Groupe de travail Réseau
Request for Comments : 2182
BCP : 16
Catégorie : Bonne practiques actuelles
Traduction Claude Brière de L'Isle

R. Elz, University of Melbourne
R. Bush, RGnet, Inc.
S. Bradner, Harvard University
M. Patton, Consultant
juillet 1997

Sélection et fonctionnement des serveurs secondaires du DNS

Statut du présent mémoire
Ce document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le système des noms de domaine exige que plusieurs serveurs existent pour chaque domaine délégué (zone). Le présent document expose le choix des serveurs secondaires pour les zones du DNS. La localisation physique et topologique de chaque serveur pose des problèmes matériels lors du choix des serveurs secondaires. Le nombre de serveurs approprié pour une zone est aussi discuté, et certaines questions générales de la maintenance des serveurs secondaires sont examinées.

Table des Matières

1. Introduction

Un certain nombre de problèmes du fonctionnement du DNS sont aujourd'hui attribuables à de mauvais choix de serveurs secondaires pour les zones du DNS. Le placement géographique ainsi que la diversité de connexité réseau exhibée par l'ensemble des serveurs du DNS pour une zone peuvent accroître la fiabilité de cette zone tout en améliorant les performances globales du réseau et les caractéristiques d'accès. D'autres considérations sur le choix des serveurs peuvent diminuer de façon inattendue la fiabilité ou imposer des exigences supplémentaires au réseau.

Le présent document discute beaucoup de ces questions qui devraient être prises en considération lors du choix des serveurs secondaires pour une zone. Il propose des lignes directrices sur la façon de faire le meilleur choix pour desservir une zone donnée.

2. Définitions

Pour les besoins du présent document, et à cette seule fin, on appliquera les définitions suivantes :

DNS Système des noms de domaine [RFC1034], [RFC1035].

Zone Partie de l'arborescence du DNS, qui est traitée comme une unité.

Zone de transmission Zone contenant des données qui transposent des noms en adresses d'hôtes, cibles d'échange de messagerie, etc.

Zone inverse Zone contenant des données utilisées pour transposer des adresses en noms.

Serveur Mise en œuvre des protocoles du DNS, capables de fournir des réponses aux interrogations. Les réponses peuvent être à partir d'informations connues du serveur, ou des informations obtenues d'autres serveurs.

Serveur d'autorité Serveur qui connaît le contenu d'une zone DNS à partir d'une connaissance locale, et peut donc répondre aux interrogations sur cette zone sans avoir besoin d'interroger d'autres serveurs.

Serveur inscrit Serveur d'autorité pour lequel il y a un enregistrement de ressource (RR, *resource record*) "NS" dans la zone.

Serveur principal Serveur d'autorité pour lequel les informations de zone sont configurées localement. Parfois appelé serveur maître.

Serveur secondaire Serveur d'autorité qui obtient d'un serveur principal des informations sur une zone via un mécanisme de transfert de zone. Parfois appelé un serveur esclave.

Serveur furtif Serveur d'autorité, généralement secondaire, qui n'est pas un serveur inscrit.

Résolveur Client du DNS qui cherche les informations contenues dans une zone en utilisant les protocoles du DNS.

3. Serveurs secondaires

La principale raison pour l'exigence de plusieurs serveurs pour chaque zone est de permettre aux clients de tout l'Internet, c'est à dire du monde entier, d'avoir sur la zone des informations fiables et largement disponibles, même lorsque un serveur est indisponible ou injoignable.

La multiplicité des serveurs étale aussi la charge de la résolution des noms, et améliore l'efficacité globale du système en plaçant les serveurs plus près des résolveurs. Ces points ne seront pas évoqués plus avant ici.

Avec plusieurs serveurs, un serveur sera généralement le serveur principal, et les autres seront les serveurs secondaires. Noter que bien que certaines configurations inhabituelles utilisent plusieurs serveurs principaux, il peut en résulter des incohérences dans les données, et ceci n'est pas conseillé.

La distinction entre serveur principal et serveurs secondaires n'est pertinente que pour les serveurs pour la zone concernée ; pour le reste du DNS, ce sont simplement plusieurs serveurs. Tous sont traités également en première instance, même par le serveur parent qui délègue la zone. Les résolveurs mesurent souvent les performances des divers serveurs, choisissent le "meilleur", pour une certaine définition de meilleur, et le préfèrent pour la plupart des interrogations. Ceci est automatique, et n'est pas examiné ici.

Le serveur principal détient la copie maîtresse du fichier de la zone. C'est-à-dire que c'est le serveur où les données sont entrées dans le DNS à partir de sources situées en-dehors du DNS. Les serveurs secondaires obtiennent les données pour la zone en utilisant les mécanismes de protocole du DNS pour obtenir la zone auprès du serveur principal.

3.1 Choix des serveurs secondaires

Pour choisir les serveurs secondaires, il faut faire attention à la probabilité des divers modes de défaillances. Les serveurs devraient être disposés de façon qu'il soit probable qu'au moins un serveur sera disponible pour toutes les parties significatives de l'Internet, pour toute défaillance probable.

Par conséquent, placer tous les serveurs au site local, bien que facile à faire et facile à gérer, n'est pas une bonne politique. En cas de défaillance d'une seule liaison, ou du site, ou peut-être même du bâtiment, de la pièce, ou d'une panne d'électricité, une telle configuration peut conduire à ce que tous les serveurs soient déconnectés de l'Internet.

Les serveurs secondaires doivent être placés dans des localisations dispersées à la fois topologiquement et géographiquement sur l’Internet, pour minimiser la probabilité qu'une seule défaillance les désactive tous.

C'est à dire que les serveurs secondaires devraient être dans des localisations géographiquement distantes, afin qu'il soit peu vraisemblable que des événements comme des pannes d'électricité, etc., les interrompent tous simultanément. Ils devraient aussi être connectés à la Toile via des chemins assez divers. Cela signifie que la défaillance de n'importe laquelle de ces liaisons, ou de l'acheminement au sein d'un segment du réseau (comme un fournisseur de service) ne rendra pas tous les serveurs injoignables.

3.2 Configurations inappropriées

Bien que ce soit malheureusement assez courant, les serveurs pour une zone ne devraient certainement pas être tous placés sur le même segment de LAN dans la même pièce du même bâtiment – ou un seul de ceux là. Une telle configuration réduit presque à néant l'exigence, et l'utilité, d'avoir plusieurs serveurs. La seule redondance habituellement apportée dans cette configuration est pour le cas où un serveur serait défaillant, alors qu'il y a beaucoup d'autres modes de défaillance possibles, comme des pannes d'électricité, y compris celles de longue durée, à considérer.

3.3 Fin d'un mythe

On avance occasionnellement l'argument qu'il n'y a pas besoin de serveurs de noms de domaines pour qu'un domaine soit accessible si les hôtes du domaine sont injoignables. Cet argument est fallacieux.

+ Les clients réagissent différemment à l'incapacité à résoudre qu'à l'incapacité à se connecter, et les réactions à la première ne sont pas toujours celles désirées.
+ Si la zone est résoluble et que le nom particulier ne l'est pas, un client peut alors éliminer la transaction plutôt que de réessayer et de faire peser une charge indésirable sur le réseau.
+ Alors que les résultats positifs du DNS sont usuellement placés en antémémoire, l'absence de résultat ne l'est pas. Donc, une incapacité inutile à résoudre crée une charge indésirable sur la toile.
+ Tous les noms de la zone peuvent ne pas se résoudre en adresses au sein du réseau détaché. Cela devient plus probable au fil du temps. Donc, une hypothèse de base du mythe devient souvent fausse.

Il est important qu'il y ait des serveurs de noms capables de répondre à des interrogations, toujours disponibles, pour toutes les zones de transmission.

4. Serveurs injoignables

Une autre classe de problèmes est causée par les serveurs inscrits qui ne peuvent pas être atteints à partir de grandes parties du réseau. Cela pourrait venir de l'inscription du nom d'une machine qui est complètement isolée derrière un pare-feu, ou seulement une adresse secondaire sur une machine à double rattachement qui n'est pas accessible de l'extérieur. Les noms des serveurs inscrits dans des enregistrements NS devraient se résoudre en adresses qui soient accessibles à partir de la région à laquelle les enregistrements NS sont à retourner. Inclure des adresses que la plus grande partie du réseau ne peut pas atteindre n'apporte aucune fiabilité, et cause plusieurs problèmes, qui peuvent, finalement, affaiblir la fiabilité de la zone.

D'abord, la seule façon dont les résolveurs peuvent déterminer que ces adresses sont, en fait, injoignables, est de les essayer. Il doivent ensuite attendre une absence de fin de temporisation de réponse (ou occasionnellement une réponse d'erreur ICMP) pour savoir que l'adresse ne peut pas être utilisée. De plus, même cela est généralement non distinguable d'une simple perte de paquet, de sorte que la séquence doit être répétée, plusieurs fois, pour avoir une réelle évidence d'un serveur injoignable. Toutes ces vérifications et fins de temporisations peuvent prendre suffisamment de temps pour que le programme client ou utilisateur d'origine décide qu'aucune réponse n'est disponible, ce qui conduit à une défaillance apparente de la zone. De plus, tout cela doit être répété de temps en temps pour faire la distinction entre un serveur d'indisponibilité permanente et celui dont l'indisponibilité n'est que temporaire.

Et finalement, toutes ces étapes vont devoir éventuellement être subies par les résolveurs tout le long du réseau. Cela augmente le trafic, et probablement la charge des filtres sur chaque pare-feu qui bloque cet accès. Toutes ces charges supplémentaires ne font effectivement que diminuer la fiabilité du service.

4.1 Serveurs derrière des connexions intermittentes

Un problème similaire survient avec les serveurs DNS localisés dans des parties de la toile qui sont souvent déconnectées de l'Internet global. Par exemple, ceux qui se connectent via une connexion intermittente qui est souvent coupée. De tels serveurs devraient normalement être traités comme si ils étaient derrière un pare-feu, et injoignables par le réseau à tout moment.

4.2 Autres cas de problème

Des problèmes similaires surviennent lorsque un traducteur d'adresse réseau (NAT, *Network Address Translator*) [RFC1631] existe entre un résolveur et un serveur. En dépit de ce que suggère la [RFC1631], en pratique, les NAT ne traduisent pas les adresses incorporées dans les paquets, mais seulement ceux qui sont dans les en-têtes. Comme le suggère la [RFC1631], ceci pose un problème au DNS. Cela peut parfois être surmonté si le NAT est accompagné, ou remplacé par une passerelle de couche application (ALG, *Application Layer Gateway*). Un tel appareil va comprendre le protocole DNS et traduire toutes les adresses de façon appropriée lorsque les paquets passent au travers. Même avec un tel appareil, il est vraisemblable qu'il vaut mieux dans tous ces cas adopter la solution décrite dans le paragraphe suivant.

4.3 Solution

Pour éviter ces problèmes, les enregistrements NS retournés dans n'importe quelle réponse pour une zone ne devraient faire la liste que des serveurs auxquels le résolveur ayant demandé les informations, il est vraisemblablement capable de les atteindre. Certains résolveurs sont simultanément des serveurs effectuant des recherches au nom d'autres résolveurs. Les enregistrements NS retournés devraient être joignables non seulement par le résolveur qui a demandé les informations, mais aussi par tout autre résolveur qui va transmettre ces informations. Toutes les adresses de tous les serveurs retournés doivent être accessibles. Comme les adresses de chaque serveur forment un ensemble d'enregistrement de ressource (RRset, *Resource Record Set*) [RFC2181], toutes doivent être retournées (ou aucune) donc, il n'est pas acceptable d'effacer les adresses des serveurs qui sont injoignables, ou de les retourner avec un faible TTL (tout en retournant les autres avec un TTL supérieur).

En particulier, lorsque des serveurs sont derrière un pare-feu, une connexion intermittente, ou un NAT, qui interdit, ou a des problèmes avec les questions ou les réponses du DNS, leurs noms, ou adresses, ne devraient pas être retournés aux clients extérieurs au pare-feu. De même, les serveurs extérieurs au pare-feu ne devraient pas être révélés aux clients qui sont à l'intérieur, si les clients vont être dans l'incapacité d'interroger ces serveurs. La mise en œuvre de cela exige habituellement deux établissements du DNS, un pour usage interne, l'autre pour usage externe. Un tel établissement résout souvent d'autres problèmes dans de tels environnements.

Lorsque un serveur est à la frontière d'un pare-feu, accessible des deux côtés, mais utilisant des adresses différentes, ce serveur devrait recevoir deux noms, chacun étant associé à l'enregistrement A approprié, de sorte que chacun apparaisse comme joignable par le seul côté approprié du pare-feu. Cela devrait alors être traité comme deux serveurs, un de chaque côté du pare-feu. Un serveur mis en œuvre dans une ALG va normalement être dans ce cas. Une attention particulière doit être apportée à permettre à un tel serveur de retourner les réponses correctes aux clients de chaque côté. C'est-à-dire, ne retourner que les informations sur les hôtes accessibles de chaque côté et les adresses IP correctes pour l'hôte vu de ce côté.

Les serveurs dans cet environnement ont souvent besoin de dispositions particulières pour donner leur accès aux serveurs racine. Cela est souvent accompli via des configurations de "fausse racine". Dans un tel cas, les serveurs devraient rester bien isolés du reste du DNS, de crainte que la configuration inhabituelle ne pollue les autres.

5. Combien de secondaires ?

La spécification du DNS et les règles d'enregistrement des noms de domaine exigent au moins deux serveurs pour chaque zone. C'est à dire, normalement un principal et un secondaire. Bien que deux, placés avec soin, soient souvent suffisants, les occasions où deux sont insuffisants sont assez fréquentes pour qu'on conseille l'utilisation de plus de deux serveurs inscrits. Divers problèmes peuvent causer l'indisponibilité d'un serveur pendant de longues périodes – durant de telles périodes, une zone qui n'a que deux serveurs inscrits ne fonctionne en réalité qu'avec un seul. Comme tout serveur peut être occasionnellement indisponible, pour toutes sortes de raisons, cette zone va vraisemblablement, de temps en temps, ne plus avoir du tout de serveur en état de fonctionnement.

D'un autre côté, avoir un grand nombre de serveurs ne rapporte qu'un faible avantage, tout en ayant un coût. Au niveau le

plus simple, plus de serveurs veut dire des paquets plus gros, ce qui exige plus de bande passante. Cela peut sembler trivial, et l'est en fait. Cependant, il y a une limite à la taille d'un paquet du DNS, et ce qui ferait atteindre cette limite a de plus sérieuses implications sur les performances. Il paraît sage de s'en tenir à bonne distance. Plus de serveurs accroît aussi la probabilité qu'un serveur soit mal configuré, ou fonctionne mal, sans être détecté.

Il est recommanda que trois serveurs soient fournis pour la plupart des zones de niveau organisation, avec au moins un qui doit être très à l'écart des autres. Pour les zones où une fiabilité encore plus forte est exigée, quatre ou même cinq serveurs peuvent être souhaitables. Deux, ou éventuellement trois sur cinq, seraient sur un site local, et les autres ne seraient pas proches géographiquement ou topologiquement proches du site, ou les uns des autres.

Les zones inverses, c'est-à-dire, les sous-domaines de .IN-ADDR.ARPA, tendent à être moins cruciaux, et moins de serveurs, moins répartis, vont souvent suffire. Cela parce que les traductions d'adresse en nom ne sont normalement nécessaires que lorsque des paquets sont reçus de l'adresse en question, et seulement par des résolveurs à la destination des paquets ou à proximité de celle-ci. Cela donne quelques assurances que les serveurs situés à la source des paquets ou à sa proximité, par exemple, sur le même réseau, seront accessibles à partir des résolveurs qui ont besoin d'effectuer les recherches. Donc, certains des modes de défaillance qui doivent être pris en considération lors de la planification des serveurs dans les zones de transmission peuvent être moins pertinents lorsque il s'agit de zones inverses.

5.1 Serveurs furtifs

Les serveurs qui sont d'autorité pour la zone, mais qui ne sont pas inscrits dans les enregistrements NS (aussi connus sous le nom de "serveurs furtifs") ne sont pas inclus dans le compte des serveurs.

Il peut souvent être utile que tous les serveurs d'un site soient d'autorité (secondaire), mais que seuls un ou deux soient des serveurs inscrits, le reste étant des serveurs non inscrits pour toutes les zones locales, c'est-à-dire, des serveurs furtifs.

Cela permet à ces serveurs de fournir directement des réponses aux interrogations locales, sans avoir besoin de consulter un autre serveur. Si il était nécessaire de consulter un autre serveur, il serait alors normalement nécessaire de consulter les serveurs de la racine, afin de suivre l'arborescence des délégations – car il ne serait pas connu que la zone est locale. Cela signifierait que certaines interrogations locales ne pourraient pas recevoir de réponse si les communications externes se trouvaient interrompues.

Faire la liste de tous ces serveurs dans les enregistrements NS, si il en a plus de un ou deux, causerait au reste de l'Internet des efforts en pure perte pour tenter de contacter tous les serveurs sur le site alors que tout le site est inaccessible du fait de défaillances de liaison ou d'acheminement.

6. Trouver les serveurs secondaires convenables

Le fonctionnement d'un serveur secondaire est normalement une tâche presque automatique. Une fois établi, le serveur fonctionne généralement tout seul, sur la base des actions du serveur principal. À cause de cela, un grand nombre d'organisations acceptent de fournir un serveur secondaire, si on le leur demande. La meilleure approche est normalement de trouver une organisation de taille similaire, et de se mettre d'accord pour échanger les zones secondaires – chaque organisation acceptant de fournir un serveur pour agir comme serveur secondaire pour les zones de l'autre organisation. Noter qu'il n'y a pas ici de perte de données confidentielles, les ensembles de données échangés seront disponibles quels que soient les serveurs.

7. Maintenance du numéro de série

Les serveurs secondaires utilisent le numéro de série de l'enregistrement SOA de la zone pour déterminer quand il est nécessaire de mettre à jour leur copie locale de la zone. Les numéros de série sont simplement des entiers non signés de 32 bits qui reviennent à zéro depuis la plus grande valeur possible. Voir la [RFC1982] pour une définition plus rigoureuse du numéro de série.

Le numéro de série doit être incrémenté chaque fois qu'est fait un changement, ou groupe de changements, à la zone du serveur principal. Cela informe les serveurs secondaires qu'ils doivent mettre à jour leur copie de la zone. Noter qu'il n'est pas possible de décrémenter un numéro de série, les incréments sont la seule modification définie.

À l'occasion, du fait d'erreurs d'édition, ou d'autre facteurs, il peut être nécessaire de faire qu'un numéro de série devienne

plus petit. Cela ne diminue jamais le numéro de série. Les serveurs secondaires vont ignorer ce changement, et de plus, ils vont ignorer tous les incréments ultérieurs jusqu'à ce que soit dépassée la plus grande valeur antérieure.

Au lieu de cela, étant donné que les numéros de série reviennent du plus grand au plus petit, en termes absolus, incrémenter le numéro de série, plusieurs fois, jusqu'à ce qu'il atteigne la valeur désirée. À chaque étape, attendre que tous les serveurs secondaires aient mis à jour la nouvelle valeur avant de continuer.

Par exemple, supposons que le numéro de série d'une zone soit 10, mais qu'il ait été accidentellement réglé à 1000, et qu'on désire le ramener à 11. On ne va pas simplement changer la valeur de 1000 à 11. Un serveur secondaire qui a vu la valeur de 1000 (et en pratique, il y en a toujours au moins un) va ignorer ce changement, et continuer d'utiliser la version de zone avec le numéro de série 1000, jusqu'à ce que le numéro de série du serveur principal excède cette valeur. Cela peut durer longtemps – en fait, le serveur secondaire arrive souvent à l'expiration de la copie de la zone avant que la zone ne soit à nouveau mise à jour.

Au lieu de cela, pour cet exemple, régler le numéro de série du serveur principal à 2 000 000 000, et attendre que les serveurs secondaires mettent à jour cette zone. La valeur de 2 000 000 000 est choisie comme étant très supérieure à la valeur actuelle, mais moins que 2^31 plus grande (2^31 est 2 147 483 648). C'est alors un incrément du numéro de série [RFC1982].

Ensuite, après que tous les serveurs qui ont besoin de mettre à jour ont la zone avec ce numéro de série, celui-ci peut être réglé à 4 000 000 000. 4 000 000 000 est 2 000 000 000 de plus que 2 000 000 000 (très clairement) et c'est donc un autre incrément (la valeur ajoutée est inférieure à 2^31).

Une fois que cette copie du fichier de la zone existe chez tous les serveurs, le numéro de série peut être simplement réglé à 11. Dans l'arithmétique des numéros de série, un changement de 4 000 000 000 à 11 est un incrément. Les numéros de série reviennent à zéro à 2^32 (4 294 967 296) de sorte que 11 est identique à 4 294 967 307 (4 294 967 296 + 11). 4 294 967 307 est juste 294 967 307 fois plus grand que 4 000 000 000, et 294 967 307 est très inférieur à 2^31, ce qui est donc un incrément.

En suivant cette procédure, il est essentiel de vérifier que tous les serveurs pertinents ont été mis à jour à chaque étape, sans préjuger de rien. Négliger de le faire peut résulter en un désordre bien plus grand que celui qui existait avant la tentative de correction. Il faut aussi bien faire attention que c'est la relation entre les valeurs des divers numéros de série qui est importante, et non les valeurs absolues. Les valeurs utilisées ci-dessus sont correctes pour ce seul exemple.

Il est possible dans presque tous les cas de corriger le numéro de série en deux étapes en étant plus agressif dans les choix de numéros de série. Cela fait cependant que les numéros utilisés sont moins "gentils", et exigent des soins plus considérables.

Noter aussi que toutes les mises en œuvre de serveur de noms ne mettent pas correctement en œuvre les opérations sur les numéros de série. Avec de tels serveurs comme secondaires, il n'y a normalement pas moyen de faire diminuer le numéro de série, autrement qu'en contactant l'administrateur du serveur et de demander que toutes les données existantes pour la zone soient purgées. Puis que le secondaire soit rechargé à partir du principal, comme si c'était pour la première fois.

Il reste qu'il est sûr de suivre la procédure ci-dessus, car les dysfonctionnements de serveurs vont nécessiter dans tous les cas une intervention manuelle. Après la séquence des changements de numéro de série décrite ci-dessus, les serveurs secondaires conformes seront rétablis. Puis, lorsque le serveur principal a le numéro de série correct (désiré), contacter les serveurs secondaires restants et corriger manuellement leur compréhension du numéro de série correct. On peut peut-être aussi suggérer qu'ils mettent leur logiciel au niveau d'une mise en œuvre conforme standard.

Un serveur qui ne met pas en œuvre cet algorithme est défectueux, et peut être détecté comme suit. À un certain stade, normalement lorsque la valeur absolue entière du numéro de série devient plus petite, un serveur qui a ce défaut particulier va ignorer le changement. Les serveurs qui ont ce type de défaut peuvent être détectés en attendant au moins le temps spécifié dans le champ Rafraîchissement de la SOA puis en envoyant ensuite une interrogation de la SOA. Les serveurs qui ont ce défaut vont encore avoir le vieux numéro de série. On ne connaît pas d'autre moyen de détecter ce défaut.

Considérations pour la sécurité

On pense que rien dans ce document n'aggrave de problèmes de sécurité qui peuvent exister avec le DNS, ni ne fasse quelque chose pour les atténuer.

Les administrateurs devraient cependant être conscients que la compromission d'un serveur pour un domaine peut, dans

certaines situations, compromettre la sécurité des hôtes du domaine. Il faut veille lors qu choix des serveurs secondaires à minimiser cette menace.

Références

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987.

[RFC1631] K. Egevang, P. Francis, "Le traducteur d'adresse réseau (NAT) IP", juin 1994. *(Info., remplacé par 3022)*

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série ", août 1996. (MàJ RFC1034, RFC1035) *(P.S.)*

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(Information)*

Remerciements

Brian Carpenter et Yakov Rekhter ont suggéré de mentionner les NAT et les ALG comme compagnons de texte des pare-feu. Dave Croquer a suggéré explicitement de démolir le mythe.

Adresse des auteurs

Robert Elz
Computer Science
University of Melbourne
Parkville, Vic, 3052
Australia.
mél : kre@munnari.oz.au

Randy Bush
RGnet, Inc.
5147 Crystal Springs Drive NE
Bainbridge Island, Washington, 98110
United States.
mél : randy@psg.com

Scott Bradner
Harvard University
1350 Mass Ave
Cambridge, MA, 02138
United States.
mél : sob@harvard.edu

Michael A. Patton
33 Blanchard Road
Cambridge, MA, 02138
United States.
mél : map@pobox.com