réseau si tous les nœuds qui interprètent le

format ne s'accordent pas sur sa sémantique.

11.3 Exemples

Les adresses suivantes

fe80::1234 (sur la première liaison du nœud)
ff02::5678 (sur la cinquième liaison du nœud)
ff08::9abc (sur la dixième organisation du nœud)

seraient représentées comme suit :

fe80::1234%1
ff02::5678%5
ff08::9abc%10

(On suppose ici une traduction naturelle d'un indice de zone en partie <identifiant_de_zone>, où la N^{ème} zone de toute portée est traduite en "N".)

Si on utilise les noms d'interface comme <identifiant_de_zone>, ces adresses pourraient aussi être représentées comme suit :

fe80::1234%ne0
ff02::5678%pvc1.3
ff08::9abc%interface10

où l'interface "ne0" appartient à la première liaison, "pvc1.3" appartient à la cinquième liaison, et "interface10" appartient à la dixième organisation.

11.4 Exemples d'utilisation

Les applications qui sont supposées être utilisées dans les hôtes d'extrémité tels que telnet, ftp, et ssh peuvent ne pas prendre en charge explicitement la notion de portée d'adresse, en particulier celle des adresses de liaison locale. Cependant, un utilisateur expert (par exemple, un administrateur de réseau) a parfois besoin de donner même des adresses de liaison locale à de telles applications.

Voici un exemple concret. Considérons un routeur multi liaison appelé "R1" qui a au moins deux interfaces point à point (liaisons). Chacune des interfaces est connectée à un autre routeur, respectivement "R2" et "R3". On suppose aussi que les interfaces point à point ont seulement des adresses de liaison locale.

Supposons maintenant que le système d'acheminement sur R2 raccroche et doive être ré invoqué. Dans cette situation, on peut n'être pas capable d'utiliser une adresse mondiale de R2, parce que c'est un acheminement difficile et qu'on ne peut pas espérer avoir assez de chemins pour une accessibilité mondiale de R2.

Donc, on doit d'abord connecter R1 puis essayer de connecter R2 en utilisant des adresses de liaison locale. Dans ce cas, on doit donner l'adresse de liaison locale aussi à R2, par exemple, telnet. On suppose ici que l'adresse est fe80::2.

Noter qu'on ne peut juste taper

```
% telnet fe80::2
```

ici, car R1 a plus d'une liaison et que donc la commande telnet ne peut pas détecter quelle liaison il devrait essayer d'utiliser pour se connecter. À la place, on devrait taper l'adresse de liaison locale avec l'indice de liaison comme suit :

```
% telnet fe80::2%3
```

où le "3" après le caractère délimiteur `%' correspond à l'indice de liaison de la liaison point à point.

11.5 API en rapport

Une extension de l'API de base recommandée définit comment le format des adresses non mondiales devrait être traité dans les fonctions de librairie qui traduisent un nom de nœud en adresse, ou vice versa [11].

11.6 Omission des indices de zone

Le format défini dans le présent document n'est pas destiné à invalider le format original pour les adresses non mondiales ; c'est-à-dire, le format sans la portion indice de zone. Comme décrit à la Section 6, dans certains cas courants avec la notion d'indice de zone par défaut, il ne peut pas y avoir d'ambiguïté sur les zones de portées. Dans un tel environnement, la mise en œuvre peut omettre la partie "%<identifiant_de_zone>". Par suite, elle peut agir bien qu'elle ne prenne pas du tout en charge le format étendu.

11.7 Combinaisons des caractères de délimitation

Il y a d'autres sortes de caractères délimiteurs définis pour les adresses IPv6. Dans ce paragraphe, on décrit comment ils devraient être combinés avec le format pour les adresses non mondiales.

L'architecture d'adressage IPv6 [RFC3513] définit aussi la syntaxe des préfixes IPv6. Si la portion adresse d'un préfixe est non mondiale et si sa zone de portée devait être précisée, la portion adresse DEVRAIT être dans le format. Par exemple, un préfixe de liaison locale fe80::/64 sur la seconde liaison peut être représenté comme suit :

fe80::%2/64

Dans cette combinaison, il est important de placer la portion indice de zone avant la longueur de préfixe lorsque on envisage d'analyser le format par une fonction de bibliothèque de nom à adresse [11]. C'est-à-dire qu'on peut d'abord séparer l'adresse de l'indice de zone de la longueur de préfixe, et juste passer l'indice à la fonction de bibliothèque.

Le format préféré pour les adresses IPv6 littérales dans les URL est aussi défini dans la [RFC2732]. Lorsque un usager tape le format préféré pour une adresse IPv6 non mondiale dont la zone devrait être explicitement spécifiée, l'usager pourrait utiliser le format pour l'adresse non mondiale combinée avec le format préféré.

Cependant, l'URL tapé est souvent envoyé sur le réseau, et il va être source de confusion si une application ne supprime pas la portion <identifiant_de_zone> avant l'envoi. Noter que les applications ne devraient pas avoir besoin de se soucier de la sorte d'adresses qu'elles utilisent, beaucoup moins que d'analyser ou supprimer la portion <identifiant_de_zone> de l'adresse.

Aussi, le format pour les adresses non mondiales peut entrer en conflit avec la syntaxe d'URI [RFC3986], car cette syntaxe définit le caractère délimiteur ('%') comme étant le caractère d'échappement. Ce conflit pourrait exiger, par exemple, que la partie <identifiant_de_zone> pour la zone 1 avec le délimiteur soit représentée par '%251'. Cela signifie aussi qu'on ne pourrait pas simplement copier un format non échappé à partir d'autres sources comme entrée de l'analyseur d'URI. De plus, si l'analyseur d'URI ne convertit pas le format échappé avant de le passer à une bibliothèque de nom en adresses, la conversion va échouer. Tous ces problèmes vont diminuer l'intérêt de la représentation textuelle décrite dans ce paragraphe.

Donc, le présent document ne spécifie pas comment le format des adresses non mondiales devrait être combiné avec le format préféré pour les adresses littérales IPv6. Dans tous les cas, il est recommandé d'utiliser un FQDN plutôt qu'une adresse IPv6 littérale dans un URL, chaque fois qu'un FQDN est disponible.

12. Considérations pour la sécurité

Une adresse de portée limitée sans un indice de zone a des implications pour la sécurité et ne peut pas être utilisée dans certains contextes de sécurité. Par exemple, une adresse de liaison locale ne peut pas être utilisée dans un sélecteur de trafic d'une association de sécurité établie par l'échange de clés Internet (IKE, *Internet Key Exchange*) lorsque les messages IKE sont portés sur des adresses mondiales. Aussi, une adresse de liaison locale sans indice de zone ne peut pas être utilisée dans des listes de contrôle d'accès.

La section Acheminement du présent document spécifie un ensemble de lignes directrices par lesquelles les routeurs peuvent empêcher des informations spécifiques d'une zone de fuir hors de chaque zone. Si, par exemple, des routeurs frontières de limite de site permettent que des informations d'acheminement du site soient transmises en dehors du site, l'intégrité du site

pourrait être compromise.

Comme l'utilisation de la représentation textuelle des adresses non mondiales est restreinte au sein d'un seul nœud, elle ne crée pas de faiblesse de sécurité provenant de l'extérieur du nœud. Cependant, un nœud malveillant pourrait envoyer un paquet qui contient une adresse textuelle IPv6 non mondiale avec un indice de zone, dans l'intention de tromper le nœud receveur quant à la zone de l'adresse non mondiale. Donc, une mise en œuvre devrait faire attention lorsque elle reçoit des paquets qui contiennent comme données des adresses textuelles non mondiales.

13. Contributeurs

Le présent document est une combinaison de plusieurs efforts séparés. Atsushi Onoe a joué un rôle significatif dans l'un d'eux et a largement contribué au contenu de la Section 11 comme coauteur d'une des propositions séparées.

14. Remerciements

De nombreux membres du groupe de travail IPv6 ont fourni d'utiles commentaires et retours sur le présent document. En particulier, Margaret Wasserman et Bob Hinden ont conduit le groupe de travail à un consensus sur l'adressage IPv6 local. Richard Draves a proposé une règle supplémentaire pour traiter l'en-tête Routing contenant des adresses calibrées. Dave Thaler et Francis Dupont ont fait de précieuses suggestions pour définir la sémantique des indices de zone en termes d'API en rapport. Pekka Savola a révisé très attentivement une version de ce document et fait des commentaires détaillés sur de sérieux problèmes. Steve Bellovin, Ted Hardie, Bert Wijnen, et Timothy Gleeson ont révisé et aidé à améliorer le document durant la préparation de sa publication.

15 Références

15.1 Références normatives

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

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par* 5095*,* 6564 *; D.S)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

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

15.2 Références pour information

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

[RFC2473] A. Conta, S. Deering, "Spécification du tunnelage générique de paquet dans IPv6", décembre 1998. *(P.S.)*

[RFC2732] R. Hinden, B. Carpenter et L. Masinter, "Format pour les adresses littérales IPv6 dans les URL", décembre 1999. *(Obsolète, voir* RFC3986) *(P.S.)*

[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)*

[RFC3879] C. Huitema, B. Carpenter, "Les adresses IPv6 de site local en envoi individuel sont déconseillées", septembre 2004. *(P.S.)*

[RFC3927] S. Cheshire, B. Aboba, E. Guttman, "Configuration dynamique des adresses IPv4 de liaison locale", mai 2005. *(P.S.)*

[RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiant de ressource uniforme (URI) : Syntaxe générique", STD 66, janvier 2005.

[11] Gilligan, R., "Scoped Address Extensions to the IPv6 Basic Socket API", Non publiée, juillet 2002.

Adresse des auteurs

Stephen E. Deering
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Brian Haberman
Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099
USA
téléphone : +1-443-778-1319
mél : brian@innovationslab.net

Brian D. Zill
Microsoft Research
One Microsoft Way
Redmond, WA 98052-6399
USA
téléphone : +1-425-703-3568
mél : bzill@microsoft.com

Tatuya Jinmei
Corporate Research & Development Center, Toshiba Corporation
1 Komukai Toshiba-cho, Saiwai-ku
Kawasaki-shi, Kanagawa 212-8582
Japan
téléphone : +81-44-549-2230
Fax : +81-44-520-1841
mél : jinmei@isl.rdc.toshiba.co.jp

Erik Nordmark
17 Network Circle
Menlo Park, CA 94025
USA
téléphone : +1 650 786 2921
Fax: +1 650 786 5896
mél : Erik.Nordmark@sun.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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