Groupe de travail Réseau
Request for Comments : 3834
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Moore
University of Tennessee
août 2004

Recommandations pour les réponses automatiques à la messagerie électronique

Statut du présent mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright
Copyright (C) The Internet Society (2004).

Résumé
Le présent mémoire fait des recommandations pour les logiciels qui répondent automatiquement aux messages électroniques entrants, incluant les générateurs de réponse "en déplacement" ou "en vacances", les logiciels de filtrage de messagerie, les services d'information fondés sur la messagerie électronique, et autres répondeurs automatiques. L'objet de ces recommandations est de décourager les comportements indésirables qui sont causés ou aggravés par de tels logiciels, d'encourager un comportement uniforme (lorsque c'est approprié) des répondeurs automatiques de messagerie, et de dissiper certaines sources de confusion parmi les mises en œuvre de répondeurs automatiques de messagerie.

1. Introduction

Il existe actuellement de nombreux programmes qui répondent automatiquement à la messagerie électronique. Bien que ces programmes varie largement par leurs fonctions, plusieurs problèmes ont été observés avec cette classe de programmes, incluant un nombre significatifs de réponses sans utilité ou involontaires, et des réponses envoyées à des adresses inappropriées, et l'incidence occasionnelle de boucles ou du mode "apprenti sorcier". Le présent mémoire recommande un comportement pour les programmes qui répondent automatiquement à la messagerie électronique afin de réduire le nombre de problèmes causés par de tels programmes.

(Note : le terme "mode apprenti sorcier" se définit comme une faute dans un protocole où, dans certaines circonstances, la réception d'un message cause l'envoi de multiples messages, dont chacun, lorsque reçu, déclenche la même faute.) (D'après [JARGON])

La portée du présent document se limite aux messages électroniques de l'Internet et beaucoup de ses recommandations sont spécifiquement destinées aux éléments de protocole et modèles de données utilisés dans les messages électroniques de l'Internet et les enveloppes de transport SMTP. L'utilisation de ces recommandations dans d'autres contextes de messagerie tels que la messagerie instantanée, les SMS ou Usenet n'a pas été envisagée et sort du domaine d'application du présent document.

1.1 Types de réponses automatiques

Il y a plusieurs types différents de réponses automatiques. Au moins deux types de réponses automatiques ont été définis dans des normes de l'IETF – Notifications d'état de livraison [RFC3464] qui sont destinées à faire rapport de l'état de la livraison d'un message par le système de transport de messages, et Notifications de disposition de message [RFC3798] qui sont destinées à faire rapport de la disposition d'un message après qu'il a atteint la boite aux lettres d'un destinataire. Ces réponses sont définies ailleurs et ne sont généralement pas dans le domaine visé par le présent document, sauf lorsque il recommande des cas spécifiques où ils devraient être ou non utilisés.

Les autres types de réponse automatique d'utilisation courante incluent :

- les avis "en déplacement" ou "en vacances", qui sont destinées à informer l'envoyeur d'un message que celui-ci a peu de chances d'être lu, ou de susciter une réaction, pendant un certain temps,

- les avis de "changement d'adresse", destinés à informer l'envoyeur d'un message que l'adresse du receveur qu'il a utilisé est obsolète et qu'une adresse différente devrait être utilisée à la place (que le message sujet ait été ou non transmis à l'adresse actuelle),

- les "défis", qui exigent de l'envoyeur d'un message qu'il montre une certaine compréhension et/ou volonté d'accepter certaines conditions avant que le message sujet soit délivré au receveur (souvent pour minimiser les effet de "pourriels" ou de virus sur le receveur),

- les services d'informations fondés sur la messagerie électronique, qui acceptent des demandes (provenant probablement de personnes) via la messagerie électronique, fournissent un service, et produisent aussi des réponses via la messagerie électronique. (Les listes de diffusion qui acceptent des demandes d'adhésion via la messagerie électronique entrent aussi dans cette catégorie),

- les servies d'informations similaires à ceux mentionnés ci-dessus sauf ceux qui sont destinés à accepter des messages provenant d'autres programmes, et

- diverses sortes de filtres de messagerie (incluant les "analyseurs de virus") qui agissent au nom d'un receveur pour altérer le contenu des messages avant de les transmettre à ce receveur, et produisent des réponses au cas où un message est altéré.

En reconnaissant la grande variété des types de réponses utilisées, ces recommandations distinguent entre plusieurs classes de répondeurs automatiques selon la partie ou le service au nom duquel agit le répondeur :

- Les "répondeurs de service" existent pour fournir l'accès à un certain service via des demandes et réponses par messagerie électronique. Ils sont associés en permanence à une ou plusieurs adresses de messagerie électronique, et lors d'un envoi à une telle adresse, l'envoyeur s'attend vraisemblablement à une réponse automatique. Un service de restitution de fichier fondé sur la messagerie électronique est un exemple de répondeur de service. Un service de calendrier qui permet de faire des demandes de rendez-vous par messagerie électronique, et qui répond à de telles demandes, serait un autre exemple de répondeur de service.

- Les "répondeurs personnels" existent pour faire des réponses automatiques au nom d'une seule adresse de receveur, en plus, ou à la place, de la lecture du message par le receveur. Ces répondeurs fonctionnent selon des critères spécifiés par le receveur lui-même. Le programme "vacation" de UNIX est un exemple de répondeur personnel. Un répondeur qui accepte des messages envoyés à une seule adresse, tente d'analyser et classer les contenus, et produit ensuite une réponse qui dépend de ce classement, est aussi un répondeur personnel.

- Les "répondeurs de groupe" existent pour faire des réponses automatiques au nom de tout ensemble significatif d'adresses de receveurs (disons tous les receveurs d'un domaine DNS particulier) avant, ou à la place d'une réponse du receveur réel. Les répondeurs de groupe sont similaires aux répondeurs personnels sauf que dans le cas d'un répondeur de groupe les critères de réponse ne sont pas établis receveur par receveur. Un programme "analyseur de virus" qui filtre tous les messages envoyés à un certain receveur sur un serveur particulier, et envoie des réponses lorsque un message a été rejeté ou livré sous une forme altérée, serait un exemple de répondeur de groupe.

Le comportement approprié pour un répondeur varie d'une classe à l'autre. Un comportement qui serait approprié pour un répondeur de service (où l'envoyeur s'attend à une réponse automatique) peut n'être pas approprié de la part d'un répondeur personnel. Par exemple, un répondeur de service peut envoyer une très longue réponse à une demande, ou une réponse qui n'est pas lisible par l'homme, selon les besoins de ce service. Cependant un répondeur personnel devrait supposer que c'est une personne qui va lire la réponse, et envoyer seulement de brèves réponses en clair.

1.2 Notation et définitions

Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "NON RECOMMANDÉ", et "PEUT" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

Le terme "message sujet" est utilisé pour se référer à un message qui cause l'envoi d'une réponse.

Le terme "réponse" se réfère à un message qui est automatiquement produit à réception d'un message sujet par un répondeur.

Un "répondeur" est un processus qui répond automatiquement aux messages sujets dans des conditions bien définies.

Sauf spécifié autrement, le terme "receveur" se réfère aux adresses de messagerie électronique auxquelles un message sujet a été livré (plutôt que, par exemple, l'adresse où la réponse a été envoyée). Une adresse de "receveur" peut être associée de façon permanente à un répondeur, ou peut être l'adresse d'une personne dans la messagerie est, dans certaines conditions, traitée par

un répondeur.

2. Quand envoyer (ne pas envoyer) des réponses automatiques

Un répondeur automatique NE DOIT PAS envoyer aveuglément une réponse à chaque message reçu. En pratique, il y a toujours des raisons pour refuser de répondre à certaines sortes de messages reçus, par exemple, pour la prévention des boucles, pour éviter de répondre aux "pourriels" ou virus, pour éviter d'être utilisé comme moyen de lancer ou d'amplifier des messages insultants, pour éviter de révéler de façon inappropriée des informations personnelles sur le receveur (par exemple, pour éviter une indication automatique qu'un receveur n'a pas lu ses messages récemment) et pour déjouer les attaques de déni de service contre le répondeur. Les critères pour décider de répondre ou non vont différer d'un répondeur à l'autre, selon l'objet du répondeur. En général, il faut veiller à éviter d'envoyer des réponses inutiles ou redondantes, et éviter de contribuer aux boucles de messages ou de faciliter les attaques de déni de service.

Voici quelques grandes lignes directrices générales :

- Les réponses automatiques NE DEVRAIENT PAS être produites en réponse à un message qui contient un champ d'en-tête Auto-Submitted (voir ci-dessous) lorsque ce champ a toute valeur autre que "no".

- Les réponses personnelles et de groupe qui sont destinées à notifier à l'envoyeur d'un message l'incapacité du receveur à lire ou répondre au message (par exemple, les notifications "en déplacement" ou "trop occupé") NE DEVRAIENT PAS produire la même réponse au même envoyeur plus d'une fois dans une période de plusieurs jours, même si cet envoyeur a envoyé plusieurs messages. Une période de sept jours est RECOMMANDÉE par défaut.

- Les réponses personnelles et de groupe dont l'objet est de notifier à l'envoyeur d'un message une absence temporaire du receveur (par exemple, les notices "en vacances" et "en déplacement") NE DEVRAIENT PAS être produites sauf si une adresse valide pour le receveur est explicitement incluse dans un champ de receveur (par exemple, To, Cc, Bcc, Resent-To, Resent-Cc, ou Resent-Bcc) du message sujet. Comme un receveur peut avoir plusieurs adresses transmises à la même boîte aux lettres, les receveurs DEVRAIENT être capables de spécifier au répondeur un ensemble d'adresses qu'il va reconnaître comme valides pour ce receveur.

Note: Le paragraphe 3.6.3 de la RFC2822 permet de varier les utilisations du champ Bcc, dont certaines permettaient à l'envoyeur du message sujet de spécifier explicitement l'adresse du receveur comme receveur "Bcc" sans qu'un champ Bcc apparaisse dans le message délivré, ou sans le champ Bcc dans le message délivré contenant l'adresse du receveur. Cependant, peut-être parce que les champs Bcc sont rarement utilisés, l'heuristique de ne pas répondre aux messages pour lesquels le receveur ne figure pas explicitement dans un champ d'en-tête To, CC, ou Bcc s'est trouvée bien fonctionner en pratique.

- Les répondeurs personnels et de groupe PEUVENT refuser de générer des réponses sauf à des correspondants ou adresses connus ou des individus "de confiance". Ces répondeurs PEUVENT aussi générer différentes sortes de réponses pour les adresses "de confiance" et à celles qui ne le sont pas. Cela peut être utile, par exemple, pour éviter des divulgations inappropriées d'informations personnelles à des adresses arbitraires.

- Les répondeurs NE DOIVENT PAS générer de réponse pour laquelle la destination de cette réponse serait une adresse nulle (par exemple, une adresse pour laquelle SMTP MAIL FROM ou Return-Path est <>) car la réponse ne serait pas livrée à une destination utile. Les répondeurs PEUVENT refuser de générer des réponses pour des adresses couramment utilisées comme adresses de retour par les répondeurs - par exemple, celles avec les parties locales correspondent à "owner-*", "*-request", "MAILER-DAEMON", etc. Les répondeurs sont encouragés à vérifier la validité de l'adresse de destination avant de générer la réponse, pour éviter de générer des réponses qui ne peuvent pas être livrées ou sont probablement inutiles.

- Afin d'éviter de répondre à des pourriels et à certaines formes d'attaques, les réponses automatiques de la part des répondeurs de service NE DEVRAIENT PAS être envoyées pour des demandes extrêmement mal formées. Cela peut inclure de vérifier que le message sujet a un type de contenu et un contenu appropriés à ce service.

- Comme la grande majorité de la messagerie électronique n'est pas authentifiée, et que les adresses de retour sont facilement falsifiées, pour éviter d'être utilisé comme moyen d'attaque de déni de service (c'est-à-dire, d'inonder les boîtes aux lettres de contenu indésirable) les répondeurs de service NE DEVRAIENT PAS retourner de grosses réponses (disons, de plus de quelques kilooctets) sans connaissance spécifique que la demande est en fait autorisée par la partie associée à l'adresse à laquelle la réponse va être envoyée. De même, les répondeurs de service NE DEVRAIENT PAS causer d'effets collatéraux indésirables (comme d'abonner l'envoyeur à une liste de diffusion) sans une assurance raisonnable que la demande était autorisée par la partie affectée.

Note : Comme chaque répondeur a un objet différent et qu'il peut être soumis à un ensemble de menaces potentielles différent , la question d'un moyen d'authentification particulier approprié pour un certain répondeur sort du domaine d'application du présent document.

- Un répondeur PEUT refuser d'envoyer une réponse à un message sujet qui contient un en-tête ou un contenu qui fait apparaître au répondeur qu'une réponse ne serait pas appropriée. Par exemple, si le message sujet contenait un champ d'en-tête Precedence [RFC2076] d'une valeur de "liste", le répondeur peut deviner que le trafic est arrivé d'une liste de diffusion, et ne va pas répondre si la réponse est seulement destinée à des messages personnels. Pour des raisons similaires, un répondeur PEUT ignorer tout message sujet avec un champ List-* [RFC2369]. (Parce que Precedence n'est pas un champ d'en-tête standard, et que son utilisation et son interprétation varie largement dans la réalité, aucun comportement particulier de répondeur en présence de Precedence n'est recommandé dans la présente spécification.)

3. Format des réponses automatiques

Les paragraphes qui suivent spécifient les détails du contenu des réponses automatiques, incluant l'en-tête du message de réponse, le contenu de la réponse, et l'enveloppe dans laquelle la réponse est transmise au système de transport de messagerie électronique.

3.1 En-tête de message

Les champs de l'en-tête de message devraient être réglés comme suit :

3.1.1 Champ From

Dans les correspondances entre personnes, le champ From sert à plusieurs objets : il identifie l'auteur du message (ou dans certains cas, la ou les parties au nom desquelles le message a été envoyé) et il est la destination par défaut des réponses des personnes. Malheureusement, certains systèmes de messagerie électronique envoient encore des rapports de non livraison et autres sortes de réponses automatiques à l'adresse From.

Pour les réponses automatiques, le rôle du champ From pour déterminer la destination des répliques à une réponse provenant d'une personne a moins d'importance, parce que dans la plupart des cas, il n'est pas utile ou approprié pour une personne (ou qui que ce soit) de répondre à une réponse automatique. L'exception est lorsque il y a un problème avec la réponse ; il devrait être possible de fournir un retour à la personne qui contrôle le répondeur.

Donc dans la plupart des cas, l'adresse From dans une réponse automatique doit être choisie selon les critères suivants :
- pour donner une indication de la partie ou de l'agent au nom duquel la réponse est envoyée,
- pour fournir une adresse à laquelle le receveur d'une réponse inappropriée peut demander que la situation soit corrigée, et
- pour diminuer le potentiel de messages en boucle.

Le comportement suivant est donc recommandé :

- Pour les réponses envoyés par des répondeurs de service, le champ From DEVRAIT contenir une adresse qui puisse être utilisée pour joindre le gestionnaire (humain) de ce service. La portion lisible par l'homme du champ From (le nom d'affichage précédant l'adresse) DEVRAIT contenir un nom ou une description du service pour l'identifier aux personnes.

- Pour les réponses envoyées par des répondeurs personnels, le champ From DEVRAIT contenir le nom du receveur du message sujet (c'est-à-dire, l'usager au nom duquel la réponse est envoyée) et une adresse choisie par le receveur du message sujet pour être reconnu par les correspondants. Ce sera souvent la même adresse qu'utilisée pour envoyer le message sujet à ce receveur. Dans le cas d'un receveur qui a plusieurs adresses de messagerie transmises sur la même boîte aux lettres (et répondeur) un répondeur personnel PEUT utiliser une heuristique pour deviner, sur la base des informations disponibles dans divers champs d'en-tête de message, laquelle de ces adresses pour ce receveur l'envoyeur aura vraisemblablement utilisé, et utiliser cette adresse dans le champ From de la réponse. Cependant il DOIT être possible à un receveur au nom duquel le répondeur agit de spécifier explicitement le nom et l'adresse lisibles par l'homme à utiliser dans les champs d'en-tête From des réponses.

Note : pour des raisons de confidentialité il peut être inapproprié que les répondeurs divulguent une adresse qui est déduite, par exemple, des informations d'amorçage du receveur (par exemple, le nom d'utilisateur POP ou IMAP ou un nom de compte sur un ordinateur multi utilisateurs) ou divulguent le nom spécifique de l'ordinateur lorsque la réponse a été générée. De plus, cela ne produit pas nécessairement une adresse de messagerie électronique publique valide pour le receveur. Pour cette raison, les répondeurs personnels DOIVENT permettre que le champ From d'une réponse

personnelle soit réglé par le receveur au nom duquel agit le répondeur.

- Pour les répondeurs de groupe, l'adresse From DEVRAIT contenir une adresse de messagerie électronique qui puisse être utilisée pour joindre le gestionnaire de répondeur de groupe. L'utilisation de l'adresse du Postmaster à cette fin est NON RECOMMANDÉE.

La portion lisible par l'homme de l'adresse From (la "phrase" avant l'adresse, voir le paragraphe 3.2.6 de la [RFC2822]) DEVRAIT contenir une indication de la fonction assumée par le répondeur de groupe et au nom duquel il opère (par exemple, "filtre de virus de l'agence Exemple").

3.1.2 Champ Reply-To

Si une réplique est attendue du répondeur, le champ Reply-To de la réponse DEVRAIT être réglé à l'adresse à laquelle la réplique est attendue, même si c'est l'adresse du même répondeur ou d'un autre. Les répondeurs qui demandent l'envoi d'une réplique aux répondeurs DOIVENT empêcher les messages en boucle et le mode apprenti sorcier. Noter que comme (conformément à la section précédente) le champ From de la réponse DEVRAIT contenir l'adresse d'une personne, si le champ Reply-To de la réponse est utilisé pour diriger les répliques sur un répondeur, elle ne sera pas la même que l'adresse du champ From.

Discussion : ceci suppose que l'agent d'utilisateur du receveur humain va normalement envoyer la réplique à l'adresse de Reply-To (si elle est présente) comme recommandé dans la [RFC0822] depuis 1982, mais il est encore possible qu'un receveur réponde à l'adresse From si il le trouve utile. Ceci est cohérent avec la destination de ces champs dans les [RFC0822] et [RFC2822].

3.1.3 Champ To

Le champ d'en-tête To DEVRAIT indiquer le receveur de la réponse. En général, il DEVRAIT y avoir seulement un receveur de toute réponse automatique. Cela minimise le potentiel de mode apprenti sorcier et les attaques de déni de service.

3.1.4 Champ Date

Le champ d'en-tête Date DEVRAIT indiquer la date et l'heure de génération de la réponse. Ceci NE DOIT PAS être pris comme l'indication de la date de livraison du message sujet, ni de l'heure à laquelle la réponse est envoyée.

3.1.5 Champ Subject

Le champ Subject DEVRAIT contenir une brève indication que le message est une réponse automatique, suivi par le contenu du champ Subject (ou une portion de celui-ci) du message sujet. Le préfixe "Auto:" PEUT être utilisé comme indication. Si il est utilisé, ce préfixe DEVRAIT être suivi par un caractère ASCII ESPACE (0x20).

Note : tout comme le préfixe "Re:" (dérivé du latin) qui est couramment utilisé pour indiquer des réponses générées par des personnes est parfois traduit dans d'autres langues par les agents d'utilisateur de messagerie, ou autrement interprété par les agents d'utilisateur de messagerie comme l'indication que le message est une réponse, le préfixe (grec) "Auto:" peut aussi être traduit ou utilisé comme indication générique que le message est une réponse automatique. Cependant l'indication "Auto:" est destinée seulement à aider les personnes à traiter le message. Le logiciel de traitement de messagerie NE DEVRAIT PAS supposer que la présence de "Auto:" au début d'un champ Subject est l'indication que le message a été soumis automatiquement.

Noter que le champ Subject du message sujet peut contenir des mots codés formatés conformément aux [RFC2047] et [RFC2231], et un tel texte PEUT être inclus dans le champ Subject d'une réponse. En générant des réponses qui contiennent de tels champs, il est rarement besoin de décoder et recoder un tel texte. Il est généralement suffisant de laisser ces mots codés comme ils sont dans le message sujet, en y ajoutant "Auto: " ou une autre indication. Cependant, il est quand même nécessaire de s'assurer qu'aucune ligne dans le champ Subject résultant qui contient un mot codé ne fait plus de 76 caractères ASCII (ceci se réfère à la forme codée, et non au nombre de caractères dans le texte codé). Aussi, si le répondeur tronque le champ Subject du message sujet, il est nécessaire d'éviter de tronquer le texte de Subject au milieu d'un mot codé.

3.1.6 Champs In-Reply-To et References

Les champs In-Reply-To et References DEVRAIENT être fournis dans l'en-tête d'un message de réponse si il y avait un champ Message-ID dans le message sujet, conformément aux règles du paragraphe 3.6.4 de la [RFC2822].

3.1.7 Champ Auto-Submitted

Le champ Auto-Submitted, avec la valeur de "auto-replied", DEVRAIT être inclus dans l'en-tête de message de toute réponse automatique. Voir la Section 5.

3.1.8 Champ Precedence

Une réponse PEUT inclure un champ Precedence [RFC2076] afin de décourager les réponses provenant de certaines sortes de répondeurs plus anciens que la présente spécification. Le corps de champ de Precedence PEUT consister en le texte "junk", "list", "bulk", ou autre texte réputé approprié par le répondeur. Parce que le champ Precedence est non standard et que son interprétation varie largement, l'utilisation de Precedence n'est pas spécifiquement recommandé par cette spécification, pas plus qu'elle ne recommande de valeur particulière pour ce champ.

3.2 Contenu de message

En général, les messages envoyés par des répondeurs personnels ou de groupe DEVRAIENT être brefs, et en format text/plain. Une construction multipart/alternative PEUT être utilisée pour communiquer des réponses en plusieurs langages, en particulier si ce faisant il est souhaitable d'utiliser plusieurs jeux de caractères.

Les messages de réponse NE DEVRAIENT PAS inclure de contenu significatif du message sujet. En particulier, les réponses personnelles et de groupe NE DEVRAIENT PAS contenir de contenu non textuel provenant du message sujet, et elles NE DEVRAIENT PAS inclure de pièces jointes du message sujet. Aucune de ces conditions ne s'applique aux répondeurs qui existent spécifiquement dans le but d'altérer ou traduire les contenus qui leur sont envoyés (par exemple, un traducteur de FORTRAN en C) ; cependant, de tels répondeurs DOIVENT employer des mesures pour éviter d'être utilisés comme moyen de lancer ou transmettre des contenus indésirables, comme les pourriels ou les virus.

Noter que lorsque du texte provenant du champ Subject ou un autre champ de l'en-tête du message sujet est inclus dans le corps de la réponse, il est nécessaire de décoder tous les mots codés qui apparaissent dans ces champs avant de les inclure dans le corps de message, et d'utiliser un type de contenu, jeu de caractères et codage de transfert de contenu appropriés. Dans certains cas, il peut être nécessaire de transposer du texte du jeu de caractères utilisé dans l'en-tête du message sujet dans le jeu de caractères utilisé dans le corps de la réponse. (Il est beaucoup plus facile de mettre en œuvre un répondeur si le texte de d'en-tête du message sujet n'a jamais besoin d'apparaître dans le corps de la réponse.)

3.2.1 Utilisation des DSN et MDN au lieu de cette spécification

En général, il est approprié d'utiliser les notifications d'état de livraison (DSN, *Delivery Status Notification*) pour les réponses qui sont générées par le système de transport de messagerie par suite de tentatives de relais, transmission, ou livraison de messages, et c'est seulement quand l'objet de cette réponse est de fournir à l'envoyeur du message sujet des informations sur l'état de cette livraison de message. Par exemple, un "analyseur de virus" qui est activé par un processus de livraison de messages pour filtrer les contenus dommageables avant de les livrer, pourrait retourner une DSN avec le champ Action réglé à "échec" avec un code d'état de 5.7.1 (Livraison non autorisée, message refusé) si le message entier n'a pas été livré pour des raisons de sécurité; ou il pourrait retourner une DSN avec le champ Action réglé à "relayé" ou "délivré" (comme approprié) avec un code d'état de 2.6.4 (conversion avec pertes effectuée) si le message a été relayé ou délivré avec le contenu présumé dommageable retiré. La spécification de DSN [RFC3464], plutôt que le présent document, gouverne la génération et le format des DSN.

De même, il est approprié d'utiliser les notifications de disposition de message (MDN, *Message Disposition Notification*) pour les seules réponses générées au nom du receveur, qui sont générées à la livraison ou après livraison à la boite aux lettres du receveur, et pour lesquelles l'objet de la réponse est d'indiquer la disposition du message. La spécification MDN [RFC3798], et non le présent document, gouverne la génération et le format des MDN.

Le présent document n'est pas destiné à modifier les spécifications DSN ou MDN. Les réponses qui rentrent dans les critères de DSN ou MDN sont définies par leur spécifications respectives, et elles devraient être générées conformément aux spécifications DSN ou MDN plutôt que par le présent document. Les réponses qui ne rentrent pas dans ces ensembles de critères devraient être générées conformément au présent document.

3.3 Enveloppe de message

L'adresse SMTP MAIL FROM, ou une autre adresse d'enveloppe retour utilisée pour envoyer le message, DEVRAIT être choisie de telle façon que cela rendre improbable la réalisation d'une boucle. Une boucle peut se produire, par exemple, si l'envoyeur et le receveur d'un message ont chacun un répondeur automatique - le répondeur du receveur envoie un message au répondeur de l'envoyeur, qui renvoie un message au répondeur du receveur.

Le principal objet de l'adresse MAIL FROM est de servir de destination aux messages d'état de livraison et autres réponses automatiques. Comme dans la plupart des cas, il n'est pas approprié de répondre à une réponse automatique, et que le répondeur n'est pas intéressé par la livraison des messages d'état, une adresse MAIL FROM de <> PEUT être utilisée à cette fin. Une adresse MAIL FROM qui est choisie spécifiquement dans le but d'envoyer des réponses automatiques, et qui ne va pas répondre automatiquement à tout message qui lui est envoyé, PEUT être utilisée à la place de <>.

L'adresse RCPT TO sera (bien sûr) l'adresse du receveur prévue de la réponse. Il est RECOMMANDÉ que le paramètre NOTIFY=NEVER de la commande RCPT soit spécifié si le serveur SMTP prend en charge l'option DSN [RFC3461].

4. Où envoyer les réponses automatiques (et où ne pas les envoyer)

En général, les réponses automatiques DEVRAIENT être envoyées *(à l'adresse indiquée)* au champ Return-Path si elles sont générées après la livraison. Si la réponse est générée avant la livraison, la réponse DEVRAIT être envoyée selon le champ reverse-path de la commande SMTP MAIL FROM, ou (dans un système non SMTP) à l'adresse d'enveloppe de retour qui sert de destination aux rapports de non livraison.

Si la réponse doit être générée après la livraison, et si il n'y a pas de champ Return-Path dans le message sujet, il y a une erreur de mise en œuvre ou de configuration dans le serveur SMTP qui a livré le message ou a fait la passerelle de sortie de SMTP pour le message. Un répondeur personnel ou de groupe NE DEVRAIT PAS livrer de réponse à toute adresse autre que celle du champ Return-Path, même si ce champ manque. Il vaut mieux régler le problème avec le système de livraison de la messagerie électronique que de s'appuyer sur une heuristique pour deviner la destination appropriée de la réponse. Une telle heuristique est connue pour avoir causé des problèmes.

Un répondeur de service PEUT livrer la réponse à la ou aux adresses du champ >From, ou à une autre adresse tirée de la charge utile de la demande, pourvu que ce comportement soit défini avec précision dans la spécification de ce service. Les répondeurs de services NE DEVRAIENT PAS utiliser le champ Reply-To à cette fin.

Le champ Reply-To NE DEVRAIT PAS être utilisé comme destination pour les réponses automatiques provenant de répondeurs personnels ou de groupes. En général, ce champ est réglé par la personne qui envoie sur la base de son anticipation de la façon dont le receveur humain va répondre au contenu spécifique de ce message. Par exemple, un envoyeur humain peut utiliser Reply-To pour demander que les réponses soient envoyées à toute une liste de diffusion. Même pour les répliques humaines, il y a des cas où il n'est pas approprié de répondre à l'adresse Reply-To, en particulier si l'envoyeur a demandé que les réponses soient envoyées à un groupe et/ou une liste de diffusion. Comme un répondeur personnel ou de groupe fonctionne au nom de la personne receveuse, il est plus sûr de supposer que tout champ Reply-To présent dans le message a été établi par la personne qui envoie dans l'hypothèse que toute réponse viendrait d'une personne qui comprendra les rôles de l'envoyeur et des autres receveurs. Un répondeur automatique manque des informations nécessaires pour comprendre ces rôles. L'envoi des réponses automatiques aux adresses Reply-To peut donc résulter en ce qu'un grand nombre de gens reçoivent des messages inutiles ou indésirables ; cela peut aussi contribuer à des messages en boucle.

L'utilisation du champ From comme destination pour les réponses automatiques a quelques uns des mêmes problèmes que celle de Reply-To. En particulier, le champ From peut énumérer plusieurs adresses, alors que les réponses automatiques ne devraient être envoyées qu'à une seule adresse. En général, les adresses From et Reply-To sont utilisées de diverses façons selon les circonstances, et c'est pour cette raison que les répondeurs personnels ou de groupe ne peuvent pas supposer de façon fiable qu'une adresse dans le champ From ou Reply-To est une destination appropriée pour la réponse. Pour ces raisons, le champ From NE DEVRAIT PAS être utilisé comme destination pour les réponses automatiques.

De même, le champ Sender NE DEVRAIT PAS être utilisé comme destination pour les réponses automatiques. Ce champ est seulement destiné à identifier la personne ou l'entité qui a envoyé le message, et il n'est pas obligé de contenir une adresse de réponse valide.

L'adresse Return-Path est réellement la seule parmi les en-têtes de message qu'on peut s'attendre à trouver qui selon le protocole, soit convenable pour les réponses automatiques qui n'ont pas été anticipées par l'envoyeur.

5. Champ d'en-tête Auto-Submitted

L'objet du champ d'en-tête Auto-Submitted est d'indiquer que le message a été généré par un processus automatique, ou un répondeur automatique, plutôt que par une personne ; et pour faciliter le filtrage automatique des messages provenant de chemins de signalisation pour lesquels les messages générés automatiquement et les réponses automatiques ne sont pas

souhaitables.

5.1 Syntaxe

La syntaxe de Auto-Submitted est la suivante, en utilisant la notation ABNF de la [RFC2234] :

auto-submitted-field = "Auto-Submitted:" [CFWS] auto-submitted [CFWS] CRLF

auto-submitted = ("no" / "auto-generated" / "auto-replied" / extension) opt-parameter-list

extension = jeton

opt-parameter-list = *([CFWS] ";" [CFWS] paramètre)

Les symboles "CFWS" et "CRLF" sont définis dans la [RFC2822]. Les symboles "jeton", et "paramètre" sont définis dans la [RFC2045] (telle qu'amendée par la [RFC2231]).

Le nombre maximum de champs Auto-Submitted qui peuvent apparaître dans un en-tête de message est de 1.

5.2 Sémantique

Le champ d'en-tête Auto-Submitted NE DEVRAIT PAS être fourni pour les messages qui ont été soumis manuellement par une personne. (Cependant, les agents d'utilisateur qui permettent aux envoyeurs de spécifier des champs arbitraires NE DEVRAIENT PAS empêcher les personnes d'établir le champ Auto-Submitted, parce que il est parfois utile pour les essais.)

Le mot clé auto-generated :
- DEVRAIT être utilisé sur les messages générés par des processus (souvent périodiques) automatiques (comme le "cron jobs" UNIX) qui ne sont pas des réponses directes à d'autres messages,
- NE DOIT PAS être utilisé sur des messages générés manuellement,
- NE DOIT PAS être utilisé sur un message produit dans une réponse directe à un autre message,
- NE DOIT PAS être utilisé pour marquer des notifications d'état de livraison (DSN) [RFC3464], ou des notifications de disposition de message (MDN) [RFC3798], ou d'autres rapports de (non) réception ou (non) livraison de message. Noter que certaines mises en œuvre largement diffusées de SMTP utilisent actuellement "auto-generated" pour étiqueter des rapports de non livraison. Ceci devrait être changé pour utiliser "auto-replied" à la place.

Le mot-clé auto-replied :
- DEVRAIT être utilisé sur des messages envoyés en réponse directe à un autre message par un processus automatique,
- NE DOIT PAS être utilisé sur des messages générés manuellement,
- PEUT être utilisé sur des notifications d'état de livraison (DSN) et des notifications de disposition de message (MDN),
- NE DOIT PAS être utilisé sur des messages générés par des processus automatiques ou périodiques, sauf pour les messages qui sont des réponses automatiques à d'autres messages.

Le mot clé "no" PEUT être utilisé pour indiquer explicitement qu'un message a été généré par une personne, si cela est trouvé approprié pour une raison quelconque.

Des mots clés d'extension pourront être définis à l'avenir, bien que cela semble improbable. La syntaxe et la sémantique de tels mots clés devront être publiées comme RFC et approuvées en utilisant le processus de consensus de l'IETF [RFC2434]. Les mots clés commençant par "x-" sont réservés aux expérimentations et utilisés entre des parties consentantes. Les receveurs de messages contenant un champ Auto-Submitted avec un mot clé autre que "no" PEUVENT supposer que le message n'a pas été soumis manuellement par une personne.

Des paramètres facultatifs peuvent aussi être définis par un processus de consensus de l'IETF. La syntaxe des paramètres facultatifs est donnée ici pour permettre une future définition si ils se révélaient nécessaires. Les mises en œuvre de Auto-Submitted qui se conforment à la présente spécification NE DOIVENT PAS échouer à reconnaître un champ Auto-Submitted et le mot clé qui contient des paramètres facultatifs syntaxiquement valides, mais de telles mises en œuvre PEUVENT ignorer ces paramètres si ils sont présents. Les noms de paramètres qui commencent par "x-" sont réservés aux expérimentations et sont utilisés entre des parties consentantes.

La construction syntaxique "commentaire" de la [RFC2822] peut être utilisée pour indiquer la raison pour laquelle ce message a fait l'objet d'une soumission automatique.

6. Considérations sur la sécurité

Les répondeurs automatiques introduisent un potentiel pour plusieurs sortes d'attaques, incluant :
- l'utilisation de ces répondeurs pour relayer un contenu dommageable ou offensant (vers, virus, pourriels, et mouchards) dans le but d'une plus large distribution du contenu ou de masquer la source de ce contenu ;
- l'utilisation de ces répondeurs pour monter des attaques de déni de service en utilisant les répondeurs pour relayer les messages à de grands nombres d'adresses, ou pour inonder des boîtes aux lettres individuelles de grandes quantités de contenus indésirables, ou les deux ;
- l'utilisation délibérée ou accidentelle de ces répondeurs pour construire des boucles de messages ou le "mode de l'apprenti sorcier", taxant ainsi les ressources du système de transport de la messagerie ;
- l'utilisation de ces répondeurs pour déterminer si les adresses de receveurs sont valides, en particulier lorsque de telles informations ne sont pas fournies autrement (par exemple, les réponses aux commandes SMTP RCPT ou VRFY) et ne sont pas destinées à être divulguées ;
- l'utilisation de tels répondeurs pour obtenir des informations personnelles sur les receveurs, incluant des informations sur les utilisations récentes par le receveur de sa boîte aux lettres ou ses activités récentes ;
- de plus, le répondeur lui-même peut être soumis à attaque par l'envoi d'un grand nombre de demandes.

Le présent document tente de réduire la vulnérabilité des répondeurs à de telles attaques, en particulier en
- recommandant que les répondeurs ne relayent pas de contenu significatif du message sujet (minimisant ainsi le potentiel d'utilisation des répondeurs pour lancer ou amplifier un contenu choisi par l'attaquant) ;
- recommandant que les répondeurs marquent clairement les réponses avec le champ d'en-tête "Auto-Submitted: auto-replied" pour les distinguer des messages générés par des personnes (en partie, pour minimiser le potentiel de boucles et d'attaques de déni de service),
- recommandant que les répondeurs personnels et de groupe limitent le nombre de réponses envoyées à un individu par période de temps (limitant aussi les dommages potentiels causés par des boucles),
- recommandant que les répondeurs répondent au plus à une adresse par message entrant (pour minimiser le potentiel de déni de service délibéré ou accidentel via la "multiplication" ou le mode apprenti sorcier),
- recommandant que les réponses des répondeurs personnels et de groupe soient brèves et en clair (pour minimiser la possibilité que les répondeurs de messagerie soient utilisés comme mécanisme de transmission de contenus dommageables et/ou de déguiser la source du contenu dommageable).

Cependant, comme il est facile de falsifier les adresses de messagerie, des attaques sont encore possibles pour tout répondeur de messagerie qui ne limite pas l'accès et n'exige pas l'authentification avant de produire une réponse. Les mesures ci-dessus tentent de limiter les dommages qui peuvent être faits, mais elles ne peuvent pas entièrement empêcher les attaques.

Cette section décrit les vulnérabilités inhérentes à la réponse automatique à la messagerie. D'autres vulnérabilités sont associées à certains services fondés sur la messagerie qui répondent automatiquement aux messages électroniques, mais elles ne sont pas causées par le fait que le serveur répond automatiquement aux messages entrants. En général, tout service fondé sur le réseau (incluant ceux auxquels on accède par messagerie) ont besoin de fournir une sécurité qui est suffisante pour empêcher le service d'être utilisé comme moyen d'accéder de façon inappropriée ou destructive aux ressources accessibles par le service.

Il a aussi été noté que les répondeurs personnels et de groupe divulguent parfois de façon inappropriée les informations personnelles des receveurs. Cela peut se faire automatiquement (comme quand un répondeur de groupe fournit automatiquement le numéro de téléphone personnel ou mobile du receveur comme information de contact de remplacement) ou "manuellement". Les informations générées automatiquement NE DEVRAIENT PAS inclure des informations personnelles sur le receveur qui ne seraient pas déjà connues, ou facilement disponibles, de l'envoyeur du message sujet. Les interfaces d'utilisateur qui permettent aux receveurs de fournir un texte de réponse DEVRAIENT dire clairement à l'utilisateur que ces informations seront disponibles non seulement aux collègues locaux, mais aussi à l'Internet tout entier, incluant de potentiels agresseurs.

7. Exemple : programme de vacances

Cette section illustre comment ces recommandations peuvent s'appliquer à un hypothétique programme "vacances" qui a pour objet de répondre à la messagerie d'un seul receveur durant les périodes dans lesquelles le receveur est occupé ou absent et dans l'incapacité de répondre personnellement. Ceci n'est qu'aux fins d'illustration et n'est pas un élément normatif de ce document.

Le programme vacances est un répondeur personnel.

Le programme vacances refuse de répondre à tout message qui :

- paraît être un pourriel (par exemple, si il a été marqué comme publicité par l'envoyeur ou comme pourriel potentiel par un intermédiaire),
- paraît contenir un virus (par exemple, si il contient une pièce jointe exécutable),
- contient un champ d'en-tête Auto-Submitted,
- a reçu une réponse dans les sept dernier jours,
- ne contient pas une des adresses du receveur dans un champ To, CC, Bcc, Resent-To, Resent-CC, ou Resent-Bcc,
- contient un champ Precedence d'une valeur de "list", "junk", ou "bulk",
- n'a pas d'adresse de Return-Path, ou
- a une adresse de Return-Path de <>, ou une adresse de Return-Path d'une forme fréquemment utilisée par des rapports de non livraison.

Le format de la réponse vacances est le suivant :
- Le champ d'en-tête From est réglé à un nom et une adresse de messagerie spécifiés par l'usager au nom duquel les réponses sont envoyées. (Sur certains systèmes, il peut être raisonnable d'avoir un réglage par défaut pour le champ From des réponses de vacances qui se fonde sur le nom de compte de l'usager et le nom de domaine du système.)
- Le champ Reply-To n'est établi que si il est explicitement configuré par l'usager au nom duquel les réponses sont envoyées. Par exemple, un usager peut diriger les réponses sur un secrétariat ou un camarade de travail à qui a été déléguée la tâche de traiter les affaires importantes durant son absence.
- Le champ To contient l'adresse du receveur de la réponse, telle qu'obtenue du champ Return-Path du message sujet.
- Le champ Date contient la date et l'heure de génération de la réponse.
- Le champ Subject contient Auto: suivi par une chaîne choisie par l'usager au nom duquel les réponses sont envoyées. Un réglage par défaut de quelque chose comme "loin de ma messagerie" peut être approprié. Si le champ Subject contient des caractères non ASCII, ils seront codés conformément à la [RFC2047].
- Les champs In-Reply-To et References sont générés à partir du message sujet selon la [RFC2822].
- Le champ Auto-Submitted a la valeur "auto-replied".
- Le corps de message contient un texte spécifié par l'usager au nom duquel la réponse est envoyée. Un bref sommaire du message sujet est aussi inclus, consistant en From, To, Subject, Date, et quelques lignes de texte de message tiré du message sujet. Aucune pièce jointe ou partie de corps non textuelle n'est incluse dans la réponse.

L'adresse SMTP MAIL FROM de l'enveloppe de message est <>. L'adresse RCPT TO dans l'enveloppe de message est l'adresse de l'usager auquel la réponse est envoyée. NOTIFY=NEVER est aussi établi dans la ligne RCPT TO si c'est permis par le serveur SMTP.

8. Considérations relatives à l'IANA

La Section 5 de ce document définit deux nouveaux mécanismes d'extension – de nouveaux mots clés pour le champ d'en-tête Auto-Submitted, et de nouveaux paramètres facultatifs pour le champ Auto-Submitted. Si à l'avenir de nouveaux mots clés ou paramètres étaient approuvés (par le processus de consensus de l'IETF) il pourrait être approprié que l'IANA crée un registre de ces mots clés ou paramètres.

9. Remerciements

Dans le milieu des années 1990, Jeroen Houttuin de TERENA a rédigé une série de projets Internet sur le "Comportement des serveurs de messagerie", et en particulier, un document sur les "serveurs répondeurs". Bien que ces documents n'aient jamais (à la connaissance de l'auteur) été formellement publiés, ils ont fourni le premier argument bien raisonné (connu de l'auteur) sur la meilleure façon pour que de tels serveurs assurent l'interface avec les systèmes et protocoles de messagerie électronique.

L'idée du champ Auto-Submitted vient du système de messagerie X.400/MHS [X420]. La [RFC2156] définissait un champ "Autosubmitted" à utiliser lors du passage entre la messagerie X.400 et Internet. Jacob Palme a écrit un projet Internet définissant l'utilisation du champ "Auto-Submitted" pour la messagerie Internet, qui est parvenu jusqu'au dernier appel sans objections significatives, mais s'est fait recaler en tentant de résoudre des objections non substantielles. La définition de Auto-Submitted dans le présent document est dérivée (c'est-à-dire, légèrement simplifiée) de celle de ce document, avec des emprunts à son texte.

Des remerciements sont aussi dus à ceux qui ont contribué par des suggestions au présent document : Russ Allbery, Adam Costello, Ned Freed, Lawrence Greenfield, Arnt Gulbrandsen, Eric Hall, Tony Hansen, Vivek Khera, Dan Kohn, Bruce Lilly, Charles Lindsey, der Mouse, Lyndon Nerenberg, Richard Rognlie, Markus Stumpf, Florian Weimer, et Dan Wing.

10. Références

10.1 Références normatives

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par* 2184, 2231, 5335.)

[RFC2047] K. Moore, "MIME (Extensions de messagerie Internet multi-objets) Partie trois : extensions d'en-tête de message pour texte non ASCII", novembre 1996. (*MàJ par* RFC2184, RFC2231) *(D.S.)*

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

[RFC2231] N. Freed, K. Moore, "Extensions MIME Valeur de paramètre et Mot codé : jeux de caractères, langages, et continuations", novembre 1997. *(P.S.)*

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822, STD 11, Remplacée par RFC5322)

[RFC3461] K. Moore, "Extension de service du protocole simple de transfert de messagerie (SMTP) pour les notifications d'état de livraison (DSN)", janvier 2003. (*MàJ par* RFC3798, RFC3885, RFC5337, RFC6533) *(D.S.)*

10.2 Références pour information

[JARGON] "Sorcerer's apprentice mode", à l'origine d'après le fichier Jargon tenu par le MIT-AI et SAIL ; maintenant collecté en divers endroits de la Toile. Voir par exemple, http://www.jargon.net/

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC2076] J. Palme, "En-têtes communs de message Internet", février 1997. *(Information)*

[RFC2156] S. Kille, "MIXER (Relais amélioré Mime Internet X.400) : transposition entre X.400 et la RFC0822/MIME ", janvier 1998. *(Remplace* RFC0987, RFC1026, RFC1138, RFC1148, RFC1327, RFC1495) *(MàJ* RFC0822) *(P.S.)*

[RFC2369] G. Neufeld, J. Baer, "Utilisation des URL comme méta syntaxe pour les commandes centrales de liste de messagerie et leur transport à travers les champs d'en-tête de message", juillet 1998. *(P.S.)*

[RFC3464] K. Moore, G. Vaudreuil, "Format extensible de message pour les notifications d'état de livraison", janvier 2003. (*MàJ par* RFC4865, RFC5337, RFC6533) *(D.S.)*

[RFC3798] T. Hansen et G. Vaudreuil, éd., "Notification de disposition de message", mai 2004. (*MàJ par* RFC5337, RFC6533) *(D.S.)*

[X420] Recommandation UIT-T X.420 (1992). "Technologies de l'information – Systèmes de traitement de message (MHS) : système de messagerie interpersonnelle".

Adresse de l'auteur

Keith Moore
Innovative Computing Laboratory
University of Tennessee, Knoxville
1122 Volunteer Blvd, #203
Knoxville, TN 37996-3450
USA
mél : moore@cs.utk.edu

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle
L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org .

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