Groupe de travail Réseau
**Request for Comments : 2874**
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Crawford, Fermilab
C. Huitema, Microsoft Corporation
juillet 2000

# Extensions au DNS pour la prise en charge de l'agrégation et le dénumérotage des adresses IPv6



**Résumé**
Le présent document définit des changements au système des noms de domaines pour prendre en charge l'adressage IPv6 dénumérotable et agrégeable. Les changements incluent un nouveau type d'enregistrement de ressource pour mémoriser une adresse IPv6 d'une manière qui active le dénumérotage de réseau et la mise à jour des définitions des types existants d'interrogations qui retournent des adresses Internet au titre du traitement de la section supplémentaire.

Pour les recherches chiffrées sur des adresses IPv6 (souvent appelées des recherches inverses) le présent document définit une nouvelle structure de zone qui permet qu'une zone soit utilisée sans modification pour des copies parallèles d'un espace d'adresses (comme pour un fournisseur ou site multi rattachements) et lors d'événements de dénumérotage de réseau.

## Table des matières

1. Introduction....1
2. Vue d'ensemble....2
  2.1 Recherche de nom pour une adresse....2
  2.2 Mécanismes sous-jacents pour la recherche inverse....2
3. Spécifications....3
  3.1 Type d'enregistrement A6....3
  3.2 Structure de zone pour recherches inverses....4
4. Modifications des types d'interrogation existants....5
5. Exemples d'utilisations....5
  5.1 Chaînes d'enregistrements A6....5
  5.2 Zones de transposition inverse....8
  5.3 Recherches....8
  5.4 Note sur le fonctionnement....9
6 Transition de la RFC 1886 et notes de déploiement....9
  6.1 Transition de AAAA et coexistence avec les enregistrements A....10
  6.2 Transition des étiquettes de quartet aux étiquettes binaires....10
7. Considérations sur la sécurité....10
8. Considérations relatives à l'IANA....11
9. Remerciements....11
10. Références....11
11. Adresse des auteurs....11
12. Déclaration complète de droits de reproduction....12

## 1. Introduction

La maintenance des informations d'adresses dans le DNS est un des divers obstacles qui ont empêché le dénumérotage de site et de fournisseur d'être faisables dans IP version 4. Les arguments sur l'importance d'un dénumérotage de réseau pour la préservation d'un système stable d'acheminement et pour d'autres objets peuvent être lus dans les [RFC1900], [RFC2071], [RFC2101]. Pour prendre en charge la mémorisation des adresses IPv6 sans entraver le dénumérotage, on définit les

extensions suivantes :

- Un nouveau type d'enregistrement de ressource, "A6", est défini pour transposer un nom de domaine en une adresse IPv6, avec la fourniture d'une indication pour les bits de "préfixe" de tête.

- Les interrogations existantes qui effectuent un traitement de la section supplémentaire pour localiser les adresses IPv4 sont redéfinies pour faire le traitement pour les adresses IPv4 et IPv6.

- Un nouveau domaine, IP6.ARPA, est défini pour prendre en charge les recherches sur la base d'une adresse IPv6.

- Une nouvelle méthode de délégation de préfixe est définie, qui s'appuie sur les nouvelles caractéristiques du DNS [RFC2672], [RFC2673].

Les changements sont destinés à être compatibles avec les interfaces de programmation d'application existantes. La prise en charge existante pour les adresses IPv4 est conservée. Les questions de transition relatives à la coexistence des adresses IPv4 et IPv6 dans le DNS sont discutées dans la [RFC1933].

Le présent mémoire propose un remplacement de la spécification de la [RFC1886] et une séparation d'avec les pratiques actuelles de mise en œuvre. Les changements sont destinés à faciliter le dénumérotage de réseau et le multi rattachements. Les domaines qui emploient l'enregistrement A6 pour les adresses IPv6 peuvent insérer les enregistrements AAAA générés automatiquement dans les fichiers de zone pour faciliter la transition. Il est prévu qu'après un délai raisonnable la RFC1886 devienne Historique.

Les trois Sections majeures suivantes de ce document sont une vue d'ensemble des facilités définies ou employées par la présente spécification, la spécification elle-même, et des exemples d'utilisation.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Le mot-clé "SUGGÉRÉ" signifie une force entre PEUT et DEVRAIT : il est estimé que la conformité avec la suggestion a un bénéfice tangible dans la plupart des instances.

## 2. Vue d'ensemble

Cette Section donne une vue d'ensemble des facilités du DNS pour la mémorisation des adresses IPv6 et pour les recherches fondées sur une adresse IPv6, incluant celles définies ici et ailleurs.

### 2.1 Recherche de nom pour une adresse

Les adresses IPv6 sont mémorisées dans un ou plusieurs enregistrements de ressource A6. Un seul enregistrement A6 peut inclure une adresse IPv6 complète, ou une portion contiguë d'une adresse et des informations conduisant à un ou plusieurs préfixes. Les informations de préfixe comportent une longueur de préfixe et un nom DNS qui est lui-même le possesseur d'un ou plusieurs enregistrements A6 qui définissent le ou les préfixes qui sont nécessaires pour former une ou plusieurs adresses IPv6 complètes. Quand la longueur de préfixe est zéro, aucun nom DNS n'est présent et tous les bits de tête de l'adresse sont significatifs. Il peut y avoir plusieurs niveaux d'indication et l'existence de plusieurs enregistrements A6 à tout niveau multiplie le nombre des adresses IPv6 qui sont formées.

Une application qui cherche une adresse IPv6 va généralement causer l'accès du résolveur DNS à plusieurs enregistrements A6, et plusieurs adresses IPv6 peuvent être retournées même si le nom interrogé était le propriétaire d'un seul enregistrement A6. L'authenticité de la ou des adresses retournées ne peut pas être directement vérifiée par la sécurité du DNS [RFC2535]. Les enregistrements A6 qui ont contribué à la ou les adresses peuvent bien sûr être vérifiés si ils sont signés.

Les mises en œuvre doivent se rappeler la nécessité de limiter la quantité de travail qu'un résolveur va effectuer en réponse à la demande d'un client. Ce principe DOIT être étendu aussi à limiter la génération de demandes au DNS en réponse à une demande de recherche de nom en adresse (ou d'adresse en nom).

### 2.2 Mécanismes sous-jacents pour la recherche inverse

Ce paragraphe décrit les nouvelles caractéristiques du DNS qu'exploite le présent document. Elle donne une vue d'ensemble, et non une spécification de ces caractéristiques. Le lecteur se reportera aux documents référencés sur les détails de chacune.

#### 2.2.1 Délégation sur frontières arbitraires

Ce nouveau schéma des recherches inverses s'appuie sur un nouveau type d'étiquette DNS appelée "'étiquette de chaîne binaire" [RFC2673]. Cette étiquette représente sous forme compacte une chaîne arbitraire de bits qui est traitée comme une séquence hiérarchique d'étiquettes de domaine d'un bit. Les enregistrements de ressources peuvent ainsi être mémorisés à des limites de bit arbitraires.

Les exemples de la Section 5 vont employer les représentation textuelles suivantes pour des étiquettes de chaîne binaire, qui est un sous ensemble de la syntaxe définie dans la [RFC2673]. Un indicateur de base "x" pour hexadécimal et une séquence de chiffres hexadécimaux est enclose entre "\[" et "]". Les bits notés par les chiffres représentent une séquence d'étiquettes de domaine d'un bit ordonnées du plus significatif au moins significatif. (C'est l'opposé de l'ordre dans lequel elles apparaîtraient si elles étaient listées un bit à la fois, mais cela paraît être une notation convenable.) La chaîne de chiffres peut être suivie par une barre oblique ("/") et un compte décimal. Si il est omis, le compte implicite est égal à quatre fois le nombre de chiffres hexadécimaux.

Les étiquettes consécutives de chaîne binaire sont équivalentes (jusqu'à la limite imposée par la taille du champ Compte de bits) à une seule étiquette de chaîne binaire contenant tous les bits des étiquettes consécutives dans l'ordre approprié. Par exemple, l'un ou l'autre des noms de domaine suivants pourrait être utilisé dans une interrogation QCLASS=IN, QTYPE=PTR pour trouver le nom du nœud qui a l'adresse IPv6 3ffe:7c0:40:9:a00:20ff:fe81:2b32.

\[x3FFE07C0004000090A0020FFFE812B32/128].IP6.ARPA.

\[x0A0020FFFE812B32/64].\[x0009/16].\[x3FFE07C00040/48].IP6.ARPA.

#### 2.2.2 Zones réutilisables

La délégation d'espace d'adresses du DNS est mise en œuvre non par coupure de zone et enregistrements NS, mais par un nouvel enregistrement analogue à l'enregistrement CNAME, appelé enregistrement de ressource DNAME [RFC2672]. L'enregistrement DNAME fournit une dénomination de remplacement pour une sous arborescence entière de l'espace de noms de domaines, plutôt que pour un seul nœud. Cela cause la substitution de certains suffixes d'un nom interrogé par un nom du RDATA de l'enregistrement DNAME.

Par exemple, un résolveur ou serveur qui assure la récurrence, lors d'une recherche sur un QNAME a.b.c.d.e.f peut rencontrer un enregistrement DNAME

d.e.f. DNAME w.xy.

qui va le faire chercher a.b.c.w.xy.

## 3. Spécifications

### 3.1 Type d'enregistrement A6

Le type d'enregistrement A6 est spécifique de la classe IN (Internet) et a le numéro de type 38 (décimal).

#### 3.1.1 Format

La portion RDATA de l'enregistrement A6 contient deux ou trois champs.

```
+------------------+-----------------+------------------+
|Longueur de préfixe| Suffixe d'adresse|  Nom de préfixe   |
|      (1 octet)    |  (0..16 octets)  |  (0..255 octets)  |
+------------------+-----------------+------------------+
```

- Une longueur de préfixe, codée comme entier non signé de huit bits avec une valeur entre 0 et 128 inclus.

- Un suffixe d'adresse IPv6, codé dans l'ordre des octets du réseau (octet de poids fort en premier). Il DOIT y avoir exactement assez d'octets dans ce champ pour contenir un nombre de bits égal à 128 moins la longueur de préfixe, avec 0 à 7 bits de bourrage en tête pour faire du champ un nombre entier d'octets. Les bits de bourrage, si il en est, DOIVENT être réglés à zéro lors du chargement d'un fichier de zone et ignorés (sauf pour la vérification de SIG [RFC2535]) à réception.

- Le nom du préfixe, codé comme un nom de domaine. Selon les règles de la [RFC1035], ce nom NE DOIT PAS être compressé.

Le composant nom de domaine NE DEVRA PAS être présent si la longueur de préfixe est zéro. Le composant suffixe d'adresse NE DEVRA PAS être présent si la longueur de préfixe est 128.

Il est SUGGÉRÉ qu'un enregistrement A6 destiné à être utilisé comme préfixe pour d'autres enregistrements A6 ait tous les bits non significatifs de queue dans son champ de suffixe d'adresse réglés à zéro.

### 3.1.2 Traitement

Une interrogation avec QTYPE=A6 cause le traitement de la section supplémentaire de type A6 et de type NS pour les noms de préfixes, si il y en a, dans le champ RDATA des enregistrements A6 dans la section réponse. Ce traitement DEVRAIT être appliqué de façon récurrente aux noms de préfixes des enregistrements A6 inclus comme données additionnelles. Quand l'espace dans le paquet de réponse est limité, l'inclusion d'enregistrements A6 supplémentaires a la priorité sur les enregistrements NS.

C'est une erreur pour un enregistrement A6 avec longueur de préfixe L1 > 0 de se référer à un nom de domaine qui possède un enregistrement A6 avec une longueur de préfixe L2 > L1. Si une telle situation est rencontrée par un résolveur, l'enregistrement A6 avec la longueur de préfixe erronée (plus grande) DOIT être ignoré. La robustesse empêche le signalement d'une erreur si les adresses peuvent quand même être formées à partir d'enregistrements A6 valides, mais il est SUGGÉRÉ que les conservateurs de zone vérifient de temps en temps tous les enregistrements A6 que référencent leurs zones.

### 3.1.3 Représentation textuelle

La représentation textuelle de la portion RDATA de l'enregistrement de ressource A6 dans un fichier de zone comprend deux ou trois champs séparés par des espaces :
- Une longueur de préfixe, représentée comme un nombre décimal entre 0 et 128 inclus,
- La représentation textuelle d'une adresse IPv6 comme définie dans la [RFC2373] (bien que certains bits de tête et/ou de queue puissent n'être pas significatifs),
- Un nom de domaine, si la longueur de préfixe n'est pas zéro.

Le nom de domaine DOIT être absent si la longueur de préfixe est zéro. L'adresse IPv6 PEUT être absente si la longueur de préfixe est 128. Un nombre de bits d'adresse de tête égal à la longueur de préfixe DEVRAIT être à zéro, soit implicitement (par la notation ::) soit explicitement, comme spécifié au paragraphe 3.1.1.

### 3.1.4 Procédure de résolution de nom

Pour obtenir la ou les adresses IPv6 qui appartiennent à un certain nom, un client DNS DOIT obtenir une ou plusieurs chaînes complètes d'enregistrements A6, chaque chaîne commençant par un enregistrement possédé par le nom en question et inclure un enregistrement possédé par le nom de préfixe dans cet enregistrement, et ainsi de suite de façon récurrente, se terminant par un enregistrement A6 avec une longueur de préfixe de zéro. Une adresse IPv6 est formée à partir d'une telle chaîne en prenant la valeur de chaque position de bit dans le premier enregistrement A6 dans la chaîne qui couvre de façon valide cette position, comme indiqué par la longueur de préfixe. L'ensemble de toutes les adresses IPv6 pour le nom en question comprend les adresses formées à partir de toutes les chaînes complètes d'enregistrements A6 commençant à ce nom, en éliminant les enregistrements qui ont des longueurs de préfixe invalides comme défini au paragraphe 3.1.2.

Si certaines interrogations A6 échouent et d'autres réussissent, un client pourrait obtenir un ensemble non vide mais incomplet d'adresses IPv6 pour un hôte. Ceci peut être acceptable dans de nombreuses situations. La complétude d'un ensemble d'enregistrements A6 peut toujours être déterminée par inspection.

### 3.2 Structure de zone pour recherches inverses

Très peu des nouvelles données du schéma apparaissent sous IP6.ARPA ; seul le premier niveau de délégation a besoin d'être sous ce domaine. Plus de niveaux de délégation pourraient être placés sous IP6.ARPA si des délégations de niveau supérieur étaient faites via des enregistrements NS au lieu d'enregistrements DNAME, mais cela entraînerait des coûts de facilité de dénumérotage au niveau des TLA [RFC2374]. Donc, on déclare ici que toutes les délégations d'espace d'adresses DEVRAIENT être faites par le mécanisme DNAME plutôt que NS.

De plus, comme l'uniformité du déploiement va simplifier la maintenance des délégations d'adresses, il est SUGGÉRÉ que les informations d'adresse et de préfixe soient mémorisées immédiatement en dessous d'une étiquette DNS "IP6". Dit autrement, la conformité avec cette suggestion signifierait que "IP6" est la première étiquette dans le champ RDATA des enregistrements DNAME qui prennent en charge les recherches inverses IPv6.

Quand des bits "réservé" ou "doit être zéro" sont adjacents à une frontière de délégation, l'entité de niveau supérieur DOIT conserver ces bits dans son propre contrôle et déléguer seulement les bits sur lesquels l'entité de niveau inférieur a autorité.

Pour trouver le nom d'un nœud étant donnée son adresse IPv6, un client DNS DOIT effectuer une interrogation avec QCLASS=IN, QTYPE=PTR sur le nom formé à partir de l'adresse de 128 bits comme une ou plusieurs étiquettes de chaîne binaire [RFC2673], suivies par les deux étiquettes standard "IP6.ARPA". Si un service récurrent n'a pas été obtenu d'un serveur et si l'enregistrement PTR désiré n'a pas été retourné, le résolveur DOIT traiter les enregistrements DNAME retournés comme spécifié dans la [RFC2672], et les enregistrements NS comme spécifié dans la [RFC1034], et itérer.

## 4. Modifications des types d'interrogation existants

Tous les types d'interrogation existants qui effectuent le traitement de la section supplémentaire de type A, c'est-à-dire les types d'interrogation Serveur de noms (NS, *Name Server*), Échange de messagerie (MX, *Mail eXchange*), et Boîte aux lettres (MB, *MailBox*) et les types expérimentaux Base de données AFS (AFSDB, *AFS Data Base*) et Chemin traversé (RT, *Route Through*) doivent être redéfinis pour effectuer le traitement de la section supplémentaire de type A, A6 et AAAA, le type A ayant la priorité supérieure pour l'inclusion et le type AAAA l'inférieure. Cette redéfinition signifie qu'un serveur de noms peut ajouter toutes les informations pertinentes d'adresse IPv4 et IPv6 disponibles en local à la section supplémentaire d'une réponse quand il traite une des interrogations ci-dessus. L'inclusion récurrente des enregistrements A6 référencés par les enregistrements A6 déjà inclus dans la section supplémentaire est FACULTATIVE.

## 5. Exemples d'utilisations

La présente section donne des exemples d'utilisation des mécanismes définis à la section précédente. Toutes les adresses et tous les domaines mentionnés ici sont fictifs et seulement destinés à des fins d'illustration. Les exemples de délégations ne sont sur des limites de 4 bits que pour la lisibilité ; la présente spécification est indifférente à l'alignement sur l'octet.

L'utilisation du format d'adresse agrégeable IPv6 de la [RFC2374] est supposé dans les exemples.

### 5.1 Chaînes d'enregistrements A6

Prenons l'exemple d'un site X qui est en multi rattachement sur deux fournisseurs "intermédiaires" A et B. Le fournisseur A est lui-même multi rattachements sur deux fournisseurs de "transit", C et D. Le fournisseur B obtient son service de transit d'un seul fournisseur, E. Pour simplifier supposons que C, D et E appartiennent tous au même agrégat de niveau supérieur (TLA, T*op-Level Aggregate*) avec l'identifiant (incluant le préfixe de format) "2345", et l'autorité de TLA à ALPHA-TLA.ORG alloue à C, D et E les préfixes d'agrégat de prochain niveau (NLA, *Next Level Aggregate*) respectifs de 2345:00C0::/28, 2345:00D0::/28 et 2345:000E::/32.

C alloue le préfixe NLA 2345:00C1:CA00::/40 à A, D alloue le préfixe 2345:00D2:DA00::/40 à A et E alloue 2345:000E:EB00::/40 à B.

A alloue à X l'identification d'abonné "11" et B alloue l'identification d'abonné "22". Par suite, le site X hérite de trois préfixes d'adresse :
o 2345:00C1:CA11::/48 de A, pour les chemins à travers C.
o 2345:00D2:DA11::/48 de A, pour les chemins à travers D.

o 2345:000E:EB22::/48 de B, pour les chemins à travers E.

Supposons que N soit un nœud dans le site X, à qui est alloué le numéro de sous réseau 1 dans ce site, et qu'il utilise l'identifiant d'interface "1234:5678:9ABC:DEF0". Dans notre configuration, ce nœud va avoir trois adresses :
o 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
o 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
o 2345:000E:EB22:0001:1234:5678:9ABC:DEF0

### 5.1.1 Données d'autorité

On va supposer que le site X est représenté dans le DNS par le nom de domaine X.EXAMPLE, tandis que A, B, C, D et E sont représentés par A.NET, B.NET, C.NET, D.NET et E.NET. Dans chacun de ces domaines, on suppose un sous domaine "IP6" qui va détenir les préfixes correspondants. Le nœud N est identifié par le nom de domaine N.X.EXAMPLE. Les enregistrements suivants vont alors apparaître dans le DNS de X.

```
$ORIGIN X.EXAMPLE.
N           A6 64 ::1234:5678:9ABC:DEF0 SUBNET-1.IP6
SUBNET-1.IP6 A6 48 0:0:0:1::  IP6
IP6         A6 48 0::0      SUBSCRIBER-X.IP6.A.NET.
IP6         A6 48 0::0      SUBSCRIBER-X.IP6.B.NET.
```

Et ailleurs, ils vont apparaître

```
SUBSCRIBER-X.IP6.A.NET. A6 40 0:0:0011:: A.NET.IP6.C.NET.
SUBSCRIBER-X.IP6.A.NET. A6 40 0:0:0011:: A.NET.IP6.D.NET.

SUBSCRIBER-X.IP6.B.NET. A6 40 0:0:0022:: B-NET.IP6.E.NET.

A.NET.IP6.C.NET. A6 28 0:0001:CA00:: C.NET.ALPHA-TLA.ORG.

A.NET.IP6.D.NET. A6 28 0:0002:DA00:: D.NET.ALPHA-TLA.ORG.

B-NET.IP6.E.NET. A6 32 0:0:EB00::    E.NET.ALPHA-TLA.ORG.

C.NET.ALPHA-TLA.ORG. A6 0 2345:00C0::
D.NET.ALPHA-TLA.ORG. A6 0 2345:00D0::
E.NET.ALPHA-TLA.ORG. A6 0 2345:000E::
```

### 5.1.2 Glu

Quand, comme c'est courant, certains ou tous les serveurs DNS pour X.EXAMPLE sont dans la zone X.EXAMPLE elle-même, la zone de niveau supérieur EXAMPLE doit porter assez d'informations "glu" pour permettre aux clients DNS d'accéder à ces serveurs de noms. C'est vrai dans IPv6 tout comme dans IPv4. Cependant, l'enregistrement A6 permet des choix à l'administrateur DNS. La glu pourrait être :
o un ensemble minimal d'enregistrements A6 dupliqués de la zone X.EXAMPLE,
o un ensemble (éventuellement plus petit) d'enregistrements qui percute la structure de cet ensemble minimal,
o ou un ensemble d'enregistrements A6 avec la longueur de préfixe zéro, donnant les adresses mondiales entières des serveurs.

Le compromis est entre la facilité de maintenance et la robustesse. Le meilleur et le pire des deux peut être d'avoir mis en œuvre ensemble la première ou la seconde option avec la troisième. Pour illustrer les options de glu, supposons que X.EXAMPLE est desservi par deux serveurs de noms NS1.X.EXAMPLE et NS2.X.EXAMPLE, ayant les identifiants d'interface ::1:11:111:1111 et ::2:22:222:2222 respectivement sur les sous réseaux 1 et 2. La zone de niveau supérieur EXAMPLE va alors inclure un (ou plus) des ensembles d'enregistrements A6 suivants comme glu :

```
$ORIGIN EXAMPLE.          ; première option
X           NS NS1.X
            NS NS2.X
NS1.X       A6 64 ::1:11:111:1111 SUBNET-1.IP6.X
NS2.X       A6 64 ::2:22:222:2222 SUBNET-2.IP6.X
```

```
SUBNET-1.IP6.X  A6 48 0:0:0:1::      IP6.X
SUBNET-2.IP6.X  A6 48 0:0:0:2::      IP6.X
IP6.X           A6 48 0::0           SUBSCRIBER-X.IP6.A.NET.
IP6.X           A6 48 0::0           SUBSCRIBER-X.IP6.B.NET.

$ORIGIN EXAMPLE.            ; seconde option
X             NS NS1.X
              NS NS2.X
NS1.X           A6 48 ::1:1:11:111:1111 SUBSCRIBER-X.IP6.A.NET.
              A6 48 ::1:1:11:111:1111 SUBSCRIBER-X.IP6.B.NET.
NS2.X           A6 48 ::2:2:22:222:2222 SUBSCRIBER-X.IP6.A.NET.
              A6 48 ::2:2:22:222:2222 SUBSCRIBER-X.IP6.B.NET.

$ORIGIN EXAMPLE.            ; troisième option
X             NS NS1.X
              NS NS2.X
NS1.X           A6 0  2345:00C1:CA11:1:1:11:111:1111
              A6 0  2345:00D2:DA11:1:1:11:111:1111
              A6 0  2345:000E:EB22:1:1:11:111:1111
NS2.X           A6 0  2345:00C1:CA11:2:2:22:222:2222
              A6 0  2345:00D2:DA11:2:2:22:222:2222
              A6 0  2345:000E:EB22:2:2:22:222:2222
```

La première et la seconde options de glu sont robustes contre le dénumérotage des préfixes de X.EXAMPLE par les fournisseurs A.NET et B.NET, mais vont échouer si le propre DNS de ces fournisseurs est injoignable. Les enregistrements de glu de la troisième option sont robustes contre les défaillances du DNS ailleurs que dans les zones EXAMPLE et X.EXAMPLE elles-mêmes, mais doivent être mis à jour quand l'espace d'adresses de X est dénuméroté.

Si la zone EXAMPLE inclut des enregistrements glu redondants, par exemple l'union des enregistrements A6 de la première et de la troisième options, alors dans des circonstances normales les adresses IPv6 dupliquées vont être déduites par les clients DNS. Mais si le fournisseur DNS échoue, les adresses vont encore être obtenues d'enregistrements de longueur de préfixe zéro, tandis que si la zone EXAMPLE reste derrière une dénumérotation de X.EXAMPLE, la moitié des adresses obtenues par les clients DNS va encore être à jour.

Les enregistrements de glu de longueur de préfixe zéro peuvent bien sûr être générés automatiquement et/ou vérifiés en pratique.

### 5.1.3 Variantes

Plusieurs hypothèses plus ou moins arbitraires sont reflétées dans la structure ci-dessus. Tous les choix suivants auraient été différents, selon la notion de ce qui convient à quelqu'un ou qu'il existe un accord entre deux parties.

D'abord, que le site X a choisi de mettre les informations de sous réseau dans un enregistrement A6 séparé plutôt que de l'incorporer dans les enregistrements A6 de chaque nœud.

Ensuite, que le site X est appelé "SUBSCRIBER-X" par les deux fournisseurs A et B.

Troisièmement, que le site X choisit d'envoyer ses informations de fournisseur à travers les enregistrements A6 à IP6.X.EXAMPLE ne contenant pas de bits significatifs. Une autre solution aurait été de dupliquer chaque enregistrement de sous réseau pour chaque fournisseur.

Quatrièmement, B et E ont utilisé entre eux-mêmes une convention de dénomination de préfixe légèrement différente de ce qu'ont fait A, C et D. Chaque paire hiérarchique d'entités réseau doit arranger entre elles ces conventions de désignation.

Cinquièmement, que la chaîne de référence de préfixes vers le haut a pour sommet ALPHA-TLA.ORG. Il y aurait pu y avoir un autre niveau qui alloue les valeurs de TLA et garde les enregistrements A6 contenant ces bits.

Finalement, la structure ci-dessus reflète l'hypothèse que les champs d'adresse alloués par une certaine entité sont seulement enregistrés dans des enregistrements A6 détenus par cette entité. Ces bits pourraient à la place être entrés dans des enregistrements A6 dans la zone de l'entité de niveau inférieur, donc :

```
IP6.X.EXAMPLE. A6 40 0:0:11::   IP6.A.NET.
IP6.X.EXAMPLE. A6 40 0:0:22::   IP6.B.NET.

IP6.A.NET.     A6 28 0:1:CA00:: IP6.C.NET.
```

et ainsi de suite.

Ou les entités de niveau supérieur pourraient détenir les deux sortes d'enregistrements A6 (avec des noms différents de possesseur DNS) et permettre aux entités de niveau inférieur de choisir l'un ou l'autre mode de chaînage A6. Mais le principe général d'éviter la duplication de données suggère que l'endroit approprié pour mémoriser les valeurs allouées est avec l'entité qui les a allouées.

Il est possible, mais pas nécessairement recommandé, qu'un teneur de zone entreprenne la prise en charge du dénumérotage permis par le chaînage des enregistrements A6 et enregistre les adresses IPv6 entières au sein d'un fichier de zone.

### 5.2 Zones de transposition inverse

Supposons que les allocations d'espace d'adresses dans les TLA avec le préfixe de format binaire (001) et que les identifiants 0345, 0678 et 09AB soient tenus dans des zones appelées ALPHA-TLA.ORG, BRAVO-TLA.ORG et CHARLIE-TLA.XY, alors la zone IP6.ARPA inclurait

```
$ORIGIN IP6.ARPA.
\[x234500/24]   DNAME   IP6.ALPHA-TLA.ORG.
\[x267800/24]   DNAME   IP6.BRAVO-TLA.ORG.
\[x29AB00/24]   DNAME   IP6.CHARLIE-TLA.XY.
```

Huit bits de zéros en queue ont été inclus dans chaque identifiant de TLA pour refléter les huit bits réservés dans le format actuel d'adresses d'envoi individuel mondiales agrégeables [RFC2374].

#### 5.2.1 Niveau TLA

Les allocations de ALPHA-TLA aux fournisseurs de réseau C, D et E sont reflétées dans les données inverses comme suit .

```
\[xC/4].IP6.ALPHA-TLA.ORG.   DNAME  IP6.C.NET.
\[xD/4].IP6.ALPHA-TLA.ORG.   DNAME  IP6.D.NET.
\[x0E/8].IP6.ALPHA-TLA.ORG.  DNAME  IP6.E.NET.
```

#### 5.2.2 Niveau FAI

Les fournisseurs A à E portent les informations de délégation suivantes dans leurs fichiers de zone.

```
\[x1CA/12].IP6.C.NET.  DNAME  IP6.A.NET.
\[x2DA/12].IP6.D.NET.  DNAME  IP6.A.NET.
\[xEB/8].IP6.E.NET.    DNAME  IP6.B.NET.
\[x11/8].IP6.A.NET.    DNAME  IP6.X.EXAMPLE.
\[x22/8].IP6.B.NET.    DNAME  IP6.X.EXAMPLE.
```

Noter que certains noms de domaine apparaissent dans le RDATA de plus d'un enregistrement DNAME. Dans ce cas, une zone est utilisée pour transposer plusieurs préfixes.

#### 5.2.3 Niveau Site

Considérons le consommateur X.EXAMPLE qui utilisé IP6.X.EXAMPLE pour les traductions d'adresse en nom. Ce domaine est maintenant référencé par deux enregistrements DNAME différents détenus par deux fournisseurs différents.

```
$ORIGIN IP6.X.EXAMPLE.
\[x0001/16]                 DNAME   SUBNET-1
\[x123456789ABCDEF0].SUBNET-1  PTR     N.X.EXAMPLE.
et so on.
```

SUBNET-1 n'a pas besoin d'avoir été nommé dans un enregistrement DNAME ; les bits de sous réseau pourraient avoir été

joints avec l'identifiant d'interface. Mais si les sous réseaux sont traités de la même façon dans les enregistrements A6 et dans la zone inverse, il va toujours être possible de garder les données de définition vers l'avant et inverses pour chaque préfixe dans une zone.

### 5.3 Recherches

Un résolveur DNS qui cherche un d'hôte pour l'adresse 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0 va acquérir certains des enregistrements DNAME montrés ci-dessus et va former de nouvelles interrogations. En supposant qu'il commence le processus en sachant les serveurs pour IP6.ARPA, mais qu'aucun des serveurs qu'il consulte ne fournisse la récurrence et qu'aucun n'ait d'autres informations supplémentaires utiles en antémémoire, la séquence des noms interrogés et des réponses va être (toutes avec QCLASS=IN, QTYPE=PTR) :

À un serveur pour IP6.ARPA :
  QNAME=\[x234500C1CA110001123456789ABCDEF0/128].IP6.ARPA.

Réponse :
    \[x234500/24].IP6.ARPA. DNAME IP6.ALPHA-TLA.ORG.

À un serveur pour IP6.ALPHA-TLA.ORG :
  QNAME=\[xC1CA110001123456789ABCDEF0/104].IP6.ALPHA-TLA.ORG.

Réponse :
    \[xC/4].IP6.ALPHA-TLA.ORG. DNAME IP6.C.NET.

À un serveur pour IP6.C.NET. :
  QNAME=\[x1CA110001123456789ABCDEF0/100].IP6.C.NET.

Réponse :
    \[x1CA/12].IP6.C.NET. DNAME IP6.A.NET.

À un serveur pour IP6.A.NET. :
  QNAME=\[x110001123456789ABCDEF0/88].IP6.A.NET.

Réponse :
    \[x11/8].IP6.A.NET. DNAME IP6.X.EXAMPLE.

À un serveur pour IP6.X.EXAMPLE. :
  QNAME=\[x0001123456789ABCDEF0/80].IP6.X.EXAMPLE.

Réponse :
    \[x0001/16].IP6.X.EXAMPLE. DNAME SUBNET-1.IP6.X.EXAMPLE.
    \[x123456789ABCDEF0/64].SUBNET-1.X.EXAMPLE. PTR N.X.EXAMPLE.

Tous les enregistrements DNAME (et NS) acquis le long du chemin peuvent être mis en antémémoire pour traiter la résolution des adresses topologiquement près de cette adresse. Et si une autre adresse mondiale de N.X.EXAMPLE est résolue dans le TTL de l'enregistrement PTR final, cet enregistrement n'aurait pas à être cherché à nouveau.

### 5.4 Note sur le fonctionnement

Dans les illustrations du paragraphe 5.1, les entités hiérarchiquement adjacentes, comme un fournisseur de réseau et un consommateur, doivent s'accorder sur un nom DNS qui va posséder la définition du ou des préfixes délégués. Une convention simple serait d'utiliser une étiquette de chaîne binaire représentant exactement les bits qui sont alloués à l'entité de niveau inférieur par celle de niveau supérieur. Par exemple, "SUBSCRIBER-X" pourrait être remplacé par "\[x11/8]". Cela placerait le ou les enregistrements A6 qui définissent le préfixe délégué exactement au même point dans l'arborescence DNS que l'enregistrement DNAME associé à cette délégation. Le coût de cette simplification est que la zone de niveau inférieur doit mettre à jour ses enregistrements A6 qui pointent vers le haut quand elle est dénumérotée. Ce coût peut être trouvé assez acceptable en pratique.

# 6 Transition de la RFC 1886 et notes de déploiement

Quand des préfixes ont été "délégués vers le haut" avec les enregistrements A6, le nombre d'enregistrements de ressource DNS requis pour établir une seule adresse IPv6 augmente d'un facteur non trivial. Ces enregistrements vont normalement, mais pas nécessairement, venir de zones DNS différentes (qui peuvent subir des défaillances indépendantes pour les raisons habituelles). Quand on obtient plusieurs adresses IPv6 ensemble, cette augmentation du compte de RR va être proportionnellement moindre -- et la taille totale d'une réponse DNS pourrait même diminuer -- si les adresses sont dans une grappe topologique. Mais les enregistrements pourraient encore facilement excéder l'espace disponible dans une réponse UDP qui retourne un gros ensemble de RR [RFC2181] à une interrogation MX, NS, ou SRV, par exemple. Les possibilités d'une dégradation globale des performances et de la fiabilité des recherches dans le DNS sont nombreuses, et augmentent avec le nombre de délégations de préfixes impliquées, en particulier quand ces délégations pointent sur des enregistrements dans d'autres zones.

La sécurité du DNS [RFC2535] vise la véracité des données en antémémoire, qui est un problème intrinsèque du DNS, mais le coût de son application à une adresse IPv6 est multiplié par un facteur qui peut être supérieur au nombre de délégations de préfixes impliquées si différentes chaînes de signatures doivent être vérifiées pour les différents enregistrements A6. Si un serveur centralisé de mise en antémémoire de confiance (comme dans la [RFC2845], par exemple) est utilisé, ce coût pourrait être amorti à des niveaux acceptables. Un nouveau phénomène est la possibilité que les adresses IPv6 puissent être formées à partir des enregistrements A6 d'une combinaison de zones sûres et non sûres.

Jusqu'à ce que plus d'expérience de déploiement soit obtenue sur l'enregistrement A6, il est recommandé que les délégations de préfixes soient limitées à un ou deux niveaux. Un mécanisme raisonnable d'adaptation serait de commencer sans délégation de préfixes (tous les enregistrements A6 ayant une longueur de préfixe de 0) et ensuite de passer à l'utilisation d'un seul niveau de délégation au sein d'une seule zone. (Si le TTL des enregistrements A6 de "préfixe" est gardé à une durée appropriée, la capacité d'un dénumérotage rapide n'est pas perdue.) Une délégation d'une souplesse plus agressive pourrait être introduite pour un sous ensemble d'hôtes à des fins d'expérimentation.

## 6.1 Transition de AAAA et coexistence avec les enregistrements A

Les administrateurs de zones qui contiennent des enregistrements A6 peuvent facilement s'accommoder des résolveurs déployés qui comprennent les enregistrements AAAA mais pas les enregistrements A6. Ces administrateurs peuvent faire une génération automatique des enregistrements AAAA pour tous les noms d'une zone qui possèdent des enregistrements A6 par un processus qui imite la résolution d'un nom d'hôte en une adresse IPv6 (voir au paragraphe 3.1.4). Il faut faire attention au TTL alloué à un enregistrement AAAA généré, qui DOIT être pas plus que le minimum des TTL des enregistrements A6 qui ont été utilisés pour former l'adresse IPv6 dans cet enregistrement. Pour une robustesse complète, les changements (du TTL ou RDATA) de ces enregistrements A6 qui étaient dans des zones différentes devraient être surveillés même quand il n'y a pas de changement à la zone pour laquelle des enregistrements AAAA sont générés. Si la zone est sûre [RFC2535], les enregistrements AAAA générés DOIVENT être signés ainsi que le reste des données de zone.

Une heuristique spécifique de zone PEUT être utilisée pour éviter de générer des enregistrements AAAA pour des enregistrements A6 qui enregistrent des préfixes, bien que de tels enregistrements superflus soient relativement peu nombreux et sans danger. Des exemples de telles heuristiques incluent d'omettre les enregistrements A6 avec une longueur de préfixe inférieure à la plus grande valeur trouvée dans le fichier de zone, ou les enregistrements qui ont un champ de suffixe d'adresse avec un certain nombre de bits à zéro en queue.

Du côté client, quand on cherche une adresse IPv6, l'ordre des interrogations A6 et AAAA PEUT être configurable pour être un de : A6, puis AAAA ; AAAA, puis A6 ; A6 seulement; ou les deux en parallèle. L'ordre par défaut (ou seulement l'ordre, si il n'est pas configurable) DOIT être d'essayer A6 d'abord, puis AAAA. Si et quand le AAAA deviendra déconseillé, un nouveau document changera l'ordre par défaut.

Les lignes directrices et les options pour la préséance entre adresses IPv4 et IPv6 sont spécifiées dans la [RFC1933]. Toutes les mentions d'enregistrements AAAA dans le présent document sont donc à interpréter comme signifiant des enregistrements A6 et/ou AAAA dans l'ordre spécifié au paragraphe précédent.

## 6.2 Transition des étiquettes de quartet aux étiquettes binaires

Les mises en œuvre qui se conforment à la [RFC1886] effectuent les recherches inverses comme suit :

Une adresse IPv6 est représentée comme un nom dans le domaine IP6.INT par une séquence de quartets séparés par des

points avec le suffixe ".IP6.INT". La séquence de quartets est codée en ordre inverse, c'est-à-dire que le quartet de moindre poids est codé en premier, suivi par le prochain quartet de moindre poids et ainsi de suite. Chaque quartet est représenté par un chiffre hexadécimal. Par exemple, un nom pour l'adresse 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0 de l'exemple du paragraphe 5.3 va être vu comme le nom DNS "0.f.e.d.c.b.a.9.- 8.7.6.5.4.3.2.1.1.0.0.0.1.1.a.c.1.c.0.0.5.4.3.2.ip6.int."

Les mises en œuvre qui se conforment à la présente spécification vont effectuer une recherche d'étiquette binaire dans IP6.ARPA comme spécifié au paragraphe 3.2. Il est RECOMMANDÉ que pour une période de transition, les mises en œuvre cherchent d'abord l'étiquette binaire dans IP6.ARPA et si cela échoue d'essayer de chercher l'étiquette "quartet" dans in IP6.INT.

## 7. Considérations sur la sécurité

L'autorité signataire [RFC2535] pour les enregistrements A6 qui détermine une adresse IPv6 est distribuée antre plusieurs entités, reflétant le chemin de délégation de l'espace d'adresses qu'occupe cette adresse. La sécurité du DNS est pleinement applicable aux étiquettes de chaîne binaire et enregistrements DNAME. Et tout comme dans IPv4, la vérification des transpositions de nom en adresse est logiquement indépendante de la vérification des transpositions d'adresse en nom.

Avec ou sans DNSSEC, le scénario d'adresse incomplète mais non vide du paragraphe 3.1.4 pourrait être causé par une interférence sélective avec les recherches dans le DNS. Si dans certaines situations ceci serait plus dommageable qu'un échec complet du DNS, cela pourrait être atténué du côté client en refusant d'agir sur un ensemble incomplet, ou du côté serveur en faisant la liste de toutes les adresses dans les enregistrements A6 qui ont une longueur de préfixe de 0.

## 8. Considérations relatives à l'IANA

Une valeur de type de 38 a été allouée à l'enregistrement de ressource A6.

## 9. Remerciements

Les auteurs tiennent à remercier les personnes suivantes des discussions profitables et de leurs relectures : Mark Andrews, Rob Austein, Jim Bound, Randy Bush, Brian Carpenter, David Conrad, Steve Deering, Francis Dupont, Robert Elz, Bob Fink, Olafur Gudmundsson, Bob Halley, Bob Hinden, Edward Lewis, Bill Manning, Keith Moore, Thomas Narten, Erik Nordmark, Mike O'Dell, Michael Patton et Ken Powell.

## 10. Références

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC1886] S. Thomson, C. Huitema, "Extensions au DNS pour la prise en charge de IP version 6", décembre 1995. (*Obsolète, voir* RFC3596) (*MàJ par* RFC2874, RFC3152) *(P.S.)*

[RFC1900] B. Carpenter, Y. Rekhter, "Un dénumérotage représente du travail", février 1996. *(Information)*

[RFC1933] R. Gilligan, E. Nordmark, "Mécanismes de transition pour hôtes et routeurs IPv6", avril 1996. (*Obs., voir* RFC2893)*(P.S.)*

[RFC2071] P. Ferguson, H. Berkowitz, "Généralités sur la renumérotation du réseau : pourquoi on la veut et ce qu'elle est", janvier 1997. *(Information)*

[RFC2101] B. Carpenter, J. Crowcroft, Y. Rekhter, "Comportement actuel des adresses IPv4", février 1997. *(Information)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(P.S., MàJ par* RFC4035, RFC2535, RFC4343, RFC4033, RFC4034, RFC5452, RFC8767)

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

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

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC2672] M. Crawford, "Renumérotage d'un sous-ensemble non terminal du DNS", août 1999. (*MàJ par* RFC4592, RFC6604)) (*Remplacée par la* RFC6672) *(P.S.)*

[RFC2673] M. Crawford, "Étiquettes binaires dans le système des noms de domaine", août 1999. *(Remplacée par* RFC6891)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

## 11. Adresse des auteurs

Matt Crawford
Fermilab
MS 368
PO Box 500
Batavia, IL 60510
USA
téléphone : +1 630 840-3461
mél : crawdad@fnal.gov

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

## 12. Déclaration complète de droits de reproduction

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