Groupe de travail Réseau
Request for Comments : 3364
RFC mises à jour : 2673, 2874
Catégorie : Information

R. Austein
Bourgeois Dilettant
août 2002
Traduction Claude Brière de L'Isle

Compromis pour la prise en charge de IPv6 par le système des noms de domaine (DNS)

Résumé
L'IETF a reçu deux propositions différentes sur la façon dont le DNS prend en charge IPv6, et n'a jusqu'à présent pas réussi à trouver un clair consensus sur l'approche la meilleure. La présente note tente d'examiner le pour et le contre de chaque approche, dans l'espoir de préciser le débat afin qu'on puisse le conclure et passer à autre chose.

Introduction

La [RFC1886] spécifiait des mécanismes directs pour la prise en charge des adresses IPv6 dans le DNS. Ces mécanismes ressemblent beaucoup aux mécanismes utilisés pour la prise en charge de IPv4, avec une amélioration mineure au mécanisme de transposition inverse fondée sur l'expérience de CIDR. La RFC1886 figure actuellement sur la liste des propositions de norme.

La [RFC2874] spécifiait des mécanismes améliorés pour la prise en charge des adresses IPv6 dans le DNS. Ces mécanismes apportent de nouvelles caractéristiques qui rendent possible qu'une adresse IPv6 mémorisée dans le DNS soit cassée en plusieurs enregistrements de ressource du DNS sous des formes qui peuvent refléter la topologie du réseau sous-jacente à l'adresse, rendant ainsi possible que les données mémorisées dans le DNS reflètent certaines formes de changements de la topologie du réseau ou des architectures d'acheminement qui soient impossibles ou plus difficiles à représenter sans ces mécanismes. La RFC2874 est aussi actuellement sur la liste des propositions de norme.

Ces deux propositions de norme ont été le résultat du groupe de travail IPNG. Toutes deux ont été mises en œuvre bien que la mise en œuvre de la [RFC1886] soit plus répandue, à la fois parce qu'elle a été spécifiée avant et parce que sa mise en œuvre est plus simple.

Il ne fait pas de doute que les mécanismes proposés dans la [RFC2874] sont plus généraux que ceux qui sont proposés dans la [RFC1886], et que ces mécanismes améliorés seraient précieux si l'évolution de IPv6 va dans certaines directions. La question est de savoir si on a réellement besoin de mécanismes plus généraux, quels nouveaux problèmes d'utilisation pourraient survenir avec les mécanismes améliorés, et quel effet tout cela va avoir sur le déploiement de IPv6.

La seule chose sur laquelle il semble y avoir un large accord est que l'on devrait prendre une décision au plus tôt.

Principaux avantages de A6

Bien que le RR A6 proposé dans la [RFC2874] soit très général et fournisse un super ensemble des fonctionnalités fournies par le RR AAAA de la [RFC1886], de nombreuses caractéristiques de A6 peuvent aussi être mises en œuvre avec les RR AAAA via un prétraitement durant la génération du fichier de zone.

Il y a un domaine spécifique où les RR A6 fournissent quelque chose qui ne peut pas être fourni avec les RR AAAA: Les RR A6 peuvent représenter des adresses dans lesquelles une portion de préfixe de l'adresse peut changer sans aucune action (ou même peut-être sans qu'elles le sachent) de la part des parties qui contrôlent la zone DNS qui contient la portion terminale (les bits de moindre poids) de l'adresse. Cela inclut aussi bien ce qu'on appelle les scénarios de "dénumérotage rapide" (où le préfixe de tout un réseau peut être changé très rapidement) et les architectures d'acheminement telles que l'ancienne proposition "GSE" [GSE] (où la portion "acheminement" d'une adresse peut être soumise à changer sans

avertissement). Les RR A6 ne suppriment pas complètement le besoin de mise à jour des zones d'extrémité durant tous les événements de dénumérotage (par exemple, changer de FAI va normalement exiger un changement sur le pointeur de délégation vers l'amont) mais un usage prudent des RR A6 pourrait garder au minimum le nombre de RR qui ont besoin d'être changés durant un tel événement.

Noter que la construction des RR AAAA via un prétraitement durant la génération du fichier de zone exige exactement le type d'informations que mémorisent les RR A6 dans le DNS. Cela amène la question de savoir où le pré-processeur hypothétique obtient ces informations si il ne les obtient pas du DNS.

Noter aussi que le RR A6, lorsque il se restreint à sa forme de préfixe de longueur zéro ("A6 0") est sémantiquement équivalent à un RR AAAA (avec un octet "perdu" dans la représentation pour la transmission sur le réseau) de sorte que tout ce qui peut être fait avec un RR AAAA peut aussi être fait avec un RR A6.

Principaux avantages du passage sur AAAA

Le RR AAAA proposé dans la [RFC1886], tout en ne fournissant qu'un sous-ensemble de la fonctionnalité fournie par le RR A6 proposé dans la [RFC2874], a deux points principaux qui plaident en faveur de sa recommandation :

- Les RR AAAA sont essentiellement identiques (en dehors de leur longueur) aux RR A de IPv4, de sorte que nous avons plus de 15 années d'expérience pour nous aider à prédire les schémas d'utilisation, les scénarios d'échec, etc., associés aux RR AAAA.

- Les RR AAAA sont "optimisés pour la lecture", en ce sens que, en mémorisant une adresse complète plutôt qu'en faisant que le résolveur aille chercher l'adresse par morceaux, il minimise les efforts impliqués pour aller chercher les adresses dans le DNS (au dépens d'un accroissement des efforts impliqués par l'injection de nouvelles données dans le DNS).

Arguments moins convaincants en faveur de A6

Comme le RR A6 permet à un administrateur de zone d'écrire les fichiers de zone dont la description des adresses se transpose en la topologie sous-jacente du réseau, les RR A6 peuvent être construits comme un "meilleur" moyen de représenter les adresses que AAAA. Cela peut bien être une capacité utile, mais par lui-même c'est plus un argument en faveur de meilleurs outils pour que les administrateurs de zone les utilisent lors de la construction des fichiers de zone qu'une justification pour changer le protocole de résolution utilisé sur le réseau.

Arguments moins convaincants en faveur de AAAA

Une partie de la pression pour passer à AAAA plutôt qu'à A6 semble se fonder sur le plus large déploiement de AAAA. Comme il est possible de construire des outils de transition (voir la discussion du AAAA de synthèse, plus loin dans cette note) il ne semble pas que ce soit un argument convaincant si A6 fournit les caractéristiques dont on a réellement besoin.

Un autre argument en faveur de la supériorité des RR AAAA sur les RR A6 paraît être que les capacités améliorées du RR A6 augmentent le nombre de façons par lesquelles les administrateurs de zone peuvent construire des configurations qui ne fonctionnent pas. Alors que les questions de fonctionnement sont certainement importantes, ceci est plus l'argument que nous avons besoin de meilleurs outils pour les administrateurs de zone que ce n'est une justification pour se détourner de A6 si A6 apporte des caractéristiques dont nous avons réellement besoin.

Problèmes potentiels avec A6

Les capacité améliorées du RR A6, bien qu'intéressantes, ne sont pas par elles-mêmes une justification pour choisir A6 si on n'a pas réellement besoin de ces capacités. Le RR A6 est "optimisé pour l'écriture", en ce sens que, en rendant possible la mémorisation d'adresses IPv6 fragmentées dans le DNS, il rend possible la réduction des efforts nécessaires pour injecter de nouvelles données dans le DNS (au dépens d'un accroissement de l'effort impliqué par la recherche des données dans le DNS). Cela peut être justifié si on s'attend à ce que l'effort impliqué par la maintenance d'entrées du DNS du style AAAA soit prohibitif, mais en général, on s'attend à ce que les données du DNS soient lues plus fréquemment qu'elles ne sont écrites, de sorte qu'on doit évaluer très soigneusement ce compromis particulier.

Il y a aussi plusieurs problèmes potentiels avec les RR A6 qui découlent directement des caractéristiques qui les rendent différents des RR AAAA : la capacité de construire des adresses au moyen d'un enchaînement.

Résoudre une chaîne de RR A6 implique de résoudre une série de ce qui sont presque des interrogations indépendantes, mais pas tout à fait. Chacune de ces sous interrogation prend une quantité de temps différente de zéro, sauf si la réponse se trouve être déjà dans l'antémémoire locale du résolveur. En supposant comme base de calcul que la résolution d'un RR AAAA prend un temps T, on peut supposer que, en moyenne, il faudra quelque chose qui approche le temps N*T pour résoudre une chaîne de N liens de RR A6, bien qu'on puisse s'attendre a avoir un fort facteur de mise en antémémoire pour les fragments A6 qui représentent les bits de poids fort d'une adresse. Cela nous laisse avec le choix entre deux options, dont ni l'une ni l'autre n'est très bonne : on peut diminuer le temps que le résolveur accepte d'attendre pour chaque fragment, ou on peut augmenter la quantité de temps qu'un résolveur accepte d'attendre avant de retourner un échec au client. Le peu de données que nous avons sur ce sujet nous suggère que les usagers sont déjà impatients avec les lenteurs de la résolution des RR A dans l'Internet IPv4, ce qui suggère qu'ils ne seront vraisemblablement pas très patients avec des délais significativement plus longs dans l'Internet IPv6. En même temps, terminer prématurément les interrogations est à la fois un gaspillage de ressources et une autre source de frustration de l'usager, on est forcé de conclure qu'une utilisation sans discrimination de longues chaînes A6 va vraisemblablement conduire à des problèmes.

Pour empirer les choses, les endroits où les RR A6 ont des chances d'être les plus critiques pour un dénumérotage rapide ou un acheminement de style GSE sont les situations où le champ de nom de préfixe du RR A6 pointe sur une cible qui n'est pas seulement en dehors de la zone DNS qui contient le RR A6, mais est administrées par une organisation différente (par exemple, dans le cas du site d'un utilisateur final, le nom de préfixe va très vraisemblablement pointer sur un nom qui appartient à un FAI qui fournit la connexité pour le site). Bien qu'en soi, les pointeurs hors zone ne posent pas de problème, les pointeurs sur d'autres organisations sont un peu plus difficiles à entretenir et moins susceptibles d'automatisation que le seraient les pointeurs au sein d'une seule organisation. L'expérience aussi bien avec les RR glu qu'avec les RR PTR dans l'arborescence IN-ADDR.ARPA suggère que de nombreux administrateurs de zone ne comprennent pas bien comment établir et entretenir correctement ces pointeurs, et on n'a pas de raisons particulières de croire que ces administrateurs de zone feront un meilleur travail avec les chaînes A6 que ce qu'ils font aujourd'hui. Pour être cependant honnête, la solution de remplacement de construire des RR AAAA via un prétraitement avant de charger les *(fichiers de)* zones pose sensiblement les mêmes problèmes ; au mieux, on peut avancer qu'utiliser les RR AAAA pour cela permettrait aux clients du DNS d'avoir la mauvaise réponse un peu plus efficacement qu'avec les RR A6.

Finalement, en supposant une ignorance presque totale de la probabilité d'échec d'une interrogation, celle d'une chaîne A6 de N liens paraîtrait en gros proportionnelle à N, car chaque interrogation impliquée dans la résolution d'une chaîne A6 aurait la même probabilité d'échec qu'une seule interrogation AAAA. Noter encore que ce commentaire s'applique aux échecs dans le traitement de résolution d'une interrogation, et non aux données obtenues via ce processus. On peut bien sûr avancer que dans un monde idéal, les RR A6 augmenteraient la probabilité que la réponse obtenue par le client soit (finalement) juste, en supposant que rien n'aille de travers dans le traitement de l'interrogation, mais on n'a pas la moindre idée de la façon de quantifier cette hypothèse même avec la méthode d'approximation grossière utilisée ailleurs dans cette note.

Un problème potentiel qui a été soulevé dans le passé au sujet des RR A6 s'est révélé sans fondement. Le concept de A6 inclut la possibilité qu'il y ait plus d'un RR A6 qui corresponde à la portion de nom de préfixe d'un RR A6 d'extrémité. C'est-à-dire qu'une chaîne A6 peut n'être pas une simple liste avec un lien ; elle peut en fait être une arborescence, où chaque branche représente un préfixe possible. Certains critiques de A6 craignent que cela conduise à une expansion incontrôlée des interrogations, mais il se révèle que ce n'est pas un problème si un résolveur suit simplement la recommandation 1 de "limiter la quantité de travail par interrogation" décrite au paragraphe 5.3.3 de la RFC1034. Cette recommandation s'applique à tout le travail résultant de tentatives de traitement d'une interrogation, sans considération de si c'est une interrogation simple, une chaîne de CNAME, une arborescence A6, ou une boucle infinie. Le client ne peut pas obtenir une réponse utile dans les cas où la zone a été configurée de travers, mais une mise en œuvre appropriée ne devrait pas produire une explosion d'interrogations même à la suite du traitement de l'arborescence chaîne ou boucle A6 la plus perverse.

Interactions avec DNSSEC

Un des domaines dans lequel diffèrent les RR AAAA et A6 est celui des détails précis de la façon dont ils interagissent avec DNSSEC. Les commentaires qui suivent ne s'appliquent qu'aux RR A6 de préfixe différent de zéro (on répète que les RR A6 0 sont sémantiquement équivalents à des RR AAAA).

Toutes choses égales par ailleurs, le temps que prend la réallocation des adresses dans une zone après un événement de dénumérotage est plus long avec des RR AAAA qu'avec des RR A6 (parce que chaque enregistrement d'adresse doit être re-signé plutôt que de juste faire signer un RR A6 de préfixe commun et quelques RR A6 0 associés aux serveurs de nom de la zone). Noter cependant, qu'en général cela ne présente pas un problème d'adaptation sérieux, parce que la signature a lieu dans les zones d'extrémité.

Toutes choses égales par ailleurs, il y a plus de travail pour la vérification des signatures reçues en retour pour les RR A6, parce que chaque fragment d'adresse a une signature associée distincte. De même, un message DNS qui contient un ensemble de fragments d'adresse A6 et leurs signatures associées sera plus grand que le paquet équivalent avec un seul AAAA (ou A6 0) et une seule signature associée.

Comme les RR AAAA ne peuvent pas réellement très bien représenter des scénarios de dénumérotage rapide ou d'acheminement de style GSE, on ne serait pas surpris que les signatures DNSSEC des RR AAAA posent aussi quelques problèmes. Dans les cas où les RR AAAA devraient être changés très rapidement pour rester en ligne avec des changements de préfixes, le temps nécessaire pour resigner les RR AAAA peut être prohibitif.

Un essai empirique par Bill Sommerfeld [Sommerfeld] suggère que l'ordinateur individuel Celeron à 333 MHz avec une antémémoire de couche 2 de 128 k octet et 64 M octet de RAM fonctionnant avec le programme BIND-9 dnssec-signzone sous NetBSD peut générer en gros 40 signatures RSA à 1024 bits par seconde. En extrapolant à partir de cela, et en supposant un RR A, un RR AAAA, et un RR NXT par hôte, cela suggère qu'il faudrait à cet ordinateur quelques heures pour signer une zone faisant la liste de 10**5 hôtes, ou environ une journée pour signer une zone faisant la liste de 10**6 hôtes en utilisant des RR AAAA.

Cela suggère que l'effort supplémentaire pour re-signer une grande zone pleine de RR AAAA durant un événement de dénumérotage, bien que ne passant pas inaperçu, ne sera vraisemblablement prohibitif que dans le cas de dénumérotage rapide où les RR AAAA ne fonctionnent de toutes façons pas très bien.

Interactions avec la mise à jour dynamique

La mise à jour dynamique du DNS paraît fonctionner également bien pour les RR AAAA ou A6, avec une exception mineure : avec les RR A6, le client de mise à jour dynamique a besoin de savoir la longueur et le nom du préfixe. À présent, aucun mécanisme n'existe pour informer un client de mise à jour dynamique de ces valeurs, mais on peut supposer qu'un tel mécanisme pourrait être fourni via une extension à DHCP, ou quelque autre équivalente.

Transition de AAAA à A6 via AAAA de synthèse

Alors que AAAA est à présent plus largement déployé que A6, il est possible de faire une transition d'un logiciel DNS à capacité AAAA à un logiciel DNS à capacité A6. Un plan pour ce faire a été présenté dans ses grandes lignes à l'IETF-50 à Minneapolis et a été discuté sur la liste de diffusion ipng. Si l'IETF arrive à la conclusion que les capacités améliorées de A6 sont nécessaires, il devrait être possible d'assurer la transition de AAAA à A6.

Les détails de cette transition figurent dans un autre document, mais l'idée générale est que le résolveur qui effectue une résolution itérative au nom d'un programme client DNS pourrait synthétiser les RR AAAA qui représentent le résultat des opérations d'interrogations A6 équivalentes. Noter que dans ce cas, il n'est pas possible de générer une signature DNSSEC équivalente pour le RR AAAA, de sorte que les clients qui tiennent à effectuer la validation DNSSEC pour eux-mêmes devront produire des interrogations A6 directement plutôt que de s'appuyer sur le AAAA de synthèse.

Étiquettes binaires

Bien que les différences entre les RR AAAA et A6 aient généré la plus grande partie de la discussion jusqu'à aujourd'hui, deux mécanismes sont aussi proposés pour construire l'arborescence de transposition inverse (l'équivalent IPv6 de l'arborescence IN-ADDR.ARPA de IPv4).

La [RFC1886] propose un mécanisme très similaire au mécanisme IN-ADDR.ARPA utilisé pour les adresses IPv4 : le nom du RR est la représentation hexadécimale de l'adresse IPv6r, inversée et concaténée avec un suffixe bien connu, séparé par un point entre chaque chiffre hexadécimal. Les noms DNS résultants sont assez fastidieux à taper pour les humains, mais il est très facile à un programme de les générer. Faire de chaque chiffre hexadécimal une étiquette séparée signifie que la délégation sur des frontières arbitraires de bit va résulter en un maximum de 16 ensembles de RR NS par niveau d'étiquette ; là encore, le mécanisme est assez fastidieux pour l'homme, mais très facile à programmer. Comme avec l'arborescence IN-ADDR.ARPA de IPv4, le seul endroit où ce schéma est faible est dans le traitement des délégations dans l'étiquette de moindre poids ; cependant, comme il apparaît qu'il n'y a pas de besoin réel de déléguer les quatre bits de moindre poids d'une adresse IPv6, ceci ne paraît pas être une restriction sérieuse.

La [RFC2874] proposait une façon radicalement différente de désigner les entrées dans l'arborescence de transposition

inverse : plutôt que d'utiliser des représentations textuelles des adresses, elle proposait d'utiliser une nouvelle sorte d'étiquette DNS (une "étiquette binaire") pour représenter directement les adresses binaires dans le DNS. Cela présente l'avantage d'être significativement plus compact que la représentation textuelle, et ceci aurait éventuellement pu être une meilleure solution pour le DNS de l'utiliser à cette fin si cela avait été conçu dans le protocole depuis le début. Malheureusement, l'expérience jusqu'à ce jour suggère que le développement d'un nouveau type d'étiquette DNS est très dur : tous les serveurs de noms du DNS qui sont d'autorité pour n'importe quelle portion du nom en question doivent être mis à niveau avant que le nouveau type puisse être utilisé, tout comme le doivent tous les résolveurs impliqués dans le processus de résolution. Tout serveur de noms qui n'aurait pas été mis à niveau pour comprendre le nouveau type d'étiquette rejetterait l'interrogation comme étant mal formée.

Comme le principal avantage de l'approche de l'étiquette binaire paraît être une capacité dont on a pas réellement besoin (la délégation dans les quatre bits de moindre poids d'une adresse IPv6) et comme le problème de la mise à niveau va vraisemblablement rendre les étiquettes binaires inutilisables jusqu'à ce qu'une portion significative de la base de code du DNS ait été mise à niveau, il est difficile d'échapper à la conclusion que la solution textuelle est assez bonne.

RR DNAME

La [RFC2874] propose aussi d'utiliser les RR DNAME comme moyen de fournir l'équivalent des adresses fragmentées de A6 dans l'arborescence de transposition inverse. C'est à dire qu'en utilisant les RR DNAME, on peut écrire des fichiers de zone pour l'arborescence de transposition inverse qui aient la même capacité de traiter le dénumérotage rapide ou l'acheminement de style GSE qu'offrent les RR A6 dans la portion principale de l'arborescence du DNS. Par conséquent, le besoin d'utiliser le DNAME dans l'arborescence de transposition inverse apparaît étroitement lié au besoin d'utiliser le A6 fragmenté dans l'arborescence principale : si l'un est nécessaire, l'autre l'est aussi, et si l'un n'est pas nécessaire, l'autre non plus.

D'autres utilisations ont aussi été proposées pour le RR DNAME, mais comme elles sortent du domaine d'application de la discussion sur les adresses IPv6, on n'en parlera pas ici.

Recommandation

Quand on réduit les comparaisons de caractéristiques ci-dessus à leurs éléments clés, les questions importantes paraissent être :

(a) IPv6 va-t-il faire des dénumérotages rapides ou des acheminements de style GSE ?

(b) L'arborescence de transposition inverse pour IPv6 va t-elle exiger la délégation dans les quatre bits de moindre poids de l'adresse ?

La question (a) apparaît être la clé du débat. C'est réellement une décision qui doit être prise par la communauté IPv6, et non par la communauté du DNS.

La question (b) est aussi posée à la communauté IPv6, mais il semble assez évident que la réponse est "non".

Recommandations sur la base de ces questions :

(1) Si le groupe de travail IPv6 a sérieusement l'intention de spécifier et déployer le dénumérotage rapide ou l'acheminement de style GSE, on devrait faire la transition vers l'utilisation du RR A6 dans l'arborescence principale et l'utilisation des RR DNAME autant que nécessaire dans l'arborescence inverse.

(2) Autrement, on devrait garder la solution plus simple d'AAAA dans l'arborescence principale et ne pas utiliser les RR DNAME dans l'arborescence inverse.

(3) Dans l'un et l'autre cas, l'arborescence inverse devrait utiliser la représentation textuelle décrite dans la [RFC1886] plutôt que la représentation d'étiquette binaire décrite dans la [RFC2874].

(4) Si on est conduit à utiliser les RR A6 dans l'arborescence principale et à utiliser les RR DNAME dans l'arborescence inverse, on devrait écrire des déclaration d'applicabilité et des lignes directrices de mise en œuvre conçues pour déconseiller des utilisations excessivement complexes de ces caractéristiques ; en général, tout réseau qui peut être décrit de façon adéquate en utilisant les RR A6 0 et sans utiliser les RR DNAME devrait être décrit de cette façon, et les caractéristiques améliorées ne devraient être utilisées que lorsque absolument nécessaire, au moins jusqu'à ce que nous ayons plus d'expérience d'elles et une meilleure compréhension de leurs modes d'échec.

Considérations pour la sécurité

Cette note compare deux mécanismes qui ont des caractéristiques de sécurité similaires, mais il y a quelques implications pour la sécurité dans le choix entre ces deux mécanismes :

(1) Les deux mécanismes ont des interactions similaires mais non identiques avec DNSSEC. Prière de se reporter à la section intitulée "Interactions avec DNSSEC" (ci-dessus) pour l'exposé de ces questions.

(2) Dans la mesure où la complexité du fonctionnement est ennemie de la sécurité, le compromis sur la complexité de fonctionnement qui est exposé tout au long de cette note a un impact sur la sécurité.

(3) Dans la mesure ou cette complexité du protocole est ennemie de la sécurité, la complexité supplémentaire du protocole de la [RFC2874] par rapport à celle de la [RFC1886] a un certain impact sur la sécurité.

Considérations relatives à l'IANA

Aucune, car tous ces types de RR ont déjà été alloués.

Remerciements

La présente note se fonde sur un certain nombre de discussions publiques et privées sur une période (d'au moins) huit ans, mais des remerciements particuliers vont à Alain Durand, Bill Sommerfeld, Christian Huitema, Jun-ichiro itojun Hagino, Mark Andrews, Matt Crawford, Olafur Gudmundsson, Randy Bush, et Sue Thomson ; aucun d'entre eux n'est responsable de ce que l'auteur a fait de leurs idées.

Références

[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.)*

[RFC2874] M. Crawford, C. Huitema, "Extensions de DNS pour la prise en charge de l'agrégation et du rénumérotage d'adresse IPv6", juillet 2000. (*MàJ par* RFC3152, RFC3226, RFC3363, RFC3364) *(Expérimentale)*

[Sommerfeld] Message privé à l'auteur de Bill Sommerfeld daté du 21 mars 2001, résumant les résultats des expériences qu'il a réalisées sur une copie de la zone MIT.EDU.

[GSE] "GSE" était une évolution de ce qu'on appelait la proposition "8+8" discutée par le groupe de travail IPng en 1996 et 1997. la proposition GSE elle-même a été rédigée comme projet Internet, qui est arrivé depuis longtemps à expiration. Les lecteurs intéressés par les détails et l'histoire de GSE devraient revoir les archives de la liste de diffusion du groupe de travail IPng ainsi que les comptes-rendus de cette période.

Adresse de l'auteur

Rob Austein
mél : sra@hactrn.net

Déclaration de droits de reproduction

reproduction définis dans les processus des normes pour Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation a un objet particulier.

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