Groupe de travail Réseau
Request for Comments : 2821
RFC rendues obsolètes : 821, 974, 1869
RFC mises à jour : 1123
Catégorie : Sur la voie de la normalisation

J. Klensin, éditeur
AT&T Laboratories
avril 2001

Traduction Claude Brière de L'Isle

Protocole simple de transfert de messagerie

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

Résumé

Le présent document est une spécification complète du protocole de base de transport de messagerie électronique Internet. Il consolide, met à jour et précise, mais n'ajoute aucune nouvelle fonctionnalité ni ne change une fonctionnalité existante :
- de la spécification SMTP (protocole simple de transfert de messagerie) originale de la RFC 821 [30],
- des exigences et implications du système de nom de domaine pour le transport de messagerie des RFC 1035 [22] et 974 [27],
- des précisions et déclarations d'applicabilité de la RFC 1123 [2], et
- des matériaux tirés des mécanismes d'extension SMTP [19].

Il rend obsolètes les RFC 821 et RFC 974, et met à jour la RFC 1123 (il remplace les matériaux de transport de messagerie de la RFC 1123). Cependant, la RFC 821 spécifie quelques dispositifs qui n'avaient pas une utilisation significative dans l'Internet vers le milieu des années 1990 et (dans les appendices) des modèles de transport supplémentaires. Ces sections sont omises ici pour des raison de clarté et de brièveté ; les lecteurs qui en ont besoin se reporteront à la RFC 821.

Il comporte aussi des éléments supplémentaires provenant de la RFC 1123 et qui nécessitent quelques développements. Ces éléments ont été identifiés de plusieurs façons, surtout par des échanges d'idées sur diverses listes de diffusion et groupes de nouvelles et des problèmes de compréhension ou d'interprétation qui sont apparus lors du déploiement des extensions SMTP. Lorsque la présente spécification va au-delà de la simple consolidation et diffère effectivement des documents précédents, elle se substitue à eux techniquement aussi bien que textuellement.

Bien que SMTP ait été conçu comme protocole de transport et livraison de messagerie, la présente spécification contient aussi des informations qui sont importantes pour son utilisation comme protocole de "présentation de messagerie", tel que recommandé pour POP [3], [26] et IMAP [6]. Des questions supplémentaires de présentation sont exposées dans la RFC 2476 [15].

Le paragraphe 2.3 donne des définitions des termes spécifiques du présent document. Excepté lorsque la terminologie historique est nécessaire pour la précision, le présent document utilise la terminologie actuelle de "client" et "serveur"' pour identifier respectivement le processus d'envoi et de réception SMTP.

Un document voisin [32] discute des en-têtes de message, des corps et formats de message et de leurs structures, et leurs relations.

Table des matières

1 Introduction

L'objectif du protocole simple de transfert de messagerie (SMTP, *Simple Mail Transfer Protocol*) est de transférer la messagerie de façon fiable et efficace. SMTP est indépendant du sous système particulier de transmission et n'exige qu'un canal de flux de données ordonnées fiable. Alors que le présent document expose spécifiquement le transport sur TCP, d'autres modes de transport sont possibles. Les appendices à la RFC 821 en décrivent plusieurs.

Une caractéristique importante de SMTP est sa capacité à transporter la messagerie à travers les réseaux, appelée habituellement le "relais de messagerie SMTP" (voir au paragraphe 3.8). Un réseau consiste en hôtes TCP mutuellement accessibles sur l'Internet public, en hôtes mutuellement accessibles par TCP sur un Intranet TCP/IP isolé par un pare-feu, ou en hôtes dans un autre environnement de LAN ou WAN qui utilise un protocole de niveau transport non TCP. En utilisant SMTP, un processus peut transférer de la messagerie à un autre processus sur le même réseau ou à un autre réseau via un processus de relais ou de passerelle accessible aux deux réseaux.

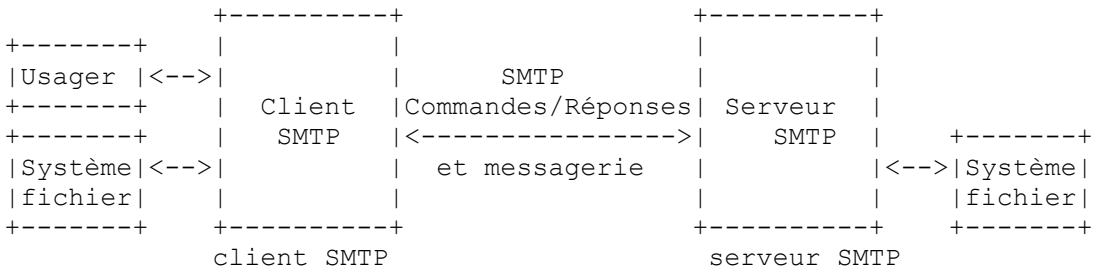
De cette façon, un message électronique peut passer à travers un certain nombre d'hôtes relais ou passerelles intermédiaires

sur son chemin de l'envoyeur au receveur ultime. Le mécanisme d'échange de messagerie du système de nom de domaine [22], [27] (et de la section 5 du présent document) est utilisé pour identifier le prochain bond de destination approprié pour un message transporté.

2 Le modèle SMTP

2.1 Structure de base

Le concept SMTP peut être figuré comme suit :



Lorsqu'un client SMTP a un message à transmettre, il établit un canal de transmission bidirectionnel avec un serveur SMTP. La responsabilité d'un client SMTP est de transférer les messages électroniques à un ou plusieurs serveurs SMTP, ou rapporter l'échec de ce transfert.

Les moyens par lesquels un message électronique est présenté à un client SMTP, et la façon dont ce client détermine le ou les noms de domaine auxquels les messages sont à transférer sont une affaire locale, et ne sont pas examinés dans le présent document. Dans certains cas, le ou les noms de domaine transférés à, ou déterminés par, un client SMTP vont identifier la ou les destinations finales du message. Dans d'autres cas, courants lorsque les clients SMTP sont associés aux mises en œuvre des protocoles POP [3], [26] ou IMAP [6], ou lorsque le client SMTP est à l'intérieur d'un environnement de service de transport isolé, le nom de domaine déterminé va identifier une destination intermédiaire à travers laquelle tous les messages vont être relayés. Les clients SMTP qui transfèrent tout le trafic, sans considération des noms de domaine cibles associés aux messages individuels, ou qui n'entretiennent pas de files d'attente pour réessayer les transmissions de message qui n'ont pu être achevées initialement, peuvent par ailleurs se conformer à la présente spécification mais ne sont pas considérés comme en étant pleinement capables. Les mises en œuvre SMTP de pleine capacité, y compris les relais utilisés par celles de moindre capacité, et leurs destinations, sont supposées prendre aussi en charge toute la mise en file d'attente, le réessai, et les fonctions d'adresse de remplacement exposées dans la présente spécification.

Les moyens par lesquels un client SMTP, une fois qu'il a déterminé un nom de domaine cible, détermine l'identité d'un serveur SMTP auquel doit être transférée une copie d'un message, puis effectue ce transfert, sont traités par le présent document. Pour effectuer un transfert de messagerie à un serveur SMTP, un client SMTP établit un canal de transmission bidirectionnel avec ce serveur SMTP. Un client SMTP détermine l'adresse d'un hôte approprié qui fait fonctionner un serveur SMTP en résolvant un nom de domaine de destination soit à un hôte échangeur de messagerie intermédiaire soit un hôte cible final.

Un serveur SMTP peut soit être la destination ultime soit un "relais" intermédiaire (c'est-à-dire qu'il peut assumer le rôle d'un client SMTP après la réception du message) ou "passerelle" (c'est-à-dire qu'il peut transporter plus loin le message en utilisant un protocole autre que SMTP). Les commandes SMTP sont générées par le client SMTP et envoyées au serveur SMTP. Les réponses SMTP sont envoyées du serveur SMTP au client SMTP en réponse aux commandes.

En d'autres termes, le transfert de message peut survenir dans une seule connexion entre l'envoyeur SMTP original et le receveur SMTP final, ou peut intervenir dans une série de bonds à travers les systèmes intermédiaires. Dans les deux cas, un passage formel de la responsabilité du message survient : le protocole exige qu'un serveur accepte la responsabilité soit de livrer un message, soit de rapporter de façon appropriée l'échec de la livraison.

Une fois le canal de transmission établi et la prise de contact initiale terminée, le client SMTP initie normalement une transaction de messagerie. Une telle transaction consiste en une série de commandes pour spécifier l'origine et la destination du message et la transmission du contenu du message (y compris tous les en-têtes ou autres structures) lui-même. Lorsque le même message est envoyé à plusieurs receveurs, ce protocole recommande la transmission d'une seule

copie des données pour tous les receveurs du même hôte de destination (ou relais intermédiaire).

Le serveur répond à chaque commande par une réponse ; les réponses peuvent indiquer que la commande a été acceptée, que des commandes supplémentaires sont attendues, ou qu'une condition d'erreur temporaire ou permanente existe. Les commandes qui spécifient l'envoyeur ou les receveurs peuvent inclure des demandes d'extension de service SMTP permises par le serveur comme exposé au paragraphe 2.2. Le dialogue est délibérément en mode rigide, un à la fois, bien que ceci puisse être modifié d'accord mutuel par des demandes d'extension comme l'intubation de commandes [13].

Une fois qu'un message donné a été transmis, le client peut demander que la connexion soit close ou peut initier d'autres transactions de messagerie. De plus, un client SMTP peut utiliser une connexion avec un serveur SMTP pour des services auxiliaires tels que la vérification des adresses de courrier électronique ou la restitution d'adresses d'abonnés à des listes de diffusion.

Comme suggéré plus haut, le présent protocole fournit des mécanismes pour la transmission de courrier. Cette transmission survient normalement directement à partir de l'hôte de l'utilisateur qui envoie vers l'hôte de l'utilisateur qui reçoit lorsque les deux hôtes sont connectés au même service de transport. Lorsqu'ils ne sont pas connectés au même service de transport, la transmission se fait via un ou plusieurs serveurs relais SMTP. Un hôte intermédiaire qui agit comme relais SMTP ou comme passerelle vers un autre environnement de transmission est habituellement choisi grâce à l'utilisation du mécanisme d'échange de messagerie (MX, *Mail Exchanger*) du service de nom de domaine (DNS).

Normalement, les hôtes intermédiaires sont déterminés via l'enregistrement MX DNS, et non par un acheminement explicite de "source" (voir la section 5 et les appendices C et F.2).

2.2 Modèle d'extension

2.2.1 Fondements

Grâce à un effort débuté en 1990, approximativement dix ans après l'achèvement de la RFC 821, le protocole a été modifié par un modèle "d'extensions de service" qui permettent au client et au serveur de se mettre d'accord pour utiliser des fonctionnalités partagées allant au-delà des exigences originales de SMTP. Le mécanisme d'extension SMTP définit les moyens qui permettent à un client et un serveur SMTP étendus de se reconnaître l'un l'autre, et le serveur peut informer le client des extensions de service qu'il prend en charge.

Les mises en œuvre SMTP contemporaines DOIVENT accepter les mécanismes de base d'extension. Par exemple, les serveurs DOIVENT accepter la commande EHLO même si ils ne mettent en œuvre aucune extension spécifique et les clients DEVRAIENT utiliser de préférence EHLO plutôt que HELO. (Cependant, pour la compatibilité avec les mises en œuvre conformes plus anciennes, les clients et les serveurs SMTP DOIVENT accepter les mécanismes du HELO original comme position de repli.) Sauf lorsque les différentes caractéristiques de HELO doivent être identifiées pour les besoins de l'interopérabilité, le présent document ne discute que de EHLO.

SMTP est largement développé et des mises en œuvre de grande qualité se sont révélées très robustes. Cependant, la communauté de l'Internet estime maintenant que certains services importants n'ont pas été prévus lors de la conception du protocole. Si la prise en charge de ces services doit se faire, cela doit être d'une façon qui permette aux plus anciennes mises en œuvre de continuer de fonctionner d'une façon acceptable. Le cadre d'extension consiste en :
- la commande SMTP EHLO, qui se substitue à l'ancien HELO,
- un registre des extensions de service SMTP,
- des paramètres supplémentaires pour les commandes SMTP MAIL et RCPT, et
- des remplacements facultatifs pour les commandes définies dans ce protocole, comme pour DATA dans les transmissions non-ASCII [33].

La force de SMTP vient principalement de sa simplicité. L'expérience de nombreux protocoles a montré que les protocoles avec peu d'options tendent à l'omniprésence, alors que les protocoles avec de nombreuses options rentrent dans l'obscurité.

Chacune de ces extension, indépendamment de ses avantages, doit être soigneusement évaluée au regard de ses coûts de mise en œuvre, développement, et interopérabilité. Dans de nombreux cas, le coût de l'extension du service SMTP sera vraisemblablement supérieur aux avantages retirés.

2.2.2 Définition et enregistrement des extensions

L'IANA tient un registre des extensions de service SMTP. Une valeur de EHLO correspondante est associée à chaque

extension. Chaque extension de service enregistrée auprès de l'IANA doit être définie dans un document formel de protocole expérimental en cours de normalisation ou approuvé par l'IESG. La définition doit comporter :

- le nom textuel de l'extension de service SMTP ;
- la valeur du mot clé EHLO associé à l'extension ;
- la syntaxe et les valeurs possibles des paramètres associés à la valeur du mot clé EHLO ;
- tout verbe SMTP supplémentaire associé à l'extension (les verbes supplémentaires auront habituellement, sans y être obligés, la même valeur que celle du mot clé EHLO) ;
- tout nouveau paramètre que l'extension associe aux verbes MAIL ou RCPT ;
- une description de la façon dont la prise en charge de l'extension affecte le comportement du serveur et client SMTP ;
- l'incrément avec lequel l'extension augmente la longueur maximum des commandes MAIL et/ou RCPT, au delà de ce qui est spécifié dans la présente norme.

De plus, toute valeur de mot clé EHLO commençant par un "X" majuscule ou minuscule se réfère à une extension de service SMTP locale utilisée exclusivement par accord bilatéral. Les mots clé commençant par "X" NE DOIVENT PAS être utilisés dans une extension de service enregistrée. Au contraire, les valeurs de mot clé présentées dans la réponse EHLO qui ne commencent pas par "X" DOIVENT correspondre à une extension de service SMTP expérimentale normalisée, en cours de normalisation, ou approuvée par l'IESG, et enregistrée auprès de l'IANA. Un serveur conforme NE DOIT PAS offrir de valeurs de mot clé préfixées par autre chose que "X" qui ne soient pas décrites dans une extension enregistrée.

Les verbes et noms de paramètres supplémentaires sont liés par les mêmes règles que les mots clé EHLO ; en particulier, les verbes commençant par "X" sont des extensions locales qui peuvent n'être pas enregistrées ou normalisées. Au contraire, les verbes qui ne commencent pas par "X" doivent toujours être enregistrés.

2.3 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit ci-dessous :

1. DOIT : ce mot, ou les termes "EXIGE" ou "DEVRA", signifie que la définition est une exigence absolue de la spécification.

2. NE DOIT PAS : cette phrase, ou la phrase "NE DEVRA PAS", signifie que la définition est une interdiction absolue de cette spécification.

3. DEVRAIT : ce mot, ou l'adjectif "RECOMMANDÉ", signifie qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer un élément particulier, mais que les pleines implications doivent en être comprises et soigneusement pesées avant de faire un choix différent.

4. NE DEVRAIT PAS : cette phrase, ou la phrase "NON RECOMMANDÉ" signifie qu'il peut exister des raisons valides dans des circonstances particulières où le comportement particulier est acceptable ou même utile, mais que les pleines implications doivent en être comprises et soigneusement pesées avant de mettre en œuvre tout comportement décrit avec cette mention.

5. PEUT : ce mot, ou l'adjectif "FACULTATIF", signifie qu'un élément est vraiment facultatif. Un fabricant peut choisir d'inclure l'élément parce qu'un marché particulier l'exige ou parce que le fabricant estime que cela améliore son produit, alors qu'un autre fabricant peut omettre le même élément. Une mise en œuvre qui n'inclut pas une option particulière DOIT être prête à interopérer avec une autre mise en œuvre qui l'inclut, bien que peut-être avec des fonctionnalités réduites. De la même façon, une mise en œuvre qui n'inclut pas une option DOIT être prête à interopérer avec une autre mise en œuvre qui ne l'inclut pas (sauf bien sûr, la caractéristique fournie par l'option.)

2.3.1 Objets de messagerie

SMTP transporte un objet de messagerie. Un objet de messagerie contient une enveloppe et un contenu.

L'enveloppe SMTP est envoyée comme une série d'unités de protocole SMTP (décrites à la Section 3). Elle consiste en une adresse d'origine (à laquelle devraient être envoyés les rapports d'erreur) ; une ou plusieurs adresses de réception ; et du matériel d'extension de protocole facultatif. Historiquement, des variantes de la commande de spécification d'adresse de réception (RCPT TO) pourraient être utilisées pour spécifier des mode de livraison de remplacement, comme l'affichage

immédiat ; ces variantes sont maintenant déconseillées (voir au paragraphe F.6).

Le contenu SMTP est envoyé dans l'unité de protocole SMTP DATA et a deux parties : les en-têtes et le corps. Si le contenu se conforme aux autres normes contemporaines, les en-têtes forment une collection de paires champ/valeur structurées comme dans la spécification de format de message [32] ; le corps, s'il est structuré, est défini conformément à MIME [12]. Le contenu est textuel par nature, exprimé en utilisant le répertoire US-ASCII [1]. Bien que les extensions SMTP (comme "8BITMIME" [20]) puissent assouplir cette restriction pour le corps du contenu, les en-têtes du contenu sont toujours codés en utilisant le répertoire US-ASCII. Une extension MIME [23] définit un algorithme de représentation des valeurs d'en-tête en-dehors du répertoire US-ASCII, tout en les codant toujours à l'aide de ce répertoire.

2.3.2 Envoyeurs et receveurs

Dans la RFC 821, les deux hôtes qui participent à une transaction SMTP étaient décrits comme "envoyeur SMTP" et "receveur SMTP". Ce document a été modifié pour refléter la terminologie actuelle de l'industrie et se réfère donc à eux comme respectivement le "client SMTP" (ou parfois juste "le client") et le "serveur SMTP" (ou juste "le serveur"). Comme un hôte donné peut agir à la fois comme serveur et client dans une situation de relais, la terminologie "receveur" et "envoyeur" est toujours utilisée lorsque c'est nécessaire à la clarté du texte.

2.3.3 Agents de messagerie et mémorisation de message

Une terminologie supplémentaire des systèmes de messagerie est devenue courante après la publication de la RFC 821 et, lorsque c'est utile, elle est utilisée dans la présente spécification. En particulier, les serveurs et clients SMTP fournissent un service de transport de messagerie et agissent donc comme "Agents de transfert de messagerie" (MTA, *Mail Transfer Agent*). Les "agents d'utilisateur de messagerie" (MUA ou UA, *Mail User Agent*) sont normalement vus comme les sources et cibles du courrier. À la source, un MUA peut collecter la messagerie à transmettre en provenance d'un utilisateur et la passer à un MTA ; le MTA final ("livreur") serait vu comme passant le courrier à un MUA (ou au moins lui en transférant la responsabilité, par exemple, en déposant le message dans une "mémoire de messages"). Cependant, alors que ces termes sont utilisés avec au moins l'apparence d'une grande précision dans d'autres environnements, les frontières impliquées entre les MUA et les MTA ne correspondent souvent pas précisément aux pratiques courantes et conformes de la messagerie Internet. Et donc, le lecteur devrait être prudent dans ses déductions sur les fortes relations et responsabilités que pourraient impliquer ces termes s'ils étaient utilisés dans un autre environnement.

2.3.4 Hôte

Pour les besoins de la présente spécification, un hôte est un système informatique rattaché à l'Internet (ou, dans certains cas, à un réseau TCP/IP privé) et qui prend en charge le protocole SMTP. Les hôtes sont connus par des noms (voir "domaine") ; les identifier par des adresses numériques est déconseillé.

2.3.5 Domaine

Un domaine (ou nom de domaine) consiste en un ou plusieurs composants séparés par un point. Ces composants ("étiquettes" dans la terminologie DNS [22]) sont restreints pour les besoins de SMTP à consister en une séquence de lettres, chiffres, et tirés extraits de l'ensemble de caractères ASCII [1]. Les noms de domaine sont utilisés comme noms d'hôtes et d'autres entités de la hiérarchie des noms de domaine. Par exemple, un domaine peut se référer à un alias (étiquette d'un CNAME RR) ou à l'étiquette d'enregistrements d'échange de messagerie à utiliser pour livrer le courrier au lieu de représenter un nom d'hôte. Voir [22] et la section 5 de la présente spécification.

Le nom de domaine, tel que décrit dans le présent document et en [22], est le nom entier, pleinement qualifié (souvent désigné comme un "FQDN"). Un nom de domaine qui n'est pas en forme FQDN n'est rien de plus qu'un alias local. Les alias locaux NE DOIVENT PAS apparaître dans les transactions SMTP.

2.3.6 Mémoire tampon et tableau d'état

Les sessions SMTP sont sans état, les deux parties maintenant avec soin une vision commune de l'état en cours. Dans le présent document nous modélisons cet état par une "mémoire tampon" et un "tableau d'état" virtuels sur le serveur qui peuvent être utilisés par le client pour, par exemple, "vider la mémoire tampon" ou "remettre le tableau d'état à zéro" causant l'élimination des informations de la mémoire tampon et le retour de l'état à un stade antérieur.

2.3.7 Lignes

Les commandes SMTP et, sauf altérées par une extension de service, les données du message, sont transmises en "lignes". Les lignes consistent en zéro, un ou plusieurs caractères de données terminés par la séquence de caractère ASCII "CR" (valeur hexadécimale de 0D) suivie immédiatement par le caractère ASCII "LF" (valeur hexadécimale 0A). Cette séquence de terminaison est notée par <CRLF> dans le présent document. Les mises en œuvre conformes NE DOIVENT PAS reconnaître ou générer d'autre caractère ou séquence de caractère comme terminaison de ligne. Des limites PEUVENT être imposées à la longueur de ligne par les serveurs (voir au paragraphe 4.5.3).

De plus, l'apparition de caractères "nus" "CR" ou "LF" dans le texte (c'est-à-dire, l'un sans l'autre) a une longue histoire des problèmes causés dans les mises en œuvre et applications de messagerie qui utilisent le système de messagerie comme outil. Les mises en œuvre de client SMTP NE DOIVENT PAS transmettre ces caractères sauf lorsqu'ils sont destinée à terminer les lignes et DOIVENT alors, comme indiqué ci-dessus, ne les transmettre que comme séquence <CRLF>.

2.3.8 Systèmes d'origine, de livraison, de relais, et de passerelle

La présente spécification fait une distinction entre quatre types de systèmes SMTP, sur la base du rôle que jouent ces systèmes dans la transmission du courrier électronique. Un système "d'origine" (parfois appelé une origine SMTP) introduit la messagerie dans l'Internet ou, plus généralement, dans un environnement de service de transport. Un système SMTP de "livraison" est celui qui reçoit la messagerie d'un environnement de service de transport et le passe à un agent d'utilisateur de messagerie ou le dépose dans une mémoire de messages à laquelle l'agent d'utilisateur de messagerie est supposé accéder ultérieurement. Un système SMTP "relais" (qu'on appelle habituellement simplement un "relais") reçoit le courrier d'un client SMTP et le transmet, sans modification des données du message autres que l'ajout des informations de traçage, à un autre serveur SMTP pour un autre relais ou livraison.

Un système SMTP de "passerelle" SMTP (qu'on appelle habituellement simplement une "passerelle") reçoit le courrier d'un système client dans un environnement de transport et le transmet à un système serveur dans un autre environnement de transport. Des différences de protocoles ou de la sémantique des messages entre les environnements de transport d'un côté ou de l'autre d'une passerelle peuvent exiger que le système de passerelle effectue des transformations du message qui ne sont pas permises aux systèmes de relais SMTP. Pour les besoins de la présente spécification, les pare-feu qui réécrivent les adresses devraient être considérés comme des passerelles, même si SMTP est utilisé des deux côtés (voir [11]).

2.3.9 Contenu de message et données de messagerie

Les termes "contenu du message" et "données de messagerie" sont interchangeables dans le présent document pour décrire le matériel transmis après l'acceptation de la commande DATA et avant la transmission de l'indication de fin des données. Le contenu de message inclut les en-têtes de message et le corps de message éventuellement structuré. La spécification MIME [12] donne les mécanismes standard pour la structuration des corps de message.

2.3.10 Boîte à lettres et adresse

Telle qu'utilisée dans la présente spécification, une "adresse" est une chaîne de caractères qui identifie un usager à qui du courrier sera envoyé sur une localisation à laquelle le courrier sera déposé. Le terme de "boîte aux lettres" se réfère à ce dépôt. Les deux termes sont normalement interchangeables sauf dans le cas où une distinction entre la localisation dans laquelle le courrier est placé (la boîte aux lettres) et une référence à celle-ci (l'adresse) est importante. Une adresse consiste normalement en une spécification d'un usager et d'un domaine. La convention standard de dénomination de boîte aux lettres est définie comme étant "partie-locale@domaine" : l'usage actuel permet un ensemble beaucoup plus large d'applications que le simple "nom d'usager". Par conséquent, et du fait d'une longue histoire de problèmes quand des hôtes intermédiaires ont essayé d'optimiser le transport en les modifiant, la partie locale ne DOIT être interprétée et recevoir une sémantique que par l'hôte spécifié dans la partie domaine de l'adresse.

2.3.11 Réponse

Une réponse SMTP est un accusé de réception (positif ou négatif) envoyé du receveur à l'envoyeur via le canal de transmission en réponse à une commande. La forme générale d'une réponse est un code numérique d'achèvement (indiquant échec ou succès) habituellement suivi d'une chaîne de texte. Les codes sont à utiliser par des programmes et le texte est normalement destiné à l'utilisateur humain. Des travaux récents [34] ont spécifié une évolution de la structure des chaînes de réponses, incluant l'utilisation de codes d'achèvement supplémentaires et plus spécifiques.

2.4 Principes généraux de syntaxe et modèle de transaction

Les commandes SMTP et les réponses ont une syntaxe rigide. Toutes les commandes commencent par un verbe de commande. Toutes les réponses commencent par un code numérique à trois chiffres. Dans certaines commandes et réponses, les arguments DOIVENT suivre le verbe ou code de réponse. Certaines commandes n'acceptent pas d'argument (après le verbe), et certains codes de réponse sont suivis, parfois de façon facultative, par du texte en forme libre. Dans les deux cas, lorsque du texte apparaît, il est séparé du verbe ou code de réponse par un caractère espace. Les définitions complètes des commandes et réponses figurent à la Section 4.

Les valeurs des verbes et d'arguments (par exemple, "TO:" ou "to:" dans la commande RCPT et les mots clés de nom d'extension) ne sont pas sensibles à la casse, avec la seule exception, dans la présente spécification, de la partie locale d'une boîte aux lettres (les extensions SMTP peuvent explicitement spécifier des éléments sensibles à la casse). C'est à dire qu'un verbe de commande, une valeur d'argument autre qu'une partie locale de boîte à lettre, et du texte de forme libre PEUVENT être codés en majuscule, en minuscule ou tout mélange de majuscules et minuscules sans impact sur leur signification. Cela N'EST PAS vrai de la partie locale d'une boîte aux lettres. La partie locale d'une boîte aux lettres DOIT être traitée comme sensible à la casse. Donc, les mises en œuvre SMTP DOIVENT veiller à préserver la casse des parties locales des boîtes aux lettres. Les domaines de boîte à lettre ne sont pas sensibles à la casse. En particulier, pour certains hôtes, l'usager "smith" est différent de l'usager "Smith". Cependant, l'exploitation de la sensibilité à la casse de la partie locale des boîtes aux lettres entrave l'interopérabilité et est déconseillée.

Quelques serveurs SMTP, en violation de la présente spécification (et de la RFC 821) exigent que les verbes de commande soient codés par les clients en majuscules. Les mises en œuvre PEUVENT souhaiter employer ce codage pour arranger ces serveurs.

Le champ argument consiste en une chaîne de caractères de longueur variable qui se termine à la fin de la ligne, c'est-à-dire, avec la séquence de caractères <CRLF>. Le receveur ne fera rien tant que cette séquence n'est pas reçue.

La syntaxe de chaque commande figure avec l'exposé sur cette commande. Les éléments et paramètres communs figurent au paragraphe 4.1.2.

Les commandes et réponses se composent de caractères provenant du jeu de caractères ASCII [1]. Lorsque le service de transport fournit un canal de transmission à octets de 8 bits, chaque caractère de 7 bits est transmis justifié à droite dans un octet avec le bit de plus fort poids (de gauche) mis à zéro. Plus précisément, le service SMTP sans extension ne fournit que sept bits de transport. Un client SMTP d'origine qui n'a pas réussi à négocier une extension appropriée avec un serveur particulier NE DOIT PAS transmettre des messages avec les informations dans des octets à ordre supérieur binaire. Si de tels messages sont transmis en violation de cette règle, les serveurs SMTP qui reçoivent PEUVENT effacer le bit d'ordre supérieur ou rejeter le message comme invalide. En général, un relais SMTP DEVRAIT supposer que le contenu du message qu'il a reçu est valide et, en supposant que l'enveloppe permette de le faire, le relayer sans inspecter ce contenu. Bien sûr, si le contenu est mal marqué et si le chemin de données ne peut pas accepter le contenu réel, il peut en résulter la livraison finale d'un message sévèrement embrouillé au receveur. Les systèmes de livraison SMTP PEUVENT rejeter ("refuser") de tels messages plutôt que de les livrer. Aucun système SMTP d'envoi n'est autorisé à envoyer des commandes d'enveloppe dans un jeu de caractères autre que US-ASCII ; les systèmes de réception DEVRAIENT rejeter de telles commandes, en utilisant normalement des réponses "500 erreur de syntaxe - caractère invalide".

La transmission d'un contenu de message à 8 bits PEUT être demandée au serveur par un client en utilisant les facilités de SMTP étendu, notamment l'extension "8BITMIME" [20]. 8BITMIME DEVRAIT être acceptée par les serveurs SMTP. Cependant, elle NE DOIT PAS être vue comme l'autorisation de transmettre sans restriction du matériel à huit bits. 8BITMIME NE DOIT PAS être demandé par l'envoyeur pour un matériau à huit bits qui n'est pas en format MIME avec un codage approprié de transfert de contenu ; les serveurs PEUVENT rejeter de tels messages.

La notation métalinguistique utilisée dans le présent document correspond au "BNF augmenté" utilisé dans d'autres documents du système de messagerie Internet. Le lecteur qui n'est pas familiarisé avec cette syntaxe devrait consulter la spécification ABNF [8]. Les termes du métalangage utilisé dans le texte courant sont entourés de crochets angulaires (par exemple, <CRLF>) pour plus de clarté.

3 Procédures SMTP : généralités

La présente section contient la description des procédures utilisées dans SMTP : initiation de session, transaction de messagerie, transmission de message, vérification des noms de boîte aux lettres et développement des listes de diffusion de messagerie, ouverture et fermeture des échanges. Des commentaires sur le relais, une note sur les domaines de messagerie, et une discussion sur les changements de rôles sont inclus à la fin de la section. Plusieurs scénarios complets sont présentés à l'appendice D.

3.1 Initiation de session

Une session SMTP est initiée quand un client ouvre une connexion avec un serveur et que le serveur répond par un message d'ouverture.

Les mises en œuvre de serveur SMTP PEUVENT inclure l'identification de leurs informations de logiciel et de version dans la réponse d'accueil de connexion après le code 220, pratique qui permet un isolement et une réparation plus efficaces de tous problèmes. Les mises en œuvre PEUVENT prendre des dispositions pour que les serveurs SMTP désactivent l'annonce de logiciel et de version lorsque cela cause des problèmes de sécurité. Bien que certains systèmes identifient aussi leur point de contact pour les problèmes de messagerie, cela ne peut se substituer à la fourniture exigée de l'adresse du "maître de poste" (voir au paragraphe 4.5.1).

Le protocole SMTP permet à un serveur de rejeter formellement une transaction tout en permettant comme suit la connexion initiale : une réponse 554 PEUT être donnée dans le message initial d'ouverture de la connexion au lieu de la réponse 220. Un serveur qui adopte cette approche DOIT quand même attendre que le client envoie un QUIT (voir au paragraphe 4.1.1.10) avant de clore la connexion et DEVRAIT répondre à toute commande qui interviendrait par "503 Mauvaise séquence de commandes". Comme une tentative d'établir une connexion SMTP avec un tel système est probablement une erreur, un serveur qui retourne une réponse 554 à l'ouverture d'une connexion DEVRAIT fournir assez d'informations dans le texte de réponse pour faciliter la correction d'erreur sur le système d'envoi.

3.2 Initiation du client

Une fois que le serveur a envoyé le message d'accueil et que le client l'a reçu, le client envoie normalement la commande EHLO au serveur, qui indique l'identité du client. En plus de l'ouverture de la session, l'utilisation du EHLO indique que le client est capable de traiter les extensions de service et demande que le serveur fournisse une liste des extensions qu'il accepte. Les plus anciens systèmes SMTP qui ne sont pas capables de prendre en charge les extensions de service et les clients actuels qui ne demandent pas d'extension de service dans la session de messagerie initialisée PEUVENT utiliser HELO à la place de EHLO. Les serveurs NE DOIVENT PAS retourner la réponse de style EHLO étendu à une commande HELO. Pour un essai de connexion particulier, si le serveur retourne une réponse "commande non reconnue" à EHLO, le client DEVRAIT être capable de se replier sur l'envoi de HELO.

Dans la commande EHLO, l'hôte qui envoie la commande s'identifie ; la commande peut être interprétée comme disant "Hello, je suis <domaine>" (et, dans le cas de EHLO, "et je prend en charge les demandes d'extension de service").

3.3 Transactions de messagerie

Il y a trois étapes pour les transactions de messagerie SMTP. La transaction débute par une commande MAIL qui donne l'identification de l'envoyeur. (En général, la commande MAIL ne peut être envoyée que quand aucune transaction de messagerie n'est en cours ; voir au paragraphe 4.1.4.) Une série d'une ou plusieurs commandes RCPT suit, qui donne les informations sur le receveur. Puis une commande DATA initialise le transfert des données de messagerie et se termine par l'indicateur "fin de message", qui confirme aussi la transaction.

La première étape de la procédure est la commande MAIL.

MAIL FROM:<chemin inverse> [SP <paramètres de message>] <CRLF>

Cette commande dit au receveur SMTP qu'une nouvelle transaction de messagerie débute et de remettre à zéro tous ses tableaux d'état et ses mémoires tampon, y compris toutes données de réception ou de messagerie. La portion <chemin inverse> du premier ou seul argument contient la boîte aux lettres de source (entre les crochet "<" et ">"), qui peut être utilisée pour rapporter des erreurs (voir au paragraphe 4.2 l'exposé sur le rapport d'erreur). S'il accepte, le serveur SMTP

retourne une réponse 250 OK. Si la spécification de la boîte à lettre n'est pas acceptable pour une raison quelconque, le serveur DOIT retourner une réponse qui indique si la défaillance est permanente (c'est-à-dire, se produira à nouveau si le client essaye encore la même adresse) ou temporaire (c'est-à-dire, l'adresse pourrait être acceptée si le client réessaye plus tard). En dépit de la portée apparente de cette exigence, il y a des circonstances dans lesquelles l'acceptabilité du chemin inverse ne peut pas être déterminée jusqu'à ce qu'un ou plusieurs chemins de retour (dans les commandes RCPT) puissent être examinés. Dans de tels cas, le serveur PEUT raisonnablement accepter le chemin inverse (avec une réponse 250) et rapporter les problèmes après la réception et l'examen des chemins de retour. Normalement, les défaillances produisent des réponses 550 ou 553.

Historiquement, le <chemin-inverse> peut contenir plus d'une boîte aux lettres, cependant, les systèmes contemporains NE DEVRAIT PAS utiliser l'acheminement de source (voir l'appendice C).

Le <paramètres de messagerie> facultatif est associé aux extensions de service SMTP négociées (voir au paragraphe 2.2).

La seconde étape de la procédure est la commande RCPT.

RCPT TO:<chemin-de-retour> [SP <paramètres-rcpt>] <CRLF>

Le premier ou seul argument pour cette commande inclut un chemin de retour (normalement une boîte aux lettres et un domaine, toujours entourés de crochets "<" et ">") identifiant un receveur. S'il l'accepte, le serveur SMTP retourne une réponse 250 OK et mémorise le chemin de retour. Si le receveur est connu pour n'être pas une adresse de livraison, le serveur SMTP retourne une réponse 550, normalement avec une chaîne du genre "usager inconnu" et le nom de la boîte aux lettres (d'autres circonstances et codes de réponse sont possibles). Cette étape de la procédure peut être répétée sans limitations.

Le <chemin-de-retour> peut contenir plus qu'une seule boîte aux lettres. Dans le passé, le <chemin-de-retour> pouvait être une liste d'acheminements de source des hôtes et des boîtes aux lettres de destination, cependant, les client SMTP contemporains NE DEVRAIENT PAS utiliser les routes de source (voir l'appendice C). Les serveurs DOIVENT être prêts à rencontrer une liste des routes de source dans le chemin de retour, mais DEVRAIENT ignorer les routes ou PEUVENT décliner la prise en charge du relais qu'elles impliquent. De même, les serveurs PEUVENT refuser d'accepter les messages destinés à d'autres hôtes ou systèmes. Ces restrictions rendent un serveur sans utilité comme relais pour les clients qui ne prennent pas en charge la pleine fonctionnalité SMTP. Par conséquent, les clients à capacités restreintes NE DOIVENT PAS supposer que tout serveur SMTP sur l'Internet peut être utilisé comme site de traitement (relais) de messagerie. Si une commande RCPT apparaît sans une commande MAIL antérieure, le serveur DOIT retourner une réponse 503 "Mauvaise séquence de commandes". Le <paramètres-rcpt> facultatif est associé aux extensions de service SMTP négociées (voir au paragraphe 2.2).

La troisième étape de la procédure est la commande DATA (ou une solution de remplacement spécifiée dans une extension de service).

DATA <CRLF>

S'il accepte, le serveur SMTP retourne une réponse intermédiaire 354 et considère toutes les lignes suivantes jusqu'à la fin de l'indicateur de données de messagerie, non inclus, comme le texte du message. Quand la fin du texte est bien reçue et mémorisée, le receveur SMTP envoie une réponse 250 OK.

Comme les données de messagerie sont envoyées sur le canal de transmission, la fin des données de messagerie doit être indiquée de façon que le dialogue de commandes et réponses puisse se terminer. SMTP indique la fin des données de message en envoyant une ligne contenant seulement un "." (point). Une procédure transparente est utilisée pour empêcher l'interférence avec le texte de l'utilisateur (voir au paragraphe 4.5.2).

La fin de l'indicateur de données de messagerie confirme aussi la transaction de messagerie et dit au serveur SMTP de traiter maintenant les données mémorisées de receveur et messagerie. S'il accepte, le serveur SMTP retourne une réponse 250 OK. La commande DATA ne peut échouer qu'en deux points de l'échange de protocole :

- S'il n'y avait pas de commande MAIL, ou pas de RCPT, ou si toutes ces commandes ont été rejetées, le serveur PEUT retourner une réponse "commande hors séquence" (503) ou "pas de receveur valide" (554) en réponse à la commande DATA. Si une de ces réponses (ou toute autre réponse 5yz) est reçue, le client NE DOIT PAS envoyer les données du message ; plus généralement, les données de message NE DOIVENT PAS être envoyées en dehors de la réception d'une réponse 354.
- Si le verbe est initialement accepté et la réponse 354 produite, la commande DATA ne devrait échouer que si la

transaction de messagerie est incomplète (par exemple, pas de receveur), ou si les ressources sont indisponibles (y compris, bien sûr, si le serveur devient inopinément indisponible), ou si le serveur détermine que le message devrait être rejeté pour des raisons de politique ou autre.

Cependant, en pratique, certains des serveurs n'effectuent pas de vérification du receveur avant la réception du texte du message. Ces serveurs DEVRAIENT traiter une défaillance pour un ou plusieurs receveurs comme une "défaillance ultérieure" et retourner un message comme exposé à la section 6. Utiliser un code de réponse "550 boîte à lettre introuvable" (ou équivalent) après l'acceptation des données rend difficile ou impossible pour le client de déterminer quel récepteur a fait défaut.

Lorsque le format de la RFC 822 [7, 32] est utilisé, les données de messagerie comportent les éléments d'en-tête de mémo tels que Date, Sujet, To, Cc, From. Les systèmes de serveur SMTP NE DEVRAIENT PAS rejeter de messages sur la base de défauts de l'en-tête de message ou du corps de message par rapport à la RFC 822 ou MIME [12]. En particulier, ils NE DOIVENT PAS rejeter les messages dans lesquels les numéros des champs Resent ne correspondent pas ou dans lesquels Resent-to apparaît sans Resent-from et/ou Resent-date.

Les commandes de transaction de messagerie DOIVENT être utilisées dans l'ordre exposé ci-dessus.

3.4 Transmission de correction d'adresse ou de mise à jour

La prise en charge de la transmission est exigée le plus souvent pour confirmer et simplifier les adresses au sein de, ou par rapport à une entreprise et moins fréquemment pour établir des adresses destinées à relier l'adresse précédente d'une personne avec l'adresse actuelle. La transmission silencieuse des messages (sans notification du serveur à l'envoyeur) pour des raisons de sécurité ou de non divulgation, est courante dans l'Internet contemporain.

Aussi bien dans le cas de l'entreprise que de la "nouvelle adresse", des considérations touchant à la dissimulation des informations (et parfois à la sécurité) militent contre l'exposition de l'adresse "finale" à travers le protocole SMTP comme un effet secondaire de l'activité de transmission. Cela peut être particulièrement important lorsque l'adresse finale ne peut pas être atteinte même par l'envoyeur. Par conséquent, les mécanismes de "transmission" décrits au paragraphe 3.2 de la RFC 821, et en particulier les codes de réponse 251 (destination corrigée) et 551 provenant de RCPT doivent être évalués avec soin par les développeurs et, quand ils sont disponibles, par ceux qui configurent les systèmes.

En particulier :

* Les serveurs PEUVENT transmettre les messages lorsqu'ils sont au courant d'un changement d'adresse. Lorsqu'ils le font, ils PEUVENT fournir des informations de mise à jour d'adresse avec un code 251, ou bien transmettre "en silence" et retourner un code 250. Mais, si un code 251 est utilisé, ils NE DOIVENT PAS supposer que le client va réellement mettre à jour les informations d'adresse ou même retourner ces informations à l'usager.

Autrement,

* Les serveurs PEUVENT rejeter ou faire rebondir les messages quand ils ne sont pas livrables lors de l'envoi. Quand c'est le cas, ils PEUVENT soit fournir des informations de mise à jour d'adresse avec un code 551, soit rejeter le message comme non délivrable avec un code 550 et pas d'informations spécifiques de l'adresse. Mais, si un code 551 est utilisé, ils NE DOIVENT PAS supposer que le client va réellement mettre à jour les informations d'adresse ou même retourner ces informations à l'usager.

Les mises en œuvre de serveur SMTP qui prennent en charge les codes de réponse 251 et/ou 551 sont vivement encouragées à fournir des mécanismes de configuration faisant en sorte que les sites qui penseraient qu'ils vont malencontreusement divulguer des informations puissent désactiver ou restreindre leur utilisation.

3.5 Commandes pour le débogage d'adresses

3.5.1 Généralités

SMTP fournit des commandes pour vérifier un nom d'utilisateur ou obtenir le contenu d'une liste de diffusion. Ceci est fait avec les commandes VRFY et EXPN, qui ont des arguments de chaîne de caractères. Les mises en œuvre DEVRAIENT prendre en charge VRFY et EXPN (cependant, voir les paragraphes 3.5.2 et 7.3).

Pour la commande VRFY, la chaîne est un nom d'utilisateur ou un nom d'utilisateur et un domaine (voir ci-dessous). Si une réponse normale (c'est-à-dire, 250) est retournée, la réponse PEUT inclure le nom d'utilisateur complet et DOIT inclure la boîte aux lettres de l'utilisateur. Elle DOIT être de l'une des formes suivantes :

Nom-d'utilisateur <partie-locale@domaine>
partie-locale@domaine

Lorsque un nom qui est l'argument de VRFY pourrait identifier plus d'une boîte aux lettres, le serveur PEUT noter l'ambiguïté ou identifier les alternatives. En d'autres termes, toutes les réponses suivantes sont légitimes pour VRFY :
553 Usager ambigu
ou
553- Ambigu ; les possibilités sont
553-Joe Smith <jsmith@foo.com>
553-Harry Smith <hsmith@foo.com>
553 Melvin Smith <dweep@foo.com>
ou
553- Ambigu ; possibilités
553- <jsmith@foo.com>
553- <hsmith@foo.com>
553 <dweep@foo.com>

Dans des circonstances normales, un client qui reçoit une réponse 553 serait supposé exposer les résultats à l'usager. L'utilisation des formes exactes données, et les mots clés "usager ambigu" ou "ambigu", éventuellement accompagnés des codes de réponse étendus tels que ceux décrits en [34], va faciliter la traduction automatique dans d'autres langues en tant que de besoin. Bien sûr, un client très automatisé ou qui fonctionne dans une autre langue que l'anglais, peut choisir d'essayer de traduire la réponse, pour retourner à l'usager d'autres indications que le texte littéral de la réponse, ou prendre une action automatique comme de consulter un service d'annuaire pour des informations supplémentaires avant de faire rapport à l'usager.

Pour la commande EXPN, la chaîne identifie une liste de diffusion, et la réponse multi ligne de succès (c'est-à-dire, 250) PEUT inclure le nom complet des usagers et DOIT donner les boîtes aux lettres sur la liste de diffusion.

Dans certains hôtes, la distinction entre une liste de diffusion et un alias pour une seule boîte aux lettres est un peu confuse, car une structure de données commune peut détenir les deux types d'entrées, et il est possible d'avoir des listes de diffusion qui ne contiennent qu'une seule boîte aux lettres. Si on fait une demande d'application de VRFY à une liste de diffusion, une réponse positive PEUT être donnée si un message ainsi adressé sera livré à chacun de la liste ; autrement, une erreur DEVRAIT être rapportée (par exemple, "550 C'est une liste de diffusion, pas un usager" ou "252 Incapable de vérifier les membres de la liste de diffusion"). Si on fait une demande d'expansion d'un nom d'utilisateur, le serveur PEUT retourner une réponse positive consistant en une liste ne contenant qu'un nom, ou PEUT rapporter une erreur (par exemple, "550 C'est un nom d'usager, pas une liste de diffusion").

Dans le cas de réponse multi ligne de succès (normal pour EXPN) exactement une boîte aux lettres est à spécifier sur chaque ligne de la réponse. Le cas d'une demande ambiguë est exposé plus haut.

"Nom d'utilisateur" est un terme flou et a été utilisé délibérément. Une mise en œuvre des commandes VRFY ou EXPN DOIT inclure au moins la reconnaissance des boîtes aux lettres locales comme "noms d'utilisateur". Cependant, comme la pratique habituelle de l'Internet résulte souvent en un seul hôte traitant la messagerie pour plusieurs domaines, les hôtes, et particulièrement les hôtes qui fournissent cette fonctionnalité, DEVRAIENT accepter la forme "partie-locale@domaine" comme un "nom d'utilisateur" ; les hôtes PEUVENT aussi choisir de reconnaître d'autres chaînes comme "noms d'utilisateur".

Le cas de l'expansion d'une liste de boîtes aux lettres exige une réponse multi ligne, telle que :
C: EXPN Example-People
S: 250-Jon Postel <Postel@isi.edu>
S: 250-Fred Fonebone <Fonebone@physics.foo-u.edu>
S: 250 Sam Q. Smith <SQSmith@specific.generic.com>

ou
C: EXPN Executive-Washroom-List
S: 550 Accès refusé.

Les arguments de la chaîne de caractères des commandes VRFY et EXPN ne peuvent pas être plus contraints du fait de la diversité des mises en œuvre des concepts de nom d'utilisateur et de liste de diffusion. Dans certains systèmes il peut être

approprié pour l'argument de la commande EXPN d'être un nom de fichier pour un fichier contenant une liste de diffusion, mais il y a aussi une grande diversité de conventions de nommage dans l'Internet. De même, les variations historiques dans ce qui est retourné par ces commandes sont telles que la réponse DEVRAIT être interprétée avec une grande prudence, si elle doit l'être, et ne DEVRAIT en général être utilisé que pour des diagnostics.

3.5.2 Réponse normale VRFY

Lorsque des réponses normales (2yz ou 551) sont retournées d'une demande VRFY ou EXPN, la réponse comporte normalement le nom de la boîte aux lettres, c'est-à-dire que "<partie-locale@domaine>", où "domaine" est un nom de domaine pleinement qualifié, DOIT apparaître dans la syntaxe. Dans des circonstances suffisamment exceptionnelles pour justifier la violation des intentions de la présente spécification, du texte de forme libre PEUT être retourné. Afin de faciliter l'analyse aussi bien par les ordinateurs que par les personnes, les adresses DEVRAIENT apparaître entre des crochets angulaires. Lorsque les adresses sont retournées, plutôt que des informations de correction d'erreur de forme libre, EXPN et VRFY DOIVENT ne retourner que des adresses de domaine valides utilisables dans les commandes RCPT de SMTP. Par conséquent, si une adresse implique la livraison à un programme ou autre système, le nom de la boîte aux lettres utilisé pour atteindre cette cible DOIT être donné. Les chemins (routes de source explicites) NE DOIVENT PAS être retournés par VRFY ou EXPN.

Les mises en œuvre de serveur DEVRAIENT accepter aussi bien VRFY que EXPN. Pour des raisons de sécurité, les mises en œuvre PEUVENT fournir à des installations locales un moyen de désactiver l'une ou/et l'autre de ces commandes par des options de configuration ou équivalent. Lorsque ces commandes sont acceptées, il n'est pas obligé qu'elles fonctionnent à travers les relais lorsque le relais est pris en charge. Comme elles étaient toutes deux facultatives dans la RFC 821, elles DOIVENT figurer dans la liste des extensions de service dans une réponse EHLO, si elles sont acceptées.

3.5.3 Signification de la réponse de succès VRFY ou EXPN

Un serveur NE DOIT PAS retourner un code 250 en réponse à une commande VRFY ou EXPN tant qu'il n'a pas réellement vérifié l'adresse. En particulier, un serveur NE DOIT PAS retourner 250 si tout ce qu'il a fait a été de vérifier que la syntaxe donnée est valide. Dans ce cas, 502 (Commande non mise en œuvre) ou 500 (Erreur de syntaxe, commande non reconnue) DEVRAIT être retourné. Comme mentionné ailleurs, la mise en œuvre (au sens de valider réellement les adresses et retourner les informations) de VRFY et EXPN est vivement recommandée. Et donc, les mises en œuvre qui retournent 500 ou 502 pour VRFY ne sont pas en pleine conformité avec la présente spécification.

Il peut y avoir des circonstances dans lesquelles une adresse paraît être valide mais ne peut raisonnablement être vérifiée en temps réel, en particulier lorsque un serveur agit comme échangeur de messagerie pour un autre serveur ou domaine. La "validité apparente" devrait dans ce cas impliquer normalement au moins la vérification de la syntaxe et pourrait comporter la vérification que tous les domaines spécifiés sont de ceux vers lesquels l'hôte s'attend à être capable de relayer du courrier. Dans ces situations, le code de réponse 252 DEVRAIT être retourné. Ces cas font un parallèle à l'exposé sur la vérification de RCPT au paragraphe 2.1. De même, l'exposé du paragraphe 3.4 s'applique à l'utilisation des codes de réponse 251 et 551 avec VRFY (et EXPN) pour indiquer les adresses qui sont reconnues mais qui feraient l'objet d'une retransmission ou d'un rebond si du courrier était reçu pour elles. Les mises en œuvre DEVRAIENT généralement être plus agressives sur la vérification d'adresse dans le cas de VRFY que dans le cas de RCPT, même si cela prend un peu plus longtemps pour le faire.

3.5.4 Sémantique et applications de EXPN

EXPN est souvent très utile pour corriger les erreurs et comprendre les problèmes des listes de diffusion et des alias à plusieurs adresses cibles. Certains systèmes ont essayé d'utiliser l'expansion de source des listes de diffusion comme moyen d'éliminer les duplications. La propagation des systèmes de nom d'emprunt (alias) avec la messagerie sur l'Internet, pour les hôtes (normalement avec les enregistrements MX et CNAME DNS), pour les boîtes aux lettres (divers types d'alias d'hôte local), et dans divers arrangements de mandataires, a rendu presque impossible le fonctionnement cohérent de ces stratégies, et les systèmes de messagerie NE DEVRAIENT PAS les essayer.

3.6 Domaines

Seuls les noms de domaine pleinement qualifiés (FQDN) solubles sont permis lorsque les noms de domaine sont utilisés dans SMTP. En d'autres termes, les noms qui peuvent se résoudre en RR MX ou RR A (comme exposé à la section 5) sont permis, comme le sont les RR CNAME dont les cibles sont solubles en RR MX ou A. Les sobriquets locaux ou noms non qualifiés NE DOIVENT PAS être utilisés. Il y a deux exceptions à la règle qui exige des FQDN :

- Le nom de domaine donné dans la commande EHLO DOIT être un nom principal d'hôte (nom de domaine qui se

résout en RR A) ou, si l'hôte n'a pas de nom, une adresse littérale comme décrit au paragraphe 4.1.1.1.
- Le nom de boîte aux lettres réservé de "postmaster" peut être utilisé dans une commande RCPT sans qualification de domaine (voir au paragraphe 4.1.1.3) et DOIT être accepté s'il est utilisé ainsi.

3.7 Relais

En général, la disponibilité des enregistrements de Mail eXchanger dans le système de noms de domaine [22, 27] rend l'utilisation de routes de source explicites inutile dans le système de messagerie Internet. De nombreux problèmes historiques de leur interprétation ont rendu leur utilisation indésirable. Les client SMTP NE DEVRAIENT PAS générer de routes de source explicites sauf dans des circonstances inhabituelles. Les serveurs SMTP PEUVENT refuser d'agir comme relais de messagerie ou d'accepter des adresses qui spécifient des routes de source. Lorsqu'ils rencontrent des informations de route, les serveurs SMTP peuvent aussi ignorer les informations de route et envoyer simplement à la destination finale spécifiée comme dernier élément de la route et DEVRAIENT le faire. Il y a eu une pratique non valide d'utilisation de noms qui n'apparaissent pas dans le DNS comme noms de destination, les envoyeurs comptant sur les hôtes intermédiaires spécifiés dans l'acheminement de source pour résoudre tous les problèmes. Si les routes de source sont enlevées, cette pratique causera des défaillances. C'est une des raisons pour lesquelles les clients SMTP NE DOIVENT PAS générer des routes de source invalides ou dépendantes de la résolution d'une série de noms.

Lorsque les routes de source ne sont pas utilisées, le processus décrit dans la RFC 821 pour construire un chemin inverse à partir du chemin de retour n'est pas applicable et le chemin inverse au moment de la livraison sera simplement l'adresse qui apparaît dans la commande MAIL.

Un serveur SMTP relais est habituellement la cible d'un enregistrement MX DNS qui le désigne, plutôt que le système de livraison final. Le serveur relais peut accepter ou rejeter la tâche de relayer la messagerie de la même façon qu'il accepte ou refuse la messagerie d'un usager local. Si il accepte la tâche, il devient alors un client SMTP, établit un canal de transmission avec le prochain serveur SMTP spécifié dans le DNS (conformément aux règles de la Section 5), et lui envoie le courrier. Si il refuse de relayer la messagerie à une adresse particulière pour des raisons de politique, une réponse 550 DEVRAIT être retournée.

Il existe de nombreux clients qui envoient de la messagerie, en particulier en conjonction avec des dispositifs qui reçoivent de la messagerie via POP3 ou IMAP, qui ont des capacités limitées pour prendre en charge certaines des exigences de la présente spécification, comme la capacité à mettre en file d'attente les messages afin de tenter ultérieurement leur livraison. Pour ces clients, il est de pratique courante de faire des arrangements privés pour envoyer tous les messages à un seul serveur pour le traitement et la distribution qui s'ensuit. SMTP, tel que spécifié ici, n'est pas conçu idéalement pour ce rôle, et le travail est en cours pour normaliser des protocoles de présentation de messagerie qui pourraient éventuellement remplacer les pratiques actuelles. Dans tous les cas, comme ces arrangements sont privés et sortent du domaine d'application de la présente spécification, ils ne sont pas décrits ici.

Il est important de noter que les enregistrements MX peuvent pointer sur les serveurs SMTP qui agissent comme passerelles vers d'autres environnements, et pas simplement comme relais SMTP et systèmes de livraison finale ; voir le paragraphe 3.8 et la section 5.

Si un serveur SMTP a accepté la tâche de relayer la messagerie et trouve ensuite que la destination est incorrecte ou que le courrier ne peut être livré pour quelque autre raison, il DOIT alors construire un message de notification "message non livrable" et l'envoyer à l'origine du message non livrable (comme indiqué par le chemin inverse). Les formats spécifiés pour les rapports de non livraison par d'autres normes (voir, par exemple, [24, 25]) DEVRAIENT être utilisés si possible.

Ce message de notification doit être du serveur SMTP à l'hôte relais ou à l'hôte qui a le premier déterminé que cette livraison ne pouvait pas être réalisée. Bien sûr, les serveurs SMTP NE DOIVENT PAS envoyer de messages de notification sur des problèmes de transport de messages de notification. Une façon d'empêcher les boucles de rapport d'erreur est de spécifier un chemin inverse nul dans la commande MAIL d'un message de notification. Lorsqu'un tel message est transmis, le chemin inverse DOIT être réglé à nul (voir au paragraphe 4.5.5 pour des précisions). Une commande MAIL avec un chemin inverse nul apparaît comme suit :

MAIL FROM:<>

Comme exposé au paragraphe 2.4.1, un relais SMTP n'a pas besoin d'inspecter les en-têtes ou corps des données de message ou d'agir sur elles et NE DOIT PAS le faire sauf pour y ajouter son propre en-tête "Received:" (paragraphe 4.4) et, facultativement, pour essayer de détecter une boucle dans le système de messagerie (voir au paragraphe 6.2).

3.8 Passerelles de messagerie

Alors que la fonction de relais exposée ci-dessus opère au sein de l'environnement SMTP de service de transport Internet, les enregistrements MX ou diverses formes d'acheminement explicite peuvent exiger qu'un serveur SMTP intermédiaire effectue une fonction de traduction entre un service de transport et un autre. Comme exposé au paragraphe 2.3.8, lorsqu'un tel système est à la frontière entre deux environnements de service de transport, nous l'appelons une "passerelle" ou "passerelle SMTP".

Établir des passerelles de messagerie entre des environnements de messagerie différents, comme des formats et protocoles de message différents est complexe et ne se prête pas facilement à normalisation. Cependant, quelques exigences générales peuvent être données pour une passerelle entre l'Internet et un autre environnement de messagerie.

3.8.1 Champs d'en-tête dans l'utilisation de passerelles

Des champs d'en-tête PEUVENT être réécrits quand nécessaire lorsque les messages sont passés par une passerelle à travers des frontières d'environnement de messagerie. Cela peut impliquer d'inspecter le corps de message ou d'interpréter la partie locale de l'adresse de destination en dépit des interdictions du paragraphe 2.4.1.

D'autres systèmes de messagerie passés par passerelle à l'Internet utilisent souvent un sous-ensemble des en-têtes de la RFC 822 ou fournissent des fonctionnalités similaires avec une syntaxe différente, mais certains de ces systèmes de messagerie n'ont pas l'équivalent de l'enveloppe SMTP. Donc, lorsque un message quitte l'environnement Internet, il peut être nécessaire de replier les informations de l'enveloppe SMTP dans l'en-tête du message. Une solution possible serait de créer de nouveaux champs d'en-tête pour porter les informations d'enveloppe (par exemple, "X-SMTP-MAIL:" et "X-SMTP-RCPT:"); cependant, cela exigerait des changements des programmes de messagerie dans des environnements étrangers et pourrait risquer de divulguer des informations privées (voir au paragraphe 7.2).

3.8.2 Lignes reçues dans l'utilisation de passerelles

Lors de la transmission d'un message dans ou vers l'environnement Internet, une passerelle DOIT ajouter une ligne Received:, mais elle NE DOIT altérer en aucune façon une ligne Received: qui serait déjà dans l'en-tête.

Les champs "Received:" des messages provenant d'autres environnements peuvent n'être pas exactement conformes à la présente spécification. Cependant, l'utilisation la plus importante des lignes Received: est pour corriger les fautes de messagerie, et ce débogage peut être sévèrement entravé par des passerelles aux bonnes intentions qui essayent de "corriger" une ligne Received:. Comme autre conséquence de l'apparition de champs trace dans des environnements non SMTP, les systèmes récepteurs NE DOIVENT PAS rejeter du courrier sur la base du format d'un champ de trace et DEVRAIENT être extrêmement robustes en présence d'informations ou formats inattendus dans ces champs.

La passerelle DEVRAIT indiquer l'environnement et le protocole dans les clauses "via" du ou des champs Received qu'elle fournit.

3.8.3 Adresses dans l'utilisation de passerelles

Du côté Internet, la passerelle DEVRAIT accepter tous les formats d'adresse valides dans les commandes SMTP et dans les en-têtes de la RFC 822, et tous les messages RFC 822 valides. Les adresses et en-têtes générés par des passerelles DOIVENT se conformer aux normes applicables de l'Internet (y compris celle-ci et la RFC 822). Les passerelles sont, bien sûr, soumises aux mêmes règles de traitement des routes de source que décrit pour les autres systèmes SMTP au paragraphe 3.3.

3.8.4 Autres champs d'en-tête dans l'utilisation de passerelles

La passerelle DOIT s'assurer que tous les champs d'en-tête d'un message qu'elle transmet dans l'environnement de messagerie de l'Internet satisfont aux exigences de la messagerie Internet. En particulier, toutes les adresses dans les champs "From:", "To:", "Cc:", etc., DOIVENT être transformées (si nécessaire) pour satisfaire à la syntaxe de la RFC 822, DOIVENT ne faire référence qu'à des noms de domaine pleinement qualifiés, et DOIVENT être efficaces et utiles pour l'envoi des réponses. L'algorithme de traduction utilisé pour convertir les messages des protocoles Internet en protocoles d'un autre environnement DEVRAIT garantir que les messages d'erreur provenant de l'environnement de messagerie étranger sont livrés au chemin de retour tiré de l'enveloppe SMTP, et non à l'envoyeur figurant dans le champ "From:" (ou autres champs) du message RFC 822.

3.8.5 Enveloppes dans l'utilisation de passerelles

De même, lors de la transmission d'un message provenant d'un autre environnement vers l'Internet, la passerelle DEVRAIT régler le chemin de retour de l'enveloppe en accord avec l'adresse de retour de message d'erreur, si elle est fournie par l'environnement étranger. Si l'environnement étranger n'a pas de concept équivalent, la passerelle doit choisir et utiliser la meilleure approximation, avec l'adresse d'origine du message par défaut en dernier ressort.

3.9 Fin des sessions et des connexions

Une connexion SMTP se termine lorsque le client envoie une commande QUIT. Le serveur répond par un code de réponse positif, après quoi il ferme la connexion.

Un serveur SMTP NE DOIT PAS clore intentionnellement la connexion sauf :
- Après avoir reçu une commande QUIT et avoir répondu par une réponse 221.
- Après avoir détecté la nécessité de fermer le service SMTP et avoir retourné un code de réponse 421. Ce code de réponse peut être produit après que le serveur a reçu une commande quelconque ou, si nécessaire, sans coordination avec la réception de la commande (en supposant que le client la recevra après la production de la prochaine commande).

En particulier, un serveur qui ferme les connexions en réponse à des commandes qu'il ne comprend pas viole la présente spécification. On attend des serveurs qu'ils soient tolérants à l'égard des commandes inconnues, qu'ils produisent une réponse 500 et attendent d'autres instructions de la part du client.

Un serveur SMTP qui est contraint de clore via des moyens externes DEVRAIT tenter d'envoyer une ligne contenant un code de réponse 421 au client SMTP avant de quitter. Le client SMTP va normalement lire le code de réponse 421 après l'envoi de sa prochaine commande.

Les clients SMTP qui font face à la clôture, réinitialisation ou autre défaut de communication d'une connexion, due à des circonstances qui échappent à leur contrôle (en violation des intentions de la présente spécification mais parfois inévitables) DEVRAIENT, pour conserver la robustesse du système de messagerie, traiter la transaction de messagerie comme si une réponse 451 avait été reçue et agir en conséquence.

3.10 Listes de messagerie et alias

Un hôte disposant de la capacité SMTP DEVRAIT prendre en charge aussi bien les alias que les modèles de liste d'expansion d'adresse pour les livraisons multiples. Lorsque un message est délivré ou transmis à chaque adresse d'une forme de liste étendue, l'adresse de retour dans l'enveloppe ("MAIL FROM:") DOIT être changée pour l'adresse d'une personne ou autre entité qui administre la liste. Cependant, dans ce cas, l'en-tête de message [32] DOIT rester inchangé ; en particulier, le champ "From" de l'en-tête du message n'est pas affecté.

Un dispositif important pour la messagerie est le mécanisme de livraison multi destinations dans un seul message, en transformant (ou "éclatant" ou "explosant") une adresse de pseudo boîte aux lettres en une liste d'adresses de boîtes aux lettres de destination. Lorsque un message est envoyé à une telle pseudo boîte aux lettres (parfois appelée un "exploseur"), des copies sont transmises ou redistribuées à chaque boîte aux lettres dans la liste éclatée. Les serveurs DEVRAIENT simplement utiliser les adresses de la liste ; l'application de règles d'heuristique ou autres règles de correspondance pour éliminer certaines adresses, comme celle de l'origine, est fortement déconseillée. On classe de telles pseudo boîtes aux lettres dans la catégorie des "alias" ou des "listes", selon les règles d'expansion.

3.10.1 Alias

Pour étendre un alias, le messageur receveur remplace simplement tour à tour dans l'enveloppe l'adresse de la pseudo boîte aux lettres par chaque adresse issue de l'éclatement ; le reste de l'enveloppe et le corps de message restent inchangés. Le message est alors délivré ou transmis à chaque adresse issue de l'éclatement de la pseudo boîte aux lettres.

3.10.2 Liste

Une liste de diffusion peut être dite fonctionner par "redistribution" plutôt que par "transmission". Pour éclater une liste, le messageur de réception remplace dans l'enveloppe les adresses de la pseudo boîte aux lettres par toutes les adresses éclatées. L'adresse de retour dans l'enveloppe est changée de sorte que tous les messages d'erreur générés par les livraisons

finales soient retournés à l'administrateur de la liste, et non à l'origine du message, qui n'a généralement aucun contrôle sur le contenu de la liste et va normalement trouver fâcheux ces messages d'erreur.

4 Les spécifications SMTP

4.1 Commandes SMTP

4.1.1 Sémantique et syntaxe des commandes

Les commandes SMTP définissent le transfert de messagerie ou la fonction de système de messagerie requis par l'usager. Les commandes SMTP sont des chaînes de caractères terminées par <CRLF>. Les commandes elles-mêmes sont des caractères alphabétiques terminés par <SP> si des paramètres suivent et <CRLF> autrement. (Dans l'intérêt de l'interopérabilité, il est conseillé aux receveurs SMTP de tolérer l'espace blanche en queue avant le <CRLF> de terminaison.) La syntaxe de la partie locale d'une boîte aux lettres doit se conformer aux conventions de site du receveur et à la syntaxe spécifiée au paragraphe 4.1.2. Les commandes SMTP sont exposées plus loin. Les réponses SMTP sont exposées au paragraphe 4.2. Une transaction de messagerie implique plusieurs objets de données qui sont communiqués comme arguments pour différentes commandes. Le chemin inverse est l'argument de la commande MAIL, le chemin de transmission est l'argument de la commande RCTP, et les données de messagerie sont l'argument de la commande DATA. Ces arguments ou objets de données doivent être transmis et conservés en attendant la confirmation communiquée par l'indication de fin des données de messagerie qui finalise la transaction. Le modèle de ce comportement est que des mémoires tampon distinctes sont fournies pour détenir les types d'objets de données, c'est-à-dire qu'il y a une mémoire tampon de chemin inverse, une mémoire tampon de chemin de transmission, et une mémoire tampon de données de messagerie. Des commandes spécifiques provoquent l'ajout des informations à une mémoire tampon spécifique, ou causent le vidage d'une ou plusieurs mémoires tampon.

Plusieurs commandes (RSET, DATA, QUIT) sont spécifiées comme ne permettant pas de paramètres. En l'absence d'extensions spécifiques offertes par le serveur et acceptées par le client, les clients NE DOIVENT PAS envoyer de tels paramètres et les serveurs DEVRAIENT rejeter les commandes qui les contiennent comme ayant une syntaxe invalide.

4.1.1.1 Extension de HELLO (EHLO) ou HELLO (HELO)

Ces commandes sont utilisées pour identifier le client SMTP auprès du serveur SMTP. Le champ d'argument contient le nom de domaine pleinement qualifié du client SMTP s'il en est un disponible. Dans les situations dans lesquelles le système SMTP client n'a pas de nom de domaine significatif (par exemple, quand son adresse est allouée de façon dynamique et qu'aucun enregistrement de chemin inverse n'est disponible), le client DEVRAIT envoyer une adresse littérale (voir au paragraphe 4.1.3), facultativement suivie par des informations qui aideront à identifier le système client. Le serveur SMTP s'identifie lui-même auprès du client SMTP dans la réponse d'accueil de connexion et dans la réponse à cette commande.

Un client SMTP DEVRAIT commencer une session SMTP par la production de la commande EHLO. Si le serveur SMTP accepte les extensions de service SMTP, il donnera une réponse de succès, une réponse d'échec, ou une réponse d'erreur. Si le serveur SMTP, en violation de la présente spécification, ne prend en charge aucune extension de service SMTP, il générera une réponse d'erreur. Les vieux systèmes clients SMTP PEUVENT, comme exposé ci-dessus, utiliser HELO (qui était spécifié dans la RFC 821) au lieu de EHLO, et les serveurs DOIVENT accepter la commande HELO et y répondre de façon appropriée. Dans tous les cas, un client DOIT produire un HELO ou EHLO avant de commencer une transaction de messagerie.

Ces commandes, et une réponse "250 OK" à l'une d'elles, confirment que le client SMTP et le serveur SMTP sont tous deux dans l'état initial, c'est-à-dire qu'il n'y a pas de transaction en cours et que tous les tableaux d'état et toutes les mémoires tampon ont été vidés.

Syntaxe :
ehlo = "EHLO" SP Domaine CRLF
helo = "HELO" SP Domaine CRLF

Normalement, la réponse à EHLO sera une réponse multi ligne. Chaque ligne de la réponse contient un mot clé et, facultativement, un ou plusieurs paramètres. Suivant la syntaxe normale pour les réponses multi lignes, ces mots clés suivent le code (250) et un trait d'union pour toutes sauf la dernière ligne, et le code et une espace pour la dernière ligne. La syntaxe pour une réponse positive, en utilisant la notation ABNF et les symboles terminaux de [8], est :

```
ehlo-ok-rsp =    ( "250"    domain [ SP ehlo-greet ] CRLF )
                 / (    "250-"   domain [ SP ehlo-greet ] CRLF
                 *( "250-"   ehlo-line              CRLF )
                 "250"    SP ehlo-line           CRLF  )
ehlo-greet  =    1*(%d0-9 / %d11-12 / %d14-127)
                 ; chaîne de tous caractères autres que CR ou LF

ehlo-line   =    ehlo-keyword *( SP ehlo-param )

ehlo-keyword =   (ALPHA / DIGIT) *(ALPHA / DIGIT / "-")
                 ; la syntaxe supplémentaire de ehlo-params dépend de ehlo-keyword

ehlo-param   = 1*(%d33-127)
                 ; tout caractère sauf <SP> et tout caractère de contrôle (US-ASCII 0 à 31 inclus)
```

Bien que le mot clé EHLO puisse être spécifié en majuscules, minuscules ou en casse mixte, il DOIT toujours être reconnu et traité de façon insensible à la casse. Ceci est simplement une extension des pratiques spécifiées dans la RFC 821 et au paragraphe 2.4.1.

4.1.1.2 MAIL (MAIL)

Cette commande est utilisée pour initier une transaction de messagerie dans laquelle les données de messagerie sont livrées à un serveur SMTP qui peut à son tour, les livrer à une ou plusieurs boîtes aux lettres ou les passer à un autre système (éventuellement en utilisant SMTP). Le champ d'argument contient un chemin inverse et peut contenir des paramètres facultatifs. En général, la commande MAIL ne peut être envoyée que quand aucune transaction de messagerie n'est en cours, voir au paragraphe 4.1.4.

Le chemin inverse est la boîte aux lettres de l'envoyeur. Historiquement, cette boîte aux lettres pouvait facultativement être précédée d'une liste d'hôtes, mais ce comportement est maintenant déconseillé (voir l'appendice C). Dans certains types de messages de rapport pour lesquels une réponse va vraisemblablement causer une boucle (par exemple, notifications de livraison de message et de non livraisons), le chemin inverse peut être nul (voir au paragraphe 3.7).

Cette commande vide la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission, et la mémoire tampon de données de messagerie, et insère les informations de chemin inverse à partir de cette commande dans la mémoire tampon de chemin inverse.

Si des extensions de service ont été négociées, la commande MAIL peut aussi porter des paramètres associés à une extension de service particulière.

Syntaxe :
"MAIL FROM:" ("<>" / Chemin-inverse) [SP paramètres de messagerie] CRLF

4.1.1.3 RECEVEUR (RCPT)

Cette commande est utilisée pour identifier un receveur individuel des données de messagerie ; plusieurs receveurs sont spécifiés par plusieurs utilisations de cette commande. Le champ d'argument contient un chemin de transmission et peut contenir des paramètres facultatifs.

Le chemin de transmission comporte normalement les boîtes aux lettres de destination requises. Les systèmes d'envoi NE DEVRAIENT PAS générer la liste facultative des hôtes connus comme une route de source. Les systèmes de réception DOIVENT reconnaître la syntaxe de route de source mais DEVRAIENT effacer la spécification de la route de source et utiliser le nom de domaine associé à la boîte aux lettres comme si la route de source n'avait pas été fournie.

De même, les hôtes relais DEVRAIENT effacer ou ignorer les routes de source, et les noms NE DOIVENT PAS être copiés dans le chemin inverse. Lorsque le message atteint sa destination ultime (le chemin de transmission contient seulement une boîte aux lettres de destination), le serveur SMTP l'insère dans la boîte aux lettres de destination conformément aux conventions de messagerie de son hôte.

Par exemple, la messagerie reçue à l'hôte relais xyz.com avec des commandes d'enveloppe

MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>
sera normalement envoyée directement à l'hôte d.bar.org avec des commandes d'enveloppe
MAIL FROM:<userx@y.foo.org>
RCPT TO:<userc@d.bar.org>

Comme indiqué à l'Appendice C, xyz.com PEUT aussi choisir de relayer le message à hosta.int, en utilisant les commandes d'enveloppe
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>
ou à jkl.org, en utilisant les commandes d'enveloppe
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@jkl.org:userc@d.bar.org>

Bien sûr, comme les hôtes ne sont pas obligés de relayer du tout la messagerie, xyz.com peut aussi rejeter le message entièrement à réception de la commande RCTP, en utilisant un code 550 (car c'est une "raison de politique").

Si des extensions de service ont été négociées, la commande RCTP peut aussi porter des paramètres associés à une extension de service particulière offerte par le serveur. Le client NE DOIT PAS transmettre de paramètres autres que ceux associés à une extension de service offerte par le serveur dans sa réponse EHLO.

Syntaxe :
"RCPT TO:" ("<Postmaster@" domaine ">" / "<Postmaster>" / Chemin de transmission) [SP paramètres-Rcpt] CRLF

4.1.1.4 DONNÉES (DATA)

Le receveur envoie normalement une réponse 354 à DATA, et traite ensuite les lignes (les chaînes se terminant par une séquence <CRLF>, comme décrit au paragraphe 2.3.7) qui suivent la commande comme données de messagerie provenant de l'envoyeur. Cette commande provoque l'ajout des données de messagerie à la mémoire tampon de données de messagerie. Les données de messagerie peuvent contenir tous les 128 codes de caractère ASCII, bien que l'expérience ait montré que l'utilisation des caractères de contrôle autres que SP, HT, CR, et LF puisse causer des problèmes et DEVRAIT être évitée autant que possible.

Les données de messagerie sont terminées par une ligne qui contient seulement un point, c'est-à-dire, la séquence de caractères "<CRLF>.<CRLF>" (voir au paragraphe 4.5.2). C'est l'indication de la fin des données de messagerie. Noter que le premier <CRLF> de cette séquence de fin est aussi le <CRLF> qui termine la ligne finale des données (texte du message) ou, si il n'y avait pas de données, termine la commande DATA elle-même. Un <CRLF> supplémentaire NE DOIT PAS être ajouté, car cela causerait l'ajout d'une ligne vide au message. La seule exception à cette règle surviendrait si le corps de message était passé à l'envoyeur SMTP d'origine avec une "ligne" finale qui ne se terminerait pas par un <CRLF> ; dans ce cas, le système SMTP d'origine DOIT rejeter le message comme invalide ou ajouter le <CRLF> afin que le serveur SMTP receveur reconnaisse la condition "fin des données".

La coutume d'accepter des lignes se terminant seulement par un <LF>, concession au comportement non-conformiste de la part de certains systèmes UNIX, s'est révélée causer plus de problèmes d'interopérabilité qu'elle n'en résout, et les systèmes serveurs SMTP NE DOIVENT PAS le faire, même au nom d'une robustesse améliorée. En particulier, la séquence "<LF>.<LF>" (sauts à la ligne nus, sans retour chariot) NE DOIT PAS être traitée comme équivalente à <CRLF>.<CRLF> comme indication de fin des données de messagerie.

La réception de l'indication de fin des données de messagerie oblige le serveur à traiter les informations de transaction de messagerie mémorisées. Ce traitement consomme les informations qui sont dans la mémoire tampon de chemin inverse, dans la mémoire tampon de chemin de transmission, et dans la mémoire tampon de données de messagerie, et à l'achèvement de cette commande, ces mémoires tampon sont vidées. Si le traitement est réussi, le receveur DOIT envoyer une réponse OK. Si le traitement échoue, le receveur DOIT envoyer une réponse d'échec. Le modèle SMTP ne permet pas d'échecs partiels à ce point : soit le message est accepté par le serveur pour livraison et une réponse positive est retournée, soit il n'est pas accepté et une réponse d'échec est retournée. En envoyant une réponse d'achèvement positive à l'indication de fin des données, le receveur prend la pleine responsabilité du message (voir au paragraphe 6.1). Les erreurs qui sont diagnostiquées ultérieurement DOIVENT être rapportées dans un message, comme exposé au paragraphe 4.4.

Lorsque le serveur SMTP accepte un message à relayer ou pour livraison finale, il insère un enregistrement de trace (aussi appelé de façon interchangeable une "ligne d'horodatage" ou ligne "Received") au sommet des données de messagerie. Cet

enregistrement de trace indique l'identité de l'hôte qui envoie le message, l'identité de l'hôte qui reçoit le message (et qui insère l'horodatage), et la date et l'heure de réception du message. Les messages relayés auront plusieurs lignes d'horodatage. Des précisons sur la formation de ces lignes, y compris leur syntaxe, figurent au paragraphe 4.4.

Un exposé supplémentaire sur le fonctionnement de la commande DATA figure au paragraphe 3.3.

Syntaxe :
"DATA" CRLF

4.1.1.5 REINITIALISER (RSET)

Cette commande spécifie que la transaction de messagerie en cours va être interrompue. Tout envoyeur, receveur, et données de messagerie mémorisés DOIVENT être éliminés, et toutes les mémoires tampon et tableaux d'état vidés. Le receveur DOIT envoyer une réponse "250 OK" à une commande RSET sans argument. Une commande de réinitialisation peut être produite par le client à tout moment. Elle est effectivement équivalente à un NOOP (c'est-à-dire, si elle n'a pas d'effet) si elle est produite immédiatement après EHLO, avant que EHLO soit produit dans la session, après l'envoi et l'accusé de réception d'un indicateur de fin de données, ou immédiatement avant un QUIT. Un serveur SMTP NE DOIT PAS clore la connexion en résultat de la réception d'un RSET ; cette action est réservée pour QUIT (voir le paragraphe 4.1.1.10).

Comme EHLO implique un traitement et une réponse supplémentaires du serveur, RSET sera normalement plus efficace que de reproduire cette commande, même si leur sémantique formelle est identique.

Il y a des circonstances, contraires aux intentions de la présente spécification, dans lesquelles un serveur SMTP peut recevoir l'indication que la connexion TCP sous-jacente a été close ou réinitialisée. Pour préserver la robustesse du système de messagerie, les serveurs SMTP DEVRAIENT être prêts pour cette condition et DEVRAIENT la traiter comme si un QUIT avait été reçu avant que la connexion ne disparaisse.

Syntaxe :
"RSET" CRLF

4.1.1.6 VÉRIFIER (VRFY)

Cette commande demande au receveur de confirmer que l'argument identifie un usager ou une boîte aux lettres. Si c'est un nom d'utilisateur, l'information est retournée comme spécifié au paragraphe 3.5.

Cette commande n'a pas d'effet sur la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission, ni sur la mémoire tampon de données de messagerie.

Syntaxe :
"VRFY" SP Chaîne CRLF

4.1.1.7 EXPAND (EXPN)

Cette commande demande au receveur de confirmer que l'argument identifie une liste de diffusion, et s'il en est ainsi, de retourner les adhérents de cette liste. Si la commande réussit, une réponse est retournée qui contient les informations telles que décrites au paragraphe 3.5. Cette réponse aura plusieurs lignes excepté dans le cas trivial d'une liste d'un seul membre.

Cette commande n'a pas d'effet sur la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission, ni sur la mémoire tampon de données de messagerie et peut être produite à tout moment.

Syntaxe :
"EXPN" SP Chaîne CRLF

4.1.1.8 AIDE (HELP)

Cette commande amène le serveur à envoyer des informations utiles au client. La commande PEUT prendre un argument (par exemple, tout nom de commande) et retourner en réponse des informations plus spécifiques.

Cette commande n'a pas d'effet sur la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission,

ni sur la mémoire tampon de données de messagerie et peut être produite à tout moment.

Les serveurs SMTP DEVRAIENT accepter HELP sans argument et PEUVENT l'accepter avec des arguments.

Syntaxe :
"HELP" [SP Chaîne] CRLF

4.1.1.9 NOOP (NOOP)

Cette commande n'affecte aucun paramètre ou commande faite précédemment. Elle ne spécifie aucune action autre que l'envoi d'une réponse OK par le receveur.

Cette commande n'a pas d'effet sur la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission, ni sur la mémoire tampon de données de messagerie et peut être produite à tout moment. Si une chaîne de paramètres est spécifiée, les serveurs DEVRAIT l'ignorer.

Syntaxe :
"NOOP" [SP Chaîne] CRLF

4.1.1.10 QUITTER (QUIT)

Cette commande spécifie que le receveur DOIT envoyer une réponse OK, puis clore le canal de transmission.

Le receveur NE DOIT PAS clore intentionnellement le canal de transmission avant de recevoir une commande QUIT et y avoir répondu (même si c'était une erreur). L'envoyeur NE DOIT PAS clore intentionnellement le canal de transmission avant d'avoir envoyé une commande QUIT et DEVRAIT attendre jusqu'à recevoir la réponse (même si c'était une réponse d'erreur à une commande précédente). Si la connexion est close prématurément à cause d'une violation de ce qui figure ci-dessus ou d'une défaillance du système ou du réseau, le serveur DOIT annuler toute transaction en cours, mais ne doit pas défaire une transaction précédemment achevée, et DOIT généralement agir comme si la commande ou transaction en cours avait reçu une erreur temporaire (c'est-à-dire, une réponse 4yz).

La commande QUIT peut être produite à tout moment.

Syntaxe :
"QUIT" CRLF

4.1.2 Syntaxe de l'argument de commande

La syntaxe des champs d'argument des commandes ci-dessus (en utilisant la syntaxe spécifiée en [8] le cas échéant) est donnée ci-dessous. Certaines des constructions données ci-dessous ne sont utilisées qu'en conjonction avec les routes de source, comme décrit à l'Appendice C. Les caractères terminaux non définis dans le présent document, comme ALPHA, DIGIT, SP, CR, LF, CRLF, sont définis dans le "cœur" de la syntaxe [8 (section 6)] ou dans la syntaxe de format de message [32].

```
Reverse-path = Path
Forward-path = Path
Path = "<" [ A-d-l ":" ] Mailbox ">"
A-d-l = At-domain *( "," A-d-l )
                        ; Noter que cette forme, ce qu'on appelle la "route de source", DOIT être acceptée, NE DEVRAIT
                        PAS être générée, et DEVRAIT être ignorée.
At-domain = "@" domaine
Mail-parameters = esmtp-param *(SP esmtp-param)
Rcpt-parameters = esmtp-param *(SP esmtp-param)
esmtp-param     = esmtp-keyword ["=" esmtp-value]
esmtp-keyword   = (ALPHA / DIGIT) *(ALPHA / DIGIT / "-")
esmtp-value     = 1*(%d33-60 / %d62-127)
                        ; tout caractère sauf "=", SP, et caractères de contrôle
Keyword  = Ldh-str
Argument = Atom
Domain = (sub-domain 1*("." sub-domain)) / address-literal
```

```
sub-domain = Let-dig [Ldh-str]
address-literal = "[" IPv4-address-literal / IPv6-address-literal / General-address-literal "]"
                        ; voir le paragraphe 4.1.3
Mailbox = Local-part "@" Domain
Local-part = Dot-string / Quoted-string
                        ; PEUT être sensible à la casse
Dot-string = Atom *("." Atom)
Atom = 1*atext
Quoted-string = DQUOTE *qcontent DQUOTE
String = Atom / Quoted-string
```

Bien que la définition ci-dessus pour partie-locale soit relativement permissive, pour une interopérabilité maximale, un hôte qui s'attend à recevoir des messages DEVRAIT éviter de définir des boîtes aux lettres où la partie locale aurait besoin de (ou utiliserait) la forme Chaîne entre guillemets *(Quoted-string)* ou où la partie locale serait sensible à la casse. Pour tout ce qui est de générer ou comparer des parties locales (par exemple, à la recherche de noms de boîte aux lettres spécifiques), toutes les formes entre guillemets DOIVENT être traitées comme équivalentes et le système d'envoi DEVRAIT transmettre la forme qui utilise le minimum de citations possible.

Les systèmes NE DOIVENT PAS définir de boîtes aux lettres d'une façon qui exige l'utilisation de caractères non ASCII en SMTP (octets avec le bit de plus fort poids mis à un) ou "de caractères de contrôle" ASCII (valeur décimale de 0 à 31 et 127). Ces caractères NE DOIVENT PAS être utilisés dans les commandes MAIL ou RCTP ou dans d'autres commandes qui réclament des noms de boîte aux lettres.

Noter que la barre oblique inverse, "\", est un caractère déclaratif, qui est utilisé pour indiquer que le prochain caractère est à utiliser littéralement (au lieu de son interprétation normale). Par exemple, "Joe\,Smith" indique un seul champ d'utilisateur de neuf caractères où la virgule est le quatrième caractère du champs.

Pour promouvoir l'interopérabilité et en cohérence avec les plus anciennes directives pour une utilisation prudente du système DNS dans les dénominations et les applications (par exemple, voir le paragraphe 2.3.1 du document de base DNS, la RFC 1035 [22]), les caractères en dehors de l'ensemble de l'alphabet, des chiffres, et des tirets NE DOIVENT PAS apparaître dans les marqueurs de nom de domaine pour les clients ou les serveurs SMTP. En particulier, le caractère souligné *(underscore)* n'est pas permis. Les serveurs SMTP qui reçoivent une commande dans laquelle des codes de caractère invalides ont été utilisés, et pour lesquels il n'y aurait pas d'autres raisons de rejet, DOIVENT rejeter cette commande avec une réponse 501.

4.1.3 Adresses littérales

Parfois, un hôte n'est pas connu du système de nom de domaine et la communication (et, en particulier, la communication pour rapporter et réparer l'erreur) est bloquée. Pour franchir cette barrière, une forme littérale particulière de l'adresse est permise comme solution de remplacement pour un nom de domaine. Pour les adresses IPv4, cette forme utilise quatre petits entiers décimaux séparés par des points et entourés de crochets tels que [123.255.37.2], qui indique une adresse Internet (IPv4) en forme de séquence d'octets. Pour IPv6 et autres formes d'adressage qui pourraient éventuellement être normalisées, la forme consiste en un "marqueur" normalisé qui identifie la syntaxe de l'adresse, deux points, et l'adresse elle-même, dans un format spécifié au titre de la norme IPv6 [17].

Précisément :

```
IPv4-address-literal = Snum 3("." Snum)
IPv6-address-literal = "IPv6:" IPv6-addr
General-address-literal = Standardized-tag ":" 1*dcontent
Standardized-tag = Ldh-str
        ; DOIT être spécifié dans une RFC en cours de normalisation et enregistré auprès de l'IANA

Snum = 1*3DIGIT         ; représentant une valeur d'entier décimal dans la gamme de 0 à 255
Let-dig = ALPHA / DIGIT
Ldh-str = *( ALPHA / DIGIT / "-" ) Let-dig

IPv6-addr = IPv6-full / IPv6-comp / IPv6v4-full / IPv6v4-comp
IPv6-hex  = 1*4HEXDIG
IPv6-full = IPv6-hex 7(":" IPv6-hex)
IPv6-comp = [IPv6-hex *5(":" IPv6-hex)] "::" [IPv6-hex *5(":" IPv6-hex)]
```

; Le "::" représente au moins deux groupes de 16 bits de zéros. Pas plus de 6 groupes en plus de "::" ne peuvent être présents

IPv6v4-full = IPv6-hex 5(":" IPv6-hex) ":" IPv4-address-literal

IPv6v4-comp = [IPv6-hex *3(":" IPv6-hex)] "::" [IPv6-hex *3(":" IPv6-hex) ":"] IPv4-address-literal

; Le "::" représente au moins deux groupes de 16 bits de zéros. Pas plus de 4 groupes en plus de "::" et de l'adresse littérale IPv4 ne peuvent être présents.

4.1.4 Ordre des commandes

Il y a des restrictions sur l'ordre dans lequel ces commandes peuvent être utilisées.

Une session qui va contenir des transactions de messagerie DOIT d'abord être initialisée par l'utilisation de la commande EHLO. Un serveur SMTP DEVRAIT accepter des commandes pour des non-transactions de messagerie (par exemple, VRFY ou EXPN) sans cette initialisation.

Une commande EHLO PEUT être produite par un client plus tard dans la session. Si elle est produite après le début de la session, le serveur SMTP DOIT vider toutes les mémoires tampon et réinitialiser l'état exactement comme si une commande RSET avait été produite. En d'autres termes, la séquence de RSET suivie immédiatement par EHLO est redondante, mais sans dommage autre que dans le coût en performances de l'exécution de commandes inutiles.

Si la commande EHLO n'est pas acceptable pour le serveur SMTP, des réponses d'échec 501, 500, ou 502 DOIVENT être retournée selon le cas approprié. Le serveur SMTP DOIT rester dans le même état après la transmission de ces réponses que celui dans lequel il était avant la réception du EHLO.

Le client SMTP DOIT, si possible, s'assurer que le paramètre domaine pour la commande EHLO est un nom d'hôte principal valide (pas un CNAME ou un nom MX) pour son hôte. Si ce n'est pas possible (par exemple, lorsque l'adresse du client est allouée de façon dynamique et que le client n'a pas un nom évident) une adresse littérale DEVRAIT être substituée au nom de domaine et des informations supplémentaires fournies pour aider à l'identification du client.

Un serveur SMTP PEUT vérifier que le paramètre de nom de domaine dans la commande EHLO correspond réellement à l'adresse IP du client. Cependant, le serveur NE DOIT PAS refuser d'accepter un message pour cette raison si la vérification échoue : l'information sur l'échec de la vérification n'est que pour la journalisation et le traçage.

Les commandes NOOP, HELP, EXPN, VRFY, et RSET peuvent être utilisées à tout moment durant une session, ou sans avoir préalablement initialisé une session. Les serveurs SMTP DEVRAIENT les traiter normalement (c'est-à-dire, ne pas retourner un code 503) même si aucune commande EHLO n'a encore été reçue ; les clients DEVRAIENT ouvrir une session avec EHLO avant d'envoyer ces commandes.

Si ces règles sont suivies, l'exemple de la RFC 821 qui donne "550 L'accès vous est refusé" en réponse à une commande EXPN est incorrect sauf si une commande EHLO précède le EXPN ou si le refus d'accès se fonde sur l'adresse IP du client ou autre mécanisme d'authentification ou de détermination d'autorisation.

La commande MAIL (ou les commandes obsolètes SEND, SOML, ou SAML) commence une transaction de messagerie. Une fois commencée, une transaction de messagerie consiste en une commande de début de transaction, une ou plusieurs commandes RCTP, et une commande DATA, dans cet ordre. Une transaction de messagerie peut être interrompue par une commande RSET (ou une nouvelle commande EHLO). Il peut y avoir zéro, une, ou plusieurs transactions dans une session. MAIL (ou SEND, SOML, ou SAML) NE DOIT PAS être envoyé si une transaction de messagerie est déjà ouverte, c'est-à-dire qu'elle ne devrait être envoyée que si aucune transaction de messagerie n'a débuté dans la session, ou si la précédente s'est bien terminée avec la réussite d'une commande DATA, ou si la précédente a été interrompue avec un RSET.

Si l'argument de commande de début de transaction n'est pas acceptable, une réponse d'échec 501 DOIT être retournée et le serveur SMTP DOIT rester dans le même état. Si les commandes d'une transaction sont dans un tel désordre qu'elles ne puissent être traitées par le serveur, une réponse d'échec 503 DOIT être retournée et le serveur SMTP DOIT rester dans le même état.

La dernière commande dans une session DOIT être la commande QUIT. La commande QUIT ne peut pas être utilisée à un autre moment de la session, mais DEVRAIT être utilisée par le client SMTP pour demander la clôture de connexion, même lorsque aucune commande d'ouverture de session n'avait été envoyée ni acceptée.

4.1.5 Commandes d'utilisation privée

Comme spécifié au paragraphe 2.2.2, les commandes qui commencent par "X" peuvent être utilisées par accord bilatéral entre les agents SMTP client (envoyeur) et serveur (receveur). Un serveur SMTP qui ne reconnaît pas de telles commandes est censé répondre par "500 Commande non reconnue". Un serveur SMTP avec extensions PEUT faire la liste des noms des dispositifs associés à ces commandes privées dans la réponse à la commande EHLO.

Les commandes envoyées ou acceptées par les systèmes SMTP, qui ne commencent pas par "X" DOIVENT se conformer aux exigences du paragraphe 2.2.2.

4.2 Réponses SMTP

Les réponses aux commandes SMTP servent à s'assurer de la synchronisation des demandes et des actions dans le processus de transfert de messagerie et à garantir que le client SMTP connaît toujours l'état du serveur SMTP. Chaque commande DOIT générer exactement une réponse.

Les détails de la séquence commande-réponse sont décrits au paragraphe 4.3.

Une réponse SMTP consiste en un nombre de trois chiffres (transmis comme trois caractères numériques) suivi par du texte, sauf spécification contraire dans le présent document. Le nombre est utilisé par un automate pour déterminer dans quel état entrer ensuite ; le texte est destiné à l'utilisateur humain. Les trois chiffres contiennent assez d'information codée pour que le client SMTP n'ait pas besoin d'examiner le texte et puisse soit l'éliminer soit le passer à l'usager, en tant que de besoin. Les exceptions sont celles notées par ailleurs dans le présent document. En particulier, les codes de réponse 220, 221, 251, 421, et 551 sont associés au texte du message qui doit être analysé et interprété par les machines. Dans le cas général, le texte peut dépendre du receveur et du contexte, aussi y aura-t-il vraisemblablement des textes différents pour chaque code de réponse. Un exposé sur la théorie des codes de réponse figure au paragraphe 4.2.1. Formellement, une réponse est définie comme la séquence : un code à trois chiffres, <SP>, une ligne de texte, et <CRLF>, ou une réponse multi lignes (comme défini au paragraphe 4.2.1). Comme, en violation de la présente spécification, le texte n'est parfois pas envoyé, les clients qui ne le reçoivent pas DEVRAIENT être prêts à traiter le code seul (avec ou sans caractère espace en queue). Seules les commandes EHLO, EXPN, et HELP sont supposées résulter en réponses multi lignes dans des circonstances normales, cependant, des réponses multi lignes sont permises pour toutes les commandes.

En ABNF, les réponses de serveur sont :
Accueil = "220 " Domaine [SP texte] CRLF
Ligne de réponse = Code-de-réponse [SP texte] CRLF
où "Accueil" n'apparaît que dans la réponse 220 qui annonce que le serveur ouvre sa partie de la connexion.

Un serveur SMTP DEVRAIT n'envoyer que les codes de réponse dont la liste figure dans le présent document. Un serveur SMTP DEVRAIT utiliser le texte donné dans les exemples chaque fois que c'est approprié.

Un client SMTP ne DOIT déterminer ses actions que par le code de réponse, et non par le texte (excepté pour le "changement d'adresse" 251 et 551 et, si nécessaire, les réponses 220, 221, et 421) ; dans le cas général, tout texte, y compris pas de texte du tout (bien que les envoyeurs NE DEVRAIENT PAS envoyer de codes nus) DOIT être acceptable. L'espace (blanche) qui suit le code de réponse est considérée comme partie du texte. Chaque fois que possible, un receveur- SMTP DEVRAIT vérifier le premier chiffre (indication de sévérité) du code de réponse.

La liste des codes qui est donnée ci-dessous NE DOIT PAS être une construction permanente. Bien que l'ajout de nouveaux codes devrait être une activité rare et significative, des informations supplémentaires dans la partie textuelle de la réponse étant préférées, de nouveaux codes peuvent être ajoutés par suite de nouvelles spécifications normalisées ou en cours de normalisation. Par conséquent, un envoyeur SMTP DOIT être prêt à traiter des codes non spécifiés dans le présent document et DOIT le faire en interprétant seulement le premier chiffre.

4.2.1 Sévérité et théorie des codes de réponse

Les trois chiffres de la réponse ont chacun une signification particulière. Le premier chiffre note si la réponse est bonne, mauvaise ou incomplète. Un client SMTP non sophistiqué , ou qui reçoit un code inattendu, sera capable de déterminer sa prochaine action (procéder comme prévu, refaire, retrancher, etc.) en examinant ce premier chiffre. Un client SMTP qui veut savoir approximativement quel type d'erreur est survenu (par exemple, erreur du système de messagerie, erreur de commande, erreur de syntaxe) peut examiner le second chiffre. Le troisième chiffre et toutes les informations supplémentaires qui peuvent être présentes sont réservées au plus fin degré d'information.

Il y a cinq valeurs pour le premier chiffre de code de réponse :

1yz Réponse préliminaire positive
La commande a été acceptée, mais l'action demandée est gardée en suspens, en attendant confirmation des informations contenues dans cette réponse. Le client SMTP devrait envoyer une autre commande pour spécifier de continuer ou d'interrompre l'action. Note : SMTP sans extension n'a aucune commande qui permette ce type de réponse, et n'a donc pas de commande pour continuer ou interrompre.

2yz Réponse d'achèvement positif
L'action demandée a été terminée avec succès. Une nouvelle demande peut être initiée.

3yz Réponse intermédiaire positive
La commande a été acceptée, mais l'action demandée est gardée en suspens, en attendant la réception d'informations ultérieures. Le client SMTP devrait envoyer une autre commande spécifiant cette information. Cette réponse est utilisée dans des groupes de séquences de commandes (c'est-à-dire, dans DATA).

4yz Réponse provisoire d'achèvement négative
La commande n'a pas été acceptée, et l'action demandée ne s'est pas produite. Cependant, la condition d'erreur est temporaire et l'action peut être demandée à nouveau. L'envoyeur devrait retourner au début de la séquence de commande (s'il en est). Il est difficile d'allouer une signification à "provisoire" lorsque deux sites différents (agents SMTP receveur et envoyeur) doivent se mettre d'accord sur son interprétation. Chaque réponse de cette catégorie peut avoir une valeur temporelle différente, mais le client SMTP est encouragé à réessayer. Une règle approximative pour déterminer si une réponse va dans la catégorie 4yz ou 5yz (voir ci-dessous) est que les réponses sont 4yz si elles peuvent réussir en étant répétées sans aucun changement de la forme de la commande ou dans les propriétés de l'envoyeur ou du receveur (c'est-à-dire que la commande est répétée à l'identique et que le receveur ne lance pas une nouvelle mise en œuvre.)

5yz Réponse permanente d'achèvement négative
La commande n'a pas été acceptée et l'action demandée ne s'est pas produite. Il est déconseillé au client SMTP de répéter exactement la même demande (dans la même séquence). Même certaines conditions d'erreur "permanentes" peuvent être corrigées, aussi l'utilisateur humain peut vouloir indiquer au client SMTP de réinitialiser la commande par une action directe dans un moment (par exemple, après avoir changé la rédaction, ou que l'utilisateur ait changé l'état du compte).

Le second chiffre code les réponses dans des catégories spécifiques :

x0z Syntaxe : Ces réponses se réfèrent à des erreurs de syntaxe, à des commandes syntaxiquement correctes qui ne correspondent à aucune catégorie fonctionnelle, et à des commandes non mises en œuvre ou superflues.

x1z Information : Ce sont des réponses à des demandes d'information, comme sur l'état ou pour de l'aide.

x2z Connexions : Ce sont des réponses qui se rapportent au canal de transmission.

x3z Non spécifié.

x4z Non spécifié.

x5z Système de messagerie : Ces réponses indiquent le statut du système de messagerie du receveur vis à vis du transfert demandé ou autre action du système de messagerie.

Le troisième chiffre donne une gradation plus fine de la signification dans chaque catégorie spécifiée après le second chiffre. La liste des réponses illustre cela. Chaque texte de réponse est recommandé plutôt qu'obligatoire, et peut même changer selon la commande à laquelle il est associé. D'un autre côté, les codes de réponse doivent suivre strictement les spécifications de ce paragraphe. Les mises en œuvre de receveur ne devraient pas inventer de nouveaux codes pour des situations légèrement différentes de celles décrites ici, mais plutôt adapter les codes déjà définis.

Par exemple, une commande telle que NOOP, dont la bonne exécution n'offre au client SMTP aucune nouvelle information, va retourner une réponse 250. La réponse est 502 lorsque la commande demande une action non spécifique du site non mise en œuvre. Un raffinement est la réponse 504 pour une commande qui est mise en œuvre, mais demande un paramètre non mis en œuvre.

Le texte de la réponse peut être sur plus d'une ligne ; dans ce cas, le texte complet doit être marqué comme tel pour que le client SMTP sache quand il peut cesser de lire la réponse. Cela exige un format spécial pour indiquer une réponse multi lignes.

Le format des réponses multi lignes exige que chaque ligne, sauf la dernière, commence par le code de réponse, suivi immédiatement par un tiret, "-" (appelés aussi signe moins), suivi par le texte. La dernière ligne commencera par le code de réponse, suivi immédiatement par <SP>, du texte facultatif, et <CRLF>. Comme noté ci-dessus, les serveurs DEVRAIENT envoyer le <SP> si du texte ne suit pas, mais les clients DOIVENT être prêts s'il est omis.

Par exemple:
123-Première ligne
123-Seconde ligne
123-234 Texte commençant par des nombres
123 Dernière ligne

Dans de nombreux cas, le client SMTP a simplement alors besoin de chercher une ligne commençant par le code de réponse suivi par <SP> ou <CRLF> et d'ignorer toutes les lignes précédentes. Dans quelques cas, il y a des données importantes pour le client dans le "texte" de réponse. Le client sera capable d'identifier ces cas d'après le contexte.

4.2.2 Codes de réponse par groupes de fonction

500 Erreur de syntaxe, commande non reconnue (Cela peut inclure des erreurs telles que Ligne de commande trop longue)
501 Erreur de syntaxe dans les paramètres ou les arguments
502 Commande non mise en œuvre (voir au paragraphe 4.2.4)
503 Mauvaise séquence de commandes
504 Paramètre de commande non mis en œuvre
211 État du système, ou réponse d'aide au système
214 Message d'appel au secours (Informations sur la façon d'utiliser le receveur ou sur la signification d'une commande particulière non standard ; cette réponse n'est utile que pour l'usager humain)
220 Service <domaine> prêt
221 Service<domaine> ferme le canal de transmission
421 Service<domaine> non disponible, ferme le canal de transmission (Ce peut être une réponse à toute commande si le service sait qu'il doit fermer)
250 Action de messagerie demandée correcte, terminée
251 Usager non local ; sera transmis à <chemin de transmission> (Voir au paragraphe 3.4)
252 Impossible de vérifier (VRFY) l'usager, mais acceptera le message et tente la livraison (Voir au paragraphe 3.5.3)
450 Action de messagerie demandée non effectuée : boîte aux lettres indisponible (par exemple, boîte aux lettres occupée)
550 Action de messagerie demandée non effectuée : boîte aux lettres indisponible (par exemple, boîte aux lettres introuvable, pas d'accès, ou commande rejetée pour des raisons de politique)
451 Action demandée interrompue : erreur locale de traitement
551 Usager non local ; prière d'essayer <chemin de transmission> (Voir au paragraphe 3.4)
452 Action demandée non effectuée : mémoire système insuffisante
552 Action de messagerie demandée interrompue : allocation de mémoire dépassée
553 Action demandée non effectuée : nom de boîte aux lettres interdit (par exemple, syntaxe de boîte aux lettres incorrecte)
354 Début d'entrée de messagerie ; fin avec <CRLF>.<CRLF>
554 Échec de transaction (Ou, dans le cas de réponse à ouverture de connexion, "Pas de service SMTP ici")

4.2.3 Codes de réponse par ordre numérique

211 État du système, ou réponse d'aide au système
214 Message d'appel au secours (Informations sur la façon d'utiliser le receveur ou sur la signification d'une commande particulière non standard ; cette réponse n'est utile que pour l'usager humain)
220 Service <domaine> prêt
221 Service<domaine> ferme le canal de transmission
250 Action de messagerie demandée correcte, terminée
251 Usager non local ; sera transmis à <chemin de transmission> (Voir au paragraphe 3.4)
252 Impossible de vérifier (VRFY) l'usager, mais acceptera le message et tente la livraison (Voir au paragraphe 3.5.3)
354 Début d'entrée de messagerie ; fin avec <CRLF>.<CRLF>
421 Service<domaine> non disponible, ferme le canal de transmission (Ce peut être une réponse à toute commande si le service sait qu'il doit fermer)
450 Action de messagerie demandée non effectuée : boîte aux lettres indisponible (par exemple, boîte aux lettres occupée)
451 Action demandée interrompue : erreur locale de traitement
452 Action demandée non effectuée : mémoire système insuffisante
500 Erreur de syntaxe, commande non reconnue (Cela peut inclure des erreurs telles que ligne de commande trop longue)
501 Erreur de syntaxe dans les paramètres ou les arguments
502 Commande non mise en œuvre (Voir au paragraphe 4.2.4)
503 Mauvaise séquence de commandes
504 Paramètre de commande non mis en œuvre

550 Action demandée non effectuée : boîte aux lettres indisponible (par exemple, boîte aux lettres introuvable, pas d'accès, ou commande rejetée pour des raisons de politique)
551 Usager non local ; prière de réessayer <chemin de transmission> (Voir au paragraphe 3.4)
552 Action de messagerie demandée interrompue : allocation de mémoire dépassée
553 Action demandée non effectuée : nom de boîte aux lettres interdit (par exemple, syntaxe de boîte aux lettres incorrecte)
554 Échec de transaction (ou, dans le cas de réponse à ouverture de connexion, "Pas de service SMTP ici")

4.2.4 Code de réponse 502

Des questions se sont posées sur le moment où le code de réponse 502 (Commande non mise en œuvre) DEVRAIT être retourné de préférence à d'autres codes. 502 DEVRAIT être utilisé quand la commande est effectivement reconnue par le serveur SMTP, mais pas mise en œuvre. Si la commande n'est pas reconnue, le code 500 DEVRAIT être retourné. Les systèmes SMTP avec extensions NE DOIVENT PAS faire la liste des capacités en réponse à EHLO pour lesquelles ils retourneront des réponses 502 (ou 500).

4.2.5 Codes de réponse après DATA et le <CRLF>.<CRLF> suivant

Lorsque un serveur SMTP retourne un état d'achèvement positif (code 2yz) après que la commande DATA est terminée par <CRLF>.<CRLF>, il accepte la responsabilité :
- de livrer le message (si la boîte aux lettres receveuse existe), ou
- si les tentatives de livrer le message échouent à cause de conditions transitoires, de réessayer la livraison un nombre de fois raisonnable à des intervalles spécifiés au paragraphe 4.5.4.
- si les tentatives de livrer le message échouent à cause de conditions permanentes, ou si des tentatives répétées de livrer le message échouent à cause de conditions transitoires, de retourner la notification appropriée à l'envoyeur du message original (en utilisant l'adresse dans la commande MAIL de SMTP).

Lorsque un serveur SMTP retourne un code d'état d'erreur permanent (5yz) après que la commande DATA est terminée par <CRLF>.<CRLF>, il NE DOIT PAS faire de tentative ultérieure pour délivrer ce message. Le client SMTP conserve la responsabilité de la livraison de ce message et peut soit le retourner à l'usager, soit le remettre en file d'attente pour une tentative ultérieure (voir au paragraphe 4.5.4.1).

L'usager qui est à l'origine du message DEVRAIT être capable d'interpréter le retour d'un état d'échec transitoire (par un message électronique ou autrement) comme une indication de non livraison, comme un échec permanent serait également interprété. C'est-à-dire que si le client SMTP réussit à traiter ces conditions, l'usager ne recevra pas une telle réponse.

Lorsque un serveur SMTP retourne un code d'état d'erreur permanent (5yz) après que la commande DATA est terminée par <CRLF>.<CRLF>, il NE DOIT PAS faire de tentative ultérieure de livraison du message. Comme avec les codes d'état d'erreur temporaire, le client SMTP garde la responsabilité du message, mais NE DEVRAIT PAS essayer à nouveau de livrer au même serveur sans que l'usager révise et intervienne sur le message.

4.3 Séquençage des commandes et des réponses

4.3.1 Généralités sur le séquençage

La communication entre l'envoyeur et le receveur est un dialogue alterné, contrôlé par l'envoyeur. Comme tel, l'envoyeur produit une commande et le receveur y répond. Sauf si d'autres arrangements sont négociés à travers des extensions de service, l'envoyeur DOIT attendre la réponse avant d'envoyer d'autres commandes.

Une réponse importante est l'accueil de connexion. Normalement, un receveur enverra une réponse 220 "Service prêt" lorsque la connexion est réalisée. L'envoyeur DEVRAIT attendre ce message d'accueil avant tout envoi de commandes.

Note : Toutes les réponses de type accueil ont le nom officiel (le nom de domaine principal pleinement qualifié) de l'hôte serveur comme premier mot suivant le code de réponse. Parfois l'hôte n'a pas de nom significatif. Voir en 4.1.3 un exposé sur les solutions de remplacement dans ces situations.

Par exemple,
220 ISIF.USC.EDU Service prêt ou
220 mail.foo.com SuperSMTP v 6.1.2 Service prêt ou
220 [10.0.0.1] Clueless hôte service prêt

Le tableau ci-dessous fait la liste des réponses de succès et d'échec de remplacement pour chaque commande. Ces réponses DEVRAIENT être strictement respectées : un receveur peut substituer du texte dans les réponses, mais la signification et l'action impliquées par les numéros de code et par la séquence spécifique de réponse à la commande ne peuvent pas être altérées.

4.3.2 Séquences de commande-réponse

Chaque commande figure avec ses réponses usuelles possibles. Les préfixes utilisés devant les réponses possibles sont "I" pour intermédiaire, "S" pour succès, et "E" pour erreur. Comme certains serveurs peuvent générer d'autres réponses dans des circonstances particulières, et pour permettre les extensions futures, les clients SMTP DEVRAIENT, quand c'est possible, interpréter seulement le premier chiffre de la réponse et DOIVENT être prêts à traiter les codes de réponse inconnus en interprétant seulement le premier chiffre. Sauf à utiliser les mécanismes d'extension décrits au paragraphe 2.2, les serveurs SMTP NE DOIVENT PAS transmettre à un client SMT¨de codes de réponse autres qu'à trois chiffres ou qui ne commencent pas par un chiffre compris entre 2 et 5 inclus.

Ces règles de séquençage et, en principe, les codes eux-mêmes, peuvent être étendus ou modifiés par les extensions SMTP offertes par le serveur et acceptées (demandées) par le client.

En plus des codes dont la liste figure ci-dessous, toute commande SMTP peut retourner un des codes suivants si les circonstances inhabituelles correspondantes se rencontrent :

500 Pour le cas de la "ligne de commande trop longue" ou si le nom de la commande n'est pas reconnu. Noter que produire une erreur "commande non reconnue" en réponse au sous-ensemble demandé de ces commandes est une violation de la présente spécification.

501 Erreur de syntaxe des commandes ou des arguments. Afin de permettre des extensions futures, les commandes qui sont spécifiées dans le présent document comme n'acceptant pas d'arguments (DATA, RSET, QUIT) DEVRAIENT retourner un message 501 si des arguments sont fournis en l'absence d'extensions publiées dans EHLO.

421 Fermeture du service et clôture du canal de transmission

Les séquences spécifiques sont :

ÉTABLISSEMENT DE CONNEXION
S: 220
E: 554

EHLO ou HELO
S: 250
E: 504, 550

MAIL
S: 250
E: 552, 451, 452, 550, 553, 503

RCPT
S: 250, 251 (mais voir au paragraphe 3.4 la discussion sur 251 et 551)
E: 550, 551, 552, 553, 450, 451, 452, 503, 550

DATA
I: 354 -> data -> S: 250
E: 552, 554, 451, 452
E: 451, 554, 503

RSET
S: 250

VRFY
S: 250, 251, 252
E: 550, 551, 553, 502, 504

EXPN
S: 250, 252
E: 550, 500, 502, 504

HELP
S: 211, 214
E: 502, 504

NOOP
S: 250

QUIT

S: 221

4.4 Informations de trace

Lorsqu'un serveur SMTP reçoit un message à délivrer ou pour traitement ultérieur, il DOIT insérer des informations de trace ("horodatage" ou "Reçu") au début du contenu du message, comme indiqué au paragraphe 4.1.1.4.

Cette ligne DOIT être structurée comme suit :

- Le champ FROM, qui DOIT être fourni dans un environnement SMTP, DEVRAIT contenir à la fois (1) le nom de l'hôte de source tel que présenté dans la commande EHLO et (2) une adresse littérale contenant l'adresse IP de la source, déterminée à partir de la connexion TCP.
- Le champ ID PEUT contenir un "@" comme suggéré dans la RFC 822, mais ce n'est pas obligé.
- Le champ FOR PEUT contenir une liste d'entrées <chemin> quand plusieurs commandes RCTP ont été données. Cela peut poser quelques problèmes de sécurité et n'est habituellement pas souhaitable ; voir au paragraphe 7.2.

Un programme de messagerie Internet NE DOIT PAS changer une ligne Received: qui a été précédemment ajoutée à l'en-tête du message. Les serveurs SMTP DOIVENT ajouter des lignes Received aux messages ; ils NE DOIVENT PAS changer l'ordre des lignes existantes ou insérer des lignes Received à tout autre endroit.

Avec la croissance de l'Internet, la possibilité de comparer les champs Received est importante pour détecter les problèmes, particulièrement de relais lents. Les serveurs SMTP qui créent des champs Received DEVRAIENT utiliser des décalages explicites dans les dates (par exemple, -0800), plutôt que des noms de zone horaires de n'importe quel type. L'heure locale (avec un décalage) est préférée au temps universel (TU) quand c'est faisable. Cette formulation permet de spécifier un peu plus d'informations sur les circonstances locales. Si le TU est nécessaire, le receveur a seulement besoin d'un peu d'arithmétique simple pour convertir les valeurs. L'utilisation du TU perd des informations sur la localisation de la zone horaire du serveur. Si il est souhaité de fournir un nom de zone horaire, il DEVRAIT être inclus dans un commentaire.

Lorsque le serveur SMTP de livraison fait la "livraison finale" d'un message, il insère une ligne de chemin de retour au début des données de messagerie. Cette utilisation du chemin de retour est exigée ; les systèmes de messagerie DOIVENT la prendre en charge. La ligne chemin de retour préserve les informations dans le <chemin inverse> provenant de la commande MAIL. Ici, livraison finale signifie que le message a quitté l'environnement SMTP. Normalement, cela voudrait dire qu'il a été livré à l'usager de destination ou à un point de chute de messagerie associé, mais dans certains cas, il peut encore être traité et transmis par un autre système de messagerie.

Il est possible que la boîte aux lettres dans le chemin de retour soit différente de la boîte aux lettres de l'envoyeur réel, par exemple, si des réponses d'erreur sont à livrer à une boîte aux lettres de traitement d'erreur spéciale plutôt qu'à celle de l'envoyeur du message. Lorsque des listes de diffusion sont impliquées, cet arrangement est courant et utile comme moyen de diriger les erreurs vers celui qui tient la liste à jour plutôt que vers l'origine du message.

Le texte ci-dessus implique que les données de messagerie finales vont commencer par une ligne de chemin de retour, suivie par une ou plusieurs lignes d'horodatage. Ces lignes seront suivies par les en-têtes des données de messagerie et le corps [32].

Il est parfois difficile à un serveur SMTP de déterminer si il fait ou non la livraison finale car la transmission ou d'autres opérations peuvent survenir après l'acceptation de la livraison du message. Par conséquent, tout système postérieur (transmission, passerelle, ou relais) PEUT retirer le chemin de retour et reconstruire la commande MAIL en tant que de besoin pour s'assurer qu'exactement une seule de ces lignes apparaît dans un message délivré.

Un système SMTP générateur de message NE DEVRAIT PAS envoyer un message qui contient déjà un en-tête Return-path. Les serveurs SMTP qui remplissent une fonction de relais NE DOIVENT PAS inspecter les données du message, et en particulier pas au point de déterminer si les en-têtes Return-path sont présents. Les serveurs SMTP qui font la livraison finale PEUVENT retirer les en-têtes Return-path avant d'ajouter le leur.

Le principal objet du chemin de retour est de désigner l'adresse à laquelle les messages indiquant la non délivrance ou autres défaillances du système de messagerie sont à envoyer. Pour qu'il n'y ait pas d'ambiguïté, exactement un chemin de retour DEVRAIT être présent lorsque le message est délivré. Les systèmes qui utilisent la syntaxe de la RFC 822 avec des transports non SMTP DEVRAIENT désigner une adresse sans ambiguïté, associée à l'enveloppe de transport, à laquelle faire rapport des erreurs (par exemple, les messages de non livraison).

Note historique : Le texte de la RFC 822 qui paraît contredire l'utilisation de l'en-tête Return-path (ou l'enveloppe

d'adresse de chemin inverse tirée de la commande MAIL) comme destination des messages d'erreur n'est pas applicable sur l'Internet. L'adresse de chemin inverse (telle que copiée dans Return-path) DOIT être utilisée comme cible de tout message contenant la livraison de messages d'erreur.

En particulier :

- une passerelle de SMTP vers ailleurs DEVRAIT insérer un en-tête de chemin de retour, sauf s'il est connu que le transport "d'ailleurs" utilise aussi les adresses de domaine Internet et conserve séparément l'adresse de l'envoyeur de l'enveloppe.
- une passerelle de ailleurs vers SMTP DEVRAIT supprimer tout en-tête de chemin de retour présent dans le message, et soit copier cette information dans l'enveloppe SMTP, soit la combiner aux informations présentes dans l'enveloppe de l'autre système de transport pour construire l'argument de chemin inverse pour la commande MAIL dans l'enveloppe SMTP.

Le serveur doit réserver un traitement particulier aux cas dans lesquels le processus suivant l'indication de fin des données de messagerie n'est que partiellement réussi. Cela peut arriver si, après avoir accepté plusieurs receveurs et les données de messagerie, le serveur SMTP trouve que les données de messagerie pourraient être livrées avec succès à certains des receveurs, mais pas à tous. Dans un tel cas, la réponse à la commande DATA DOIT être une réponse OK. Cependant, le serveur SMTP DOIT composer et envoyer un message de notification "message non livrable" à l'origine du message.

Il DOIT envoyer une seule liste de notification de tous les receveurs pour lesquels il y a eu échec ou bien des messages de notification séparés pour chaque receveur pour lequel il y a eu échec. Pour épargner la quantité de traitement pour l'envoyeur, la première solution est préférée lorsque possible. Tous les messages de notification de messagerie non livrables sont envoyés en utilisant la commande MAIL (même si ils résultent du traitement des commandes obsolètes SEND, SOML, ou SAML) et un chemin de retour nul comme exposé au paragraphe 3.7.

La ligne d'horodatage et la ligne de chemin de retour sont définies formellement comme suit :

```
Ligne chemin de retour     = "Return-Path:" FWS Chemin-inverse <CRLF>
Ligne horodatage           = "Received:" FWS Horodatage <CRLF>
Horodatage                 = From-domaine By-domaine Opt-info ";"  FWS horodatage
                  ; où "horodatage" est comme défini dans [32] mais les formes "obs-", particulièrement les années
                  ; sur deux chiffres, sont interdites dans SMTP et NE DOIVENT PAS être utilisées.
From-domain                = "FROM" FWS Extended-Domain CFWS
By-domain                  = "BY" FWS Extended-Domain CFWS
Extended-Domain            = Domaine / ( Domaine FWS "(" TCP-info ")" ) / ( Adresse-littérale FWS "(" TCP-info ")" )
TCP-info                   = Adresse-littérale / ( Domaine FWS Adresse-littérale )
                  ; Information déduite par le serveur de la connexion TCP et pas du EHLO du client.
Opt-info                   = [Via] [With] [ID] [For]
Via                        = "VIA" FWS Link CFWS
With                       = "WITH" FWS Protocol CFWS
ID                         = "ID" FWS String / msg-id CFWS
For                        = "FOR" FWS 1*( Path / Mailbox ) CFWS
Link                       = "TCP" / Addtl-Link
Addtl-Link                 = Atom
                  ; Des noms standard supplémentaires pour les liaisons sont enregistrés auprès de l'Autorité d'allocation de
                  numéros de l'Internet (IANA). "Via" n'a de valeur qu'avec les transports non-Internet. Les serveurs SMTP
                  NE DEVRAIENT PAS utiliser de noms non enregistrés.
Protocol                   = "ESMTP" / "SMTP" / Attdl-Protocol
Attdl-Protocol             = Atom
                  ; Des noms standard supplémentaires de protocoles sont enregistrés auprès de l'Autorité d'allocation de
                  numéros de l'Internet (IANA). Les serveurs SMTP NE DEVRAIENT PAS utiliser de noms non enregistrés.
```

4.5 Questions de mise en œuvre supplémentaires

4.5.1 Mise en œuvre minimum

Pour rendre SMTP exploitable, la mise en œuvre minimum suivante est exigée de tous les receveurs. Les commandes suivantes DOIVENT être prises en charge pour la conformité à la présente spécification :

EHLO
HELO
MAIL

RCPT
DATA
RSET
NOOP
QUIT
VRFY

Tout système qui comporte un serveur SMTP qui prend en charge le relais ou la livraison de messagerie DOIT prendre en charge la boîte aux lettres réservée "postmaster" comme un nom local insensible à la casse. Cette adresse de maître de poste n'est pas strictement nécessaire si le serveur retourne toujours 554 à l'ouverture de la connexion (comme décrit au paragraphe 3.1). L'exigence d'acceptation de la messagerie pour le maître de poste implique que les commandes RCTP qui spécifient une boîte aux lettres pour le maître de poste à tous les domaines pour lesquels le serveur SMTP fournit un service de messagerie, aussi bien que le cas particulier de "RCPT TO:<Postmaster>" (sans spécification de domaine), DOIT être satisfaite.

Les systèmes SMTP sont supposés faire tous les efforts raisonnables pour accepter les messages dirigés sur le maître de poste provenant de tous les autres systèmes sur l'Internet. Dans les cas extrêmes – comme de contenir une attaque de déni de service ou autre atteinte à la sécurité -- un serveur SMTP peut bloquer les messages adressés au maître de poste. Cependant, de tels arrangements DEVRAIENT être très encadrés de façon à éviter de bloquer les messages qui n'ont rien à voir avec l'attaque.

4.5.2 Transparence

En l'absence de dispositions pour la transparence des données, la séquence de caractères "<CRLF>.<CRLF>" termine le texte du message et ne peut pas être envoyée par l'usager. En général, les usagers ne sont pas au courant de ces séquences "interdites". Pour permettre que tous les textes composés par les usagers soient transmis de façon transparente, les procédures suivantes sont utilisées :

- Avant l'envoi d'une ligne du texte d'un message, le client SMTP vérifie le premier caractère de la ligne. Si c'est un point, un point supplémentaire est inséré au début de la ligne.
- Lorsqu'une ligne du texte d'un message est reçue par le serveur SMTP, il vérifie la ligne. Si la ligne est composée d'un seul point, elle est traitée comme la fin de l'indicateur de message. Si le premier caractère est un point et qu'il y a d'autres caractères sur la ligne, le premier caractère est supprimé.

Les données de messagerie peuvent contenir n'importe lequel des 128 caractères ASCII. Tous les caractères sont à livrer à la boîte aux lettres du receveur, y compris les espaces, les tabulations verticales et horizontales, et autres caractères de contrôle. Si le canal de transmission fournit un flux de données d'octets de 8 bits, les codes ASCII à 7 bits sont transmis justifiés à droite dans les octets, avec le bit de plus fort poids mis à zéro. Voir au paragraphe 3.7 le traitement spécial de ces conditions dans les systèmes SMTP qui remplissent une fonction de relais.

Dans certains systèmes il peut être nécessaire de transformer les données à mesure qu'elles arrivent et sont mémorisées. Cela peut être nécessaire pour les hôtes qui utilisent un jeu de caractères différent de ASCII comme jeu de caractères local, qui mémorisent les données en enregistrements plutôt qu'en chaînes, ou qui utilisent des séquences de caractères particulières comme délimiteurs à l'intérieur des boîtes aux lettres. Si de telles transformations sont nécessaires, elles DOIVENT être réversibles, particulièrement si elles sont appliquées à de la messagerie à relayer.

4.5.3 Tailles et fin de temporisation

4.5.3.1 Limites de taille et minimums

Il y a plusieurs objets qui ont des tailles minimum/maximum exigées. Chaque mise en œuvre DOIT être capable de recevoir des objets d'au moins ces tailles. Les objets plus grands que ces tailles DEVRAIENT être évités autant que possible. Cependant, certaines constructions de messagerie Internet comme les adresses codées en adresses X.400 [16] vont souvent exiger des objets plus grands : les clients PEUVENT tenter de les transmettre, mais DOIVENT être prêts à ce qu'un serveur les rejette si il ne peut pas les traiter. Dans toute la mesure du possible, les techniques de mise en œuvre qui n'imposent pas de limites à la longueur de ces objets devraient être utilisées.

partie locale
: La longueur totale maximum d'un nom d'utilisateur ou autre partie locale est de 64 caractères.

domaine

La longueur totale maximum d'un nom de domaine ou nombre est de 255 caractères.

chemin
: La longueur totale maximum d'un chemin inverse ou chemin de transmission est de 256 caractères (y compris la ponctuation et les séparateurs d'élément).

ligne de commande
: La longueur totale maximum d'une ligne de commande y compris le mot de commande et le <CRLF> est de 512 caractères. Les extensions SMTP peuvent être utilisées pour augmenter cette limite.

ligne de réponse
: La longueur totale maximum d'une ligne de réponse y compris le code de réponse et le <CRLF> est de 512 caractères. Plus d'informations peuvent être convoyées au moyen de réponses multi lignes.

ligne de texte
: La longueur totale maximum d'une ligne de texte y compris le <CRLF> est de 1000 caractères (non compté le point dupliqué en tête pour la transparence). Ce nombre peut être augmenté par l'utilisation d'extensions de service SMTP.

contenu du message
: La longueur totale maximum d'un contenu de message (incluant tous en-têtes de message et corps de message) DOIT être au moins de 64 Koctets. Depuis l'introduction des normes de l'Internet pour la messagerie multimédia [12], les longueurs de message sur l'Internet ont considérablement grandi, et les restrictions de taille de message devraient être évitées dans toute la mesure du possible. Les systèmes serveur SMTP qui doivent imposer des restrictions DEVRAIENT mettre en œuvre l'extension de service "SIZE" [18], et les systèmes SMTP clients qui envoient de gros messages DEVRAIENT l'utiliser chaque fois que possible.

mémoire tampon de réception
: Le nombre total minimum de receveurs qui doivent être mis en mémoire tampon est de cent receveurs. Le rejet de messages (pour excès de receveurs) avec moins de 100 commandes RCTP est une violation de la présente spécification. Le principe général que les serveurs SMTP relais NE DOIVENT PAS, et les serveurs SMTP de livraison NE DEVRAIENT PAS, effectuer d'essais de validation sur les en-têtes de message, suggère que rejeter un message sur la base du nombre total de receveurs d'après les champs d'en-tête est à déconseiller. Un serveur qui impose une limite au nombre de receveurs DOIT se comporter de façon cohérente, en rejetant les adresses qui dépassent sa limite plutôt que d'éliminer en silence des adresses précédemment acceptées. Un client qui a besoin de délivrer un message qui contient plus de cent commandes RCTP DEVRAIT être prêt à le transmettre en "tronçons" de 100 receveurs si le serveur refuse d'accepter plus de cent receveurs dans un seul message.

Les erreurs dues au dépassement de ces limites peuvent être rapportées en utilisant les codes de réponse. Quelques exemples de codes de réponse sont :

500 Ligne trop longue

ou

501 Chemin trop long

ou

452 Trop de receveurs (voir ci-dessous)

ou

552 Trop de données de message.

La RFC 821 [30] faisait une liste incorrecte des erreurs en attribuant à un serveur SMTP qui dépasse sa limite de mise en œuvre sur le nombre de commandes RCTP ("trop de receveurs") le code de réponse 552. Le code de réponse correct pour cette condition est 452. Les clients DEVRAIENT traiter dans ce cas un code 552 comme une défaillance temporaire plutôt que permanente selon la logique sous-jacente.

Lorsqu'un serveur SMTP conforme rencontre cette condition, il a au moins cent commandes RCTP réussies dans sa mémoire tampon de réception. Si le serveur est capable d'accepter le message, au moins ces cent adresses vont alors être retirées de la file d'attente du client SMTP. Lorsque le client tente la retransmission de ces adresses qui ont reçu des réponses 452, au moins cent d'entre elles seront capables de convenir à la mémoire tampon de réception du serveur SMTP. Chaque tentative de retransmission qui est capable de livrer quelque chose sera capable de se débarrasser d'au moins cent de ces receveurs.

Si un serveur SMTP a une limite de mise en œuvre sur le nombre de commandes RCTP et si cette limite est atteinte, il DOIT utiliser un code de réponse de 452 (mais le client DEVRAIT aussi être prêt pour un 552, comme noté ci-dessus). Si le serveur a une limitation configurée par la politique du site sur le nombre de commandes RCTP, il PEUT utiliser à la place un code de réponse 5XX. Cela pourrait être le plus approprié si la limitation de politique était destinée à s'appliquer lorsque le compte total des receveurs pour un corps de message particulier devait être appliqué même si ce corps de message est envoyé dans plusieurs transactions de messagerie.

4.5.3.2 Fins de temporisation

Un client SMTP DOIT fournir un mécanisme de fin de temporisation. Il DOIT utiliser des fins de temporisation par commande plutôt que d'essayer de fixer une limite de temps à la transaction de messagerie entière. Les fins de temporisation DEVRAIENT être facilement reconfigurables, de préférence sans recompiler le code SMTP. Pour mettre cela en œuvre, un temporisateur est établi pour chaque commande SMTP et pour chaque mémoire tampon du transfert de données. Cette dernière signifie qu'une temporisation globale est par nature proportionnelle à la taille du message.

Sur la base d'une expérience extensive des hôtes actifs dans le relais de messagerie, les valeurs minimum de temporisation par commande DEVRAIENT être les suivantes :

Message 220 initial : 5 minutes

> Un processus de client SMTP a besoin de distinguer entre une défaillance de connexion TCP et des délais dans la réception du message d'accueil initial. Beaucoup des serveurs SMTP acceptent une connexion TCP mais retardent la livraison du message 220 jusqu'à ce que la charge de leur système permette le traitement de plus de messages.

Commande MAIL : 5 minutes

Commande RCPT : 5 minutes

> Une temporisation plus longue est nécessaire si le traitement des listes de diffusion et des alias n'est pas différé jusqu'à l'acceptation du message.

Initiation de DATA : 2 minutes

> C'est le délai d'attente de la réponse "354 Début des entrées" à une commande DATA.

Bloc de données : 3 minutes

> C'est le délai d'attente de l'achèvement de chaque appel TCP SEND qui transmet un tronçon de données.

Terminaison de DATA : 10 minutes.

> C'est en attendant la réponse "250 OK". Quand le receveur obtient le point final qui termine les données du message, il effectue normalement le traitement pour la livraison du message à la boîte aux lettres d'un usager. Une temporisation parasite à ce moment pourrait être ruineuse et résulterait normalement en la livraison de plusieurs copies du message, car il a été envoyé avec succès et le serveur a accepté la responsabilité de la livraison. Voir au paragraphe 6.1 un exposé supplémentaire.

Un serveur SMTP DEVRAIT avoir une temporisation d'au moins 5 minutes lorsqu'il attend la prochaine commande de l'envoyeur.

4.5.4 Stratégies de recommencement

La structure commune des mises en œuvre d'hôte SMTP comporte la boîte aux lettres d'usager, une ou plusieurs zones pour mettre en file d'attente les messages en transit, et une ou plusieurs routines pour envoyer et recevoir le courrier. La structure exacte va varier selon les besoins des usagers sur l'hôte et le nombre et la taille des listes de diffusion prises en charge par l'hôte. On décrit plusieurs optimisations qui se sont révélées utiles, en particulier pour les messageurs qui soutiennent de hauts niveaux de trafic.

Toute stratégie de mise en file d'attente DOIT inclure des temporisations sur toutes les activités commande par commande. Une stratégie de mise en file d'attente NE DOIT envoyer en aucun cas de message d'erreur en réponse à des messages d'erreur.

4.5.4.1 Stratégie d'envoi

Le modèle général pour un client SMTP est d'avoir un ou plusieurs processus qui essayent périodiquement de transmettre les messages sortants. Dans un système normal, le programme qui compose un message a une méthode pour demander une attention immédiate à un nouvel élément de courrier sortant, alors que le courrier qui ne peut être transmis immédiatement DOIT être mis en file d'attente et réessayé périodiquement par l'envoyeur. Une entrée de file d'attente de messagerie inclura non seulement le message lui-même mais aussi les informations d'enveloppe.

L'envoyeur DOIT s'imposer un délai avant de réessayer une destination particulière après l'échec d'une tentative. En

général, l'intervalle d'essai DEVRAIT être au moins de 30 minutes ; cependant, des stratégies plus sophistiquées et variables seront bénéfiques lorsque le client SMTP peut déterminer la raison de la non livraison.

Les essais continuent jusqu'à ce que le message soit transmis ou que l'envoyeur abandonne ; le délai d'abandon a généralement besoin d'être d'au moins 4 à 5 jours. Les paramètres de l'algorithme de réessai DOIVENT être configurables.

Un client DEVRAIT tenir une liste des hôtes qu'il ne peut pas joindre et les temporisations de connexion correspondantes, plutôt que de simplement réessayer les éléments de messagerie en file d'attente.

L'expérience suggère que les défaillances sont normalement transitoires (le système cible ou sa connexion sont en panne), et milite en faveur d'une politique de deux tentatives de connexion dans la première heure de mise en file d'attente du message, puis de revenir à une tentative toutes les deux ou trois heures.

Le client SMTP peut raccourcir le délai de mise en file d'attente en coopération avec le serveur SMTP. Par exemple, si du courrier est reçu d'une adresse particulière, il est vraisemblable que les messages en file d'attente pour cet hôte peuvent maintenant être envoyés. L'application de ce principe peut, dans de nombreux cas, éliminer l'exigence d'une fonction explicite "d'envoi immédiat de la file d'attente" telle que ETRN [9].

La stratégie peut être encore modifiée par l'existence de plusieurs adresses par hôte (voir ci-dessous) pour optimiser les temps de livraison par rapport à l'utilisation des ressources.

Un client SMTP peut avoir une grosse file d'attente de messages pour chaque hôte de destination injoignable. Si tous ces messages devaient être réessayés à chaque cycle d'essais, cela créerait une redondance excessive pour l'Internet et le système d'envoi pourrait être bloqué pour de longues périodes. Noter qu'un client SMTP peut généralement déterminer qu'une tentative de livraison a échoué après seulement une temporisation de plusieurs minutes et même d'une temporisation d'une minute par connexion résultera un très fort délai si les essais sont répétés pour des douzaines, ou même des centaines, de messages en file d'attente pour le même hôte.

En même temps, les clients SMTP DEVRAIENT veiller avec grand soin à mettre en antémémoire les réponses négatives provenant des serveurs. Dans un cas extrême, si EHLO est produit plusieurs fois durant la même connexion SMTP, des réponses différentes peuvent être retournées par le serveur. Plus significatif, les réponses 5yz à la commande MAIL NE DOIVENT PAS être mises en antémémoire.

Lorsqu'un message électronique est à livrer à plusieurs receveurs, et que le serveur SMTP auquel une copie du message est à envoyer est le même pour plusieurs receveurs, une seule copie du message DEVRAIT alors être transmise. C'est à dire que le client SMTP DEVRAIT utiliser la séquence de commandes : MAIL, RCPT, RCPT,... RCPT, DATA au lieu de la séquence : MAIL, RCPT, DATA, ..., MAIL, RCPT, DATA. Cependant, si il y a de très nombreuses adresses, une limite au nombre de commandes RCTP par commande MAIL PEUT être imposée. La mise en œuvre de ce dispositif efficace est vivement encouragée.

De même, pour réaliser une livraison en temps et en heure, le client SMTP PEUT accepter plusieurs transactions de messagerie sortantes concurrentes. Cependant, des limites peuvent être appropriées pour protéger l'hôte contre le fait de consacrer toutes ses ressources à la messagerie.

4.5.4.2 Stratégie de réception

Le serveur SMTP DEVRAIT tenter de garder l'écoute à tout moment sur tous les accès SMTP. Cela exige la prise en charge de plusieurs connexions TCP pour SMTP. Certaines limites PEUVENT être imposées mais les serveurs qui ne peuvent traiter plus d'une transaction SMTP à la fois ne sont pas conformes aux intentions de la présente spécification.

Comme exposé plus haut, lorsque le serveur SMTP reçoit du courrier provenant d'une adresse d'hôte particulière, il pourrait activer ses propres mécanismes SMTP de mise en file d'attente pour réessayer tous les messages en cours pour cette adresse.

4.5.5 Messages avec un chemin inverse nul

Il y a plusieurs types de messages de notification dont il est exigé par les normes existantes et proposées qu'ils soient envoyés avec un chemin inverse nul, à savoir les notifications de non livraison exposées au paragraphe 3.7, d'autres sortes de notifications d'état de livraison (DSN, *Delivery Status Notification*) [24], et aussi les notifications de disposition de message (MDN, *Message Disposition Notification*) [10]. Toutes ces sortes de messages sont des notifications au sujet de

messages précédents, et elles sont envoyées sur le chemin inverse du message électronique précédent. (Si la livraison d'un tel message de notification échoue, cela indique habituellement un problème du système de messagerie de l'hôte auquel le message de notification est adressé. Pour cette raison, sur certains hôtes le MTA est réglé pour transmettre de tels messages de notification en échec à quelqu'un qui est capable de régler les problèmes du système de messagerie, par exemple, via l'alias du maître de poste.)

Tous les autres types de messages (c'est-à-dire, tout message dont il n'est pas exigé par une RFC en cours de normalisation d'avoir un chemin inverse nul) DEVRAIENT être envoyés avec un chemin inverse valide, non nul.

Les développeurs de processeur automatique de messagerie électronique devraient veiller à s'assurer que les diverses sortes de messages de chemin inverse nul sont traités correctement. En particulier, de tels systèmes NE DEVRAIENT PAS répondre aux messages à chemin inverse nul.

5 Résolution d'adresse et traitement de messagerie

Une fois qu'un client SMTP a identifié lexicalement un domaine auquel du courrier sera livré pour traitement (comme décrit aux paragraphes 3.6 et 3.7), une recherche DNS DOIT être effectuée pour résoudre le nom de domaine [22]. Les noms sont supposés être des noms de domaine pleinement qualifiés (FQDN) : les mécanismes pour déduire les FQDN des noms partiels ou d'alias locaux sortent du domaine d'application de la présente spécification et, du fait de nombreux problèmes, sont généralement déconseillés. La recherche vise d'abord à localiser un enregistrement MX associé au nom. Si un enregistrement CNAME est trouvé à la place, le nom résultant est traité comme s'il était le nom initial. Si aucun enregistrement MX n'est trouvé, mais qu'un RR A est trouvé, le RR A est traité comme s'il était associé à un RR MX implicite, avec une préférence de 0, pointant sur cet hôte. Si un ou plusieurs RR MX sont trouvés pour un nom donné, les systèmes SMTP NE DOIVENT utiliser aucun RR A associé à ce nom à moins qu'il soit localisé en utilisant les RR MX ; la règle "MX implicite" donnée plus haut ne s'applique que si aucun enregistrement MX n'est présent. Si des enregistrements MX sont présents, mais qu'aucun d'eux n'est utilisable, cette situation DOIT être rapportée comme erreur.

Lorsque la recherche réussit, la transposition peut résulter en une liste d'adresses de livraison de remplacement plutôt qu'en une seule adresse, à cause de plusieurs enregistrements MX, d'une origine multiple, ou des deux. Pour fournir une transmission de messagerie fiable, le client SMTP DOIT être capable d'essayer (et réessayer) chacune des adresses pertinentes dans l'ordre de cette liste, jusqu'à la réussite d'une tentative de livraison. Cependant, il PEUT aussi y avoir une limite configurable du nombre d'adresses de remplacement qui peuvent être essayées. Dans tous les cas, le client SMTP DEVRAIT essayer au moins deux adresses.

Deux types d'informations sont utilisés pour ordonner les adresses d'hôte : les enregistrements MX multiples, et les hôtes à origine multiple.

Les enregistrements MX multiples contiennent une indication de préférence qui DOIT être utilisée pour le tri (voir ci-dessous). Les nombres inférieurs sont préférés aux nombres supérieurs. Si il y a plusieurs destinations avec la même préférence et qu'il n'y a pas de raison précise en faveur de l'une (par exemple, par reconnaissance d'une adresse facile à atteindre), l'envoyeur SMTP DOIT alors faire un choix aléatoire entre elles pour étaler la charge sur plusieurs échangeurs de messagerie pour une organisation spécifique.

L'hôte de destination (peut-être tiré de l'enregistrement MX préféré) peut être à origine multiple, auquel cas le résolveur de nom de domaine retournera une liste d'adresses IP de remplacement. Il est de la responsabilité de l'interface de résolveur de nom de domaine d'ordonner cette liste par ordre de préférence décroissante si nécessaire, et SMTP DOIT les essayer dans l'ordre présenté.
Bien que la capacité à essayer plusieurs adresses de remplacement soit exigée, des installations spécifiques peuvent vouloir limiter ou désactiver l'utilisation d'adresses de remplacement. La question de savoir si un envoyeur devrait faire des essais utilisant les différentes adresses d'un hôte à origines multiples a été controversée. Le principal argument en faveur de l'utilisation de plusieurs adresses est que cela maximise la probabilité de livraison en temps et en heure, et bien sûr quelquefois la probabilité de livraison tout court ; le contre argument est qu'il peut en résulter une consommation inutile de ressources. Noter que l'utilisation des ressources est aussi fortement déterminé par la stratégie d'envoi discutée au paragraphe 4.5.4.1.

Si un serveur SMTP reçoit un message avec une destination pour laquelle il y a un échangeur de messagerie (MX, *Mail eXchanger*) désigné , il PEUT relayer le message (éventuellement après avoir réécrit les adresses de MAIL FROM et/ou RCPT TO), faire la livraison finale du message, ou l'écarter en utilisant un mécanisme extérieur à l'environnement de transport fourni par SMTP. Bien sûr, aucun de ces derniers ne requiert que la liste des enregistrements MX soit examinée

plus avant.

Si il détermine qu'il devrait relayer le message sans réécrire l'adresse, il DOIT trier les enregistrements MX pour déterminer les candidats à la livraison. Les enregistrements sont d'abord classés par préférence, avec la préférence aux enregistrements de plus faible numéro. L'hôte relais DOIT ensuite inspecter la liste pour chercher des noms ou adresses qui pourraient être connus dans des transactions de messagerie. Si un enregistrement correspondant à ces critères est trouvé, tous les enregistrements à ce niveau de préférence et ceux de numéro de préférence plus élevé DOIVENT être éliminés de la recherche. Si il ne reste aucun enregistrement à ce point, c'est une condition d'erreur, et le message DOIT être retourné comme non livrable. Si des enregistrements subsistent, ils DEVRAIENT être essayés, le préféré en premier, comme décrit ci-dessus.

6 Détection de problème et traitement

6.1 Livraison fiable et réponses par messagerie électronique

Quand le receveur SMTP accepte de la messagerie (en envoyant un message "250 OK" en réponse à DATA), il accepte la responsabilité de livrer ou relayer le message. Il doit prendre cette responsabilité au sérieux. Il NE DOIT PAS perdre le message pour des raisons frivoles, comme une défaillance ultérieure de l'hôte ou à cause d'un manque de ressources prévisible.

Si il y a un échec de la livraison après l'acceptation d'un message, le receveur SMTP DOIT formuler un message de notification et l'envoyer. Cette notification DOIT être envoyée en utilisant un chemin inverse nul ("<>") dans l'enveloppe. Le receveur de cette notification DOIT être l'adresse tirée du chemin de retour de l'enveloppe (ou la ligne Return-Path:). Cependant, si cette adresse est nul ("<>"), le receveur SMTP NE DOIT PAS envoyer de notification. Visiblement, rien dans cette section ne peut ou ne devrait interdire des décisions locales (c'est-à-dire, au titre du même environnement système que le receveur SMTP) d'enregistrer ou autrement transmettre localement des informations sur des événements d'adresse nulle si cela est souhaité. Si l'adresse est une route de source explicite, elle DOIT être effacée lors du bond final.

Par exemple, supposons qu'une notification d'erreur doive être envoyée pour un message arrivé avec :

MAIL FROM:<@a,@b:user@d>

Le message de notification DOIT être envoyé en utilisant :

RCPT TO:<user@d>

Certains échecs de livraison après l'acceptation du message par SMTP vont être inévitables. Par exemple, il peut être impossible au serveur SMTP receveur de valider toutes les adresses de livraison dans la ou les commandes RCTP à cause d'une erreur système du domaine du "logiciel", parce que la cible est une liste de diffusion (voir plus haut la discussion de RCPT), ou parce que le serveur agit comme relais et n'a pas d'accès immédiat au système de livraison.

Pour éviter de recevoir des messages dupliqués par suite de dépassements de temporisations, un receveur SMTP DOIT chercher à minimiser le délai nécessaire pour répondre à l'indicateur <CRLF>.<CRLF> de fin de données. Voir à la RFC 1047 [28] la discussion de ce problème.

6.2 Détection de boucle

Le simple comptage du nombre d'en-têtes "Received:" dans un message s'est révélé être une méthode efficace, bien que rarement optimale, pour détecter les boucles dans les systèmes de messagerie. Les serveurs SMTP qui utilisent cette technique DEVRAIENT avoir un seuil de rejet élevé, normalement d'au moins cent entrées reçues. Quel que soit le mécanisme utilisé, les serveurs DOIVENT contenir des dispositions pour détecter et arrêter les boucles évidentes.

6.3 Compensation des irrégularités

Malheureusement, des variations, des interprétations créatives, et des violations flagrantes des protocoles de messagerie Internet apparaissent effectivement ; certains suggèrent même qu'elles surviennent assez fréquemment. Le débat sur la question de savoir si un receveur ou relais SMTP bien conformé devrait rejeter un message mal formé, tenter de le passer inchangé, ou tenter de le réparer pour accroître le score des succès de livraison (ou de réponses subséquentes) a commencé presque à l'aube de la messagerie sur les réseaux structurés et ne donne pas le moindre signe d'apaisement. Les avocats du rejet font valoir que les tentatives de réparation sont rarement parfaitement adéquates et que le rejet des mauvais messages est la seule façon d'obtenir la réparation du logiciel défectueux. Les avocats de la réparation ou de la livraison à tout va

argumentent que l'usager préfère que les messages passent quoi qu'il arrive et qu'il y a une pression significative du marché dans cette direction. En pratique, ces pressions du marché peuvent être plus importantes sur les fabricants que la stricte conformité aux normes, quelles que soient les préférences des développeurs réels.

Les problèmes associés aux messages mal formés ont été exacerbés par l'introduction des protocoles de lecture de messagerie à agent d'usager divisé [3, 26, 5, 21]. Ces protocoles ont encouragé l'utilisation de SMTP comme protocole de courrier, et les serveurs SMTP comme systèmes de relais pour ces hôtes client (qui sont souvent connectés de façon seulement intermittente à l'Internet). Historiquement, il manquait à nombre de ces machines clientes les mécanismes et les informations assumés par SMTP (et bien sûr, par le protocole de format de messagerie [7]). Certains d'entre eux ne pouvaient même pas garder une trace adéquate de l'heure ; d'autres n'avaient aucune idée du concept de zone horaire ; d'autres encore ne pouvaient pas identifier leur propre nom ou adresse ; et, bien sûr, aucun ne pouvait satisfaire aux hypothèses qui sous-tendent la conception de la RFC 822 sur les adresses authentifiées.

En réponse à ces clients SMTP faibles, de nombreux systèmes SMTP complètent maintenant les messages qui leur sont livrés en une forme incomplète ou incorrecte. Cette stratégie est généralement considérée comme appropriée lorsque le serveur peut identifier ou authentifier le client, et qu'il y a un accord préalable entre eux. À l'opposé, il y a beaucoup de souci à ce faire au sujet des corrections faites par un serveur SMTP de relais ou de livraison qui n'a que peu ou pas du tout de connaissances sur la machine cliente ou de l'usager.

Les changements suivants PEUVENT être appliqués à un message en cours de traitement, quand nécessaire, par un serveur SMTP d'origine, ou un serveur utilisé comme cible de SMTP comme protocole de messagerie initial :
- Ajout d'un champ identifiant de message lorsqu'il n'en apparaît aucun
- Ajout d'une date, heure ou zone horaire lorsqu'il n'y en a pas
- Correction des adresses au format FQDN approprié.

Moins le serveur a d'informations sur le client, moins ces changements auront de chances d'être corrects et la plus grande prudence devrait être observée lorsqu'on se demande s'il faut ou nom effectuer des réparations et comment les faire. Ces changements NE DOIVENT PAS être appliqués par un serveur SMTP qui fournit une fonction de relais intermédiaire.

Dans tous les cas, des clients qui fonctionnent de façon appropriée en fournissant des informations correctes sont préférés à des corrections par le serveur SMTP. Dans tous les cas, la documentation des actions effectuées par les serveurs (dans les champs de trace et/ou les commentaires d'en-tête) est vivement encouragée.

7 Considérations pour la sécurité

7.1 Sécurité de la messagerie et usurpation d'identité

La messagerie SMTP n'est par nature pas sûre en ce qu'il est parfaitement faisable même pour un usager très ordinaire de négocier directement avec les serveurs SMTP de réception et de relais et de créer des messages qui tromperont un receveur innocent en lui faisant croire qu'ils viennent d'autre part. La construction d'un message tel que le comportement "d'usurpation" ne puisse être détecté par un expert est un peu plus difficile, mais pas suffisamment pour être une dissuasion envers quelqu'un de déterminé et compétent. Par conséquent, comme les connaissances en matière de messagerie Internet augmentent, il est de plus en plus connu que la messagerie SMTP ne peut, par nature, être authentifiée, et que des vérifications d'intégrité ne peuvent pas être fournies, au niveau transport. La sécurité réelle de la messagerie repose seulement sur des méthodes de bout en bout qui impliquent les corps de message, comme celles qui utilisent les signatures numériques (voir [14] et, par exemple, PGP [4] ou S/MIME [31]).

Diverses extensions de protocole et options de configuration qui fournissent l'authentification au niveau transport (par exemple, d'un client SMTP à un serveur SMTP) améliorent quelque peu la situation traditionnelle décrite ci-dessus. Cependant, sauf si elles sont accompagnées de transferts prudents de responsabilité dans un environnement de confiance conçu avec soin, elles restent par nature plus faibles que des mécanismes de bout en bout qui utilisent des messages à signature numérique plutôt que de dépendre de l'intégrité du système de transport.

Les efforts pour rendre plus difficile aux usagers un réglage des champs "From" d'en-tête et chemin de retour de l'enveloppe pointant sur des adresses valides autres que la leur s'égarent dans une grande mesure : ils frustrent des applications légitimes dans lesquelles le courrier est envoyé par un usager au nom d'un autre, ou dans lesquelles des réponses d'erreur (ou normales) devraient être dirigées sur une adresse spéciale. (Les systèmes qui donnent aux utilisateurs des moyens convenables pour altérer ces champs message par message devraient essayer d'établir une adresse de boîte aux lettres principale et permanente pour l'utilisateur de telle sorte que les champs Sender au sein des données de message

puissent être générés de façon raisonnable.)

La présente spécification ne creusera pas plus loin les questions d'authentification associées à SMTP tout en plaidant qu'une fonctionnalité utile ne doit pas être désactivée dans l'espoir de fournir une maigre marge de protection contre un usager ignorant qui essaye de trafiquer la messagerie.

7.2 Copies "aveugles"

Les adresses qui n'apparaissent pas dans les en-têtes de message peuvent apparaître dans les commandes RCTP à un serveur SMTP pour un certain nombre de raisons. Les deux plus courantes impliquent l'utilisation d'une adresse de messagerie comme d'un "diffuseur de courrier" (une seule adresse qui se résout en plusieurs adresses) et l'apparition de "copies aveugles". Particulièrement lorsque plus d'une commande RCTP est présente, et afin d'éviter de contrecarrer certains des objets de ces mécanismes, les clients et les serveurs SMTP NE DEVRAIENT PAS copier tout l'ensemble des arguments de la commande RCTP dans les en-têtes, soit au titre des en-têtes de trace soit pour des en-têtes d'information ou d'extension privée. Comme cette règle est souvent violée en pratique, et ne peut pas être mise en application, les systèmes SMTP d'envoi qui sont au fait de l'utilisation "bcc" PEUVENT trouver utile d'envoyer chaque copie aveugle comme une transaction de message séparée contenant seulement une commande RCTP.

Il n'y a pas de relation inhérente entre l'adresse "inverse" (des commandes MAIL, SAML, etc.,) ou "de transmission" (RCPT) dans la transaction SMTP ("enveloppe") et l'adresse dans l'en-tête. Les systèmes receveurs NE DEVRAIENT PAS tenter de déduire de telles relations et de les utiliser pour altérer les en-têtes de message pour la livraison. L'en-tête populaire "Apparamment-pour" est une violation de ce principe ainsi qu'une source fréquence de divulgation involontaire d'informations et NE DEVRAIT PAS être utilisé.

7.3 VRFY, EXPN, et la sécurité

Comme exposé au paragraphe 3.5, les sites individuels peuvent vouloir désactiver VRFY ou/et EXPN pour des raisons de sécurité. En corollaire de ci-dessus, les mises en œuvre qui permettent cela NE DOIVENT PAS paraître avoir vérifié des adresses qui ne sont pas, en fait, vérifiées. Si un site désactive ces commandes pour des raisons de sécurité, le serveur SMTP DOIT retourner une réponse 252, plutôt qu'un code qui pourrait être confondu avec une vérification réussie ou non.

Le retour d'un code de réponse 250 avec l'adresse figurant dans la commande VRFY après avoir seulement vérifié la syntaxe viole cette règle. Bien sûr, une mise en œuvre qui "prend en charge" VRFY en retournant toujours 550 que l'adresse soit valide ou non est également non conforme.

Durant ces dernières années, le contenu des listes de diffusion est devenu populaire comme source d'informations d'adresses pour ce qu'on appelle les "polluposteurs". L'utilisation de EXPN pour "engranger" des adresses a augmenté lorsque les administrateurs de listes ont installé des protections contre les usages inappropriés des listes elles-mêmes. Les mises en œuvre DEVRAIENT encore prendre en charge EXPN, mais les sites DEVRAIENT évaluer avec soin les avantages et inconvénients. Comme des mécanismes d'authentification sont introduits dans SMTP, certains sites pourraient choisir de ne rendre EXPN disponible qu'aux demandeurs authentifiés.

7.4 Divulgation d'informations dans les annonces

Il y a eu un débat sur les avantages et les inconvénients pour la correction d'erreurs d'annoncer le type et la version du serveur (et parfois même du nom de domaine du serveur) dans la réponse d'accueil ou en réponse à la commande HELP et des désavantages de l'exposition d'informations qui pourraient être utiles à une potentielle attaque hostile. L'utilité des informations de correction d'erreurs ne fait aucun doute. Ceux qui plaident en faveur de les rendre disponibles soulignent qu'il vaut bien mieux sécuriser réellement un serveur SMTP plutôt que d'espérer que dissimuler des faiblesses connues en cachant l'identité précise du serveur fournira une meilleure protection. Les sites sont encouragés à évaluer le compromis en gardant cette question présente à l'esprit ; les mises en œuvre sont fortement encouragées à rendre disponibles au minimum les informations de type et de version de quelque façon que ce soit aux autres hôtes du réseau.

7.5 Divulgation d'informations dans les champs Trace

Dans certaines circonstances, telles que lorsque le message prend sa source au sein d'un LAN dont les hôtes ne sont pas directement sur l'Internet public, les champs de trace ("Received") produits en conformité avec la présente spécification peuvent divulguer des noms d'hôte et informations similaires qui ne seraient pas normalement disponibles. Ceci ne pose

ordinairement pas de problème, mais des sites avec des préoccupations particulières en matière de divulgation de nom devraient en être avertis. Aussi, la clause FOR facultative devrait être fournie avec prudence ou pas du tout quand plusieurs receveurs sont impliqués de peur qu'elle ne divulgue par inadvertance les identités de receveurs en "copie aveugle" aux autres receveurs.

7.6 Divulgation d'informations dans la transmission des messages

Comme exposé au paragraphe 3.4, l'utilisation des codes de réponse 251 ou 551 pour identifier les remplacements d'adresse associés à une boîte aux lettres peut divulguer par inadvertance des informations sensibles. Les sites qui sont concernés par ces questions devraient s'assurer qu'ils choisissent et configurent les serveurs de façon appropriée.

7.7 Portée du fonctionnement des serveurs SMTP

Il est un principe bien établi qu'un serveur SMTP peut refuser d'accepter des messages pour toute raison opérationnelle ou technique qui a un sens pour le site qui fournit le serveur. Cependant, c'est la coopération entre les sites et les installations qui rend l'Internet possible. Si les sites tirent un avantage excessif du droit de rejeter le trafic, l'universalité de la disponibilité de la messagerie électronique (une des forces de l'Internet) sera menacée ; il faut bien réfléchir aux conséquences et veiller à un équilibre lorsqu'un site décide d'être sélectif quant au trafic qu'il va accepter et traiter.

Dans les années récentes, l'utilisation de la fonction de relais à travers des sites choisis de façon arbitraire a été mise à profit au titre d'efforts hostiles pour cacher les origines réelles de messages. Certains sites ont décidé de limiter l'utilisation de la fonction relais à des sources connues ou identifiables, et les mises en œuvre DEVRAIENT fournir la capacité d'effectuer ce type de filtrage. Lorsque des messages sont rejetés pour cela ou pour d'autres raisons de politique, un code 550 DEVRAIT être utilisé en réponse à, selon le cas, EHLO, MAIL, ou RCPT.

8 Considérations relatives à l'IANA

IANA entretiendra trois registres à l'appui de la présente spécification. Le premier comporte les extensions de service SMTP avec les mots clés associés, et, en tant que de besoin, les paramètres et verbes. Comme spécifié au paragraphe 2.2.2, aucune entrée ne peut être faite dans ce registre qui commence par un "X". Les entrées ne peuvent être faites que pour les extensions de service (et les mots clés, paramètres ou verbes associés) qui sont définies dans les RFC en cours de normalisation ou expérimentales spécifiquement approuvées par l'IESG à cette fin.

Le second registre comporte les "marqueurs" qui identifient les formes de domaines littéraux autres que ceux pour les adresses IPv4 (spécifiés dans la RFC 821 et dans le présent document) et pour les adresses IPv6 (spécifiés dans le présent document). Des types littéraux supplémentaires devront être normalisés avant utilisation ; aucun n'est prévu pour l'instant.

Le troisième, établi par la RFC 821 et renouvelé par la présente spécification, est un registre des identifiants de lien et de protocoles à utiliser avec les sous paragraphes "via" et "with" de l'horodatage (en-tête "Received:") décrits au paragraphe 4.4. Les identifiants de lien et de protocole s'ajoutant à ceux spécifiés dans le présent document ne peuvent être enregistrés que par normalisation ou au moyen d'une extension de protocole expérimental documenté dans une RFC et approuvée par l'IESG.

9 Références

[1] American National Standards Institute (anciennement United States of America Standards Institute), X3.4, 1968, "USA Code for Information Interchange". ANSI X3.4-1968 a été remplacé par de nouvelles versions avec de légères modifications, mais la version de 1968 reste d'actualité pour l'Internet.

[2] R. Braden, "Exigenges pour les hôtes Internet - application et prise en charge", STD 3, RFC 1123, octobre 1989.

[3] M. Butler, D. Chase, J. Goldberger, J. Postel et J. Reynolds, "Protocole Post Office - version 2", RFC 937, février 1985.

[4] J. Callas, L. Donnerhacke, H. Finney et R. Thayer, "Format de message OpenPGP", RFC 2440, novembre 1998.

[5] M. Crispin, "Protocole d'accès de messagerie interactive - version 2", RFC 1176, août 1990.

[6] M. Crispin, "Protocole d'accès aux messages Internet - version 4", RFC 2060, décembre 1996.

[7] D. Crocker, "Norme pour le format des messages de texte ARPA", RFC 822, août 1982.

[8] D. Crocker et P. Overell, éd., "BNF augmenté pour les spécifications de syntaxe : ABNF", RFC 2234, novembre 1997.

[9] J. De Winter, "Extension de service SMTP pour le début de file d'attente de message distant", RFC 1985, août 1996.

[10] R. Fajman, "Format de message extensible pour les notifications de disposition de message ", RFC 2298, mars 1998.

[11] N. Freed, "Comportement des pare-feu Internet et exigences", RFC 2979, octobre 2000.

[12] N. Freed et N. Borenstein, "Extensions multi usages de messagerie Internet (MIME) Partie une : Format des corps de message Internet", RFC 2045, décembre 1996.

[13] N. Freed, "Extension de service SMTP pour la commande Pipelining *(intubation)*", RFC 2920, septembre 2000.

[14] J. Galvin, S. Murphy, S. Crocker et N. Freed, "Sécurité de Multiparts pour MIME: Multipart/Signed et Multipart/Encrypted", RFC 1847, octobre 1995.

[15] R. Gellens et J. Klensin, "Présentation de message", RFC 2476, décembre 1998.

[16] S. Kille, "Transposition entre X.400 et RFC822/MIME", RFC 2156, janvier 1998.

[17] R. Hinden et S. Deering, éd. "Architecture d'adressage de IP version 6", RFC 2373, juillet 1998.

[18] J. Klensin, N. Freed et K. Moore, "Extension de service SMTP pour la déclaration de taille de message", STD 10, RFC 1870, novembre 1995.

[19] J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker, "Extensions de service SMTP", STD 10, RFC 1869, novembre 1995.

[20] J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker, "Extension de service SMTP pour transport MIME à 8 bits", RFC 1652, juillet 1994.

[21] M. Lambert, "PCMAIL : système de messagerie répartie pour ordinateurs personnels", RFC 1056, juillet 1988.

[22] P. Mockapetris, "Noms de domaine – mise en œuvre et spécification", STD 13, RFC 1035, novembre 1987.
P. Mockapetris, "Noms de domaine - concepts et facilités", STD 13, RFC 1034, novembre 1987.

[23] K. Moore, "MIME (Extensions multi-usages de messagerie Internet) Partie 3 : Extensions d'en-tête de message pour texte non ASCII", RFC 2047, décembre 1996.

[24] K. Moore, "Extension de service SMTP pour notifications d'état de livraison", RFC 1891, janvier 1996.

[25] K. Moore et G. Vaudreuil, "Format de message extensible pour notifications d'état de livraison", RFC 1894, janvier 1996.

[26] J. Myers et M. Rose, "Protocole Post Office - version 3", STD 53, RFC 1939, mai 1996.

[27] C. Partridge, "L'acheminement de la messagerie et le système des domaines", RFC 974, janvier 1986.

[28] C. Partridge, "Messages dupliqués et SMTP", RFC 1047, février 1988.

[29] J. Postel, "Protocole de contrôle de transmission – spécification du protocole du programme DARPA Internet", STD 7, RFC 793, septembre 1981.

[30] J. Postel, "Protocole simple de transfert de messagerie", RFC 821, Août 1982.

[31] B. Ramsdell, éd., "S/MIME version 3 Spécification de message", RFC 2633, juin 1999.

[32] P. Resnick, éd., "Format des messages Internet", RFC 2822, avril 2001.

[33] G. Vaudreuil, "Extensions de service SMTP pour la transmission de grands messages MIME binaires", RFC 1830, août 1995.

[34] G. Vaudreuil, "Codes d'état du système de messagerie améliorée", RFC 1893, janvier 1996.

10 Adresse de l'éditeur

John C. Klensin
AT&T Laboratories
99 Bedford St
Boston, MA 02111 USA
Phone: 617-574-3076
mél : klensin@research.att.com

11 Remerciements

De nombreuse personne ont travaillé dur et longtemps sur les nombreuses versions du présent document. Il y a eu de larges débats au sein du groupe de travail DRUMS de l'IETF, à la fois sur sa liste de diffusion et dans des discussions face à face, sur de nombreuses questions techniques et sur le rôle d'une norme révisée pour le transport de la messagerie Internet, et de nombreux contributeurs ont aidé à formuler le texte de la présente spécification. Les centaines de participants à ces nombreuses discussions depuis la production de la RFC 821 sont trop nombreux pour qu'on les mentionne, mais ils ont tous aidé à faire de ce document ce qu'il est devenu.

APPENDICES

A Service de transport TCP

La connexion TCP prend en charge la transmission d'octets de 8 bits. Les données SMTP sont en caractères ASCII à 7 bits. Chaque caractère est transmis comme un octet de 8 bits avec le bit de plus fort poids mis à zéro. Les extensions de service peuvent modifier cette règle pour permettre la transmission d'octets de données à 8 bits pleins au titre du corps de message, mais pas pour les commandes ou réponses SMTP.

B Générer les commandes SMTP à partir des en-têtes de la RFC 822

Certains systèmes utilisent les en-têtes de la RFC 822 (uniquement) dans un protocole de présentation de message, ou autrement génèrent les commandes SMTP à partir des en-têtes de la RFC 822 lorsqu'un tel message est passé à un MTA à partir d'un agent d'utilisateur. Bien que le protocole MTA-UA soit une affaire privée, qui n'est couverte par aucune des normes de l'Internet, cette approche pose des problèmes. Par exemple, il y a eu des problèmes répétés avec le traitement approprié des copies "bcc" et des listes de redistribution lorsque des informations qui appartiennent conceptuellement à une enveloppe de message ne sont pas séparées (et gardées séparées) tôt dans le traitement des informations d'en-tête.

Il est recommandé que l'agent d'utilisateur fournisse son MTA initial ("client de présentation") avec une enveloppe séparée du message lui-même. Cependant, si l'enveloppe n'est pas fournie, les commandes SMTP DEVRAIENT être générées comme suit :

1. Chaque adresse de receveur provenant d'un champ d'en-tête TO, CC, ou BCC DEVRAIT être copiée dans la

commande RCTP (générant plusieurs copies de message si c'est nécessaire pour la mise en file d'attente ou la livraison). Cela inclut toute adresse figurant dans un "groupe" de la RFC 822. Tout champ BCC DEVRAIT alors être retiré de l'en-tête. Une fois ce processus achevé, il DEVRAIT être vérifié que les en-têtes restants ont au moins un en-tête To:, Cc:, ou Bcc:. Si aucun n'y est, un en-tête bcc: sans information supplémentaire DEVRAIT être inséré comme spécifié en [32].

2. L'adresse de retour dans la commande MAIL DEVRAIT, si possible, être déduite de l'identité du système pour l'usager (local) qui présente, et autrement le champ d'en-tête "From:". Si une identité de système est disponible, elle DEVRAIT aussi être copiée dans le champ d'en-tête Sender si il est différent de l'adresse du champ d'en-tête From. (Tout champ Sender qui se trouverait déjà là DEVRAIT être retiré.) Les systèmes peuvent fournir un moyen pour que le présentateur outrepasse l'adresse de retour d'enveloppe, mais peuvent vouloir restreindre son utilisation à des usagers privilégiés. Cela n'empêchera pas les messages frauduleux, mais peut en diminuer l'incidence ; voir le paragraphe 7.1.

Lorsqu'un MTA est utilisé de cette façon, il porte la responsabilité de s'assurer que le message transmis est valide. Les mécanismes de vérification de cette validité, et du traitement (ou du retour) des messages qui ne sont pas valides au moment de l'arrivée, font partie de l'interface MUA-MTA et ne sont pas traités par la présente spécification.

Un protocole de présentation fondé sur les seules informations de la RFC 822 NE DOIT PAS être utilisé comme passerelle pour un message provenant d'un système de messagerie étranger (non SMTP) dans un environnement SMTP. Des informations supplémentaires pour construire une enveloppe doivent d'abord venir d'une source dans l'autre environnement, d'en-têtes supplémentaires ou de l'enveloppe du système étranger.

Les tentatives pour passer des messages en utilisant seulement leurs champs d'en-tête "to" et "cc" ont causé de façon répétée des boucles de messagerie et autres comportements nocifs au bon fonctionnement de l'environnement de la messagerie Internet. Ces problèmes ont été particulièrement courants lorsque le message a pour origine une liste de diffusion Internet et est distribué dans l'environnement étranger en utilisant les informations d'enveloppe. Lorsque ces messages sont alors traités par un retraitement de messagerie qui se fonde uniquement sur les en-têtes, les boucles en retour sur l'environnement Internet (et la liste de diffusion) sont presque inévitables.

C Routes de source

Historiquement, le <chemin inverse> était une liste d'acheminement de source inversée des hôtes et une boîte aux lettres de source. Le premier hôte dans le <chemin inverse> DEVRAIT être l'hôte qui envoie la commande MAIL. De même, le <chemin-de-transmission> peut être une liste des acheminements de source des hôtes et une boîte aux lettres de destination. Cependant, en général, le <chemin-de-transmission> DEVRAIT contenir seulement une boîte aux lettres et un nom de domaine, s'appuyant sur le système de nom de domaine pour fournir si nécessaire les informations d'acheminement. L'utilisation des routes de source est déconseillée ; alors que les serveurs DOIVENT être préparés à les recevoir et les traiter comme exposé aux paragraphes 3.3 et F.2, les clients NE DEVRAIENT PAS les transmettre et ce paragraphe n'est inclus que pour décrire le contexte.

Pour les besoins du relais, le chemin de transmission peut être une route de source de la forme "@UN,@DEUX:JOE@TROIS", où UN, DEUX, et TROIS DOIVENT être des noms de domaine pleinement qualifiés. Cette forme est utilisée pour souligner la distinction entre une adresse et une route. La boîte aux lettres est une adresse absolue, et la route est l'information sur la façon de s'y rendre. Les deux concepts ne devraient pas être confondus.

Si les routes de source sont utilisées, la RFC 821 et le texte ci-dessous devraient être consultés pour les mécanismes de construction et de mise à jour des chemins de transmission et des chemins inverses.

Le serveur SMTP transforme les arguments de commande en déplaçant son propre identifiant (son nom de domaine ou celui de tout domaine pour lequel il agit comme échangeur de messagerie), si il apparaît, du chemin de transmission au début du chemin inverse.

Remarquer que le chemin de transmission et le chemin inverse apparaissent dans les commandes et les réponses SMTP, mais pas nécessairement dans le message. C'est-à-dire qu'il n'est pas nécessaire que ces chemins et particulièrement cette syntaxe apparaisse dans les champs "To:", "From:", "CC:", etc. des en-têtes de message. À l'inverse, les serveurs SMTP NE DOIVENT PAS déduire des informations de livraison finale du message des champs d'en-tête du message.

Lorsque la liste des hôtes est présente, c'est un chemin de source "inverse" et elle indique que le message a été relayé à travers chaque hôte de la liste (le premier hôte de la liste a été le relais le plus récent). Cette liste est utilisée comme route

de source pour retourner les avis de non livraison à l'envoyeur. Comme chaque hôte relais s'ajoute lui-même au début de la liste, il DOIT utiliser son nom tel que connu dans l'environnement de transport auquel il relaie le message plutôt que dans l'environnement de transport d'où provient le message (s'il sont différents).

D Scénarios

Cette section présente des scénarios complets de plusieurs types de sessions SMTP. Dans les exemples, "C:" indique ce qui est dit par le client SMTP, et "S:" indique ce qui est dit par le serveur SMTP.

D.1 Scénario de transaction SMTP typique

Cet exemple SMTP montre un message envoyé par Smith de l'hôte bar.com, à Jones, Green, et Brown à l'hôte foo.com. On suppose ici que l'hôte bar.com contacte directement l'hôte foo.com. Le message est accepté pour Jones et Brown. Green n'a pas de boîte aux lettres à hôte foo.com.

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 Nom d'utilisateur inconnu
C: RCPT TO:<Brown@foo.com>

S: 250 OK
C: DATA
S: 354 Début des entrées du message ; fin avec <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Clôture du canal de transmission du service

D.2 Scénario de transaction SMTP interrompue

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 Nom d'utilisateur inconnu
C: RSET
S: 250 OK
C: QUIT
S: 221 foo.com Clôture du canal de transmission du service

D.3 Scénario de messagerie relayée

Étape 1 -- Hôte de source à hôte relais

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<JQP@bar.com>
S: 250 OK
C: RCPT TO:<@foo.com:Jones@XYZ.COM>
S: 250 OK
C: DATA
S: 354 Début des entrées du message ; fin avec <CRLF>.<CRLF>
C: Date: Thu, 21 May 1998 05:33:29 -0700
C: From: John Q. Public <JQP@bar.com>
C: Sujet:  Prochaine réunion du conseil d'administration
C: To: Jones@xyz.com
C:
C: Bill:
C: La prochaine réunion du conseil des directeurs sera
C: mardi.
C:                  John.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Clôture du canal de transmission du service
```

Étape 2 -- Hôte relais à hôte de destination

```
S: 220 xyz.com Simple Mail Transfer Service Ready
C: EHLO foo.com
S: 250 xyz.com est en ligne
C: MAIL FROM:<@foo.com:JQP@bar.com>
S: 250 OK
C: RCPT TO:<Jones@XYZ.COM>
S: 250 OK
C: DATA
S: 354 Début des entrées du message ; fin avec <CRLF>.<CRLF>
C: Received: from bar.com by foo.com ; Thu, 21 May 1998
C:     05:33:29 -0700
C: Date: Thu, 21 May 1998 05:33:22 -0700
C: From: John Q. Public <JQP@bar.com>
C: Sujet:  Prochaine réunion du conseil d'administration
C: To: Jones@xyz.com
C:
C: Bill:
C: La prochaine réunion du bureau des directeurs sera
C: mardi.
C:                  John.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Clôture du canal de transmission du service
```

D.4 Scénario de vérification et d'envoi

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250-VRFY
S: 250 HELP
C: VRFY Crispin
S: 250 Mark Crispin <Admin.MRC@foo.com>
C: SEND FROM:<EAK@bar.com>
S: 250 OK
C: RCPT TO:<Admin.MRC@foo.com>
S: 250 OK
C: DATA
S: 354 Début des entrées du message ; fin avec <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Clôture du canal de transmission du service

E Autres questions de passerelles

En général, les passerelles entre l'Internet et les autres systèmes de messagerie DEVRAIENT essayer de préserver toute la sémantique de stratification à travers les frontières entre les deux systèmes de messagerie impliqués. Les approches de traduction de passerelle qui essayent de prendre des raccourcis par des transpositions, (comme celle des informations d'enveloppe d'un système en en-têtes de message ou corps de message de l'autre) se sont généralement révélées être inadéquates de façon importante. Les traductions de systèmes entre des environnements qui ne prennent en charge ni les enveloppes ni les en-têtes et la messagerie Internet doivent être rédigées en comprenant que des pertes d'information sont presque inévitables.

F Dispositifs déconseillés de la RFC 821

Quelques dispositifs de la RFC 821 se sont révélés être problématiques et NE DEVRAIENT PAS être utilisés dans la messagerie Internet.

F.1 TURN

Cette commande, décrite dans la RFC 821, soulève d'importantes questions de sécurité car, en l'absence de forte authentification de l'hôte demandant que client et serveur intervertissent leur rôles, elle peut aisément être utilisée pour détourner des messages de leur destination correcte. Son utilisation est déconseillés ; les systèmes SMTP NE DEVRAIENT PAS l'utiliser à moins que le serveur puisse authentifier le client.

F.2 Acheminement de source

La RFC 821 utilisait le concept d'acheminement explicite de source pour obtenir du courrier d'un hôte à un autre via une série de relais. L'exigence d'utiliser les routes de source dans le trafic régulier de messagerie a été éliminée par l'introduction de l'enregistrement "MX" du système de nom de domaine et sa dernière justification significative a été éliminée par l'introduction, dans la RFC 1123, d'une exigence claire que les adresses suivant un "@" soient toutes un nom de domaine pleinement qualifié. Par conséquent, les seules justifications restantes pour l'utilisation des routes de source sont leur soutien par de très vieux clients SMTP ou MUA et dans la correction d'erreur des systèmes de messagerie. Il peut, cependant, être encore utile dans ce dernier cas et pour acheminer des messages lors de problèmes sérieux mais temporaires, tels que des problèmes avec les enregistrements DNS pertinents.

Les serveurs SMTP DOIVENT continue d'accepter la syntaxe de route de source comme spécifié dans le corps principal de ce document et dans la RFC 1123. Ils PEUVENT, si nécessaire, ignorer les routes et n'utiliser que le domaine cible dans l'adresse. Si ils utilisent quand même la route de source, le message DOIT être envoyé dans le premier domaine indiqué dans l'adresse. En particulier, un serveur NE DOIT PAS penser à des raccourcis au sein de la route de source.

Les clients NE DEVRAIENT PAS utiliser d'acheminement de source explicite excepté dans des circonstances exceptionnelles, comme la correction d'erreurs ou un relais potentiel autour d'un pare-feu ou d'erreurs de configuration du système de messagerie.

F.3 HELO

Comme exposé aux paragraphes 3.1 et 4.1.1, EHLO est fortement préféré à HELO quand le serveur accepte le premier. Les serveurs doivent continuer d'accepter et traiter HELO afin de prendre en charge les plus vieux clients.

F.4 Caractère

La RFC 821 prévoyait la spécification d'une adresse Internet par un numéro d'hôte en entier décimal préfixé d'un signe dièse, "#". En pratique, cette forme est obsolète depuis l'introduction de TCP/IP. Elle est déconseillée et NE DOIT PAS être utilisée.

F.5 Dates et ans

Lorsque des dates sont insérée dans les messages par les clients ou les serveurs SMTP (par exemple, dans les champs de trace), l'année en quatre chiffres DOIT être utilisée. les années à deux chiffres sont déconseillées ; les années à trois chiffres n'ont jamais été permises dans le système de messagerie Internet.

F.6 Envoi direct contre messagerie

En plus de la spécification d'un mécanisme de livraison des messages à la boîte aux lettres des usagers, la RFC 821 prévoyait des commandes supplémentaires facultatives pour délivrer les messages directement à l'écran du terminal de l'usager. Ces commandes (SEND, SAML, SOML) ont rarement été mises en œuvre, et les changements de la technologie des postes de travail et l'introduction d'autres protocoles les auraient rendues obsolètes même si elles avaient été mises en œuvre.

Les clients NE DEVRAIT PAS fournir les services SEND, SAML, ou SOML. Les serveurs PEUVENT les mettre en œuvre. Si ils sont mis en œuvre par les serveurs, le modèle de mise en œuvre spécifié dans la RFC 821 DOIT être utilisé et les noms des commandes DOIVENT être publiés dans la réponse à la commande EHLO.

Déclaration complète de droits de reproduction

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