Groupe de travail Réseau
Request for Comments : 4786
BCP : 126
Catégorie : Bonnes practiques actuelles

J. Abley, Afilias Canada
K. Lindqvist, Netnod Internet Exchange
décembre 2006
Traduction Claude Brière de L'Isle

Fonctionnement des services d'envoi à la cantonade

Statut de ce mémoire
Le présent 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
Avec la croissance de l'Internet, et avec l'omniprésence acquise par les systèmes et services en réseau au sein des entreprises, ont émergé de nombreux services avec des exigences de haute disponibilité. Ces exigences ont accru la demande de fiabilité de l'infrastructure sur laquelle s'appuient ces services.

Diverses techniques ont été employées pour augmenter la disponibilité des services déployés sur l'Internet. Le présent document présente des commentaires et recommandations pour la distribution des services qui utilisent l'envoi à la cantonade.

Table des matières

1. Introduction

Le présent document s'adresse aux exploitants de réseau qui envisagent de déployer ou faire fonctionner un service réparti en utilisant l'envoi à la cantonade. Il décrit les bonnes pratiques actuelles pour le faire, mais ne recommande aucun service particulier qui devrait ou non être déployé en utilisant l'envoi à la cantonade.

Pour distribuer un service en utilisant l'envoi à la cantonade, le service est d'abord associé à un ensemble stable d'adresses IP, et l'accessibilité de ces adresses est annoncée dans un système d'acheminement à partir de plusieurs nœuds de service indépendants. Diverses techniques pour le déploiement de services d'envoi à la cantonade sont discutées dans la [RFC1546], [ISC-TN-2003-1], et [ISC-TN-2004-1].

Les techniques et considérations décrites dans le présent document s'appliquent aux services accessibles aussi bien sur IPv4 que IPv6.

L'envoi à la cantonade est devenu de plus en plus populaire ces dernières années pour ajouter de la redondance aux serveurs DNS et pour compléter la redondance que l'architecture du DNS fournit dejà elle-même. Plusieurs opérateurs de serveurs racines du DNS ont largement réparti leurs serveurs tout autour de l'Internet, et les serveurs à la fois résolveurs et d'autorité sont couramment distribués au sein des réseaux des fournisseurs de services. La distribution en envoi à la cantonade a été utilisée par des opérateurs commerciaux de serveur d'autorité du DNS depuis plusieurs années. L'utilisation de l'envoi à la cantonade n'est pas limité au DNS, bien que l'utilisation de l'envoi à la cantonade impose des limitations supplémentaires à la nature du service distribué, incluant la longévité de transaction, l'état de transaction conservé sur les serveurs, et les capacités de synchronisation des données.

Bien que l'envoi à la cantonade soit conceptuellement simple, sa mise en œuvre introduit des traquenards pour le fonctionnement des services. Par exemple, surveiller la disponibilié du service devient plus difficile ; la disponibilité observée change selon la situation du client au sein du réseau, et la population de clients en utilisant des nœuds individuels d'envoi à la cantonade n'est ni statique, ni fiablement déterministe.

Le présent document va décrire l'utilisation de l'envoi à la cantonade pour la distribution de services de portée locale en utilisant un protocole de passerelle intérieure (IGP, *Interior Gateway Protocol*) et pour la distribution mondiale en utilisant le protocole de routeur frontière (BGP, *Border Gateway Protocol*) [RFC4271]. Beaucoup des problèmes de surveillance et de synchronisation des données sont communs aux deux, mais les questions de déploiement diffèrent substantiellement.

2. Terminologie

Adresse de service : adresse IP associée à un service particulier (par exemple, l'adresse de destination utilisée par les résolveurs du DNS pour atteindre un serveur d'autorité particulier).

Envoi à la cantonade : pratique consistant à rendre une adresse de service particulière disponible dans plusieurs localisations discrètes, autonomes, de telle sorte que les datagrammes envoyés soient acheminés à une parmi plusieurs localisations disponibles.

Nœud d'envoi à la cantonade : collection connectée en interne d'hôtes et routeurs qui ensemble fournissent un service pour une adresse de service d'envoi à la cantonade. Un nœud d'envoi à la cantonade pourrait être aussi simple qu'un seul hôte participant à un système d'acheminement avec des routeurs adjacents, ou il pourrait inclure un certain nombre d'hôtes connectés d'une façon plus élaborée ; dans l'un et l'autre cas, pour le système d'acheminement à travers lequel le service est en envoi à la cantonade, chaque nœud d'envoi à la cantonade présente un unique chemin à l'adresse de service. Le système entier d'envoi à la cantonade pour le service consiste en deux ou plus nœuds d'envoi à la cantonade séparés.

Capture : en géographie physique ,c'est une zone drainée par un cours d'eau, aussi appelé un basin de drainage. Par analogie, comme utilisé dans le présent document, la région topologique d'un réseau au sein duquel les paquets dirigés sur une adresse d'envoi à la cantonade sont acheminés à un nœud particulier.

Envoi à la cantonade de portée locale : les informations d'accessibilité pour l'adresse de service d'envoi à la cantonade sont propagées à travers un système d'acheminement de telle façon qu'un nœud particulier d'envoi à la cantonade n'est visible qu'à un sous ensemble du système d'acheminement entier.

Nœud local : nœud d'envoi à la cantonade qui fournit le service en utilisant une adresse d'envoi à la cantonade de portée locale.

Envoi à la cantonade de portée mondiale : les informations d'accessibilité pour l'adresse de service d'envoi à la cantonade sont propagées à travers un système d'acheminement de telle façon qu'un nœud particulier d'envoi à la cantonade soit potentiellement visible à tout le système d'acheminement.

Nœud mondial : nœud d'envoi à la cantonade qui fournit le service en utilisant une adresse d'envoi à la cantonade de portée mondiale.

3. Distribution du service d'envoi à la cantonade

3.1 Description générale

Envoi à la cantonade est le nom donné à la pratique de rendre une adresse de service disponible à un système d'acheminement aux nœuds d'envoi à la cantonade dans deux localisations discrètes ou plus. Le service fourni par chaque nœud est généralement cohérent sans considération du nœud particulier choisi par le système d'acheminement pour traiter une demande particulière (bien que certains services puissent bénéficier de différences délibérées de comportement des nœuds individuels, afin de faciliter un comportement spécifique de la localisation ; voir le paragraphe 4.6).

Pour les services distribués en utilisant l'envoi à la cantonade, il n'y a pas d'exigence inhérente aux références aux autres serveurs ou distribution de service fondé sur le nom ("DNS round-robin") bien que ces techniques pourraient être combinées avec la distribution de service d'envoi à la cantonade si une application l'exigeait. Le système d'acheminement décide quel nœud est utilisé pour chaque demande, sur la base du dessin topologique du système d'acheminement et le point dans le réseau auquel la demande prend son origine.

Le nœud d'envoi à la cantonade choisi pour servir une certaine interrogation peut être influencé par les capacités d'ingénierie du trafic des protocoles d'acheminement qui constituent le système d'acheminement. Le degré d'influence disponible à l'opérateur du nœud dépend de l'adaptation du système d'acheminement au sein duquel l'adresse de service est en envoi à la cantonade.

L'équilibrage de charge entre nœuds d'envoi à la cantonade est normalement difficile à réaliser (la distribution de la charge entre les nœuds est généralement déséquilibrée en termes de demandes et de charge de trafic). La répartition de la charge entre les nœuds pour les besoins de la fiabilité, et la distribution grossière de la charge afin de rendre les services populaires adaptables, peuvent cependant être souvent réalisées.

L'adaptabiité du système d'acheminement à travers lequel un service est en envoi à la cantonade peut varier d'un petit protocole de routeur intérieur (IGP, *Interior Gateway Protocol*) connectant une poignée de composants, au protocole de routeur frontière (BGP, *Border Gateway Protocol*) [RFC4271] connectant l'Internet mondial, selon la nature de la distribution de service requise.

3.2 Buts

Un service peut être en envoi à la cantonade pour diverses raisons. Les objectifs courants sont :

1. Une distribution grossière ("non équilibrée") de la charge entre les nœuds, pour permettre à l'infrastructure de s'adapter à un nombre croissant d'interrogations et s'accommoder de pointes transitoires d'interrogations ;

2. Atténuer des attaques non distribuées de déni de service en localisant les dommages à un seul nœud d'envoi à la cantonade ;

3. Contrainte d'attaque de déni de service répartie ou foules soudaines de régions locales autour de nœuds d'envoi à la cantonade. La distribution en envoi à la cantonade d'un service donne l'opportunité de traiter le trafic au plus proche de sa source, peut-être en utilisant des liaisons d'échange de trafic à hautes performances plutôt que des circuits de transit payants surencombrés ;

4. De fournir des informations supplémentaires pour aider à identifier la localisation des sources de trafic dans le cas d'un trafic d'attaque (ou d'interrogations) qui incorpore des adresses de source falsifiées. Ces informations sont déduites de la

propriété de la distribution d'un service d'envoi à a cantonade que le choix du nœud d'envoi à la cantonade utilisé pour servir une interrogation particulière peut être en relation avec la source topologique de la demande.

5. Amélioration du temps de réponse à une interrogation, en réduisant la distance du réseau entre client et serveur avec la fourniture d'un nœud d'envoi à la cantonade local. La mesure dans laquelle le temps de réponse à une interrogation est amélioré dépend de la façon dont les nœuds sont choisis pour les clients par le système d'acheminement. La proximité topologique au sein du système d'acheminement n'est, en général, pas corrélée aux performances d'aller-retour à travers un réseau ; dans certains cas, les temps de réponse peuvent ne voir aucune réduction, et peuvent s'accroître.

6. Pour réduire une liste de serveurs à une seule adresse ditribuée. Par exemple, un grand nombre de serveurs de noms d'autorité pour une zone peuvent être déployés en utilisant un petit ensemble d'adresses de service d'envoi à la cantonade ; cette approche peut accroître l'accessibilité des données de zone dans le DNS sans augmenter la taille d'une réponse référante provenant d'un serveur de noms d'autorité pour la zone parente.

4. Conception

4.1 Adaptation du protocole

Quand un service est en envoi à la cantonade entre deux nœuds ou plus, le système d'acheminement prend la décision de choix du nœud au nom du client.

Comme il est généralemnt exigé qu'une seule interaction client-serveur soit portée entre un client et le même nœud serveur pour la durée de la transaction, il s'ensuit que la décision de choix du nœud par le système d'acheminement devrait être stable pendant un temps substantiellement plus long que la durée attendue de la transaction, si le service doit être fourni de façon fiable.

Certains services ont des temps de transaction très courts, et peuvent même être réalisés en utilisant un seul paquet de demande et un seul paquet de réponse (par exemple, les transactions de DNS sur un transport UDP). D'autres services impliquent des transactions de plus longue durée (par exemple, des téléchargements de fichiers bruts et des flux directs de supports audiovisuels).

Des services peuvent être en envoi à la cantonade au sein de systèmes d'acheminement très prévisibles, qui peuvent rester stables pendant de longues périodes (par exemple, l'envoi à la cantonade au sein d'un IGP bien géré et topologiquement simple, où les changements de choix du nœud ne se produisent qu'en réponse à des défaillances du nœud). D'autres déploiements ont des caractéristiques beaucoup moins prévisibles (voir le paragraphe 4.4.7).

La stabilité du système d'acheminement, ainsi que le temps de transaction du service, devraient être comparés avec attention quand on décide si un service est convenable pour la distribution en utilisant l'envoi à la cantonade. Dans certains cas, pour de nouveaux protocoles, il peut être pratique de partager de grandes transactions en une phase d'initialisation qui est traitée par des serveurs de diffusion à la cantonade, et une phase soutenue qui est fournie par des serveurs non de diffusion à la cantonade, peut-être choisis durant la phase d'initialisation.

Le présent document évite délibérément de prescrire des règles sur quels protocoles ou services sont convenables pour la distribution par envoi à la cantonade ; tenter de le faire serait présomptueux.

Les opérateurs devraient savoir que, en particulier pour les flux de long terme, il y a, en utilisant l'envoi à la cantonade, des modes d'échec potentiels qui sont plus complexes qu'une simple défaillance de "destination injoignable" en utilisant l'envoi individuel.

4.2 Placement des nœuds

La décision de l'endroit où devraient être placés les nœuds d'envoi à la cantonade va dépendre dans une large mesure des buts de la distribution de service. Par exemple :

- Un service de résolveurs récurrents du DNS pourrait être distribué au sein du réseau d'un fournisseur de service d'accès, un nœud d'envoi à la cantonade par site.
- Un service de serveurs racines du DNS pourrait être distribué partout dans l'Internet ; les nœuds d'envoi à la cantonade pourraient être situés dans des régions avec une faible connectivité externe pour assurer que le DNS fonctionne de façon adéquate dans la région durant les périodes de défaillance du réseau externe.

- Un service mirroir de FTP pourrait inclure des nœuds locaux situés à des points d'échange, afin que les FAI connectés à ce point d'échange puissent télécharger des données en vrac à meilleur marché que si ils avaient à utiliser de coûteux circuits de transit.

En général, les décisions de placement de nœuds devraient être prises en considérant les exigences du trafic probable, le potentiel de foules soudaines ou de trafic de déni de service, la stabilité du système d'acheminement local, et les modes de défaillance par rapport à la défaillance du nœud ou de défaillance du système d'acheminement local.

4.3 Systèmes d'acheminement

4.3.1 Envoi à la cantonade au sein d'un IGP

Il y a plusieurs motifs communs pour la distribution d'une adresse de service au sein de la portée d'un IGP :

1. améliorer le temps de réponse du service en hébergeant un service proche des autres utilisateurs du réseau ;
2. améliorer la fiabilité du service en fournissant une reprise sur défaillance automatique aux nœuds de sauvegarde ; et
3. garder le trafic de service local afin d'éviter l'encombrement les liaisons de large zone.

Dans chaque cas, les décisions sur où et comment provisionner les services peuvent être prises par les ingénieurs du réseau sans exiger autant de complexité de fonctionnement que les variantes régionales dans la configuration des ordinateurs clients, ou des incohérences délibérées du DNS (causant des réponses différentes aux interrogations du DNS selon l'origine des interrogations).

Quand un service est en envoi à la cantonade au sein d'un IGP, le système d'acheminement est normalement sous le contrôle de la même organisation qui fournit le service, et donc, la relation entre les caractéristiques de la transaction de service et la stabilité du réseau est probablement bien comprise. Cette technique est par conséquent applicable à un plus grand nombre d'applications qu'un service de distribution d'envoi à la cantonade à l'échelle de l'Internet (paragraphe 4.1).

Un IGP va généralement n'avoir pas de restriction inhérente sur la longueur de préfixe qui peut lui être introduit. Dans ce cas, il n'est pas besoin de construire un préfixe couvrant pour des adresses de service particulières ; les chemins d'hôtes correspondant à l'adresse de service peuvent alors être introduits dans le système d'acheminement. Voir au paragraphe 4.4.2 la discussion de l'exigence d'un préfixe couvrant.

Les IGP ne présentent souvent que peu ou pas d'agrégation de chemins, en partie à cause de la complexité des algorithmes pour prendre en charge l'agrégation. Souvent, Il y a peu de motivation pour l'agrégation dans de nombreux IGP de réseaux, car la quantité d'informations d'acheminement portées dans l'IGP est assez petite pour que ne se posent pas les soucis d'adaptabilité dans les routeurs. Voir au paragraphe 4.4.8 la discussion des risques de l'agrégation dans les autres systèmes d'acheminement.

En réduisant la portée de l'IGP juste aux hôtes qui fournissent le service (avec un ou quelques routeurs passerelles) cette technique peut être appliquée à la construction de grappes de serveurs.Cette application est discutée en détails dans [ISC-TN-2004-1].

4.3.2 Envoi à la cantonade au sein de l'Internet mondial

Les adresses de service peuvent être en envoi à la cantonade au sein du système d'acheminement de l'Internet mondial afin de distribuer les services à travers le réseau entier. Les principales différences entre cette application et la distribution de portée IGP discutée au paragraphe 4.3.1 sont que :

1. le système d'acheminement est, en général, contrôlé par d'autres personnes ;
2. le protocole d'acheminement concerné (BGP), et les pratiques couramment acceptées de son déploiement, imposent des contraintes supplémentaires (voir le paragraphe 4.4).

4.4 Considérations pour l'acheminement

4.4.1 Signalisation de la disponibilité du service

Quand un système d'acheminement est fourni avec des informations d'accessibilité pour une adresse de service provenant d'un nœud individuel, les paquets adressés à cette adresse de service vont commencer à arriver au nœud. Comme il est essentiel que le nœud soit prêt à accepter les demandes avant qu'elles commencent à arriver, un couplage entre les informations d'acheminement et la disponibilité du service à un nœud particulier est désirable.

Lorsque une annonce d'acheminement provenant d'un nœud correspond à une seule adresse de service, ce couplage pourrait être tel que la disponibilité du service déclenche l'annnonce de chemin, et que la non disponibilité du service déclenche un retrait de chemin. Cela peut être réalisé en utilisant des mises en œuvre du protocole d'acheminement sur le même serveur. Ces mises en œuvre fournissent le service distribué et sont configurées à annoncer et supprimer l'annonce de chemin en conjonction avec la disponibilité (et la santé) du logiciel sur l'hôte qui traite les demandes de service. Un exemple d'un tel arrangement pour un service de DNS figure dans [ISC-TN-2004-1].

Lorsque une annonce d'acheminement provenant d'un nœud correspond à deux adresses de service ou plus, il peut n'être pas approprié de déclencher un retrait de chemin à cause de la non disponibilité d'un seul service. Une autre approche dans le cas où le service est indisponible à un nœud d'envoi à la cantonade est d'acheminer les demandes à un nœud d'envoi à la cantonade différent où le service fonctionne normalement. Cette approche est discutée au paragraphe 4.8.

Des oscillations rapides d'annonces/retraits peuvent causer des problèmes de fonctionnement, et les nœuds devraient être configurés de façon à ce que des oscillations rapides soient évitées (par exemple, en mettant en œuvre un délai minimum à la suite d'une suppression avant que le service puisse être réannoncé). Voir au paragraphe 4.4.4 la discussion des oscillations de chemin dans BGP.

4.4.2 Préfixe de couverture

Dans certains systèmes d'acheminement (par exemple, le système d'acheminement fondé sur BGP de l'Internet mondial) il n'est pas possible, en général, de propager un chemin d'hôte avec la certitude que le chemin va se propager dans tout le réseau. C'est une conséquence de la politique de fonctionnement, et non une restriction du ptotocole.

Dans de tels cas, il est nécessaire de propager un chemin qui couvre l'adresse de service, et qui a un préfixe suffisamment court pour n'être pas éliminé par les politique d'importation couramment déployées. Pour les adresses de service IPv4, c'est souvent un préfixe de 24 bits, mais il y a d'autres exemples bien documentés de politiques d'import IPv4 qui filtrent sur les frontières d'allocation de registre Internet régional (RIR) et donc c'est à expérimenter avec prudence. Les politiques d'importation correspondantes pour les préfixes IPv6 existent aussi. Voir au paragraphe 4.5 la discussion des adresses de service IPv6 et les chemins correspondants d'envoi à la cantonade.

La propagation d'un seul chemin par service a des questions associées d'adaptabilité, qui sont discutées au paragraphe 4.4.8.

Lorsque plusieurs adresses de service sont couvertes par le même chemin couvrant, il n'y a plus de couplage étroit entre l'annonce de ce chemin et les services individuels associés aux chemins d'hôtes couverts. L'impact résultant sur la disponibilité de signalisation des services individuels est discuté dans les paragraphes 4.4.1 et 4.8.

4.4.3 Chemins de coût égal

Certains systèmes d'acheminement prennent en charge les chemins de coût égal pour la même destination. Quand il existe plusieurs chemins de coût égal qui conduisent à des nœuds d'envoi à la cantonade différents, il y a un risque que des paquets de demande différents associés à une seule transaction puissent être livrés à plus d'un nœud. Les services fournis sur TCP [RFC0793] impliquent nécessairement des transactions avec plusieurs paquets de demande, à cause de la prise de contact de l'établissement de TCP.

Pour les services qui sont distribués à travers l'Internet mondial en utilisant BGP, les chemins de coût égal ne sont normalement pas pris en considération : l'algorithme de choix de sortie de BGP choisit généralement une seule sortie cohérente pour une seule destination sans considération de si il existe plusieurs chemins candidats. Il existe cependant des mises en œuvre de BGP qui prennent en charge le choix de sortie sur plusieurs chemins.

Les chemins de coûts égaux sont couramment pris en charge dans les IGP. Le choix de plusieurs nœud pour une seule transaction peut être évité dans la plupart des cas par un examen attentif des métriques de liaison IGP, ou en appliquant des algoritmes de choix de chemins multiples de coût égal (ECMP, *equal-cost multi-path*) qui causent les choix d'un seul nœud pour une seule transaction multi paquets. Pour un exemple de l'utilisation de choix de ECMP fondé sur le hachage dans la distribution du service d'envoi à a cantonade, voir [ISC-TN-2004-1].

D'autres algorithmes de choix d'ECMP sont couramment disponibles, incluant ceux dans lesquels il n'est pas garanti que les paquets provenant du même flux soient acheminés vers la même destination. Les algorithmes ECMP qui choisissent un chemin sur la base du paquet plutôt que du flux sont couramment désignés comme effectuant un "équilibrage de charge par paquet" (PPLB, *Per Packet Load Balancing)*.

Par rapport à la distribution de service d'envoi à la cantonade, certaines utilisations de PPLB peuvent causer la livraison de différents paquets provenant d'une seule transaction multi paquets envoyée par un client à des nœuds d'envoi à la cantonade différents, rendant en fait le service d'envoi à la cantonade indisponible. L'effet sur des services spécifiques d'envoi à la cantonade va dépendre de la façon et du lieu où sont déployés les nœuds d'envoi à la cantonade au sein du système d'acheminement, et de la façon dont le PPLB est effectué :

1. le PPLB à travers plusieurs liaisons parallèles entre la même paire de routeurs ne devrait causer aucun problème de choix de nœud ;

2. Le PPLB à travers divers chemins au sein d'un seul système autonome (AS) où les chemins convergent en une seule sortie lorsque ils quittent l'AS, ne devrait causer aucun problème de choix de nœud ;

3. le PPLB à travers des liaisons avec differents AS voisins, où les AS voisins ont choisi des nœuds différents pour une destination particulière d'envoi à la cantonade vont, en général, causer la distribution des paquets de demande à travers plusieurs nœuds d'envoi à la cantonade. Cela va avoir pour effet que le service d'envoi à a cantonade est indisponible aux clients en aval du routeur qui effectue le PPLB.

Les utilisations de PPLB ont un potentiel de mauvaise interaction avec la distribution du service d'envoi à a cantonade qui peut aussi causer un réarragement persistant des paquets. Un chemin de réseau qui réarrange de façon persistante les segments va dégrader les performance du trafic porté par TCP [Allman2000]. TCP, selon plusieurs mesures documentées, prend en compte le trafic en vrac porté sur l'Internet ([McCreary2000], [Fomenkov2004]). Par conséquent, dans de nombreux cas, il est raisonnable d'envisager que les réseaux qui font une telle utilisation de PPLB ont un problème pathologique.

4.4.4 Amortissement de chemin

Des annonces et retraits fréquents des préfixes individuels dans BGP sont connus comme des oscillations. Des oscillations rapides peuvent conduire à l'épuisement de CPU sur des routeurs assez loin de la source de l'instabilité, et pour cette raison les oscillations rapides de chemin sont fréquemment "amorties", comme décrit dans la [RFC2439].

Un chemin amorti va être supprimé par les routeurs pendant une durée qui augmente selon la fréquence de l'oscillation observée ; un chemin supprimé ne va pas être propagé. Donc, un seul routeur peut empêcher la propagation d'un préfixe oscillant au reste d'un système autonome, permettant aux autres routeurs dans le réseau de se protéger contre l'instabilité.

Certaines mises en œuvre d'amortissement d'oscillation pénalisent les annonces oscillantes sur la base de l'AS_PATH observé , et non des informations d'accessibilité de couche réseau (NLRI, *Network Layer Reachability Information)* ; voir la [RFC4271]. Pour cette raison, l'instabilité du réseau qui conduit aux oscillations de chemin à partir d'un seul nœud d'envoi à la cantonade, ne va généralement pas causer l'amortissement des annonces de la part des autres nœuds (qui ont des attributs AS_PATH differents) par ces mises en œuvre.

Pour limiter l'opportunite pour de telles mises en œuvre de pénaliser les annonces provenant de nœuds différents d'envoi à la cantonade en réponse aux oscillations d'un seul nœud, on devrait veiller à s'arranger pour que les attributs AS_PATH sur les chemins provenant de nœuds différents soient aussi divers que possible. Par exemple, les nœuds d'envoi à la cantonade devraient utiliser le même AS d'origine pour leurs annonces, mais pourraient avoir des AS amont différents.

Quand des mises en œuvre différentes d'amortissement d'oscillations sont prévalantes, l'instabilité des nœuds individuels peut résulter en ce que des nœuds stables deviennent indisponibles. Pour l'atténuer, les mesures suivantes peuvent être utiles :

1. Un déploiement judicieux de nœuds locaux en combinaison avec des nœuds mondiaux particulièrement stables (avec un écartement de chemin inter AS élevé, un matériel redondant, de la puissance, etc.) peut aider à limiter les problèmes d'oscillation aux régions d'influence limitées des nœuds locaux ;
2. un amortissement d'oscillations aggressif du préfixe de service proche de l'origine (par exemple, au sein d'un nœud d'envoi à la cantonade, ou dans les AS adjacents de chaque nœud d'envoi à la cantonade) peut aussi aider à réduire l'opportunité que les AS distants voient des oscillations.

4.4.5 Vérifications de la transmission sur le chemin inverse

Les vérifications de la transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) décrites pour la première fois dans la [RFC2267], sont couramment déployées au titre des filtres de paquet d'interface d'entrée sur les routeurs dans l'Internet afin de refuser les paquets dont les adresses de source sont usurpées (voir aussi la [RFC2827]). Les mises en œuvre déployées de RPF rendent plusieurs modes de fonctionnement disponibles (par exemple, "lâche" et "strict").

Certains modes de RPF peuvent causer le rejet de paquets non usurpés quand ils proviennent de sites multi rattachements, car les chemins choisi pourraient légitimement ne pas correspondre à l'interface d'entrée de paquets non usurpés provenant du site multi rattachements. Ce problème est discuté dans la [RFC3704].

Une collection de nœuds d'envoi à la cantonade déployée à travers l'Internet est largement indistinguable d'un site multi rattachements distribué pour le système d'acheminement, et donc, ce risque existe aussi pour les nœuds d'envoi à la cantonade, même si les nœuds individuels ne sont pas multi rattachements. On devrait veiller à s'assurer que chaque nœud d'envoi à la cantonade est traité comme un réseau multi rattachements, et que les recommandations correspondantes de la [RFC3704] à l'égard des vérifications de RPF sont prises en compte.

4.4.6 Portée de propagation

Dans le contexte de la distribution du service d'envoi à a cantonade à travers l'Internet mondial, les nœuds mondiaux sont ceux qui sont capables de fournir le service aux clients partout dans le réseau ; les informations d'accessibilité pour le service sont propagées globalement, sans restriction, en annonçant les chemins qui couvrent les adresses de service pour le transit mondial vers un ou plusieurs fournisseurs.

Plus d'un nœud mondial peut exister pour un seul service (et bien sûr, c'est souvent le cas, pour des raisons de redondance et de partage de charge).

À l'opposé, il est parfois souhaitble de déployer un nœud d'envoi à la cantonade qui ne fournit de services qu'à un bassin local de systèmes autonomes, et qui est délibérément non disponible à l'Internet entier ; de tels nœuds sont appelés des nœuds locaux dans le présent document. Un exemple de circonstances dans lesquelles un nœud local peut être approprié est celui de nœuds destinés à desservir une région avec une riche connectivité interne, mais non fiable, encombrée ou d'accès coûteux pour le reste de l'Internet.

Les nœuds locaux annoncent les chemins couvrants pour les adresses de service de façon telle que leur propagation est restreinte. Cela pourrait être fait en utilisant des attributs de chaîne de communauté bien connues comme NO_EXPORT [RFC1997] ou NOPEER [RFC3765], ou en s'arrangeant avec les homologues pour appliquer une politique d'importation conventionnelle "d'échange de trafic" au lieu d'une politique d'importation de "transit", ou une combinaison convenanble de mesures.

Annoncer l'accessibilité aux adresses de service à partir des nœuds locaux devrait idéalement être fait en utilisant une politique d'acheminement qui exige la présence d'attributs explicites pour la propagation, plutôt que de s'appuyer sur une politique implicite (par défaut). La propagation involontaire d'un chemin au delà de l'horizon prévu peut résulter en des problèmes de capacité pour les nœuds locaux, qui pourraient dégrader les performance de service sur l'ensemble du réseau.

4.4.7 Réseaux des autres

Quand des services d'envoi à la cantonade sont déployés à travers des réseaux gérés par d'autres, leur accessibilité dépend de politiques d'acheminement et de changements de topologie (plannifiés ou non) qui sont imprévisibles et parfois difficiles à identifier. Comme le système d'acheminement peut inclure des réseaux gérés par plusieurs organisations sans relations entre elles, la possibilité d'interactions imprévues résultant de la combinaisons de changements sans rapports entre eux existe aussi.

La stabilité et la prévisibilité d'un tel système d'acheminement devrait être prise en compte quand on évalue l'opportunité de l'envoi à la cantonade comme stratégie de distribution pour des services et protocoles particuliers (voir aussi au paragraphe 4.1).

Pour atténuer cela, les politiques d'acheminement utilisées par les nœuds d'envoi à la cantonade à travers de tels systèmes d'acheminement devraient être prudentes, l'infrastructure de connexion interne et externe des nœuds individuels devrait être adaptée pour supporter des charges bien au delà de la moyenne, et le service devrait être surveillé de façon pro active à partir de nombreux points afin d'éviter de mauvaises surprises (voir le paragraphe 5.1).

4.4.8 Risques de l'agrégation

La propagation d'un seul chemin pour chaque service d'envoi à a cantonade ne s'adapte pas bien pour les systèmes d'acheminement dans lesquels la charge des informations d'acheminement qui doivent être portées est un souci, et où il y a potentiellement de nombreux services à distribuer. Par exemple, un système autonome qui fournit des services à l'Internet

avec N adresses de service couvertes par un seul chemin exporté va devoir annoncer (N + 1) chemins, si chacun de ces services devait être distribué en utilisant l'envoi à la cantonade.

La pratique courante d'appliquer des filtres de longueur minimum de préfixe dans les politiques d'importation sur l'Internet (voir au paragraphe 4.4.2) signifie que pour un chemin qui couvre une adresse de service soit utilement propagé, la longueur de préfixe doit être substantiellement moindre que celle requise pour annoncer juste le chemin de l'hôte. Des annonces largement répandues de courts préfixes pour des services individuels ont donc aussi un impact négatif sur la conservation des adresses.

Ces deux problèmes peuvent être atténués dans une certaine mesure par l'utilisation d'un seul préfixe couvrant pour s'accommoder de multiples adresses de service, comme décrit au paragraphe 4.8. Cela implique cependant un découplage de l'annonce de chemin de la disponibilité du service individuel (voir au paragraphe 4.4.1) avec les risques qui en découlent pour la stabilité du service dans son ensemble (paragraphe 4.7).

En général, les problèmes d'adaptabilité décrits ici empêchent l'envoi à la cantonade d'être une approche général utile pour la distribution de service dans l'Internet mondial. Il reste, cependant, une technique utile pour distribuer un nombre limité de services critiques pour l'Internet, ainsi que dans les plus petits réseaux où les problèmes d'agrégation discutés ici ne s'appliquent pas.

4.5 Considérations sur l'adressage

Les adresses de service devraient être uniques au sein du système d'acheminement qui connecte tous les nœuds d'envoi à la cantonade à tous les clients possibles du service. Les adresses de service doivent aussi être choisies de façon à ce qu'il soit permis aux chemins correspondants de se propager au sein de ce système d'acheminement.

Pour un service à numérotation IPv4 déployé à travers l'Internet, par exemple, une adresse pourrait être choisie à partir d'un bloc où la taille minimum d'allocation du RIR est de 24 bits, et l'accessibilité à cette adresse pourrait être fournie en générant le préfixe couvrant de 24 bits.

Pour un service à numérotation IPv4 déployé au sein d'un réseau privé, une adresse localement inutilisée de la [RFC1918] pourrait être choisie, et l'accessibilité à cette adresse pourrait être signalée en utilisant un chemin d'hôte (de 32 bits).

Pour les services à numérotation IPv6, les adresses d'envoi à la cantonade ne sont pas d'une portée différente des adresses en envoi individuel. À ce titre, les lignes directrices pour la convenance de l'adresse présentées pour IPv4 sont valables pour IPv6. Noter que les interdictions historiques sur la distribution de services en envoi à la cantonade sur IPv6 ont été supprimées de la spécification de l'adressage IPv6 dans la [RFC4291].

4.6 Synchronisation des données

Bien que certains services aient été déployés dans une forme localisée (de telle sorte que soient présentés aux clients de régions perticulières des contenus pertinents pour la région) de nombreux services ont la propriété que les réponses aux demandes des clients devraient être cohérentes, sans considération de l'origine de la demande. Pour un service distribué en utilisant l'envoi à la cantonade, cela implique que différents nœuds d'envoi à la cantonade doivent opérer de manière cohérente et, lorsque ce comportement cohérent se fonde sur un ensemble de données, les données concernées soient synchronisées entre les nœuds.

Le mécanisme par lequel les données sont synchronisées dépend de la nature du service ; des exemples sont les transferts de zone pour les serveurs d'autorité du DNS et les resynchronisations pour les archives FTP. En général, la synchronisation des données entre les nœuds d'envoi à la cantonade va impliquer des transactions entre des adresses non d'envoi à la cantonade.

La synchronisation des données à travers les réseaux publics devrait être effectuée avec l'authentification et le chiffrement appropriés.

4.7 Autonomie des nœuds

Pour un déploiement d'envoi à la cantonade dont les buts incluent d’”améliorer la fiabilité par la redondance, il est important de minimiser l'opportunité qu'une seule défaillance compromette de nombreux nœuds (ou tous) ou qu'une seule défaillance

d'un nœud provoque une défaillance en cascade qui mette par terre les nœuds successifs supplémentaires jusqu'à ce que le service entier soit mis en échec.

Les codépendances sont évitées en rendant chaque nœud aussi autonome et auto-suffisant que possible. La mesure selon laquelle les nœuds peuvent survivre à une défaillance survenue ailleurs dépend de la nature du service délivré, mais pour les services qui s'accommodent d'un fonctionnement déconnecté (par exemple, la propagation programmée des changements entre serveurs maître et eslave dans le DNS) un haut degré d'autonomie peut être réalisé.

La possibilité de défaillance en cascade due à la charge peut aussi être réduite par le déploiement de nœuds mondiaux et locaux pour un seul service, car le chemin effectif de récupération sur défaillance du trafic est, en général, du nœud local au nœud mondial ; le trafic qui pourrait couler un nœud local a peu de chances de couler tous les nœuds locaux, sauf dans les cas les plus extrêmes.

Les chances de défaillance en cascade due à un défaut de logiciel dans un système d'exploitation ou serveur peuvent être réduites dans de nombreux cas en déployant des nœuds qui fonctionnent sur des mises en œuvre différentes de système d'exploitation, de logiciel de serveur, de logiciel de protocole d'acheminement, etc., de telle sorte qu'un défaut qui apparaît dans un seul composant n'affecte pas le système entier.

On devrait noter que ces approches pour augmenter l'autonomie du nœud sont, à des degrés divers, contraires aux buts pratiques de rendre un service déployé d'utilisation directe. Un service qui est trop complexe a plus de chances de subir des erreur d'opérateur qu'un service d'utilisation directe. Une considération attentive devrait être apportée à tous ces aspects afin qu'un équilibre approprié puisse être trouvé.

4.8 Nœuds multi-services

Pour un service distribué à travers un système d'acheminement où il est exigé que les préfixes couvrants annoncent l'accessibilité à une seule adresse de service (voir le paragraphe 4.4.2) une considération particulière doit être apportée au cas où plusieurs services doivent être distribués à travers un seul ensemble de nœuds. Cela résulte de l'exigence de signaler la disponibilité de services individuels au système d'acheminement afin que les demandes de service ne soient pas reçues par des nœuds qui ne sont pas capables de les traiter (voir le paragraphe 4.4.1).

Plusieurs approches sont décrites dans les paragraphes qui suivent.

4.8.1 Plusieurs préfixes couvrants

Chaque adresse de service est choisie de façon à ce que une seule adresse de service soit couverte par chaque préfixe annoncé. L'annonce et le retrait d'un seul préfixe couvrant peuvent être étroitement couplés à la disponibilité du seul service associé.

C'est l'approche la plus directe. Cependant, comme cela fait une très mauvaise utilisation des adresses uniques au monde, elle ne convient que pour l'utilisation d'un petit nombre de services critiques pour l'infrastructure comme des serveurs racine du DNS. Le déploiement général à l'échelle de l'Internet de services utilisant cette approche ne convient pas.

4.8.2 Retrait pessimiste

Plusieurs adresses de service sont choisies de façon à ce qu'elles soient couvertes par un seul préfixe. L'annonce et le retrait du seul préfixe couvrant sont couplés à la disponibilité de tous les services associés ; si un service individuel devient indisponible, le préfixe couvrant est supprimé.

Le couplage entre la disponibilité du service et l'annonce du préfixe couvrant est compliquée par l'exigence que toutes les adresses de service soient disponibles – l'annonce doit être déclenchée par la présence de tous les chemins composants, et pas seulement un seul chemin couvert.

Le fait que le dysfonctionnement d'un seul service cause la mise hors ligne de tous les services déployés dans un nœud peut rendre cette approche non acceptable pour de nombreuses applications.

4.8.3 Connexité intérieure intra-nœud

Plusieurs adresses de service sont choisies de façon à ce qu'elles soient couvertes par un seul préfixe. L'annonce et le retrait du seul préfixe couvrant sont couplés à la disponibilité de chaque service. Les nœuds ont une connexité intérieure, par

exemple, en utilisant des tunnels. Les chemins d'hôtes pour les adresses de service sont distribués en utilisant un IGP qui s'étend pour inclure des routeurs à tous les nœuds.

Dans le cas où un service est indisponible à un nœud, mais disponible aux autres nœuds, une demande peut être acheminée sur le réseau intérieur à partir du nœud receveur vers un autre nœud pour être traitée.

Dans le cas où des services locaux dans un nœud sont défaillants et où le nœud est déconnecté des autres nœuds, la continuation de l'annonce du préfixe couvrant pourrait causer un trou noir pour les demandes.

Cette approche permet une utilisation raisonnable des adresses du bloc réseau couvert par le préfixe annoncé, au prix d'une autonomie réduite des nœuds individuels ; l'IGP auquel participent tous les nœuds peut être vu comme un seul point de défaillance.

4.9 Identification du nœud par les clients

De temps en temps, tous les clients des services déployés rencontrent des problèmes, et ces problèmes exigent un diagnostic. Un service distribué en utilisant l'envoi à la cantonade impose une variable supplémentaire au processus de diagnostic sur un service simple, en envoi individuel -- le nœud particulier d'envoi à la cantonade qui traite la demande d'un client.

Dans certains cas, des outils courants de diagnostic au niveau du réseau comme un traceroute peuvent être suffisants pour identifier le nœud utilisé par un client. Cependant, l'utilisation de tels outils peut être au delà des capacités des utilisateurs sur le côté client d'une transaction, et, dans tous les cas, les conditions du réseau au moment du problème peuvent avoir changé au moment où ces outils sont appliqués.

La résolution des problèmes avec les services d'envoi à la cantonade est grandement facilitée si les mécanismes pour déterminer l'identité d'un nœud sont conçus dans le protocole. Des exemples de tels mécanismes incluent l'option NSID dans le DNS [RFC5001] et l'inclusion courante des informations de nom d'hôte dans l'accueil initial des serveurs SMTP à l'initialisation de session [RFC2821].

La fourniture de ces mécanismes dans la bande pour l'identification du nœud est fortement recommandée pour les services à distribuer en utilisant l'envoi à la cantonade.

5. Gestion du service

5.1 Surveillance

Surveiller un service qui est distribué est plus complexe que de surveiller un service non réparti, car la précision et la disponibilité observées du service sont, en général, différentes quand elles sont vues des clients rattachés aux différentes parties du réseau. Quand un problème est identifié, il n'est pas toujours aussi évident de savoir quel nœud a servi la demande, et donc quel nœud fonctionne mal.

Il est recommandé que les services distribués soient surveillés à partir de sondes distribuées de façon représentative à travers le système d'acheminement, et, lorsque possible, l'identite du nœud qui répond aux demandes individuelles soit enregistrée avec les statistiques de performance et de disponibilité. Le service RIPE NCC DNSMON [DNSMON] est un exemple d'une telle surveillance pour le DNS.

La surveillance du système d'acheminement (depuis divers endroits, dans le cas de systèmes d'acheminement où cette perspective est pertinente) peut aussi fournir d'utiles diagnostics pour réparer la disponibilité de service. Cela peut être réalisé en utilisant des sondes dédiées, ou les facilités de mesure des chemins publics sur l'Internet comme le service d'informations d'acheminement NCC de RIPE [RIS] et le projet de vues de l'acheminement de l'Université de l'Oregon [ROUTEVIEWS].

Surveiller la santé des appareils composants dans un déploiement d'envoi à la cantonade d'un service (hôtes, routeurs, etc.) est direct, et peut être réalisé en utilisant les mêmes outils et techniques couramment utilisés pour gérer les autres infrastructures connectées au réseau, sans la complexité supplémentaire impliquée dans la surveillance des adresses de service d'envoi à la cantonade.

6. Considérations pour la sécurité

6.1 Atténuation des attaques de déni de service

Le présent document décrit des mécanismes pour déployer des services sur l'Internet qui peuvent être utilisés pour atténuer la vulnérabilité à l'attaque :

1. Un nœud d'envoi à la cantonade peut agir comme réceptacle pour le trafic d'attaque généré dans sa sphère d'influence, empêchant les nœuds d'ailleurs d'avoir à traiter ce trafic ;

2. La tâche de traiter le trafic d'attaque dont les sources sont largement distribuées est elle-même distribuée à travers tous les nœuds qui contribuent au service. Comme le problème du tri entre trafic légitime et d'attaque est réparti, cela peut conduire à mieux s'adapter aux propriétés qu'un service qui n'est pas distribué.

6.2 Compromission de service

La distribution d'un service à travers plusieurs (ou de nombreux) nœuds autonomes impose une surveillance accrue ainsi qu'une charge accrue d'administration des systèmes sur l'opérateur du service, qui pourrait réduire l'efficacité de l'hôte et la sécurité du routeur.

L'avantage potentiel d'être capable de mettre hors ligne les serveurs compromis sans compromettre le service ne peut être réalisé que si il y a des procédures de fonctionnement pour le faire rapidement et de façon fiable.

6.3 Capture de service

Il est possible qu'une partie non autorisée puisse annoncer des chemins correspondant à des adresses de service d'envoi à la cantonade à travers un réseau, et ce faisant, capture du trafic de demande légitime ou traite des demandes d'une manière qui compromette le service (ou les deux). Un nœud félon d'envoi à la cantonade pourrait être difficile à détecter par les clients ou par l'opérateur du service.

Le risque de capture de service par la manipulation du système d'acheminement existe sans considération de si le service est distribué en utilisant l'envoi à la cantonade. Cependant, le fait que des nœuds d'envoi à la cantonade légitimes soient observables dans le système d'acheminement peut rendre plus difficile de détecter des nœuds félons.

De nombreux protocoles qui incorporent l'authentification ou la protection de l'intégrité fournissent ces caractéristiques de façon robuste, par exemple, en utilisant une réauthentification périodique au sein d'une seule session, ou la protection de l'intégrité soit au niveau du canal (par exemple, [RFC2845], [RFC3207]) soit au niveau du message (par exemple, [RFC4033], [RFC2311]). Les protocoles qui sont moins robustes peuvent être plus vulnérables à la capture de session. Étant donnée la plus grande opportunité de capture de session non détectée avec les services d'envoi à la cantonade, l'utilisation de protocoles robustes est recommandée pour les services d'envoi à la cantonade qui exigent l'authentification ou la protection de l'intégrité.

7. Remerciements

Les auteurs remercient de leurs contributions les divers participants au groupe de travail grow, et en particulier Geoff Huston, Pekka Savola, Danny McPherson, Ben Black, et Alan Barrett.

Ce travail a été soutenu par la US National Science Foundation (allocation de recherche SCI-0427144) et DNS-OARC.

8. Références

8.1 Références normatives

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

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

[RFC1997] R. Chandra, P. Traina, T. Li, "Attribut Community de BGP", août 1996. *(P.S.)*

[RFC2439] C. Villamizar, R. Chandra, R. Govindan, "Élimination des oscillations de chemin dans BGP", novembre 1998. *(P.S.)*

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3704] F. Baker, P. Savola, "Filtrage d'entrée pour réseaux à rattachement multiples", mars 2004. (BCP0084) (*MàJ par* RFC8704)

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

8.2 Références pour information

[Allman2000] Allman, M. and E. Blanton, "On Making TCP More Robust to Packet Reordering", janvier 2000, <http://www.icir.org/mallman/papers/tcp-reorder-ccr.ps >.

[DNSMON] "RIPE NCC DNS Monitoring Services", <http://dnsmon.ripe.net/ >.

[Fomenkov2004] Fomenkov, M., Keys, K., Moore, D., and K. Claffy, "Longitudinal Study of Internet Traffic from 1999-2003", janvier 2004, <http://www.caida.org/outreach/papers/2003/nlanr/nlanr_overview.pdf >.

[ISC-TN-2003-1] Abley, J., "Hierarchical Anycast for Global Service Distribution", mars 2003, <http://www.isc.org/pubs/tn/isc-tn-2003-1.html >.

[ISC-TN-2004-1] Abley, J., "A Software Approach to Distributing Requests for DNS Service using GNU Zebra, ISC BIND 9 and FreeBSD", mars 2004, <http://www.isc.org/pubs/tn/isc-tn-2004-1.html >.

[McCreary2000] McCreary, S. and K. Claffy, "Trends in Wide Area IP Traffic Patterns: A View from Ames Internet Exchange", septembre 2000, <http://www.caida.org/outreach/papers/2000/AIX0005/AIX0005.pdf >.

[RFC1546] C. Partridge, T. Mendez, W. Milliken, "Service d'envoi à la cantonade pour les hôtes", novembre 1993. *(Info.)*

[RFC2267] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : combattre les attaques de déni de service qui utilisent le déguisement d'adresse de source IP", janvier 1998. (*Obsolète, voir* RFC2827) *(Information)*

[RFC2311] S. Dusse et autres, "Spécification de message S/MIME, version 2", mars 1998. *(Information)*

[RFC2821] J. Klensin, éditeur, "Protocole simple de transfert de messagerie", STD 10, avril 2001. *(Obsolète, voir* RFC5321)

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

[RFC3207] P. Hoffman, "Extension de service SMTP pour un SMTP sécurisé sur TLS", février 2002. *(P.S., MàJ par* RFC7817)

[RFC3765] G. Huston, "Communauté NOPEER pour le contrôle de portée de chemin du protocole de routeur frontière (BGP)", avril 2004. *(Information)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC5001] R. Austein, "Option d'identifiant de serveur de nom du DNS (NSID)", août 2007. *(P.S.)*

[RIS] "RIPE NCC Routing Information Service (RIS)", <http://ris.ripe.net >.

[ROUTEVIEWS] "University of Oregon Route Views Project", <http://www.routeviews.org/ >.

Adresse des auteurs

Joe Abley
Afilias Canada, Corp.
204 - 4141 Yonge Street
Toronto, ON M2P 2A8
Canada
téléphone : +1 416 673 4176
mél : jabley@ca.afilias.info
URI : http://afilias.info/

Kurt Erik Lindqvist
Netnod Internet Exchange
Bellmansgatan 30
118 47 Stockholm
Sweden

mél : kurtis@kurtis.pp.se
URI : http://www.netnod.se/

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF.