Groupe de travail Réseau
Request for Comments : 5321
RFC rendue obsolète : 2821
RFC mise à jour : 1123
Catégorie : Sur la voie de la normalisation

J. Klensin
octobre 2008

Traduction Claude Brière de L'Isle

Protocole simple de transfert de messagerie

Résumé
Le présent document spécifie le protocole de base du transport de messagerie électronique de l'Internet. Il consolide, met à jour et précise plusieurs documents antérieurs, les rendant pour la plupart totalement ou partiellement obsolètes. Il couvre les mécanismes d'extension de SMTP et les bonnes pratiques pour l'Internet contemporain, mais ne fournit pas de détails sur des extensions particulières. Bien que SMTP ait été conçu comme un protocole de transport et livraison de messagerie, la présente spécification contient aussi des informations qui sont importantes pour son utilisation comme protocole de "soumission de messagerie" pour les systèmes de lecture de messagerie à "agent d'utilisateur réparti" *(split User Agent)* et les environnements mobiles.

Table des matières

1. Introduction

1.1 Transport de la messagerie électronique

L'objectif du protocole simple de transfert de messagerie (SMTP) est de transférer fiablement et efficacement la messagerie.

SMTP est indépendant du sous système de transmission particulier et n'exige qu'un canal de flux de données fiable et ordonné. Bien que le présent document expose spécifiquement le transport sur TCP, d'autres transports sont possibles. Les appendices à la [RFC0821] décrivent certains d'entre eux.

Une caractéristique importante de SMTP est sa capacité à transporter la messagerie à travers plusieurs réseaux, désignés habituellement comme "relayant la messagerie SMTP" (voir au paragraphe 3.6). Un réseau consiste en hôtes mutuellement accessibles par TCP sur l'Internet public, en hôtes mutuellement accessibles par TCP sur un Intranet TCP/IP isolé par un pare-feu, ou en hôtes dans quelque autre environnement de LAN ou de WAN utilisant un protocole de niveau transport non TCP. En utilisant SMTP, un processeur peut transférer de la messagerie à un autre processeur sur le même réseau ou sur un autre réseau via un relais ou un processeur 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. Les mécanismes d'échangeur de messagerie du système de noms de domaines ([RFC1035], [RFC0974], et Section 5 du présent document) sont utilisés pour identifier le prochain bond approprié de la destination pour un message transporté.

1.2 Historique et contexte de ce document

Le présent document est la spécification du protocole de base du transport de la messagerie électronique de l'Internet. Il consolide, met à jour et précise, mais n'ajoute ni ne change aucune fonction existante des documents suivants :

- la spécification originale SMTP (Protocole simple de transfert de messagerie) de la [RFC0821],
- les exigences et implications pour le transport de la messagerie du système des noms de domaines de la [RFC1035] et [RFC0974],
- les éclaircissements et déclarations d'applicabilité de la [RFC1123],
- le matériel tiré des mécanismes d'extension de SMTP de la [RFC1869],
- des modifications rédactionnelles et des précisions à la [RFC2821] pour faire de cette spécification un projet de norme.

Il rend obsolète les RFC0821, RFC0974, RFC1869 et RFC2821 et met à jour la RFC1123 (en remplaçant les matériaux du transport de messagerie de la RFC1123). Cependant, la RFC0821 spécifie certaines caractéristiques qui n'ont pas connu une utilisation significative dans l'Internet depuis le milieu des années 1990 et (dans les appendices) certains modèles de transport supplémentaires. Ces sections sont omises ici par souci de clarté et de concision ; les lecteurs qui en auraient besoin devraient se reporter à la RFC0821.

Il inclut et des matériaux supplémentaires provenant de la RFC1123 qui exigeaient des développements. Ces matériaux ont été identifiés de diverses façons, le plus souvent en cherchant les réactions sur les diverses listes de diffusion et groupes de nouvelles et les problèmes de formulations ou interprétations inhabituels qui sont apparus lorsque les extensions à SMTP ont été déployées. Lorsque la présente spécification va au delà de la consolidation et diffère réellement des documents antérieurs, elle se substitue à eux techniquement aussi bien que textuellement.

Bien que SMTP ait été conçu comme un protocole de transport et livraison de messagerie, la présente spécification contient aussi des informations qui sont importantes pour son utilisation comme protocole de "soumission de messagerie", comme recommandé pour le protocole Post Office (POP) ([RFC0937], [RFC1939]) et IMAP ([RFC3501]). En général, le protocole séparé de soumission de messagerie spécifié dans la [RFC4409] est maintenant préféré à l'utilisation directe de SMTP ; un exposé plus complet de ce sujet est donné dans le présent document.

Le paragraphe 2.3 donne des définitions de termes spécifiques de ce document. Sauf quand la terminologie historique est nécessaire pour la clarté, ce document utilise la terminologie courante 'client' et 'serveur' pour identifier les processus SMTP, respectivement envoyeur et receveur.

Un document d'accompagnement, la [RFC5322], discute des sections de corps et d'en-tête de message et spécifie leurs formats et structures.

1.3 Conventions du document

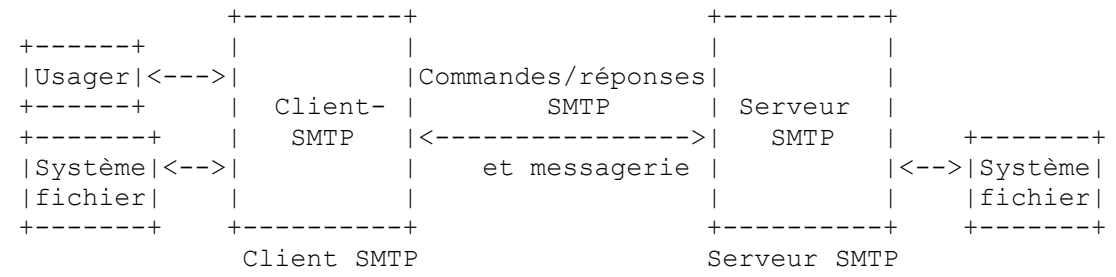
Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119]. Comme chacun de ces termes a été choisi intentionnellement et avec soin pour améliorer l'interopérabilité de la messagerie électronique, chaque utilisation de ces termes est à traiter comme une exigence de conformité.

Comme le présent document a une longue histoire et pour éviter le risque d'erreurs variées et de confusion du lecteur et des documents qui pointent sur celui-ci, la plupart des exemples et des noms de domaines qu'ils contiennent sont conservés de la RFC 2821. Le lecteur doit se souvenir que ces exemples sont de simples illustrations qui ne devraient pas être utilisées dans la réalité dans des fichiers de code ou de configuration.

2. Le modèle SMTP

2.1 Structure de base

La conception de SMTP peut être décrite comme suit :



Quand un client SMTP a un message à transmettre, il établit un canal de transmission bidirectionnel à un serveur SMTP. La responsabilité d'un client SMTP est de transférer les messages à un ou plusieurs serveurs SMTP, ou de rapporter son échec à le faire.

Les moyens par lesquels un message est présenté à un client SMTP, et comment ce client détermine le ou les identifiants ("noms") du ou des domaines auxquels les messages sont à transférés, sont une affaire locale, et ne sont pas traités par ce document. Dans certains cas, le ou les domaines désignés, ou ceux déterminés par un client SMTP, vont identifier la ou les destinations finales du message. Dans d'autres cas, communs aux clients SMTP associés aux mises en œuvre des protocoles

POP ([RFC0937], [RFC1939]) ou IMAP ([RFC3501]) ou lorsque le client SMTP est dans un environnement de service de transport isolé, le domaine déterminé va identifier une destination intermédiaire à travers laquelle tous les messages sont à relayer. Les clients SMTP qui transfèrent tout le trafic sans considération des domaines cibles associés aux messages individuels, ou qui ne tiennent pas de file d'attente pour réessayer les transmissions de messages qui ne peuvent pas initialement être achevées, peuvent par ailleurs se conformer à la présente spécification mais ne sont pas considérés comme à capacité complète. Les mises en œuvre SMTP à capacités complètes, y compris les relais utilisés par celles moins capables, et leurs destinations, sont supposées prendre en charge toutes les mises en file d'attente, réessais, et autres fonctions d'adressage discutées dans la présente spécification. Dans de nombreuses situations et configurations, les clients moins capables discutés ci-dessus DEVRAIENT utiliser le protocole de soumission de message [RFC4409] plutôt que SMTP.

Les moyens par lesquels un client SMTP, une fois qu'il a déterminé un domaine cible, détermine l'identité d'un serveur SMTP auquel une copie d'un message est à transférer, et ensuite effectue ce transfert, sont couverts par ce document. Pour effectuer un transfert de message 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 en un hôte intermédiaire d'échange de messagerie, soit en un hôte cible final.

Un serveur SMTP peut être soit la destination ultime soit un "relais" intermédiaire (c'est-à-dire, qu'il peut assumer le rôle d'un client SMTP après réception du message) soit une "passerelle" (c'est-à-dire, qu'il peut transporter le message plus loin 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 se produire dans une seule connexion entre l'envoyeur SMTP original et le receveur SMTP final, ou peut se produire dans une série de bonds à travers des systèmes intermédiaires. Dans l'un et l'autre cas, une fois que le serveur a produit une réponse de succès à la fin des données du message, un dégagement formel de responsabilité du message intervient : le protocole exige qu'un serveur accepte la responsabilité soit de livrer le message, soit de rapporter de façon appropriée l'échec de la livraison (voir aux paragraphes 6.1, 6.2, et 7.8).

Une fois établi le canal de transmission et achevée la prise de contact initiale, le client SMTP initie normalement une transaction de messagerie. Une telle transaction consiste en une série de commandes pour spécifier le générateur et la destination du message et la transmission du contenu du message lui-même (incluant toutes les lignes de la section d'en-tête ou autres structures). Lorsque le même message est envoyé à plusieurs receveurs, ce protocole encourage la transmission d'une seule copie des données pour tous les receveurs au même hôte de destination (ou relais intermédiaire).

Le serveur réplique 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 expliqué au paragraphe 2.2. Le dialogue est délibérément verrouillé, un à la fois, bien que ceci puisse être modifié par accord mutuel sur les demandes d'extension comme le traitement de commandes en parallèle [RFC2920].

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

Comme suggéré ci-dessus, ce protocole donne des mécanismes pour la transmission de messages. Historiquement, cette transmission se produisait normalement directement de l'hôte de l'utilisateur envoyeur à l'hôte de l'utilisateur receveur lorsque les deux hôtes sont connectés au même service de transport. Quand ils ne sont pas connectés au même service de transport, la transmission se fait via un ou plusieurs serveurs relais SMTP. Un cas très courant dans l'Internet d'aujourd'hui implique la soumission du message original à un intermédiaire, le serveur de "soumission de message", qui est similaire à un relais mais a des propriétés supplémentaires ; de tels serveurs sont décrits au paragraphe 2.3.10 et plus en détails dans la [RFC4409]. Un hôte intermédiaire qui agit comme relais SMTP ou comme passerelle dans d'autres environnements de transmission est généralement choisi par l'utilisation du mécanisme d'échangeur de messagerie du système des noms de domaine (DNS).

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

2.2 Modèle d'extension

2.2.1 Fondements

Dans un effort qui a commencé en 1990, approximativement dix ans après l'achèvement de la RFC 821, le protocole a été modifié avec un modèle "d'extensions de service" qui a permis au client et au serveur de s'accorder pour utiliser des fonctionnalités partagées au delà des exigences originales de SMTP. Le mécanisme d'extension de SMTP définit des moyens par lesquels un client et serveur SMTP étendus peuvent 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 prendre en charge les mécanismes d'extension de base. Par exemple, les serveurs DOIVENT prendre en charge la commande EHLO même si ils ne mettent en œuvre aucune extension spécifique et les clients DEVRAIENT de préférence utiliser EHLO plutôt que HELO. (Cependant, pour la compatibilité avec les plus anciennes mises en œuvre conformes, les clients et serveurs SMTP DOIVENT prendre en charge les mécanismes originaux de HELO comme solution de repli.) Sauf lorsque les différentes caractéristiques de HELO doivent être identifiées pour les besoins de l'interopérabilité, le présent document ne discute que du EHLO.

SMTP est largement déployé et des mises en œuvre de grande qualité ont prouvé leur robustesse. Cependant, la communauté de l'Internet considère maintenant que certains services importants n'avaient pas été prévus lors de la première conception du protocole. Si la prise en charge de ces services doit être ajoutée, cela doit être fait d'une manière qui permette aux plus anciennes mises en œuvre de continuer à fonctionner de façon acceptable. Le cadre d'extension consiste en :

- la commande SMTP EHLO remplace l'ancien HELO,
- un registre des extensions de service SMTP,
- des paramètres supplémentaires aux commandes SMTP MAIL et RCPT, et
- le remplacement facultatif de commandes définies dans ce protocole, comme pour DATA en transmissions non ASCII [RFC3030].

La force de SMTP vient principalement de sa simplicité. L'expérience de nombreux protocoles a montré que les protocoles qui ont peu d'options tendent à être partout, tandis que les protocoles avec beaucoup d'options tendent à l'obscurité.

Chaque extension, sans considération de ses avantages, doit être examinée attentivement par rapport à ses coûts de mise en œuvre, de déploiement, et d'interopérabilité. Dans de nombreux cas, le coût de l'extension du service SMTP va largement dépasser celui de ses avantages.

2.2.2 Définition et enregistrement des extensions

L'IANA tient un registre des extensions de service SMTP. Une valeur de mot clé 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 sur la voie de la normalisation ou expérimental approuvé par l'IESG. La définition doit inclure :

- le nom textuel de l'extension de service SMTP ;
- la valeur du mot clé de EHLO associée à l'extension ;
- la syntaxe et les valeurs possibles des paramètres associés à la valeur du mot clé EHLO ;
- tous les verbes SMTP supplémentaires associés à l'extension (les verbes supplémentaires vont généralement être, mais n'y sont pas obligés, les mêmes que la valeur du mot clé EHLO) ;
- tout nouveau paramètre que l'extension associe aux verbes MAIL ou RCPT ;
- une description de comment la prise en charge de l'extension affecte le comportement d'un serveur et d'un client SMTP ;
- l'incrément par lequel l'extension augmente la longueur maximum des commandes MAIL et/ou RCPT, par rapport à ce qui est spécifié dans la présente norme.

De plus, toute valeur de mot clé EHLO commençant par une lettre majuscule ou minuscule "X" se réfère à une extension de service SMTP locale utilisée exclusivement par accord bilatéral. Les mots clés commençant par "X" NE DOIVENT PAS être utilisés dans une extension de service enregistrée. À l'inverse, les valeurs de mot clé présentées dans la réponse EHLO qui ne commencent pas par "X" DOIVENT correspondre à une extension de service SMTP enregistrée auprès de l'IANA dans une norme, un document sur la voie de la normalisation ou expérimental approuvé par l'IESG. Un serveur conforme NE DOIT PAS offrir de valeurs de mot clé non préfixées "X" qui ne sont pas décrites dans une extension enregistrée.

Les verbes et noms de paramètres supplémentaires sont liés aux mêmes règles que les mots clés EHLO ; précisément, les verbes qui commencent par "X" sont des extensions locales qui peuvent n'être pas enregistrées ou normalisées. À l'inverse, les verbes qui ne commencent pas par "X" doivent toujours être enregistrés.

2.2.3 Problèmes particuliers des extensions

Les extensions qui changent des propriétés très basiques du fonctionnement de SMTP sont permises. Le texte d'autres paragraphes du présent document doit être compris dans ce contexte. En particulier, des extensions peuvent changer les

limites minimum spécifiées au paragraphe 4.5.3, peuvent changer l'exigence du jeu de caractères ASCII comme mentionné ci-dessus, ou peuvent introduire des modes facultatifs de traitement de message.

En particulier, si une extension implique que le chemin de livraison prend normalement en charge des caractéristiques spéciales de cette extension, et si un système SMTP intermédiaire trouve un prochain bond qui ne prend pas en charge l'extension requise, il PEUT choisir, sur la base de l'extension spécifique et des circonstances, de remettre en file d'attente le message et d'essayer plus tard et/ou d'essayer un hôte MX de remplacement. Si cette stratégie est employée, la temporisation pour revenir à un format sans extension (si disponible) DEVRAIT être moins que la temporisation normale pour déclarer le message comme non livrable (par exemple, si la temporisation normale est de trois jours, la temporisation de remise en file d'attente avant de tenter de transmettre le message sans l'extension pourrait être d'un jour.

2.3 Terminologie SMTP

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 (décrite à la Section 3). Elle consiste en une adresse d'origine (à laquelle les rapports d'erreur devraient être envoyés) une ou plusieurs adresses de receveur, et du matériel facultatif d'extension du protocole. Historiquement, des variantes de la commande (MAIL) de spécification d'adresse de chemin inverse (de l'origine) pouvaient être utilisées pour spécifier d'autres modes de livraison, comme un affichage immédiat ; ces variantes sont maintenant déconseillées (voir les Appendices F et F.6).

Le contenu SMTP est envoyé dans l'unité de protocole SMTP DATA et a deux parties : la section d'en-tête et le corps. Si le contenu se conforme aux autres normes contemporairnes, la section d'en-tête consiste en une collection de champs d'en-tête, consistant chacun en un nom d'en-tête, deux-points, et des données, structurées comme dans la spécification de format de message [RFC5322] ; le corps, si il est structuré, est défini en accord avec MIME [RFC2045]. Le contenu est textuel par nature, exprimé en utilisant le répertoire US-ASCII [ANSI-X3.4]. Bien que les extensions SMTP (telles que "8BITMIME", [RFC1652]) puissent relâcher cette restriction pour le corps du contenu, les champs d'en-tête du contenu sont toujours codés en utilisant le répertoire US-ASCII. Deux extensions MIME [RFC2047] et [RFC2231] définissent un algorithme pour représenter les valeurs d'en-tête en dehors du répertoire US-ASCII, tout en les codant en utilisant le répertoire US-ASCII.

2.3.2 Envoyeurs et receveurs

Dans la RFC 821, les deux hôtes qui participent à une transaction SMTP sont décrits comme "envoyeur SMTP" et "receveur SMTP". Le présent document a changé cela pour refléter la terminologie actuelle de l'industrie et se réfère donc respectivement au "client SMTP" (ou parfois juste "le client") et au "serveur SMTP" (ou juste "le serveur"). Comme un hôte peut agir à la fois comme serveur et client dans une situation de relais, la terminologie "receveur" et "envoyeur" est toujours utilisée lorsque nécessaire pour être clair.

2.3.3 Agents de messagerie et mémorisations de messages

Une terminologie supplémentaire de système de messagerie est devenue courante après la publication de la RFC 821 et lorsque c'est pratique, elle est utilisée dans la présente spécification. En particulier, les serveurs et clients SMTP fournissent un service de transport de messagerie et donc agissent comme des 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 la source et la cible du message. À la source, un MUA pourrait collecter la messagerie à transmettre en provenance d'un utilisateur et la passer à un MTA ; le MTA final ("de livraison") serait vu comme passant le message à un MUA (ou au moins lui en transférant la responsabilité, par exemple, en déposant le message dans un "magasin de messages"). Cependant, bien que ces termes soient utilisés avec au moins l'apparance d'une grande précision dans d'autres environnements, les limites implicites entre MUA et MTA ne correspondent souvent pas précisément avec les pratiques courantes et conformes de la messagerie Internet. Donc, le lecteur devrait être prudent quant à la déduction de relations et responsabilitiés fortes qui pourraient être impliquées si ces termes étaient utilisés ailleurs.

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 privé TCP/IP) et qui prend en charge le protocole SMTP. Les hôtes sont connus par des noms (voir le paragraphe suivant) ; ils NE DEVRAIENT PAS être identifiés par des adresses numériques, c'est-à-dire, par des adresses littérales comme décrit au paragraphe 4.1.2.

2.3.5 Noms de domaies

Un nom de domaine (ou souvent juste un "domaine") consiste en un ou plusieurs composants, séparés par des points si plus d'un apparaissent. Dans le cas d'un domaine de niveau supérieur utilisé par lui-même dans une adresse de message électronique, une seule chaîne est utilisée sans aucun point. Cela rend l'exigence, décrite plus en détails ci-dessous, que seuls des noms de domaine pleinement qualifiés apparaissent dans les transactions SMTP sur l'Internet public, particulièrement importantes lorsque des domaines de niveau supérieur sont impliqués. Ces composants ("étiquettes" dans la terminologie du DNS [RFC1035]) sont restreints pour les besoins de SMTP à consister en une séquence de lettres, chiffres, et tirets du jeu de caractères ASCII [ANSI-X3.4]. Les noms de domaines sont utilisés comme des noms d'hôtes et des autres entités dans la hiérarchie des noms de domaines. Par exemple, un domaine peut se référer à un alias (étiquette d'un RR CNAME) ou l'étiquette d'enregistrement d'un échangeur de messagerie être utilisée pour livrer de la messagerie au lieu de représenter un nom d'hôte. Voir la [RFC1035] et la Section 5 de la présente spécification.

Le nom de domaine, comme décrit dans le présent document et dans la [RFC1035], est le nom entier, pleinement qualifié (souvent appelé "FQDN"). Un nom de domaine qui n'est pas en forme FQDN n'est qu'un alias local. Les alias locaux NE DOIVENT PAS apparaître dans une transaction SMTP.

Seuls des noms de domaines pleinement qualifiés (FQDN, *Fully-Qualified Domain Name*) résolvables, sont permis quand des noms de domaine sont utilisés dans SMTP. En d'autres termes, les noms qui peuvent être résolus en RR MX ou en adresses (c'est-à-dire, des RR A ou AAAA, comme expliqué à la Section 5) sont permis, car ce sont des RR CNAME dont la cible peut être résolue, à son tour, en RR MX ou d'adresse. Les surnoms locaux ou les noms non qualifiés NE DOIVENT PAS être utilisés. Il y a deux exceptions à la règle qui exige des FQDN :

- o le nom de domaine donné dans la commande EHLO DOIT être un nom principal d'hôte (un nom de domaine qui se résout en un RR d'adresse) ou, si l'hôte n'a pas de nom, une adresse littérale, comme décrit au paragraphe 4.1.3 et discuté plus en détails dans l'exposé sur le EHLO du paragraphe 4.1.4 ;
- o le nom réservé de boîte aux lettres "postmaster" peut être utilisé dans une commande RCPT sans qualification de domaine (voir au paragraphe 4.1.1.3) et DOIT être accepté si il est utilisé ainsi.

2.3.6 Mémoire tampon et tableau d'état

Les sessions SMTP sont à états pleins, les deux parties conservant soigneusement une vue commune de l'état en cours. Dans ce document, on modélise cet état par une "mémoire tampon" virtuelle et un "tableau d'état" sur le serveur qui peut être utilisé par le client pour, par exemple, "vider la mémoire tampon" ou "réinitialiser le tableau d'état", causant l'élimination des informations de la mémoire tampon et le retour de l'état à un état antérieur.

2.3.7 Commandes et réponses

Les commandes SMTP et, sauf si elles sont altérées par une extension de service, les données du message, sont transmises de l'envoyeur au receveur via le canal de transmission en "lignes".

Une réponse SMTP est un accusé de réception (positif ou négatif) envoyé en "lignes" 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 l'échec ou la réussite) généralement suivi par une chaîne de texte. Les codes sont pour l'usage des programmes et le texte est généralement destiné aux utilisateur humains. La [RFC3463] spécifie plus de structures des chaînes de réponse, incluant l'utilisation de codes d'achèvement supplémentaires et plus spécifiques (voir aussi la [RFC5248]).

2.3.8 Lignes

Les lignes consistent en zéro, un ou plusieurs charactères de données terminés par la séquence de caractères ASCII "CR" (valeur hexadécimale 0D) suivie immédiatement par le caractère ASCII "LF" (valeur hexadécimale 0A). Cette séquence de terminaison est notée <CRLF> dans ce document. Les mises en œuvre conformes NE DOIVENT PAS reconnaître ou générer d'autre caractère ou séquence de caractères comme terminaison de ligne. Des limites PEUVENT être imposées à la longueur de ligne par les serveurs (voir la Section 4).

De plus, l'apparition de caractères "CR" ou "LF" "nus" dans le texte (c'est-à-dire, l'un sans l'autre) a une longue histoire de problèmes dans les mises en œuvre et applications de messagerie électronique qui utilisent le système de messagerie comme outil. Les mises en œuvre de client SMTP NE DOIVENT PAS transmettre ces caractères sauf quand ils sont destinés à la terminaison de ligne et elles DOIVENT alors, comme indiqué ci-dessus, les transmettre seulement comme une séquence <CRLF>.

2.3.9 Contenu de message et données de message

Les termes de "contenu de message" et "données de message" sont utilisés de façon interchangeable dans ce document pour décrire le materiel transmis après l'acceptation de la commande DATA et avant la transmission de l'indication de la fin des données. Le contenu de message inclut la section d'en-tête de message et le corps de message éventuellement structuré. La spécification de MIME [RFC2045] donne le mécanisme standard pour les corps de message structurés.

2.3.10 Système générateur, livraison, relais, et passerelle

La présente spécification fait une distinction entre quatre types de systèmes SMTP, fondée sur le rôle que jouent ces systèmes dans la transmission de la messagerie électronique. Un système "générateur" (parfois appelé un générateur 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 la passe à un agent d'utilisateur de messagerie ou la dépose dans un magasin de messages auquel un agent d'utilisateur de messagerie est supposé accéder ultérieurement. Un système SMTP de "relais" (généralement simplement appelé un "relais") reçoit la messagerie d'un client SMTP et la transmet, sans modification des données de message autre que d'ajouter les informations de trace, à un autre serveur SMTP pour un autre relais ou pour livraison.

Un système SMTP "passerelle" (généralement simplement appelé une "passerelle") reçoit de la messageris d'un système client dans un environnement de transport et le transmet à un système serveur dans un autre environnement de transport. Les différences de protocoles ou de sémantique de message entre les environnements de transport sur l'un ou l'autre côté d'une passerelle peuvent exiger que le système passerelle effectue des transformations au message qui ne sont pas permises aux systèmes 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 sur les deux côtés de la passerelle (voir la [RFC2979]).

2.3.11 Boîte aux lettres et adresse

Comme utilisée dans la présente spécification, une "adresse" est une chaîne de caractères qui identifie un utilisateur à qui de la messagerie va être envoyée ou une localisation à laquelle la messagerie va être déposée. Le terme "boîte aux lettres" se réfère à ce dépôt. Les deux termes sont normalement utilisés de façon interchangeable sauf si la distinction entre la localisation à laquelle est placée la messagerie (la boîte aux lettres) et une référence à cette localisation (l'adresse) est importante. Une adresse consiste normalement en la spécification d'un utilisateur et d'un domaine. La convention standard de dénomination de boîte aux lettres est définée comme "partie-locale@domaine" ; l'usage contemporain permet un ensemble beaucoup plus large d'applications que de simples "noms d'utilisateur". Par conséquent, et du fait d'une longue histoire de problèmes quand les hôtes intermédiaires ont tenté d'optimiser le transport en les modifiant, la partie locale DOIT être interprétée et n'avoir de signification qu'attribuée par l'hôte spécifié dans la partie domaine de l'adresse.

2.4 Principes généraux de syntaxe et modèle de transaction

Les commandes et réponses SMTP 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, des arguments sont exigés à la suite du verbe ou du code de réponse. Certaines commandes n'acceptent pas d'arguments (après le verbe) et certains codes de réponse sont suivis, parfois facultativement, par du texte de 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 sont à la Section 4.

Les valeurs de verbes et d'argument (par exemple, "TO:" ou "to:" dans la commande RCPT et les mots clés de nom d'extension) ne sont pas sensibles à la casse, à la seule exception dans la présente spécification de la partie locale d'une bôite aux lettres (les extensions SMTP peuvent explicitement spécifier des éléments sensibles à la casse). C'est-à-dire, un verbe de commande, une valeur d'argument autre qu'une partie locale de boîte aux lettres, et du texte de forme libre PEUVENT être codés en majuscules, en minuscuiles, ou tout mélange de majuscules et minuscules sans impact sur sa signification. 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 de la partie locale des boîtes aux lettres. En particulier, pour certains hôtes, l'usager "smith" est différent de l'usager "Smith". Cependant, exploiter la sensibilité à la casse de la partie locale des boîtes aux lettres entrave l'interopérabilité et est déconseillé. Les domaines des boîtes aux lettres suivent les règles normales du DNS et ne sont donc pas sensibles à la casse.

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 s'accommoder de ces serveurs.

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

La syntaxe de chaque commande est donnée avec l'exposé sur cette commande. Les éléments et paramètres communs sont donnés au paragraphe 4.1.2.

Les commandes et réponses sont composées de caractères tirés du jeu de caractères ASCII [ANSI-X3.4]. Quand le service de transport fournit un canal de transmission de 8 bits (octet) chaque caractère de 7 bits est transmis, justifié à droite, dans un octet dont le bit de poids fort est réglé à zéro. Plus précisément, le service SMTP non étendu fournit seulement le transport à 7 bits. Un client SMTP générateur qui n'a pas réussi à négocier une extension appropriée avec un serveur particulier (voir le paragraphe suivant) NE DOIT PAS transmettre des messages avec des informations dans le bit de poids fort des octets. Si de tels messages sont transmis en violation de cette règle, les serveurs SMTP receveurs PEUVENT mettre à zéro le bit de poids fort 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 étiqueté et si le chemin des données ne peut pas accepter le contenu réel, il peut en résulter la livraison ultime d'un message sévérement perturbé au receveur. Les systèmes SMTP de livraison PEUVENT rejeter de tels messages, ou les retourner comme indélivrables, plutôt que de les livrer. En l'absence d'une extension offerte par le serveur le permettant explicitement, il n'est pas permis à un système SMTP envoyeur d'envoyer des commandes d'enveloppe dans un jeu de caractères autre que l'US-ASCII. Les systèmes receveurs DEVRAIENT rejeter de telles commandes, en utilisant normalement des réponses "500 erreur de syntaxe – caractère invalide".

La transmission de contenu de message à 8 bits PEUT être demandée au serveur par un client en utilisant les facilités étendues de SMTP, notamment l'extension "8BITMIME" de la [RFC1652]. 8BITMIME DEVRAIT être supporté par les serveurs SMTP. Cependant, elle NE DOIT PAS être conçue comme authorisant la transmission sans restriction de matériel à 8 bits, pas plus que 8BITMIME n'autorise la transmission de matériel d'enveloppe autre que ASCII. 8BITMIME NE DOIT PAS être demandé par les envoyeurs pour du matériel dont le bit de poids fort n'est pas dans le format MIME avec un codage approprié de transfert de contenu ; les serveurs PEUVENT rejeter de tels messages.

La notation méta linguistique utilisée dans le présent document correspond au "BNF augmenté" utilisé dans les autres documents du système de messagerie Internet. Le lecteur qui ne serait pas familiarisé avec cette syntaxe devrait consulter la spécification ABNF dans la [RFC5234]. Les termes de métalangage utilisés dans le texte courant sont entourés de crochets angulaires (par exemple, <CRLF>) pour que ce soit clair. On attire l'attention du lecteur sur le fait que la grammaire exprimée dans le métalangage n'est pas complète. Il y a de nombreuses instances dans lesquelles des dispositions du texte opèrent des contraintes ou modifient par ailleurs la syntaxe ou la sémantique impliquée par la grammaire.

3. Procédures SMTP : vue d'ensemble

Cette Section contient la description des procédures utilisées dans SMTP : initialisation de session, transaction de messagerie, transmission de la messagerie, vérification des noms de boîtes aux lettres et expansion des listes de destinataires, et échanges d'ouverture et de fermeture. 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 cette section. Plusieurs scénarios complets sont présentés à l'Appendice D.

3.1 Initialisation de session

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

Les mises en œuvre de serveur SMTP PEUVENT inclure l'identification de leur logiciel et des informations de version dans la réponse d'accueil de la connexion après le code 220, pratique qui permet un isolement plus efficace de la réparation de tous problèmes. Les mises en œuvre PEUVENT prendre des dispositions pour que les serveurs SMTP désactivent les annonces de logiciel et de version lorsque cela pose des problèmes de sécurité. Bien que certains systèmes identifient aussi leur point de contact pour les problèmes de messagerie, ce n'est pas un substitut à la conservation de l'adresse exigée du "maître de poste" (voir la Section 4).

Le protocole SMTP permet à un serveur de rejeter formellement une session de messagerie tout en permettant la connexion initiale comme suit : une réponse 554 PEUT être donnée dans le message initial d'ouverture de connexion au lieu du 220. Un serveur qui prend cette approche DOIT quand même attendre que le client envoie un QUIT (voir au paragraphe 4.1.1.10) avant de clôre la connexion et DEVRAIT répondre à toutes les commandes intermédiaires avec un "503 Mauvaise séquence de commandes". Comme une tentative de faire une connexion SMTP avec un tel système est probablement une erreur, un serveur qui retourne une réponse 554 à l'ouverture de la connexion DEVRAIT fournir assez d'informations dans le texte de réponse pour faciliter le déboguage du système envoyeur.

3.2 Initialisation par le client

Une fois que le serveur a envoyé le message d'accueil (de bienvenue) et que le client l'a reçu, le client envoie normalement la commande EHLO au serveur, indiquant l'identité du client. En plus de l'ouverture de la session, le 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 prend en charge. Les plus anciens systèmes SMTP qui ne sont pas capables de prendre en charge les extensions de service, et les clients contemporains qui n'exigent pas que les extensions de service soient initialisées dans la session PEUVENT utiliser HELO au lieu de EHLO. Les serveurs NE DOIVENT PAS retourner la réponse de style EHLO étendu à une commande HELO. Pour une tentative particulière de connexion, si le serveur retourne une réponse "commande non reconnue" au EHLO, le client DEVRAIT être capable de se replier sur l'envoi du 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 du EHLO, "et je prend en charge les demandes d'extension de service").

3.3 Transactions de messagerie

Il y a trois étapes dans les transactions de messagerie SMTP. La transaction commence 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, donnant les informations sur le receveur. Ensuite, une commande DATA initie le transfert des données de messagerie et est terminée par l'indicateur de "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-messagerie>] <CRLF>

Cette commande dit au receveur SMTP qu'une nouvelle transaction de messagerie commence et qu'il doit réinitialiser tous ses tableaux d'état et ses mémoires tampons, incluant tous les receveurs ou données de messagerie. La portion <chemin-inverse> du premier ou seul argument contient la boîte aux lettres de source (entre les crochets "<" et ">") qui peut être utilisée pour rapporter des erreurs (voir au paragraphe 4.2 la discussion sur le rapport d'erreur). Si il accepte, le serveur SMTP retourne une réponse "250 OK". Si la spécification de boîte aux lettres n'est pas acceptable pour une raison ou une autre, le serveur DOIT retourner une réponse indiquant si l'échec est permanent (c'est-à-dire, va se produire de nouveau si le client essaye d'envoyer la même adresse) ou temporaire (c'est-à-dire, l'adresse pourrait être acceptée si le client essaye à nouveau 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 avant qu'un ou plusieurs chemins de transmission (dans des commandes RCPT) puissent être examinés. Dans ce cas, le serveur PEUT raisonnablement accepter le chemin inverse (avec un code de réponse 250) et rapporter alors les problèmes après que les chemins de transmission ont été reçus et examinés. Normalement, les échecs produisent des réponses 550 ou 553.

Historiquement, il était permis au <chemin-inverse> de contenir plus d'une seule boîte aux lettres ; cependant, les systèmes contemporains NE DEVRAIENT PAS utiliser l'acheminement de source (voir l'Appendixe C).

Les <paramètres-de-messagerie> facultatifs sont associés aux extensions de service SMTP négociées (voir au paragraphe 2.2).

La seconde étape de la procédure est la commande RCPT. Cette étape de la procédure peut être répétée un nombre illimité de fois.

RCPT TO:<chemin-de-transmission> [SP <paramètres-de-réception>] <CRLF>

Le premier ou seul argument de cette commande inclut un chemin de transmission (normalement une boîte aux lettres et un domaine, toujours entourés des crochets "<" et ">") qui identifie un seul receveur. Si il accepte, le serveur SMTP retourne une réponse "250 OK" et mémorise le chemin de transmission. Si le receveur est connu pour n'être pas une adresse livrable, le serveur SMTP retourne une réponse 550, normalement avec une chaîne comme "adresse inexistante - " et le nom de la boîte aux lettres (d'autres circonstances et codes de réponse sont possibles).

Le <chemin-de-transmission> peut contenir plus d'une seule boîte aux lettres. Historiquement, il était permis au <chemin-de-transmission> de contenir une liste des hôtes de l'acheminement entre la source et la boîte aux lettres de destination ; cependant, les clients SMTP contemporains NE DEVRAIENT PAS utiliser les routes de source (voir l'Appendice C). Les serveurs DOIVENT être prêts à rencontrer une liste de routes de source dans le chemin de transmission, mais ils DEVRAIENT ignorer les routes ou PEUVENT décliner la prise en charge du relais qu'elles impliquent. De même, les serveurs PEUVENT refuser d'accepter la messagerie qui est destinée à d'autres hôtes ou systèmes. Ces restrictions rendent sans objet un serveur comme relais pour les clients qui ne prennent pas en charge les pleines fonctionnalités de SMTP. Par conséquent, les clients à capacités restreintes NE DOIVENT PAS supposer que tout serveur SMTP dans l'Internet peut être

utilisé comme site de traitement (relais) de leur messagerie. Si une commande RCPT apparaît sans être précédée d'une commande MAIL, le serveur DOIT retourner une réponse 503 "Mauvaise séquence de commandes". Les <paramètres-de-réception> facultatifs sont associés aux extensions de service SMTP négociées (voir au paragraphe 2.2).

Comme cela a été une source d'erreurs constante, on notera que les espaces ne sont pas permises d'un côté ou de l'autre des deux points qui suivent FROM dans la commande MAIL ou TO dans la commande RCPT. La syntaxe est exactement celle donnée ci-dessus.

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

DATA <CRLF>

Si il accepte, le serveur SMTP retourne une réponse 354 intermédiaire et considère toutes les lignes suivantes jusqu'à, mais non inclus, l'indicateur de fin des données de messagerie, comme étant 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 afin que le dialogue de commande et réponse puisse reprendre. SMTP indique la fin des données de messagerie en envoyant une ligne contenant seulement un "." (point). Une procédure de transparence est utilisée pour empêcher cela d'interférer avec le texte de l'utilisateur (voir au paragraphe 4.5.2).

L'indicateur de fin des données de messagerie confirme aussi la transaction de messagerie et dit au serveur SMTP de traiter maintenant les receveurs et données de messagerie mémorisés. Si il accepte, le serveur SMTP retourne une réponse "250 OK". La commande DATA peut échouer seulement en deux points de l'échange de protocole :

- Si il n'y a pas de commande MAIL ou 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) à la commande DATA. Si une de ces réponses (ou toute autre réponse de style 5yz) est reçue, le client NE DOIT PAS envoyer de données de message ; plus généralement, les données de message NE DOIVENT PAS être envoyées tant qu'une réponse 354 n'est pas reçue.
- Si le verbe est initialement accepté et si la réponse 354 est produite, la commande DATA ne devrait échouer que si la transaction de messagerie est inachevée (par exemple, pas de receveur) si les ressources sont indisponibles (incluant, bien sûr, l'indisponibilité inattendue du serveur) ou si le serveur détermine que le message devrait être rejeté pour des raisons de politique ou autres.

Cependant, dans la pratique, certains serveurs n'effectuent pas la vérification du receveur tant que le texte du message n'est pas reçu. Ces serveurs DEVRAIENT traiter un échec d'un ou plusieurs receveurs comme un "échec suivant" et retourner un message comme expliqué à la Section 6 et, en particulier, au paragraphe 6.1. Utiliser un code de réponse "550 boîte aux lettres non trouvée" (ou équivalent) après que les données sont acceptées rend difficile ou impossible au client de déterminer quels receveurs sont en échec.

Quand le format des [RFC0822] [RFC5322] est utilisé, les données de messagerie incluent des champs d'en-tête comme ceux appelés Date, Subject, To, Cc, et From. Les systèmes de serveur SMTP NE DEVRAIENT PAS rejeter des messages sur la base de défauts perçus dans la section d'en-tête de message ou le corps de message de la RFC 822 ou de MIME [RFC2045]. En particulier, ils NE DOIVENT PAS rejeter les messages dans lesquels les numéros des champs Resent-header 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 indiqué ci-dessus.

3.4 Transmission pour correction ou mise à jour d'adresse

La prise en charge de la transmission est le plus souvent exigée pour consolider et simplifier les adresses au sein, ou relatives à une entreprise et moins fréquemment pour établir les adresses pour relier l'ancienne adresse d'une personne à son 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.

Dans les deux cas de l'entreprise et de la "nouvelle adresse", des considérations de dissimulation d'information (et parfois de sécurité) plaident contre l'exposition de l'adresse "finale" à travers le protocole SMTP comme effet collatéral de l'activité de transmission. Cela peut être particulièrement important quand l'adresse finale ne peut même pas être accessible 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 à RCPT doivent être évalués avec soin par les mises en œuvre et, quand ils sont disponibles, par ceux qui configurent les systèmes (voir aussi le paragraphe 7.4).

En particulier :

- o Les serveurs PEUVENT transmettre les messages quand ils sont informés d'un changement d'adresse. Quand il font ainsi, ils PEUVENT fournir les informations de mise à jour d'adresse avec un code 251, ou peuvent transmettre "en silence" et retourner un code 250. Cependant, 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 cette information à l'utilisateur.

Autrement,

- o Les serveurs PEUVENT rejeter les messages ou les retourner comme non livrables quand ils ne peuvent pas être livrés précisément comme adressés. Quand ils font ainsi, ils PEUVENT fournir les informations de mise à jour d'adresse avec un code 251, ou peuvent rejeter le message comme non livrable avec un code 550 et pas d'information spécifique d'adresse. Cependant, 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 cette information à l'utilisateur.

Les mises en œuvre de serveur SMTP qui prennent en charge les codes de réponse 251 et/ou 551 DEVRAIENT fournir des mécanismes de configuration afin que les sites qui concluent qu'ils pourraient divulguer contre leur gré des informations puissent désactiver ou restreindre leur usage.

3.5 Commandes pour déboguer les adresses

3.5.1 Vue d'ensemble

SMTP fournit des commandes pour vérifier le nom d'un utilisateur ou obtenir le contenu d'une liste de diffusion. Cela 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 aux 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 complet de l'utilisateur et DOIT inclure la boîte aux lettres de l'utilisateur. Elle DOIT être del'une des formes suivantes :

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

Quand 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 solutions de remplacement. En d'autres termes, tout ce qui suit est une réponse légitime à VRFY:

553 Utilisateur 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 va être supposé exposer le résultat à l'usager. Utiliser exactement les formes données, et les mots clés "Utilisateur ambigus" ou "ambigu", éventuellement complétés par des codes de réponse étendus, comme ceux décrits dans la [RFC3463], va faciliter la traduction automatique dans d'autres langages en tant que de besoin. Bien sûr, un client qui est très automatisé ou qui fonctionne dans une autre langue que l'anglais pourrait choisir d'essayer de traduire la réponse pour retourner une autre indication à l'usager que le texte littéral de la réponse, ou pour effectuer une action automatique comme de consulter un service de répertoire pour avoir des informations supplémentaires avant de faire rapport à l'utilisateur.

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

Chez 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 courante peut contenir les deux types d'entrées, et il est possible d'avoir des listes de diffusion

ne contenant qu'une seule boîte aux lettres. Si une demande est faire pour appliquer VRFY à une liste de diffusion, une réponse positive PEUT être donnée si un message ainsi adressé sera livré à tous ceux de la liste, autrement, une erreur DEVRAIT être rapportée (par exemple, "550 C'est une liste de diffusion, pas un utilisateur" ou "252 Incapable de vérifier les membres de la liste de diffusion"). Si une demande est faite pour l'expansion d'un nom d'utilisateur, le serveur PEUT retourner une réponse positive consistant en une liste contenant un nom, ou une erreur PEUT être rapportée (par exemple, "550 Ceci est un nom d'utilisateur, pas une liste de diffusion").

Dans le cas d'une réponse multi lignes de réussite (normale pour EXPN) exactement une boîte aux lettres doit être spécifiée sur chaque ligne de la réponse. Le cas d'une demande ambiguë a été discuté plus haut.

"Nom d'utilisateur" est un terme confus 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 "nom d'utilisateur". Cependant, comme la pratique courante de l'Internet résulte souvent en ce qu'un seul hôte traite la messagerie pour plusieurs domaines, les hôtes, et en particulier ceux 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 "nom d'utilisateur".

Le cas de l'expansion d'une liste de boîtes aux lettres exige une réponse multi lignes, comme :
C: EXPN Exemple-Personnes
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-Toilette-List
S: 550 Accès refusé.

Les arguments de chaîne de caractères des commandes VRFY et EXPN ne peuvent pas être plus réduits à cause de la diversité de mises en œuvre des concepts de nom d'utilisateur et de liste de boîte aux lettres. Dans certains systèmes, il peut être approprié que l'argument de la commande EXPN soit un nom de fichier pour un fichier contenant une liste de diffusion, mais là encore, il y a diverses conventions de désignation de fichier 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 le doit, et ne DEVRAIT généralement être utilisée que pour des besoins de diagnostic.

3.5.2 Réponse normale à VRFY

Lorsque des réponses normales (2yz ou 551) sont retournées à une demande VRFY ou EXPN, la réponse DOIT inclure le nom de <boîte aux lettres> en utilisant une construction "<partie-locale@domaine>", où "domaine" est un nom de domaine pleinement qualifié. Dans des circonstances assez exceptionnelles pour justifier la violation des intentions de la présente spécification, un texte en forme libre PEUT être retourné. Pour faciliter l'analyse par les ordinateurs et par les personnes, les adresses DEVRAIT apparaître entre crochets angulaires. Quand les adresses sont retournées, plutôt que des informations de débogage en forme libre, EXPN et VRFY DOIVENT retourner seulement des adresses de domaine valides utilisables dans les commandes SMTP RCPT. Par conséquent, si une adresse implique la livraison à un programme ou autre système, le nom de 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 prendre en charge VRFY et EXPN. Pour des raisons de sécurité, les mises en œuvre PEUVENT fournir aux installations locales un moyen pour désactiver l'une et/ou l'autre de ces commandes par des options de configuration ou équivalents (voir au paragraphe 7.3). Quand ces commandes sont prises en charge, il n'est pas exigé qu'elles fonctionnent à travers des relais quand le relais est accepté. Comme elles sont toutes deux facultatives dans la RFC 821, mais que VRFY est devenu obligatoire dans la [RFC1123], si EXPN est prise en charge, elle DOIT être mentionnée comme extension de service dans une réponse EHLO. VRFY PEUT être mentionné comme une facilité mais, comme sa prise en charge est exigée, les clients SMTP ne sont pas obligés de vérifier sa présence dans la liste des extensions avant de l'utiliser.

3.5.3 Signification d'une 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 est 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 indiqué ailleurs, la mise en œuvre (au sens d'une validation effective des adresses et des

informations de retour) de VRFY et EXPN est fortement recommandée. Donc, les mises en œuvre qui retournent 500 ou 502 pour VRFY ne sont pas pleinement conformes à la présente spécification.

Il peut y avoir des circonstances où une adresse paraît être valide mais ne peut pas raisonnablement être vérifiée en temps réel, en particulier quand un serveur agit comme échangeur de messagerie pour un autre serveur ou domaine. "Validité apparente", dans ce cas, impliquerait normalement au moins une vérification de la syntaxe et peut impliquer la vérification que tous les domaines spécifiés sont ceux auxquels l'hôte est supposé être capable de relayer des messages. Dans ces situations, le code de réponse 252 DEVRAIT être retourné. Ces cas entrent dans le cadre de la discussion de la vérification RCPT du paragraphe 2.1. De même, la discussion 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 vont être transmises ou rejetées si des messages sont reçus pour elles. Les mises en œuvre DEVRAIT généralement être plus agressives quant à la vérification d'adresse dans le cas de VRFY que dans le cas de RCPT, même si cela prend un peu plus de temps pour le faire.

3.5.4 Sémantique et applications de EXPN

EXPN est souvent très utile pour déboguer et comprendre les problèmes des listes de diffusion et des alias d'adresse à cibles multiples. Certains systèmes ont tenté d'utiliser l'expansion de source des listes de diffusion comme moyen d'éliminer les dupliqués. La propagation de systèmes d'alias avec la mesagerie sur l'Internet pour les hôtes (normalement avec des enregistrements MX et CNAME du DNS) pour les boîtes aux lettres (divers types d'alias d'hôte local) et dans divers arrangements de mandataires ont rendu presque impossible que ces stratégies fonctionnent de façon cohérente, et les systèmes de messagerie NE DEVRAIENT PAS les tenter.

3.6 Relais et acheminement de messagerie

3.6.1 Routes de source et relais

En général, la disponibilité des enregistrements l'échangeur de messagerie dans le système des noms de domaine [RFC1035], [RFC0974] rend l'utilisation des chemins explicites de source inutiles dans le système de messagerie de l'Internet. De nombreux problèmes historiques de l'interprétation des routes de source explicites ont rendu leur utilisation indésirable. Les clients SMTP NE DEVRAIENT PAS générer des 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. Quand des informations de route sont rencontrées, les serveurs SMTP PEUVENT ignorer les informations de route et simplement envoyer à la destination finale spécifiée comme dernier élément du chemin et DEVRAIT faire ainsi. Il y a eu une pratique invalide d'utiliser des 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 effacées, cette pratique cause des défaillances. C'est une des nombreuses raisons pour lesquelles les clients SMTP NE DOIVENT PAS générer des routes de source invalides ou dépendre d'une série de résolutions de noms.

Quand 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 transmission n'est pas applicable et le chemin inverse au moment de la livraison va simplement être l'adresse qui apparaissait dans la commande MAIL.

3.6.2 Enregistrements Mail eXchange et relais

Un serveur SMTP de relais est généralement la cible d'un enregistrement MX DNS qui le désigne, plutôt que le système lui-même de livraison final. Le serveur relais peut accepter ou rejeter la tâche de relayer la messagerie de la même façon qu'il accepte ou rejette les messages pour un utilisateur 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 (selon les règles de la Section 5) et lui envoie le message. Si il refuse de relayer la messagerie à une adresse particulière pour des raisons de politique, une réponse 550 DEVRAIT être retournée.

La présente spécification ne traite pas de la vérification des chemins de retour à utiliser dans les notifications de livraison. Un travail récent, comme celui sur SPF [RFC4408] et DKIM [RFC4686] [RFC4871], a été fait pour donner le moyen de s'assurer qu'une adresse est valide ou appartient à la personne qui a réellement envoyé le message. Un serveur PEUT tenter de vérifier le chemin de retour avant d'utiliser son adresse pour les notifications de livraison, mais les méthodes pour le faire ne sont pas définies ici, et aucune méthode particulière n'est recommandée pour l'instant.

3.6.3 Serveurs de soumission de message comme relais

Il existe de nombreux clients d'envoi de messagerie, en particulier en conjonction avec les facilités qui reçoivent de la messagerie via POP3 ou IMAP, qui ont des capacités limitées de prise en charge de certaines des exigences de la présente

spécification, comme la capacité de mettre les messages en file d'attente pour des tentatives de livraison ultérieures. Pour ces clients, il est de pratique courante de faire des arrangements privés pour envoyer tous les messages à un seul serveur pour traitement et distribution ultérieure. SMTP, comme il est spécifié ici, n'est pas idéal dans ce rôle. Un protocole de soumission de messagerie normalisé a été développé qui remplace graduellement les pratiques fondées sur SMTP (voir la [RFC4409]). En tous 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 dans d'autres environnements, pas seulement des relais SMTP et des systèmes de livraison finaux ; voir au paragraphe 3.7 et à 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 message ne peut pas être livré pour quelque autre raison, il DOIT alors construire un message de notification "message non livrable" et l'envoyer au générateur 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, la [RFC3461] et la [RFC3464]) DEVRAIENT être utilisés si possible.

Ce message de notification doit provenir du serveur SMTP à l'hôte relais ou à l'hôte qui le premier détermine que la livraison ne peut pas avoir lieu. 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 des boucles de rapports d'erreur est de spécifier un chemin inverse nul dans la commande MAIL d'un message de notification. Quand un tel message est transmis, le chemin inverse DOIT être réglé à nul (voir des explications supplémentaires au paragraphe 4.5.5). Une commande MAIL avec un chemin inverse nul apparaît comme suit :

MAIL FROM:<>

Comme expliqué au paragraphe 6.4, un relais SMTP n'a pas besoin d'inspecter ou d'agir sur la section d'en-tête ou de corps des données de message et NE DOIT PAS le faire sauf pour ajouter son propre champ d'en-tête "Received:" (paragraphe 4.4) et, facultativement, pour tenter de détecter des boucles dans le système de messagerie (voir au paragraphe 6.3). Bien sûr, cette interdiction s'applique aussi à toute modification de ces champs d'en-tête ou de texte (voir aussi le paragraphe 7.9).

3.7 Passerelle de messagerie

Bien que la fonction de relais discutée ci-dessus opère dans l'environnement de service de transport SMTP au sein de l'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 expliqué au paragraphe 2.3.10, quand un tel système est à la frontière entre deux environnements de service de transport, on l'appelle une "passerelle" ou "passerelle SMTP".

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

3.7.1 Champs d'en-tête dans les passerelles

Les champs d'en-tête PEUVENT être reécrits quand nécessaire lorsque des messages sont passés 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 6.4.

D'autres systèmes de messagerie passés dans l'Internet utilisent souvent un sous ensemble de la section d'en-tête de la RFC 822 ou fournissent une fonctionnalité similaire avec une syntaxe différente, mais certains de ces systèmes de messagerie n'ont pas d'équivalent de l'enveloppe SMTP. Donc, quand un message quitte l'environnement Internet, il peut être nécessaire de ranger les informations d'enveloppe SMTP dans la section d'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 la divulgation d'informations privées (voir au paragraphe 7.2).

3.7.2 Lignes reçus dans les passerelles

Lors de la transmission d'un message dans ou de l'environnement Internet, une passerelle DOIT ajouter devant une ligne Received:, mais elle NE DOIT PAS altérer une ligne Received: qui est déjà dans la section d'en-tête.

Les champs d'en-tête "Received:" des messages générés dans d'autres environnements peuvent ne pas se conformer exactement à la présente spécification. Cependant, l'usage le plus important des lignes Received: est pour corriger les fautes de messagerie, et cette correction peut être sévèrement entravée par des passerelles aux bonnes intentions qui essayent de "corriger" une ligne Received:. Une autre conséquence des champs d'en-tête de trace qui survient dans des environnements non SMTP, est que les systèmes receveurs NE DOIVENT PAS rejeter des messages sur la base du format d'un champ d'en-tête de trace et DEVRAIENT être extrêmement robustes en présence d'informations ou formats inattendus dans ces champs d'en-tête.

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

3.7.3 Adresses dans les passerelles

Du côté de l'Internet, la passerelle DEVRAIT accepter tous les formats d'adresse valides dans les commandes SMTP et dans la section d'en-tête de la RFC 822, et tous les messages RFC 822 valides. Les adresses et champs d'en-tête générés par les passerelles DOIVENT se conformer aux normes applicables (incluant celle-ci et la [RFC5322]). Les passerelles sont, bien sûr, soumises aux même règles de traitement de routes de source que celles décrites pour les autres systèmes SMTP du paragraphe 3.3.

3.7.4 Autres champs d'en-tête dans les passerelles

La passerelle DOIT s'assurer que tous les champs d'en-tête d'un message qu'elle transmet dans l'environnement de mesagerie de l'Internet satisfont aux exigences de la messagerie de l'Internet. En particulier, toutes les adresses dans les champs d'en-tête "From:", "To:", "Cc:", etc., DOIVENT être transformées (si nécessaire) pour satisfaire la syntaxe standard d'en-tête de la [RFC5322], DOIVENT faire référence uniquement à des noms de domaine pleinement qualifiés, et DOIVENT être effectives et utiles pour envoyer les réponses. L'algorithme de traduction utilisé pour convertir la messagerie des protocoles Internet en protocole d'un autre environnement DEVRAIT assurer que les messages d'erreur provenant de l'environnement de messagerie étranger sont livrés au chemin inverse à partir de l'enveloppe SMTP, et non à une adresse des champs d'en-tête "From:", "Sender:", ou similaires du message.

3.7.5 Enveloppes dans les passerelles

De même, quand on transmet un message d'un autre environnement dans l'Internet, la passerelle DEVRAIT régler le chemin de retour de l'enveloppe en accord avec l'adresse de retour d'un 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 de l'origine du message par défaut en dernier ressort.

3.8 Terminaison des sessions et connexions

Une connexion SMTP est terminée quand le client envoie une commande QUIT. Le serveur répond avec un code de réponse positif, après quoi il clôt la connexion.

Un serveur SMTP NE DOIT PAS clore intentionnellement la connexion dans les circonstances normales de fonctionnement (voir au paragraphe 7.8) sauf :

- Après avoir reçu une commande QUIT et répondu par une réponse 221.
- Après avoir détecté le besoin de fermer le service SMTP et retourné un code de réponse 421. Ce code de réponse peut être produit après que le serveur a reçu toute commande ou, si nécessaire, de façon asynchrone à partir de la commande receipt (en supposant que le client la recevra après la production de la prochaine commande).
- Après qu'une fin de temporisation se produit, comme spécifié au paragraphe 4.5.3.2, en attendant que le client envoie une commande ou des données.

En particulier, un serveur qui clôt les connexions en réponse à des commandes qui ne sont pas comprises est en violation de la présente spécification. Les serveurs sont supposés être tolérants aux commandes inconnues, produire une réponse 500 et attendre d'autres instructions de la part du client.

Un serveur SMTP qui est forcé 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 subissent une clôture de connexion, une réinitialisation, ou un autre échec de communication dû à des circonstances hors de son contrôle (en violation de l'intention de cette spécification mais parfois inévitables)

DEVRAIT, pour conserver la robustesse du système de messagerie, traiter la transaction de messagerie comme si une réponse 421 avait été reçue et agir en conséquence.

3.9 Listes de diffusion et alias

Un hôte à capacité SMTP DEVRAIT prendre en charge les deux modèles d'alias et de liste d'expansion d'adresse pour la livraison multiple. Quand un message est livré ou transmis à chaque adresse d'une forme d'expansion de liste, l'adresse de retour dans l'enveloppe ("MAIL FROM:") DOIT être changée en l'adresse d'une personne ou autre entité qui administre la liste. Cependant, dans ce cas, la section d'en-tête du message [RFC5322] DOIT rester inchangée ; en particulier, le champ "From" de la section d'en-tête n'est pas affecté.

Une facilité importante de messagerie est un mécanisme de livraison d'un seul message à plusieurs destinations, en transformant (ou "expansion" ou "explosion") d'une adresse de pseudo boîte aux lettres en adresses d'une liste de boîtes aux lettres de destination. Quand 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 expansée. Les serveurs DEVRAIT simplement utiliser les adresses de la liste ; l'application d'heuristiques ou autres règles de correspondance pour éliminer certaines adresses, comme celle de l'origine, est fortement déconseillée. On classe un telle pseudo boîte aux lettres comme "alias" ou "liste", selon les règles d'expansion.

3.9.1 Alias

Poue expanser un alias, le messageur du receveur remplace simplement l'adresse de la pseudo boîte aux lettres dans l'enveloppe par chacune des adresses expansées tour à tour ; le reste de l'enveloppe et le corps de message sont laissés inchangés. Le message est alors livré ou transmis à chaque adresse expansée.

3.9.2 Liste

Une liste de diffusion peut être dite fonctionner par "redistribution" plutôt que par "transmission". Pour expanser une liste, le messageur de réception remplace l'adresse de la pseudo boîte aux lettres dans l'enveloppe par chaque adresse expansée tout à tour. L'adresse de retour (pointant vers l'arrière) dans l'enveloppe est changée afin 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 pas le contrôle du contenu de la liste et va normalement trouver les messages d'erreur perturbants. Noter que la différence clé entre le traitement des alias (paragraphe 3.9.1) et la transmission (ce paragraphe) est le changement de l'adresse pointant vers l'arrière dans ce cas. Quand une liste contraint son traitement à l'ensemble très limité de modifications et actions décrit ici, il est tentant d'émuler un MTA ; de telles listes peuvent être traitées comme une continuation dans le transit de messagerie électronique.

Il existe des listes de diffusion qui effectuent des modifications suplémentaires, parfois extensives, à un message et son enveloppe. De telles listes de diffusion doivent être vues comme des MTA complets, qui acceptent une livraison et un envoi d'un nouveau message.

4. Spécifications SMTP

4.1 Commandes SMTP

4.1.1 Sémantique et syntaxe des commandes

Les commandes SMTP définissent la fonction de transfert de messagerie ou de système de messagerie demandée par l'utilisateur. 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. (Pour améliorer l'interopérabilité, les receveurs SMTP DEVRAIENT tolérer les espaces en queue avant le <CRLF> de terminaison.) La syntaxe de la partie locale d'une boîte aux lettres DOIT se conformer aux conventions du site receveur et à la syntaxe spécifiée au paragraphe 4.1.2. Les commandes SMTP sont exposées ci-après. Les réponses SMTP sont exposées au paragraphe 4.2.

Une transaction de messagerie implique plusieurs objets de données qui sont communiqués comme arguments aux différentes commandes. Le chemin inverse est l'argument de la commande MAIL, le chemin de transmission est l'argument de la commande RCPT, 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 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. Les commandes spécifiques causent l'ajout des informations dans une mémoire tampon spécifique, ou causent la purge 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 HELLO (EHLO) ou HELLO (HELO) étendu

Ces commandes sont utilisées pour identifier le client SMTP auprès du serveur SMTP. La clause d'argument contient le nom de domaine pleinement qualifié du client SMTP, si il en est un disponible. Dans les situations où le système client SMTP n'a pas de nom de domaine significatif (par exemple, quand son adresse est allouée de façon dynamique et qu'aucun enregistrement de transposition inverse n'est disponible) le client DEVRAIT envoyer une adresse littérale (voir au paragraphe 4.1.3).

La RFC 2821, et des pratiques antérieures informelles, encourageaient de faire suivre le littéral par des informations qui aideraient à identifier le système client. Cette convention n'était pas largement acceptée, et de nombreux serveurs SMTP la considérait comme une erreur. Dans l'intérêt de l'interopérabilité, il est probablement sage que les serveurs soient prêts à ce que cette chaîne soit produite, mais les clients SMTP NE DEVRAIENT PAS l'envoyer.

Le serveur SMTP s'identifie au client SMTP dans la réponse d'accueil de connexion et dans la réponse à cette commande.

Un client SMTP DEVRAIT commencer une session SMTP en produisant la commande EHLO. Si le serveur SMTP prend en charge les extensions de service SMTP, il va donner 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 pas en charge les extensions de service SMTP, il va générer une réponse d'erreur. Les plus anciens systèmes de client SMTP PEUVENT, comme expliqué plus haut, utiliser HELO (comme spécifié dans la RFC 821) au lieu du EHLO, et les serveurs DOIVENT prendre en charge la commande HELO et y répondre correctement. Dans tous les cas, un client DOIT produire 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'aucune transaction n'est en cours et que tous les tableaux d'état et mémoires tampon sont vides.

Syntaxe :
ehlo = "EHLO" SP (Domaine / adresse-littérale) CRLF
helo = "HELO" SP Domaine CRLF

Normalement, la réponse à EHLO va être une réponse multi lignes. Chaque ligne de la réponse contient un mot-clé et, facultativement, un ou plusieurs paramètres. Suivant la syntaxe normale des réponses multi lignes, ces mots-clés suivent le code (250) et tiret pour toutes les lignes sauf la dernière, 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 la [RFC5234], est :

```
ehlo-ok-rsp  = ( "250" SP Domaine [ SP ehlo-accueil ] CRLF )
               / ( "250-" Domaine [ SP ehlo-accueil ] CRLF
               *( "250-" ehlo-ligne CRLF )
               "250" SP ehlo-ligne CRLF )

ehlo-accueil  = 1*(%d0-9 / %d11-12 / %d14-127)          ; chaîne de tous caractères autres que CR ou LF

ehlo-ligne  = ehlo-mot-clé *( SP ehlo-param )

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

ehlo-param  = 1*(%d33-126)      ; tout caractère sauf <SP> et tous les caractères de contrôle (US-ASCII 0-31 et 127 inclus)
```

Bien que les mots-clés EHLO puissent être spécifiés en majuscules, minuscules, ou en casse mixte, ils DOIVENT toujours être reconnus et traités de façon insensible à la casse. C'est simplement une extension des pratiques spécifiées dans la RFC 821 et au paragraphe 2.4.

La réponse EHLO DOIT contenir des mots-clés (et les paramètres associés si nécessaire) pour toutes les commandes non mentionnées comme "exigées" au paragraphe 4.5.1 à l'exception des seules commandes d'utilisation privée, comme décrit au paragraphe 4.1.5. Des commandes d'utilisation privée PEUVENT être mentionnées.

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). La clause 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 consiste en la boîte aux lettres de l'envoyeur. Historiquement, cette boîte aux lettres pouvait facultativement avoir été 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 probablement causer une boucle de messages (par exemple, des notifications de livraison et de non livraison de messages) le chemin inverse peut être nul (voir au paragraphe 3.6).

Cette commande vide la mémoire tampon de chemin inverse, la mémoire tampon de chemin de transmission, et la mémoire tampon des données de messagerie, et elle insère les informations de chemin inverse à partir de sa clause d'argument dans la mémoire tampon de chemin inverse.

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

Syntaxe :
mail = "MAIL FROM:" chemin inverse [SP paramètres de messagerie] CRLF

4.1.1.3 RECIPIENT (RCPT)

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

Le chemin de transmission consiste normalement en la boîte aux lettres de destination exigée. Les systèmes envoyeurs NE DEVRAIENT PAS générer la liste facultative des hôtes connus comme route de source. Les systèmes receveurs DOIVENT reconnaître la syntaxe de route de source mais DEVRAIENT supprimer la spécification de 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 supprimer 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 en accord avec les conventions de messagerie de son hôte.

Cette commande ajoute son argument de chemin de transmission à la mémoire tampon de chemin de transmission ; cela ne change pas la mémoire tampon de chemin ni la mémoire tampon de données de messagerie.

Par exemple, le message reçu à l'hôte relais xyz.com avec les commandes d'enveloppe

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>
```

va normalement être envoyé directement à l'hôte d.bar.org avec les commandes d'enveloppe

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<userc@d.bar.org>
```

Comme indiqué à l'Appendice C, xyz.com PEUT et choisit 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>
```

Il est maintenant fortement déconseillé de tenter d'utiliser le relais de cette façon. Comme les hôtes ne sont pas du tout obligés de relayer les messages, xyz.com PEUT aussi rejeter entièrement le message quand il reçoit la commande RCPT, en utilisant un code 550 (car c'est une "raison de politique").

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

Syntaxe :
rcpt = "RCPT TO:" ("<Postmaster@" Domaine ">" / "<Postmaster>" / chemin-de-transmission) [SP paramètres de réception] CRLF

Noter que, à la différence des règles usuelles pour les parties locales, la chaîne "Postmaster" montrée ci-dessus est traitée comme insensible à la casse.

4.1.1.4 DATA (DATA)

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

Les données de messagerie sont terminées par une ligne contenant seulement un point, c'est-à-dire, la séquence de caractères "<CRLF>.<CRLF>", où le premier <CRLF> est en fait la terminaison de la ligne précédente (voir au paragraphe 4.5.2). C'est l'indication de la fin des données de messagerie. Le premier <CRLF> de cette séquence de terminaison est aussi le <CRLF> qui termine la ligne finale des données (texte du message) ou, si il n'y avait pas de données de message, termine la commande DATA elle-même (le cas "pas de données de messagerie" ne se conforme pas à la présente spécification car cela exigerait que ni les champs d'en-tête trace exigés par cette spécification ni la section d'en-tête de message requise par la [RFC5322] ne soient transmis). 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 va se produire 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 de "fin de données".

La coutume d'accepter des lignes se terminant seulement par <LF>, comme concession aux comportements non conformes de la part de certains systèmes UNIX, s'est révélée causer plus de problèmes d'interopérabilité qu'elle n'en résout, et les systèmes de serveur SMTP NE DOIVENT PAS le faire, même au nom d'une amélioration de la robustesse. En particulier, la séquence "<LF>.<LF>" (sauts à la ligne nus, sans retour charriot) 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 exige que le serveur traite les informations de transaction de messagerie mémorisées. Ce traitement consomme les informations de la mémoire tampon de chemin inverse, de la mémoire tampon de chemin de transmission, et de 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 positive d'achèvement "250 OK" à l'indication de la fin des données, le receveur prend l'entière responsabilité du message (voir au paragraphe 6.1). Les erreurs qui sont diagnostiquées ensuite DOIVENT être rapportées dans un message, comme expliqué au paragraphe 4.4.

Quand le serveur SMTP accepte un message pour le relayer ou pour sa livraison finale, il insère un enregistrement de trace (aussi appelé de façon interchangeable une "ligne d'horodatage" ou ligne "Received") par dessus les données de messagerie. Cet enregistrement de trace indique l'identité de l'hôte qui a envoyé le message, l'identité de l'hôte qui a reçu le message (et qui insère cet horodatage) et la date et l'heure de réception du message. Les messages relayés vont avoir plusieurs lignes d'horodatage. Les détails de la formation de ces lignes, y compris leur syntaxe, sont spécifiés au paragraphe 4.4.

Des explications supplémentaires sur le fonctionnement de la commande DATA figurent au paragraphe 3.3.

Syntaxe :
data = "DATA" CRLF

4.1.1.5 RESET (RSET)

Cette commande spécifie que la transaction de messagerie en cours va être interrompue. Tous les envoyeurs, receveurs, 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 “reset” peut être produite par le client à tout moment. Elle est effectivement équivalente à NOOP (c'est-à-dire, n'a pas d'effet) si elle est produite immédiatement après EHLO, avant que EHLO soit produit dans la session, après l'envoi d'un indicateur de fin des données et son accusé de réception, ou immédiatement avant un QUIT. Un serveur SMTP NE DOIT PAS clore la connexion par suite de la réception d'un RSET ; cette action est réservée pour QUIT (voir au paragraphe 4.1.1.10).

Comme EHLO implique un traitement et une réponse supplémentaire de la part du serveur, RSET va normalement être plus efficace que de produire à nouveau cette commande, même si la sémantique formelle est la même.

Il y a des circonstances, contraires aux intentions de cette spécification, dans lesquelles un serveur SMTP peut recevoir une 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 à cette condition et DEVRAIENT la traiter comme si un QUIT avait été reçu avant que la connexion disparaisse.

Syntaxe :
rset = "RSET" CRLF

4.1.1.6 VERIFY (VRFY)

Cette commande demande au receveur de confirmer que l'argument identifie un utilisateur 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, sur la mémoire tampon de chemin de transmission, ou sur la mémoire tampon de données de messagerie.

Syntaxe :
vrfy = "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 si oui, de retourner les membres de cette liste. Si la commande réussit, une réponse est retournée qui contient les informations décrites au paragraphe 3.5. Cette réponse aura plusieurs lignes sauf 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, sur la mémoire tampon de chemin de transmission, ou sur la mémoire tampon de données de messagerie, et elle peut être produite à tout moment.

Syntaxe :
expn = "EXPN" SP Chaîne CRLF

4.1.1.8 HELP (HELP)

Cette commande cause l'envoi par le serveur d'informations utiles pour le client. La commande PEUT prendre un argument (par exemple, tout nom de commande) et retourner des informations spécifiques comme réponse.

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

Les serveurs SMTP DEVRAIENT prendre en charge HELP sans argument et PEUVENT la prendre en charge avec des arguments.

Syntaxe :
help = "HELP" [SP Chaîne] CRLF

4.1.1.9 NOOP (NOOP)

Cette commande n'affecte aucun paramètre ou commande entré précédemment. Elle ne spécifie pas d'action autre que l'envoi par le receveur d'une réponse "250 OK".

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

Syntaxe :
noop = "NOOP" [SP chaîne] CRLF

4.1.1.10 QUIT (QUIT)

Cette commande spécifie que le receveur DOIT envoyer une réponse "221 OK", et alors clore le canal de transmission.

Le receveur NE DOIT PAS clore intentionnellement le canal de transmission avant d'avoir reçu et répondu à une commande QUIT (même si c'était une erreur). L'envoyeur NE DOIT PAS clore intentionnellement le canal de transmission tant qu'il n'a pas envoyé une commande QUIT, et il DEVRAIT attendre jusqu'à ce qu'il ait reçu la réponse (même si il y avait une réponse d'erreur à une commande précédente). Si la connexion est close prématurément due à des violations de ce qui est mentionné ci-dessus ou à une défaillance du système ou du réseau, le serveur DOIT annuler toute transaction en cours, mais ne doit pas annuler une transaction achevée précédemment, et généralement DOIT 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. Toute transaction de messagerie non achevée en cours va être interrompue.

Syntaxe :
quit = "QUIT" CRLF

4.1.1.11 Réponses d'erreur à des paramètres en réception

Si le serveur SMTP ne reconnaît pas ou ne peut pas mettre en œuvre un ou plusieurs des paramètres associés à une commande MAIL FROM ou RCPT TO particulière, il va retourner le code 555.

Si, pour une raison quelconque, le serveur est temporairement incapable de traiter un ou plusieurs des paramètres associés à une commande MAIL FROM ou RCPT TO, et si la définition du paramètre spécifique ne rend pas obligatoire l'utilisation d'un autre code, il devrait retourner le code 455.

Les erreurs spécifiques de paramètres particuliers et leurs valeurs vont être spécifiées dans la RFC de définition du paramètre.

4.1.2 Syntaxe d'argument de commande

La syntaxe de la clause d'argument des commandes ci-dessus (en utilisant la syntaxe spécifiée dans la [RFC5234] lorsque applicable) est donnée ci-dessous. Certaines des productions données ci-dessous ne sont utilisées qu'en conjonction avec les routes de source comme décrit à l'Appendice C. Les terminaux non définis dans le présent document, comme ALPHA, DIGIT, SP, CR, LF, CRLF, sont définis dans le "cœur" de syntaxe de l'Appendice B de la [RFC5234] ou dans la syntaxe de format de message de la [RFC5322].

Chemin-inverse = Chemin / "<>"

Chemin-de-transmission = Chemin

Chemin = "<" [A-d-l ":"] boîte aux lettres ">"

A-d-l = At-domaine *("," At-domaine) ; Noter que cette forme, ce qu'on appelle "route de source", DOIT être acceptée, NE DEVRAIT PAS être générée, et DEVRAIT être ignorée.

At-domaine = "@" Domaine

Mail-parameters = esmtp-param *(SP esmtp-param)

Rcpt-parameters = esmtp-param *(SP esmtp-param)

esmtp-param = esmtp-keyword ["=" esmtp-value]

esmtp-keyword = (ALPHA / CHIFFRE) *(ALPHA / CHIFFRE / "-")

esmtp-value = 1*(%d33-60 / %d62-126) ; tout CHAR sauf "=", SP, et les caractères de contrôle. Si cette chaîne est une adresse de messagerie électronique, c'est-à-dire, une boîte aux lettres, alors la syntaxe "xtext" [RFC3461] DEVRAIT être utilisée.

Keyword = Ldh-str

Argument = Atom

Domaine = sous-domaine *("." sous-domaines)

sous-domaine = Let-dig [Ldh-str]

Let-dig = ALPHA / CHIFFRE

Ldh-str = *(ALPHA / CHIFFRE / "-") Let-dig

address-literal = "[" (IPv4-address-literal / IPv6-address-literal / General-address-literal) "]" ; voir le paragraphe 4.1.3

boîte aux lettres = Partie-locale "@" (Domaine / address-literal)

Partie-locale = Dot-string / Quoted-string ; PEUT être sensible à la casse

Dot-string = Atom *("." Atom)

Atome = 1*atext

Quoted-string = DQUOTE *QcontentSMTP DQUOTE

QcontentSMTP = qtextSMTP / quoted-pairSMTP

quoted-pairSMTP = %d92 %d32-126 ; c'est-à-dire, barre oblique suivie par tout caractère ASCII graphique (incluant lui-même) ou espace

qtextSMTP = %d32-33 / %d35-91 / %d93-126 ; c'est-à-dire, au sein d'une chaîne entre guillemets, tout caractère ASCII graphique ou espace est permis sans signalisation par barre oblique inverse sauf guillemets doubles et la barre oblique inverse elle-même.

Chaîne = Atom / Quoted-string

Bien que la définition de Partie-locale ci-dessus soit relativement permissive, pour maximiser l'interopérabilité, un hôte qui s'attend à recevoir un message DEVRAIT éviter de définir des boîtes aux lettres où la Partie-locale exige (ou utilise) la forme Quoted-string ou où la Partie-locale est sensible à la casse. Pour tout ce qui exige de générer ou comparer les parties locales (par exemple, à des 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 moins possible de guillemets.

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

Noter que la barre oblique inverse , "\", est un caractère de citation, qui est utilisé pour indiquer que le prochain caractère est à utiliser littéralement (au lieu de son interprétation normale). Par exemple, "Joe\,Smith" indique une chaîne d'un seul nom d'utilisateur de neuf caractères avec la virgule au quatrième caractère de cette chaîne.

Pour promouvoir l'interopérabilité et conformément aux directives déjà anciennes sur l'utilisation prudente du DNS dans les désignations et applications (par exemple, voir au paragraphe 2.3.1 du document DNS de base [RFC1035]) les caractères en dehors de l'ensemble des caractères alphabétiques, chiffres, et tiret NE DOIVENT PAS apparaître dans les étiquettes de nom de domaine pour les clients ou serveurs SMTP. En particulier, le caractère souligné n'est pas permis. Les serveurs SMTP qui reçoivent une commande dans laquelle ces codes de caractère invalides ont été employés, et pour laquelle il n'y a pas d'autre raison de rejet, DOIVENT rejeter cette commande avec une réponse 501 (cette règle, comme d'autres, pourrait être outrepassée par des extensions SMTP appropriées).

4.1.3 Adresse littérale

Parfois un hôte n'est pas connu du système des noms de domaines et la communication (et, en particular, la communication pour rapporter et réparer l'erreur) est bloquée. Pour franchir cette barrière, une forme littérale spéciale de l'adresse est permise comme solution de remplacement à un nom de domaine. Pour les adresses IPv4, cette forme utilise quatre petits entiers décimaux séparés par des points et entre crochets comme dans [123.255.37.2], qui indique une adresse Internet (IPv4) en forme de séquence d'octets. Pour IPv6 et d'autres formes d'adressage qui pourraient éventuellement être normalisées, la forme consiste en une "étiquette" normalisée qui identifie la syntaxe de l'adresse, deux-points, et l'adresse elle-même, dans un format spécifié au titre des normes pertinentes (c'est-à-dire, la [RFC4291] pour IPv6).

Spécifiquement :

IPv4-address-literal = Snum 3("." Snum)

IPv6-address-literal = "IPv6:" IPv6-addr

General-address-literal = Standardized-tag ":" 1*dcontent

Standardized-tag = Ldh-str ; Standardized-tag DOIT être spécifié dans une RFC sur la voie de la normalisation et enregistré par l'IANA.

dcontent = %d33-90 / ; US-ASCII imprimable %d94-126 ; sauf "[", "\", "]"

Snum = 1*3DIGIT ; représentant une valeur d'entier décimal dans la gamme 0 à 255.

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 2 groupes de 16 bits de zéros. Pas plus de 6 groupes en plus du "::" 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 2 groupes de 16 bits de zéros. Pas plus de 4 groupes en plus du "::" et de IPv4-address-literal 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 les commandes pour les transactions qui ne sont pas 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 et si la commande EHLO est acceptable au serveur SMTP, 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 redondant, mais sans dommages autres qu'en coût de performances d'exécuter des commandes inutiles.

Si la commande EHLO n'est pas acceptable au serveur SMTP, des réponses d'échec 501, 500, 502, ou 550 DOIVENT être retournées comme approprié. Le serveur SMTP DOIT après la transmission de ces réponses rester dans le même état qu'il était avant de recevoir le EHLO.

Le client SMTP DOIT, si possible, s'assurer que le paramètre de domaine pour la commande EHLO est un nom principal d'hôte comme spécifié pour cette commande au paragraphe 2.3.5. Si ce n'est pas possible (par exemple, quand 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.

Un serveur SMTP PEUT vérifier que l'argument de nom de domaine dans la commande EHLO correspond bien à l'adresse IP du client. Cependant, si la vérification échoue, le serveur NE DOIT PAS refuser d'accepter un message sur cette base. Les informations capturées dans la tentative de vérification servent aux besoins de traçage et de journaux d'événements. Noter que cette interdiction s'applique seulement à la confrontation du paramètre à son adresse IP ; voir au paragraphe 7.9 une discussion plus développée du rejet des connexions entrantes ou des messages de la messagerie.

Les commandes NOOP, HELP, EXPN, VRFY, et RSET peuvent être utilisées à tout moment durant une session, ou sans avoir précédemment initialisé une session. Les serveurs SMTP DEVRAIENT traiter cela 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 dans la RFC 821 qui montre "550 Accès 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 un 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 RCPT, et une commande DATA, dans cet ordre. Une transaction de messagerie peut être interrompue par la commande RSET, un nouvel EHLO, ou la commande QUIT. 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, elle ne devrait être envoyée que si aucune transaction de messagerie n'a commencé dans la session, ou si la précédente s'est conclue avec succès avec une commande DATA réussie, ou si la précédente a été interrompue, par exemple, avec un RSET ou un nouvel EHLO.

Si l'argument de commande commençant la 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 dans une transaction sont déclassées au point qu'elles ne peuvent pas 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 d'une session DOIT être la commande QUIT. La commande QUIT DEVRAIT être utilisée par le client SMTP pour demander la clôture de la connexion, même quand aucune commande d'ouverture de session n'a été envoyée et acceptée.

4.1.5 Commandes d'utilisation privée

Comme spécifié au paragraphe 2.2.2, des commandes commençant par un "X" peuvent être utilisées par accord bilatéral entre les agents SMTP client (envoyeur) et serveur (receveur). Un serveur SMTP qui ne reconnaît pas ces commandes est supposé répondre par "500 Commande non reconnue". Un serveur SMTP étendu PEUT faire la liste des noms de caractéristiques associées 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 assurer la synchronisation des demandes et des actions dans le processus de transfert des messages 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 de commande-réponse sont décrits au paragraphe 4.3.

Une réponse SMTP consiste en un numéro de trois chiffres (transmis comme trois caractères numériques) suivis par du texte sauf spécification contraire dans ce document. Le numéro est à l'usage de l'automate pour déterminer dans quel état entrer ensuite ; le texte est à l'usage humain. Les trois chiffres contiennent assez d'informations codées pour que le client SMTP n'ait pas besoin d'examiner le texte et puisse soit l'éliminer, soit le passer à l'utilisateurr, comme approprié. Les exceptions sont notées plus loin dans ce document. En particulier, les codes de réponse 220, 221, 251, 421, et 551 sont associés à un texte de message qui doit être analysé et interprété par les machines. Dans le cas général, le texte peut dépendre du receveur et du contexte, de sorte qu'il y a probablement des textes différents pour chaque code de réponse. Une discussion de la théorie des codes de réponse est donnée au paragraphe 4.2.1. Formellement, une réponse est definie comme une séquence : un code de trois chiffres, <SP>, une ligne de texte, et <CRLF>, ou une réponse multi lignes (comme défini dans le même paragraphe). 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 d'espace en queue).

Seules les commandes EHLO, EXPN, et HELP sont supposées résulter en réponses multi lignse dans des circonstances normales ; cependant, les réponses multi lignes sont permises pour toute commande.

En ABNF, les réponses de serveur sont :

```
Greeting  = ( "220 " (Domaine / address-literal)
              [ SP chaîne-de-texte ] CRLF ) /
              ( "220-" (Domaine / address-literal)
              [ SP chaîne-de-texte ] CRLF
              *( "220-" [ chaîne-de-texte ] CRLF )
              "220" [ SP chaîne-de-texte ] CRLF )

chaîne-de-texte  = 1*(%d09 / %d32-126)                ; HT, SP, US-ASCII imprimable

Reply-line  = *( Reply-code "-" [ chaîne-de-texte ] CRLF )
                 Reply-code [ SP chaîne-de-texte ] CRLF

Reply-code  = %x32-35 %x30-35 %x30-39
```

où "Greeting" n'apparaît que dans la réponse 220 qui annonce que le serveur ouvre sa partie de la connexion. (Les autres réponses de serveur possibles à la connexion suivent la syntaxe de Reply-line.)

Un serveur SMTP DEVRAIT envoyer seulement les codes de réponse mentionnés dans le présent document. Un serveur SMTP DEVRAIT utiliser le texte montré dans les exemples chaque fois que c'est approprié.

Un client SMTP DOIT déterminer ses actions par le seul code de réponse, et non par le texte (sauf pour les réponses "changement d'adresse" 251 et 551 et, si nécessaire, 220, 221, et 421) ; en général, tout texte, incluant pas de texte du tout (bien que les envoyeurs NE DEVRAIENT PAS envoyer de codes nus) DOIT être acceptable. L'espace (blanche) suivant le code de réponse est considérée faire partie du texte. Chaque fois que possible, un envoyeur SMTP DEVRAIT vérifier le premier chiffre (indication de sévérité) du code de réponse.

La liste des codes qui apparaît ci-dessous NE DOIT PAS être conçue comme permanente. Bien que l'ajout de nouveaux codes devrait être une activitgé rare et significative, avec des informations supplémentaires dans la partie textuelle de la response de préférence, de nouveaux codes pourront être ajoutés par de nouvelles spécifications sur la voie de la 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.

En l'absence d'extensions négociées avec le client, les serveurs SMTP NE DOIVENT PAS envoyer de codes de réponse dont les premiers chiffres sont autres que 2, 3, 4, ou 5. Les clients qui reçoivent de tels codes hors gamme DEVRAIENT normalement les traiter comme erreurs fatales et terminer la transaction de messagerie.

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, va être capable de déterminer sa prochaine action (traiter comme précu, refaire, réformer, etc.) en examinant ce premier chiffre. Un client SMTP qui veut savoir approximativement quel sorte d'erreur s'est produite (par exemple, erreur du système de messagerie, erreur de syntaxe de commande) peut examiner le second chiffre. Le troisième chiffre et toutes les informations supplémentaires qui peuvent être présentes sont réservés pour les informations de plus fine granularité.

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

2yz : Réponse positive d'achèvement. L'action demandée a été menée à bien. Une nouvelle demande peut être initiée.

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

4yz : Réponse négative d'achèvement transitoire. 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 revenir au début de la séquence de commandes (si il en est). Il est difficile de fixer la signification de "transitoire" quand deux sites différents (agents SMTP receveur et envoyeur) doivent s'accorder sur l'interprétation. Chaque réponse dans cette catégorie pourrait avoir une valeur de temps différente, mais le client SMTP DEVRAIT

essayer encore. Une règle d'approximation pour déterminer si une réponse va dans la catégorie 4yz ou 5yz (voir ci-dessous) est que les réponses sont 4yz si elles peuvent être réussies si elles sont répétées sans changement de la forme de la commande ou des propriétés de l'envoyeur ou receveur (c'est-à-dire, la commande est répétée à l'identique et le receveur n'établit pas une nouvelle mise en œuvre).

5yz : Réponse négative d'achèvement permanente. La commande n'a pas été acceptée et l'action demandée ne s'est pas produite. Le client SMTP NE DEVRAIT PAS répéter exactement la demande (dans la même séquence). Certaines conditions d'erreur "permanentes" peuvent même être corrigées, de sorte que l'utilisateur humain peut vouloir inciter le client SMTP à réinitialiser la séquence de commandes par une action directe à l'avenir (par exemple, après un changement d'orthographe, ou que l'utilisateur a modifié l'état du compte).

On notera que le protocole de transfert de fichiers (FTP, *File Transfer Protocol*) [RFC0959] utilise une architecture de codes très similaire et que les codes SMTP se fondent sur le modèle FTP. Cependant, SMTP utilise un modèle à une commande, une réponse (tandis que FTP est asynchrone) et les codes 1yz de FTP de font pas partie du modèle SMTP.

Le second chiffre code les réponses dans des catégories spécifiques :

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

x1z : Information. Ce sont des réponses à des demandes d'informations, comme d'état ou d'aide.

x2z : Connexions. Ces réponses se refèrent au canal de transmission.

x3z : Non spécifié.

x4z : Non spécifié.

x5z : Système de messagerie. Ces réponses indiquent l'état du système de messagerie receveur vis-à-vis du transfert demandé ou d'autre action du système de messagerie.

Le troisième chiffre donne une gradation plus fine de la signification de chaque catégorie spécifiée par 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. Par ailleurs, 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 comme NOOP, dont l'exécution réussie n'offre au client SMTP aucune nouvelle information, va retourner une réponse 250. La réponse est 502 quand la commande demande une action non mise en œuvre non spécifique du site. Un rafinement de cela est la réponse 504 pour une commande qui est mise en œuvre, mais qui demande un paramètre non mis en œuvre.

Le texte de réponse peut être plus long qu'une seule ligne ; dans ce cas, le texte complet doit être marqué afin que le client SMTP sache quand il peut arrêter 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 , "-" (et aussi appelé signe moins) suivi par le texte. La dernière ligne va commencer par le code de réponse, suivi immédiatement par <SP>, un texte facultatif, et <CRLF>. Comme noté ci-dessus, les serveurs DEVRAIENT envoyer le <SP> si du texte n'est pas envoyé ensuite, mais les clients DOIVENT être prêts à ce qu'il soit omis.

Par exemple :

```
250-Première ligne
250-Seconde ligne
250-234 Texte commençant par les numéros
250 La dernière ligne
```

Dans une réponse multi lignes, le code de réponse sur chaque ligne DOIT être le même. Il est raisonnable que le client compte dessus, afin qu'il puisse prendre des décisions de traitement sur la base du code dans n'importe quelle ligne, supposant que toutes les autres seront les mêmes. Dans quelques cas, il y a des données importantes pour le client dans le "texte" de réponse. Le client va être capable d'identifier ces cas d'après le contexte.

4.2.2 Codes de réponse par groupe de fonction

500 : Erreur de syntaxe, commande non reconnue (cela peut inclure des erreurs comme une ligne de commande trop longue)
501 : Erreur de syntaxe dans les paramètres ou 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'aide (informations sur la façon d'utiliser le receveur ou la signification d'une commande non standard particulière ; cette réponse n'est utile qu'à l'utilisateur humain)
220 : Service <domaine> prêt
221 : Service <domaine> cloturant le canal de transmission
421 : Service <domaine> indisponible, cloturant le canal de transmission (ce peut être une réponse à toute commande si le service sait qu'il doit fermer)
250 : Action de messagerie bien effectuée
251 : Utilisateur non local ; sera transmis à <chemin de transmission> (voir le paragraphe 3.4)
252 : L'utilisateur ne peut pas être vérifié, mais va accepter le message et tenter la livraison (voir le paragraphe 3.5.3)
455 : Le serveur ne peut pas traiter les paramètres
555 : Les paramètres MAIL FROM/RCPT TO ne sont pas reconnus ou pas mis en œuvre
450 : Action de messagerie demandée non effectuée ; boîte aux lettres indisponible (par exemple, boîte aux lettres occupée ou temporairement bloquée pour des raisons de politique)
550 : Action demandée non effectuée : boîte aux lettres indisponible (par exemple, boîte aux lettres non trouvée, pas d'accès, ou commande rejetée pour des raisons de politique)
451 : Action demandée interrompue : erreur de traitement
551 : Utilisateur non local ; prière de réessayer <chemin-de-transmission> (voir le paragraphe 3.4)
452 : Action demandée non effectuée : système de mémorisation insuffisant
552 : Action de messagerie demandée interrompue : allocation de mémorisation dépassée
553 : Action demandée non effectuée : nom de boîte aux lettres non autorisé (par exemple, syntaxe de boîte aux lettres incorrecte)
354 : Début d'entrée de messagerie ; terminer avec <CRLF>.<CRLF>
554 : Échec de transaction (ou, dans le cas de réponse d'ouverture de connexion, "Pas de service SMTP")

4.2.3 Codes de réponse par ordre numérique

211 : État du système, ou réponse d'aide au système
214 : Message d'aide (informations sur comment utiliser le receveur ou sur la signification d'une commande non standard particulière ; cette réponse n'est utile qu'à l'utilisateur humain)
220 : Service <domaine> prêt
221 : Service <domaine> cloturant le canal de transmission
250 : Action de messagerie bien effectuée
251 : Utilisateur non local ; sera transmis à <chemin de transmission> (voir le paragraphe 3.4)
252 : L'utilisateur ne peut pas être vérifié, mais va accepter le message et tenter la livraison (voir le paragraphe 3.5.3)
354 : Début d'entrée de messagerie ; terminer avec <CRLF>.<CRLF>
421 : Service <domaine> indisponible, cloturant 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 ou temporairement bloquée pour des raisons de politique)
451 : Action demandée interrompue : erreur de traitement
452 : Action demandée non effectuée : système de mémorisation insuffisant
455 : Le serveur ne peut pas traiter les paramètres
500 : Erreur de syntaxe, commande non reconnue (cela peut inclure des erreurs comme une ligne de commande trop longue)
501 : Erreur de syntaxe dans les paramètres ou 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 non trouvée, pas d'accès, ou commande rejetée pour des raisons de politique)
551 : Utilisateur non local ; prière de réessayer <chemin-de-transmission> (voir le paragraphe 3.4)
552 : Action de messagerie demandée interrompue : allocation de mémorisation dépassée
553 : Action demandée non effectuée : nom de boîte aux lettres non autorisé (par exemple, syntaxe de boîte aux lettres incorrecte)
554 : Échec de transaction (ou, dans le cas de réponse d'ouverture de connexion, "Pas de service SMTP")

555 : Les paramètres MAIL FROM/RCPT TO ne sont pas reconnus ou pas mis en œuvre

4.2.4 Code de réponse 502

Des questions ont été soulevées sur quand le code de réponse 502 (Commande non mise en œuvre) DEVRAIT être retourné de préférence aux autres codes. 502 DEVRAIT être utilisé quand la commande est en faute reconnue par le serveur SMTP, mais non mise en œuvre. Si la commande n'est pas reconnue, le code 500 DEVRAIT être retourné. Les systèmes SMTP étendus NE DOIVENT PAS faire la liste des capacités en reponse au EHLO pour lequel ils vont retourner des réponses 502 (ou 500).

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

Quand un serveur SMTP retourne un état d'achèvement positif (code 2yz) après l'achèvement de la commande DATA avec <CRLF>.<CRLF>, il accepte la responsabilité de :

- o délivrer le message (si la boîte aux lettres receveuse existe) ou
- o si les tentatives de livraison du message échouent à cause de conditions transistoires, reessayer la livraison un nombre raisonnable de fois aux intervalles spécifié au paragraphe 4.5.4,
- o si les tentatives de livraison du message échouent à cause de conditions permanentes, ou si des tentaives répétées de livraison du message échouent à cause de conditions transitoires, retourner la notification appropriee à l'envoyeur du message original (en utilisant l'adresse dans la commande MAIL SMTP).

Quand un serveur SMTP retourne un code d'état d'erreur temporaire (4yz) après l'achèvement de la commande DATA avec <CRLF>.<CRLF>, il NE DOIT PAS faire d'autre tentative de délivrer ce message. Le client SMTP garde la responsabilité de la livraison de ce message et peut soit le retourner à l'usager soit le remetrre en file d'attente pour une tentative suivante (voir au paragraphe 4.5.4.1).

L'utilisateur qui a généré le message DEVRAIT être capable d'interpréter le retour d'un état d'échec transitoire (par un message ou autrement) comme une indication de non livraison, tout comme le serait un échec permanent. Si le client SMTP réussit à traiter ces conditions, l'utilisateur ne va pas recevoir une telle réponse.

Quand un serveur SMTP retourne un code d'état d'erreur permanent (5yz) après l'achèvement de la commande DATA avec <CRLF>.<CRLF>, il NE DOIT PAS faire d'autre tentative de livraison du message. Comme avec les codes d'état d'erreur temporaire, le client SMTP conserve la responsabilité du message, mais DEVRAIT ne pas tenter à nouveau la livraison sur le même serveur sans une revue du message et de la réponse et une intervention appropriée de l'utilisateur.

4.3 Séquence des commandes et réponses

4.3.1 Vue d'ensemble du séquençage

La communication entre l'envoyeur et le receveur est un dialogue alternatif, contrôlé par l'envoyeur. À ce tittre, l'envoyeur produit une commande et le receveur répond par une réponse. Sauf si d'autres arrangements sont négociés par des extensions de service, l'envoyeur DOIT attendre cette réponse avant d'envoyer d'autres commandes. Une réponse importante est l'accueil de connexion. Normalement, un receveur va envoyer une réponse 220 "Service prêt" quand la connexion est réalisée. L'envoyeur DEVRAIT attendre ce message d'accueil avant l'envoi d'une commande.

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 ne va pas avoir de nom significatif. Voir au paragraphe 4.1.3 une discussion des solutions de remplacement dans ces situations.

Par exemple,

220 ISIF.USC.EDU Service prêt

ou

220 mail.exemple.com SuperSMTP v 6.1.2 Service prêt

ou

220 [10.0.0.1] Hôte sans indication service prêt

Le tableau ci-dessous fait la liste des réponses de succès et d'échec pour chaque commande. Elles DEVRAIENT être strictement suivies. Un receveur PEUT changer le texte des réponses, mais la signification et les actions impliquées par les numéros de code et par la séquence spécifique de réponse à la commande DOIVENT être préservées.

4.3.2 Séquences de commande/réponse

Chaque commande est indiquée avec ses réponses usuelles possibles. Les préfixes utilisés avant 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 de futures extensions, les clients SMTP DEVRAIENT, quand c'est possible, n'interpréter que le premier chiffre de la réponse et DOIVENT être prêts à traiter des codes de réponse non reconnus en interprétant seulement le premier chiffre. Sauf extensions en utilisant les mécanismes décrits au paragraphe 2.2, les serveurs SMTP NE DOIVENT PAS transmettre des codes de réponse à un client SMTP qui soient autres que de trois chiffres ou qui ne commencent pas par un chiffre entre 2 et 5 inclus.

Ces règles de séquençage et, en principe, les codes eux-mêmes, peuvent être étendus ou modifiés par des extensions SMTP offertes par le serveur et acceptées (demandées) par le client. Cependant, si la cible a une granularité plus précise dans les codes, plutôt que des codes pour des objets complètement nouveaux, le système décrit dans la [RFC3463] DEVRAIT être utilisé de préférence à l'invention de nouveaux codes.

En plus des codes mentionnés ci-dessous, toute commande SMTP peut retourner un des codes suivants si les circonstances inhabituelles correspondantes se rencontrnent :

500 : Pour le cas "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 exigé de ces commandes est une violation de la présente spécification. De même, produire un message "commande trop longue" pour une ligne de commande de moins de 512 caractères violerait les dispositions du paragraphe 4.5.3.1.4.

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

421 : Service en cours de clôture et fermeture du canal de transmission

Les séquences spécifiques sont :

ÉTABLISSEMENT DE CONNEXION
S: 220
E: 554

EHLO ou HELO
S: 250
E: 504 (une mise en œuvre conforme pourrait retourner ce code dans les seuls cas très obscurs) 550, 502 (permis seulement avec un serveur d'ancien style qui ne prend pas en charge EHLO)

MAIL
S: 250
E: 552, 451, 452, 550, 553, 503, 455, 555

RCPT
S: 250, 251 (mais voir au paragraphe 3.4 la discussion de 251 et 551)
E: 550, 551, 552, 553, 450, 451, 452, 503, 455, 555

DATA
I: 354 -> données -> S: 250
E: 552, 554, 451, 452
E: 450, 550 (rejet pour raisons de politique)
E: 503, 554

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

Quand un serveur SMTP reçoit un message à livrer ou à traiter, il DOIT insérer des informations de trace ("Horodatage" ou "Received") au début du contenu du message, comme expliqué au paragraphe 4.1.1.4.

Cette ligne DOIT être structurée comme suit :

- La clause FROM, qui DOIT être fournie dans un environnement SMTP, DEVRAIT contenir à la fois (1) le nom de l'hôte de source comme présenté dans la commande EHLO et (2) une adresse littérale contenant l'adresse IP de la source, déterminée à partir de la connexion TCP.

- La clause ID PEUT contenir un "@" comme suggéré dans la RFC 822, mais ce n'est pas exigé.

- Si la clause FOR apparaît, elle DOIT contenir exactement une entrée <path>, même quand plusieurs commandes RCPT ont été données. Plusieurs <path> soulèvent des questions de sécurité et a été déconseillé, voir au paragraphe 7.2.

Un programme de messagerie Internet NE DOIT PAS changer ou supprimer une ligne Received: qui a été précédemment ajoutée à la section d'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 en aucun autre endroit.

Avec la croissance de l'Internet, la possibilité de comparer les champs d'en-tête Received est importante pour détecter les problèmes, en particulier les relais lents. Les serveurs SMTP qui créent des champs d'en-tête Received DEVRAIENT utiliser des décalages explicites dans les dates (par exemple, -0800) plutôt que des noms de fuseau horaire de tous types. L'heure locale (avec un décalage) DEVRAIT être utilisée plutôt que le temps universel (UT) quand c'est faisable. Cette formulation permet de spécifier un petit peu plus d'informations sur les circonstances locales. Si l'UT est nécessaire, le receveur a simplement besoin de faire une arithmétique simple pour convertir les valeurs. L'utilisation de l'UT perd les informations sur la localisation du fuseau horaire du serveur. Si on désire fournir le nom d'un fuseau horaire, cela DEVRAIT être inclus dans un commentaire.

Quand 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 return-path préserve les informations dans le <chemin inverse> de la commande MAIL. Ici, livraison finale signifie que le message a quitté l'environnement SMTP. Normalement, cela devrait signifier qu'il a été livré à l'utilisateur de destination ou à un point de dépôt de messagerie associé, mais dans certains cas, il peut être encore traité et transmis par un autre système de messagerie.

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

Le texte ci-dessus implique que les données de messagerie finales vont commencer par la ligne de chemin de retour, suivie pas une ou plusieurs lignes d'horodatage. Ces lignes vont être suivies par le reste des données de messagerie : d'abord la balance de la section d'en-tête de messagerie et ensuite le corps ([RFC5322]).

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 que le message est accepté à la livraison. Par conséquent, tout système ultérieur (de

transmission, de passerelle, ou de relais) PEUT retirer le chemin de retour et reconstruire la commande MAIL comme nécessaire pour assurer que exactement une telle ligne apparaît dans un message livré.

Un système SMTP générateur de message NE DEVRAIT PAS envoyer de message qui contienne déjà un champ d'en-tête Return-path. Les serveurs SMTP qui effectuent une fonction de relais NE DOIVENT PAS inspecter les données du message, et en particulier pas dans la mesure nécessaire pour déterminer si les champs d'en-tête Return-path sont présents. Les serveurs SMTP qui font la livraison finale PEUVENT supprimer les champs d'en-tête Return-path avant d'ajouter le leur.

Le principal objet de Return-path est de désigner l'adresse à laquelle les messages qui indiquent la non livraison ou autres défaillances du système de messagerie sont à envoyer. Pour que ceci soit sans ambiguïté, exactement une chemin de retour DEVRAIT être présent quand le message est délivré. Les systèmes qui utilisent la syntaxe de la RFC 822 avec des transports non SMTP DEVRAIENT désigner une adresse non ambiguë, associée à l'enveloppe de transport, à laquelle les rapports d'erreur (par exemple, messages de non livraison) devraient être envoyés.

Note historique : Le texte de la RFC 822 qui paraît contredire l'utilisation du champ d'en-tête Return-path (ou l'adresse d'enveloppe de chemin inverse provenant de la commande MAIL) comme destination pour les messages d'erreur n'est pas applicable sur l'Internet. L'adresse de chemin inverse (telle que copiée dans le chemin de retour) DOIT être utilisée comme cible de tout message contenant un message d'erreur de livraison.

En particulier :
- o une passerelle entre SMTP -> ailleurs DEVRAIT insérer un champ d'en-tête return-path, sauf si il est connu que le transport "ailleurs" utilise aussi des adresses de domaine Internet et tient par ailleurs l'enveloppe d'adresse d'envoyeur.
- o une passerelle entre ailleurs -> SMTP DEVRAIT supprimer tout champ d'en-tête return-path présent dans le message, et soit copier cette information dans l'enveloppe SMTP, soit la combiner avec les informations présentes dans l'enveloppe de l'autre système de transport pour construire l'argument de chemin inverse dans la commande MAIL dans l'enveloppe SMTP.

Le serveur doit effectuer un traitement particulier pour les cas où le traitement suivant l'indication de fin des données de messagerie est seulement partiellement réussi. Cela pourrait 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 tous. Dans ce cas, la réponse à la commande DATA DOIT être une réponse d'accord. Cependant, le serveur SMTP DOIT composer et envoyer un message de notification "message indélivrable" à l'origine du message.

Une seule notification faisant la liste de tous les receveurs défaillants, ou des messages de notification séparés, DOIT être envoyée pour chaque receveur défaillant. Pour l'économie du traitement par l'envoyeur, la première solution DEVRAIT être utilisée quand c'est possible. Noter que la différence clé entre traiter des alias (paragraphe 3.9.1) et transmettre (ce paragraphe) est le changement pour une adresse pointant vers l'arrière dans ce cas. Tous les messages de notification sur des messages non livrables DOIVENT être envoyés en utilisant la commande MAIL (même si cela résulte du traitement des commandes obsolètes SEND, SOML, ou SAML) et DOIVENT utiliser un chemin de retour nul comme expliqué au paragraphe 3.6.

La ligne Horodatage et la ligne Chemin de retour sont formellement définies comme suit (les définitions de "FWS" et "CFWS" sont dans la [RFC5322]) :

Return-path-line = "Return-Path:" FWS Reverse-path <CRLF>

Time-stamp-line = "Received:" FWS Stamp <CRLF>

Stamp = From-domain By-domain Opt-info [CFWS] ";" FWS date-time
; où "date-time" est défini dans la [RFC5322] mais les formes "obs-", en particulier les années à deux chiffres, sont interdites dans SMTP et NE DOIVENT PAS être utilisées.

From-domain = "FROM" FWS Extended-Domain

By-domain = CFWS "BY" FWS Extended-Domain

Extended-Domain = Domain / (Domain FWS "(" TCP-info ")") / (address-literal FWS "(" TCP-info ")")

TCP-info = address-literal / (Domain FWS address-literal)
; Information déduites par le serveur de la connexion TCP, pas du EHLO du client.

Opt-info = [Via] [With] [ID] [For] [Additional-Registered-Clauses]

Via = CFWS "VIA" FWS Link

With = CFWS "WITH" FWS Protocol

ID = CFWS "ID" FWS (Atom / msg-id) ; msg-id est défini dans la [RFC5322]

For = CFWS "FOR" FWS (Chemin / boîte aux lettres)

Additional-Registered-Clauses = 1*(CFWS Atom FWS String)
; Des clauses standard supplémentaires peuvent être ajoutées à cet endroit par de futures normes et enregistrées par l'IANA. Les serveurs SMTP NE DEVRAIENT PAS utiliser des noms non enregistrés. Voir la Section 8.

Link = "TCP" / Addtl-Link

Addtl-Link = Atom
; Les noms standard supplémentaires pour les liaisons sont enregistrés par l'IANA. "Via" est principalement utile avec les transports non Internet. Les serveurs SMTP NE DEVRAIENT PAS utiliser des noms non enregistrés.

Protocol = "ESMTP" / "SMTP" / Attdl-Protocol

Attdl-Protocol = Atom
; Les noms standard supplémentaires pour les protocoles sont enregistrés par l'IANA dans le registre "mail parameters" [RFC3848]. Les serveurs SMTP NE DEVRAIENT PAS utiliser des noms non enregistrés.

4.5 Questions de mise en œuvre supplémentaires

4.5.1 Mise en œuvre minimum

Pour que SMTP fonctionne, la mise en œuvre minimum suivante DOIT être fournie par tous les receveurs. Les commandes suivantes DOIVENT être prises en charge pour se conformer à la présente spécification :
EHLO
HELO
MAIL
RCPT
DATA
RSET
NOOP
QUIT
VRFY

Tout système qui inclut un serveur SMTP qui prend en charge le relais ou la livraison de messagerie DOIT prendre en charge la boîte aux lettres réservée "maître de poste" comme 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'accepter la messagerie pour le maître de poste implique que les commandes RCPT qui spécifient une boîte aux lettres pour le maître de poste à tout domaine pour lequel le serveur SMTP fournit du service de messagerie, ainsi que le cas particulier de "RCPT TO:<Postmaster>" (sans spécification de domaine) DOIVENT être prises en charge.

Les systèmes SMTP sont supposés faire tous les efforts raisonnables pout accepter les messages dirigés sur le maître de poste provenant de tous les autres systèmes de l'Internet. Dans des cas extrêmes – comme ceux qui contiennent une attaque de déni de service ou autre atteinte à la sécurité -- un serveur SMTP peut bloquer les messages dirigés sur le maître de poste. Cependant, de tels arrangements DEVRAIENT être très étudiés de façon à éviter de bloquer des messages qui ne font pas partie de telles attaques.

4.5.2 Transparence

Sans dispositions pour la transparence des données, la séquence de caractères "<CRLF>.<CRLF>" termine le texte de messagerie et ne peut pas être envoyée par l'utilisateur. En général, les utilisateurs ne connaissent pas ces séquences "interdites". Pour permettre à tout le texte composé par l'utilisateur d'être transmis de façon transparente, on utilise les procédures suivantes :

- Avant d'envoyer une ligne de texte de 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.

o Quand le serveur SMTP reçoit une ligne de texte de message, il vérifie la ligne. Si la ligne est composée d'un seul point, elle est traitée comme la fin d'un 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 tout caractère parmi les 128 de l'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 de 8 bits (octet) les codes ASCII de 7 bits sont transmis, justifiés à droite, dans les octets, avec les bits de poids fort réglés à zéro. Voir au paragraphe 3.6 le traitement spécial de ces conditions dans les systèmes SMTP qui exercent une fonction de relais.

Dans certains systèmes, il peut être nécessaire de transformer les données lorsqu'elles sont reçues et mémorisées. Cela peut être nécessaire pour les hôtes qui utilisent un jeu de caractères différent de l'ASCII comme jeu de caractères local, qui mémorisent les données dans des enregistrements plutôt que des chaînes, ou qui utilisent des séquences de caractère spéciales comme délimiteurs à l'intérieur des boîtes aux lettres. Si de telles transformations sont nécessaires, elles DOIVENT être réversibles, en particulier si elles sont appliquées à de la messagerie relayée.

4.5.3 Tailles et fin de temporisation

4.5.3.1 Limites et minimums de taille

Plusieurs objets ont des tailles minimum/maximum exigées. Chaque mise en œuvre DOIT être capable de recevoir des objets d'au moins cette taille. Les objets plus grands DEVRAIENT être évités autant que possible. Cependant, certaines constructions de messagerie Internet comme les adresses codées en X.400 [RFC2156] vont souvent exiger de plus grands objets. 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 la mesure maximum du possible, les techniques de mise en œuvre qui n'imposent pas de limite à la longueur de ces objets devraient être utilisées.

Les extensions à SMTP peuvent impliquer l'utilisation de caractères qui occupent chacun plus d'un seul octet. Ce paragraphe spécifie donc les longueurs en octets lorsque des longueurs absolues, plutôt que des comptes de caractères, sont prévues.

4.5.3.1.1 Partie locale

La longueur maximum d'un nom d'utilisateur ou autre partie locale est 64 octets.

4.5.3.1.2 Domaine

La longueur maximum totale d'un nom ou numéro de domaine est 255 octets.

4.5.3.1.3 Chemin

La longueur maximum totale d'un chemin inverse ou d'un chemin de transmission est 256 octets (incluant la ponctuation et les séparateurs d'éléments).

4.5.3.1.4 Ligne de commande

La longueur maximum totale d'une ligne de commande incluant le mot de commande et le <CRLF> est 512 octets. Des extensions SMTP peuvent être utilisées pour augmenter cette limite.

4.5.3.1.5 Ligne de réponse

La longueur maximum totale d'une ligne de réponse incluant le code de réponse et le <CRLF> est 512 octets. Plus d'informations peuvent être portées par des réponses multi lignes.

4.5.3.1.6 Ligne de texte

La longueur maximum totale d'une ligne de texte incluant le <CRLF> est 1000 octets (sans compter le point en tête dupliqué pour la transparence). Ce nombre peut être augmenté en utilisant des extensions de service SMTP.

4.5.3.1.7 Contenu de message

La longueur maximum totale d'un contenu de message (incluant toute section d'en-tête de message ainsi que le corps de message) DOIT être d'au moins 64 k octets. Avec l'introduction d'une norme Internet pour la messagerie multimédia [RFC2045], les longueurs de message Internet ont connu une croissance considérable, et les restrictions de taille de

message devraient être évitées si possible. Les systèmes de serveur SMTP qui doivent imposer des restrictions DEVRAIENT mettre en œuvre l'extension de service "SIZE" de la [RFC1870], et les systèmes client SMTP qui vont envoyer de grands messages DEVRAIENT l'utiliser quand c'est possible.

4.5.3.1.8 Mémoire tampon de réception

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

4.5.3.1.9 Traitement quand les limites sont dépassées

Les erreurs dues au dépassement de ces limites peuvent être rapportées en utilisant les codes de réponse. Des 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 messagerie.

4.5.3.1.10 Code Trop de receveurs

La [RFC0821] fait une liste incorrecte des erreurs où un serveur SMTP dépasse sa limite de mise en œuvre sur le nombre de commandes RCPT ("Trop de receveurs") a le code de réponse 552. Le code de réponse correct pour cette condition est 452. Les clients DEVRAIENT traiter un code 552 dans ce cas comme une défaillance temporaire, plutôt que permanente, de sorte que la logique ci-dessous fonctionne.

Quand un serveur SMTP conforme rencontre cette condition, il a au moins 100 commandes RCPT réussies dans sa mémoire tampon de receveurs. Si le serveur est capable d'accepter le message, alors au moins ces 100 adresses vont être retirées de la file d'attente du client SMTP. Quand le client tente la retransmission de ces adresses qui ont reçu des réponses 452, au moins 100 d'entre elles vont être capables de tenir dans la mémoire tampon de receveurs du serveur SMTP. Chaque tentative de retransmission qui est capable de livrer quelque chose va être capable de disposer d'au moins 100 de ces receveurs.

Si un serveur SMTP a une limite de mise en œuvre sur le nombre de commandes RCPT et si cette limite est atteinte, il DOIT utiliser un code de réponse de 452 (mais le client DEVRAIT aussi être prêt pour une 552, comme noté ci-dessus). Si le serveur a une limitation de politique configurée par le site sur le nombre de commandes RCPT, il PEUT à la place utiliser un code de réponse 5yz. En particulier, si l'intention est d'interdire les messages qui ont un nombre de receveurs supérieur à ce qui est spécifié pour un site, plutôt que simpement limiter le nombre de receveurs dans une certaine transaction de messagerie, il serait raisonnable de retourner une réponse 503 à toute commande DATA reçue à la suite d'un code 452 (ou 552) ou de simplement retourner le 503 après DATA sans retourner de réponse négative préalable.

4.5.3.2 Fins de temporisation

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

Sur la base d'une expérience étendue des hôtes de relais de mesagerie occupés, les valeurs minimum de temporisation par commande DEVRAIENT être les suivantes :

4.5.3.2.1 Message initial 220 : 5 minutes

Un processus de client SMTP a besoin de distinguer entre une connexion TCP en échec et un délai dans la réception du message d'accueil initial 220. De nombreux serveurs SMTP acceptent une connexion TCP mais retardent le message 220 jusqu'à ce que leur charge de système permette le traitement de plus de messages.

4.5.3.2.2 Commande MAIL : 5 minutes

4.5.3.2.3 Commande RCPT : 5 minutes

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

4.5.3.2.4 Initiation de DATA : 2 minutes

C'est en attendant la réponse "354 Début d'entrée" à une commande DATA.

4.5.3.2.5 Bloc de données : 3 minutes

C'est en attendant l'achèvement de chaque appel SEND TCP transmettant un tronçon de données.

4.5.3.2.6 Terminaison de données : 10 minutes.

C'est en attendant la réponse "250 OK". Quand le receveur obtient le point final terminant les données du message, il effectue normalement le traitement pour délivrer le message à une boîte aux lettres d'utilisateur. Un temporisateur parasite à ce point serait très perturbateur 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 des explications supplémentaires.

4.5.3.2.7 Temporisation de serveur : 5 minutes.

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

4.5.4 Stratégies de reessai

La structure commune d'une mise en œuvre d'hôte SMTP inclut une boîte aux lettres d 'utilisateur, une ou plusieurs zones pour mettre en file d'attente les messages en transit, et un ou plusieurs processus automatiques pour envoyer et recevoir les messages. La structure exacte va varier selon les besoins des utilisateurs 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 supportent de hauts niveaux de trafic.

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

4.5.4.1 Stratégie d'envoi

Le modèle général pour un client SMTP est un ou plusieurs processus qui tentent 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 messagerie sortante, tandis que les messages qui ne peuvent pas être transmis immédiatement DOIVENT être mis en file d'attente et réessayés périodiquement par l'envoyeur. Une entrée de file d'attente de messagerie va inclure non seulement le message lui-même mais aussi les informations d'enveloppe.

L'envoyeur DOIT différer de réessayer une destination particulière après l'échec d'une tentative. En général, l'intervalle entre les essais DEVRAIT être d'au moins 30 minutes ; cependant, des stratégies plus sophistiquées et variables seront bénéfiques quand 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 moment d'abandon doit généralement être d'au moins 4 à 5 jours. Il PEUT être approprié de fixer un nombre maximum plus court d'essais pour les notifications de non livraison et messages d'erreur équivalents que pour les messages standard. Les paramètres de l'algorithme d'essais DOIVENT être configurables.

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

L'expérience suggère que les défaillances sont normalement transitoires (le système cible ou sa connexion sont hors service) ce qui plaiderait pour une politique de deux tentatives de connexion dans la première heure où le message est dans la file d'attente, et ensuite de reculer à une 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 un message est reçu d'une adresse particulière, il est probable que les messages mis 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 des files d'attente maintenant" comme l'ETRN de la [RFC1985].

La stratégie peut être encore modifiée par suite d'adresses multiples par hôte (voir ci-dessous) pour optimiser le compromis entre heure de livraison et usage des ressources.

Un client SMTP peut avoir une grande file d'attente de messages pour chaque hôte de destination indisponible. Si tous ces messages devaient être réessayés à chaque cycle d'essai, cela ferait une surcharge excessive sur l'Internet et le système envoyeur serait bloqué pour longtemps. Noter qu'un client SMTP ne peut généralement déterminer l'échec d'une tentative de livraison qu'après une temporisation de plusieurs minutes, et même une temporisation de une minute par connexion va résulter en un très grand 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 DEVRAIT prendre grand soin de mettre en antémémoire les réponses négative 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 précisément, les réponses 5yz à la commande MAIL NE DOIVENT PAS être mises en antémémoire.

Quand un message de messagerie 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, alors une seule copie du message DEVRAIT 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 vraiment beaucoup d'adresses, une limite au nombre de commandes RCPT par commande MAIL PEUT être imposée. Cette caractéristique d'efficacité DEVRAIT être mise en œuvre.

De même, pour réaliser la livraison en temps utile, le client SMTP PEUT prendre en charge plusieurs transactions concurrentes de messagerie sortantes. Cependant, des limites peuvent être appropriées pour protéger l'hôte contre l'absorbtion de toutes ses ressources par la messagerie.

4.5.4.2 Stratégie de réception

Le serveur SMTP DEVRAIT tenter de rester tout le temps à l'écoute sur l'accès SMTP (spécifié comme accès 25 par l'IANA). Cela exige la prise en charge de plusieurs connexions TCP entrantes pour SMTP. Une limite PEUT être imposée, mais les serveurs qui ne peuvent pas traiter plus d'une transaction SMTP à la fois ne sont pas en conformité avec l'intention de la présente spécification.

Comme expliqué plus haut, quand le serveur SMTP reçoit des messages d'une adresse d'hôte particulière, il pourrait activer ses propres mécanismes de mise en file d'attente SMTP pour réessayer tous les messages en instance pour cette adresse d'hôte.

4.5.5 Messages avec un chemin inverse Nul

Il y a plusieurs types de messages de notification qui sont exigés par les normes existantes et proposées, pour être envoyés avec un chemin inverse nul, à savoir les notifications de non livraison, comme exposé au paragraphe 3.7, d'autres sortes de notifications d'état de livraison (DSN, *Delivery Status Notification*) [RFC3461], et les notifications de disposition de message (MDN, *Message Disposition Notification*) [RFC3798]. Toutes ces sortes de messages sont des notifications sur un précédent message, et elles sont envoyés sur le chemin inverse du précédent message. (Si la livraison d'un tel message de notification échoue, cela indique généralement un problème du système de messagerie de l'hôte auquel le message de notification est adressé. Pour cette raison, chez certains hôtes, le MTA est réglé à 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 de maître de poste.)

Tous les autres types de messages (c'est-à-dire, tout message qui n'est pas obligé par une RFC sur la voie de la normalisation d'avoir un chemin inverse nul) DEVRAIENT être envoyés avec un chemin inverse valide non nul.

Les mises en œuvre de processeurs automatiques de messagerie électronique devraient veiller à s'assurer que les diverses sortes de messages qui ont un chemin inverse nul sont traitées correctement. En particulier, ces systèmes NE DEVRAIENT PAS répondre aux messages qui ont un chemin inverse nul, et ils NE DEVRAIENT PAS ajouter un chemin inverse non nul, ou changer un chemin inverse nul en un non nul, à de tels messages quand ils les transmettent.

5. Résolution d'adresse et traitement de la messagerie

5.1 Localisation de l'hôte cible

Une fois qu'un client SMTP identifie lexicalement un domaine auquel de la messagerie doit être livrée pour traitement (comme décrit aux paragraphes 2.3.5 et 3.6) une recherche dans le DNS DOIT être effectuée pour résoudre le nom de domaine [RFC1035]. Les noms sont supposés être des noms de domaine pleinement qualifiés (FQDN) : les mécanismes pour déduire les FQDN à partir de noms partiels ou d'alias locaux sortent du domaine d'application de la présente spécification. Du fait d'un historique de problèmes, les serveurs SMTP utilisés pour la soumission initiale des messages NE DEVRAIENT PAS faire de telles déductions (les serveurs de soumission de message [RFC4409] ont un peu plus de souplesse) et les serveurs SMTP intermédiaires (relais) NE DOIVENT PAS les faire.

La recherche tente d'abord de localiser un enregistrement MX associé au nom. Si un enregistrement CNAME est trouvé, le nom résultant est traité comme si il était le nom initial. Si une erreur “domaine non existant” est retournée, cette situation DOIT être rapportée comme une erreur. Si une erreur temporaire est retournée, le message DOIT être mis en file d'attente et réessayé plus tard (voir au paragraphe 4.5.4.1). Si une liste vide de MX est retournée, l'adresse est traitée comme si elle était associée à un RR MX implicite, avec une préférence de 0, pointant sur cet hôte. Si des enregistrements MX sont présents, mais qu'aucun d'eux n'est utilisable, ou si le MX implicite est inutilisable, cette situation DOIT être rapportée comme une erreur.

Si un ou plusieurs RR MX sont trouvés pour un certain nom, les systèmes SMTP NE DOIVENT utiliser aucun RR d'adresse associé à ce nom sauf si elles sont localisées en utilisant les RR MX ; la règle du "MX implicite" ci-dessus ne s'applique que si il n'y a pas d'enregistrement MX présent. Si des enregistrements MX sont présents, mais si aucun d'eux n'est utilisable, cette situation DOIT être rapportée comme une erreur.

Quand un nom de domaine associé à un RR MX est recherché et que le champ de données associé est obtenu, le champ de données de cette réponse DOIT contenir un nom de domaine. Ce nom de domaine, quand il est interrogé, DOIT retourner au moins un enregistrement d'adresse (par exemple, un RR A ou AAAA) qui donne l'adresse IP du serveur SMTP auquel le message devrait être envoyé. Toute autre réponse, spécifiquement incluant une valeur qui va retourner un enregistrement CNAME quand elle est interrogée, sort du domaine d'application de la présente norme. L'interdiction des étiquettes dans les données qui se résolvent en CNAME est discutée plus en détail au paragraphe 10.3 de la [RFC2181].

Quand 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 multiples enregistrements MX, de multi rattachements, ou des deux. Pour assurer une transmission fiable de la messagerie, le client SMTP DOIT être capable d'essayer (et réessayer) chacune des adresses pertinentes dans cette liste, dans l'ordre, jusqu'à la réussite d'une tentative de livraison. Cependant, il PEUT aussi y avoir une limite configurable au nombre d'adresses de remplacement qui peuvent être essayées. En tous cas, le client SMTP DEVRAIT essayer au moins deux adresses.

Deux types d'informations sont utilisés pour classer les adresses d'hôte : les enregistrements MX multiples, et les hôtes multi rattachements.

Les enregistrements MX contiennent une indication de préférence qui DOIT être utilisée pour voir si plus d'un de ces enregistrements apparaît (voir ci-dessous). Les nombres les plus faibles indiquent une plus forte préférence que les plus élevés. Si il y a plusieurs destinations avec la même préférence et si il n'y a pas de raison claire pour en favoriser une (par exemple, en reconnaissant une adresse facilement accessible) alors l'envoyeur SMTP DOIT les rendre aléatoires pour étaler la charge sur de multiples échangeurs de messagerie pour une organisation spécifique.

L'hôte de destination (peut-être celui de l'enregistrement MX préféré) peut être multi rattachements, auquel cas le résolveur de noms de domaine va retourner une liste des adresses IP de remplacement. Il est de la responsabilité de l'interface de résolveur de noms de domaine d'ordonner cette liste par préférence décroissante si nécessaire, et l'envoyeur SMTP DOIT les essayer dans l'ordre présenté.

Bien que la capacité d'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 tenter ses essais en utilisant les différents adresses d'un hôte multi rattachements est controversée. Le principal argument pour utiliser les multiples adresses est que cela maximise la probabilité de livraison à temps, et bien sûr parfois la probabilité d'une livraison

tout court ; le contre argument est que il peut en résulter une utilisation inutile des ressources. Note que l'utilisation des ressources est aussi fortement déterminée 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 est un échangeur de messagerie désigné, il PEUT relayer le message (éventuellement après avoir reécrit les adresses MAIL FROM et/ou RCPT TO) faire la livraison finale du message, ou le passer en utilisant un mécanisme hors de l'environnement de transport fourni par SMTP. Bien sûr, aucun de ces derniers n'exige d'autre examen de la liste des enregistrements MX.

Si il détermine qu'il devrait relayer le message sans reécrire l'adresse, il DOIT trier les enregistrements MX pour déterminer les candidats à la livraison. Les enregistrements sont d'abors ordonnés par préférence, les enregistrements de plus faible numéro étant les préférés. L'hôte relais DOIT alors inspecter la liste pour voir si un des noms ou adresses pourrait être connu pour des transactions de messagerie. Si un enregistrement correspondant est trouvé, tous les enregistrements à ce niveau de préférence et ceux d'un numéro plus élevé DOIVENT être écartés. Si il ne reste plus d'enregistrements à ce point, c'est une condition d'erreur, et le message DOIT être retourné comme non livrable. Si il reste des enregistrements, ils DEVRAIENT être essayés, le préféré en premier, comme décrit ci-dessus.

5.2 IPv6 et enregistrements MX

Dans l'Internet contemporain, les clients et serveurs SMTP peuvent être hébergés sur des systèmes IPv4, des systèmes IPv6, ou des systèmes à double pile qui sont compatibles avec l'une et l'autre version du protocole Internet. Les domaines hôtes sur lesquels pointent les enregistrements MX peuvent par conséquent contenir des "RR A" (IPv4), des "RR AAAA" (IPv6) ou toutes leurs combinaisons. Bien que la [RFC3974] discute de l'expérience du fonctionnement en environnement mixte, elle n'est pas assez complète pour justifier la normalisation, et certaines de ses recommandations paraissent incompatibles avec la présente spécification. Les actions appropriées dépendent des circonstances locales, comme les performances des réseaux pertinents et toutes les conversions qui pourraient être nécessaires, ou vont être évidentes (par exemple, un client IPv6 seul n'a pas besoin de tenter une recherche de RR A ou de tenter de joindre des serveurs IPv4 seul). Les concepteurs de mises en œuvre SMTP qui pourraient fonctionner dans des environnements IPv6 ou de double pile devraient étudier les procédures ci-dessus, en particulier les commentaires sur les hôtes multi rattachements, et de préférence, fournir des mécanismes pour faciliter le réglage du fonctionnement et l'interopérabilité de la messagerie entre systèmes IPv4 et IPv6 tout en considérant les circonstances locales.

6. Détection et traitement des problèmes

6.1 Livraison fiable et réponses par messagerie électronique

Quand le receveur SMTP accepte un élément de messagerie (en envoyant un message "250 OK" en réponse à DATA) il accepte la responsabilité de la livraison ou du relais du message. Il doit prendre cette responsabilité au sérieux. Il NE DOIT PAS perdre le message pour des raisons frivoles, comme parce que l'hôte suivant est en panne ou à cause d'un manque de ressources prévisible. Certaines des raisons qui ne sont pas considérées comme frivoles sont discutées au paragraphe suivant et au paragraphe 7.8.

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

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

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

Le message de notification DOIT être envoyé en utilisant :

RCPT TO:<user@d>

Des échecs de livraison après l'acceptation du message par SMTP sont inévitables. Par exemple, il peut être impossible au serveur SMTP receveur de valider toutes les adresses de livraison dans les commandes RCPT à cause d'une erreur "logicielle" du système de domaines, parcc 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 fins de temporisations, un SMTP receveur DOIT chercher à minimiser le temps nécessaire pour répondre au <CRLF>.<CRLF> final d'indicateur de fin de données. Voir dans la [RFC1047] la discussion de ce problème.

6.2. Messages non voulus, non sollicités, et "d'attaque"

L'utilité et la prévisibilité du système de messagerie de l'Internet exigent que les messages qui peuvent être livrés devraient être livrés, sans considération de toutes fautes de syntaxe ou autres associées à ces messages ni de leur contenu. Si ils ne peuvent pas être livrés, et ne peuvent pas être rejetés par le serveur SMTP durant la transaction SMTP, ils devraient être "renvoyés" (retournés avec un message de non livraison) comme décrit ci-dessus. Dans le monde actuel, dans lequel de nombreux opérateurs de serveur SMTP ont découvert que la quantité de messages en vrac indésirables excède largement celle des messages désirés et qu'accepter un message peut déclencher du trafic indésirable supplémentaire en fournissant une vérification de l'adresse, ces principes peuvent n'être pas pratiques.

Comme expliqué aux paragraphes 7.8 et 7.9, éliminer des messages sans notification à l'envoyeur est permis en pratique. Cependant, c'est extrêmement dangereux et viole une longue tradition et les attentes de la communauté que la messagerie est soit livrée, soit retournée. Si l'élimination en silence de messages fait l'objet d'abus, cela pourrait facilement saper la confiance en la fiabilité des systèmes de messagerie de l'Internet. Donc, l'élimination en silence de messages devrait être considérée dans les seuls cas où on est vraiment sûr que les messages sont sérieusement frauduleux ou par ailleurs inappropriés.

Pour coller encore plus si possible au principe de livraison, ce peut être une politique rationnelle de ne pas livrer les messages qui ont une adresse de retour invalide, bien que l'histoire du réseau est que les utilisateurs sont normalement mieux servis en livrant tout message qui peut être livré. Déterminer de façon fiable qu'une adresse de retour est invalide peut être un processus difficile et long, en particuloier si le système envoyeur putatif n'est pas directement accessible ou ne prend pas pleinement et précisément en charge VRFY et, même si une politique de "éliminer les messages avec une adresse de retour invalide" est adoptée, elle DEVRAIT n'être appliquée que quand il y a une presque certitude que les adresses de retour sont, en fait, invalides.

À l'inverse, si un message est rejeté parce qu'on a trouvé qu'il contient un contenu hostile (décision qui est hors du domaine d'un serveur SMTP comme défini dans le présent document) des mesages de rejet ("renvoi") NE DEVRAIENT PAS être envoyés sauf si le site receveur est sûr que ces messages seront utilement livrés. La préférence et le comportement par défaut dans ces cas est d'éviter d'envoyer des messages de non livraison quand le message entrant est déterminé comme comportant un contenu hostile.

6.3 Détection de boucle

Le simple comptage du nombre de champs d'en-tête "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 utiliser un seuil de rejet élevé, normalement au moins 100 entrées de Received. Quel que soit les mécanismes utilisés, les serveurs DOIVENT contenir des dispositions pour détecter et arrêter les boucles triviales.

6.4 Compensation des irrégularités

Malheureusement, des variations, des interprétations créatives, et des violations flagrantes des protocoles de messagerie Internet se produisent bien ; certains suggèrent même qu'elles se produisent assez fréquemment. Le débat sur la question de savoir si un receveur ou relais SMTP au bon comportement devrait rejeter un message mal formé, tenter de le passer inchangé, ou tenter de le réparer pour augmenter ses chances de livraison réussie (ou de la réponse suivante) a commencé presque à l'aube de la messagerie de réseau structuré et ne montre aucun signe d'affaiblissement. Les avocats du rejet disent que les tentatives de réparation sont rarement complètement adéquates et que le rejet des mauvais messages est la seule façon d'obtenir la réparation du logiciel concerné. Les avocats de la "réparation" ou "livraison quoi qu'il en coûte" disent que les utilisateurs préfèrent que les messages passent si c'est possible et qu'il y a des pressions significatives du marché dans cette direction. En pratique, ces pressions du marché sont peut être plus importantes pour les fabricants particuliers que la stricte conformité aux normes, sans considération de la préférence des développeurs réels.

Les problèmes associés aux messages mal formés ont été exacerbés par l'introduction des protocoles de lecture de messagerie (Protocole Post Office (POP) version 2 [RFC0937], Protocole Post Office version 3 [RFC1939], IMAP version 2 [RFC1176], et PCMAIL [RFC1056]). Ces protocoles encourageaient l'usage de SMTP comme protocole d'envoi (soumission de message) et des serveurs SMTP comme systèmes de relais pour ces hôtes clients (qui sont souvent seulement connectés de façon intermittente à l'Internet). Historiquement, beaucoup de ces machines clientes manquaient des mécanismes et des informations supposées pour SMTP (et bien sûr, pour le protocole de format de messagerie [RFC0822]). Certaines ne pouvaient pas garder une trace adéquate de l'heure ; d'autres n'avaient pas de concept de zones

horaires ; d'autres encore ne pouvaient pas identifier leur propre nom ou adresse ; et bien sûr, aucune ne pouvait satisfaire les hypothèses qui sous tendent la conception d'adresses authentifiées de la RFC 822.

En réponse à ces clients SMTP faibles, de nombreux systèmes SMTP complètent maintenant les messages qui leur sont livrés en forme incomplète ou incorrecte. Cette stratégie est généralement considérée appropriée quand le serveur peut identifier ou authentifier le client, et qu'il y a des accords préalables entre eux. À l'opposé, il y a, au mieux, de grandes interrogations sur les réparations appliquées par un serveur SMTP de relais ou de livraison qui a peu ou pas du tout de connaissances sur l'utilisateur ou la machine cliente. Beaucoup de ces problèmes sont traités en utilisant un protocole séparé, comme ceux définis dans la [RFC4409], pour la soumission de message, plutôt que d'utiliser les serveurs SMTP générateurs à cette fin.

Les changements suivants à un message en cours de traitement PEUVENT être appliqués quand nécessaire par un serveur SMTP générateur , ou un utilisé comme la cible de SMTP comme protocole d'envoi initial (soumission de message) :

- ajout d'un champ message-id quand aucun n'apparaît
- ajout d'une date, heure, ou zone horaire quand aucune n'apparaît
- correction des adresses au format FQDN approprié.

Moins le serveur a d'informations sur le client, moins il est probable que ces changements soient corrects et la plus grande prudence devrait être appliquée quand on considère d'effectuer ou non les réparations et comment le faire. Ces changements NE DOIVENT PAS être appliqués par un serveur SMTP qui assure des fonctions de relais intermédiaire.

Dans tous les cas, les client qui fonctionnent proprement et fournissent des informations correctes sont préférés aux corrections par le serveur SMTP. Dans tous les cas, une documentation DEVRAIT être fournie dans les champs d'en-tête de trace et/ou le champ d'en-tête de commentaires sur les actions effectuées par les serveurs.

7. Considérations sur la sécurité

7.1 Sécurité de la messagerie à l'égard de l'usurpation d'identité

La messagerie SMTP est non sûre par nature en ce qu'il est faisable même pour des utilisateurs très occasionnels de négocier directement avec les serveurs SMTP de réception et de relais et de créer des messages qui vont tromper un receveur inexpérimenté en lui faisant croire qu'ils viennent d'ailleurs. Construire un tel message afin que le comportement "trompeur" ne puisse pas être détecté par un expert est un peu plus difficile, mais pas suffisamment pour dissuader quelqu'un qui est déterminé et capable d'apprendre. Par conséquent, comme la connaissance de la messagerie de l'Internet augmente, il est de plus en plus connu que la messagerie SMTP ne peut pas par nature être authentifiée, ou que des vérifications d'intégrité ne peuvent pas être fournies, au niveau du transport. La sécurité réelle de la messagerie repose seulement sur les méthodes de bout en bout qui impliquent les corps de message, comme celle qui utilisent les signatures numériques (voir la [RFC1847] et, par exemple, PGP (*Pretty Good Privacy*) dans la [RFC4880] ou les extensions de messagerie Internet multi-objets/sécurisé (S/MIME, *Secure/Multipurpose Internet Mail Extensions*) dans la [RFC3851]).

Diverses extensions de protocole et options de configuration qui fournissent l'authentification au niveau transport (par exemple, entre un client SMTP et un serveur SMTP) améliorent un peu la situation traditionnelle décrite ci-dessus. Cependant, en général, elles authentifient seulement un serveur auprès d'un autre plutôt qu'une chaîne de relais et serveurs, authentifiant beucoup moins les utilisateurs ou leurs machines. Par conséquent, sauf si elles sont accompagnées par de soigneuses sauvegardes de responsabilité dans un environnement de confiance soigneusement conçu, elles restent par nature plus faibles que les mécanismes de bout en bout qui utilisent des messages signés numériquement plutôt que de dépendre de l'intégrité du système de transport.

Les efforts pour rendre plus difficile aux utilisateurs de régler les champs d'enveloppe de chemin de retour et d'en-tête "From" à pointer sur des adresses valides autres que les leurs propres vont largement à contre sens : elles frustrent des applications légitimes dans lesquelles la messagerie est envoyée par un utilisateur au nom d'un autre, dans lesquelles des réponses d'erreur (ou normales) devraient être dirigées sur une adresse spéciale, ou dans lesquelles un seul message est envoyé à plusieurs receveurs sur des hôtes différents. (Les systèmes qui fournissent aux utilisateurs des moyens commodes pour altérer ces champs d'en-tête message par message devraient tenter d'établir une adresse de boîte aux lettres principale et permanente pour l'utilisateur afin que les champs d'en-tête d'envoyeur au sein des données de message puissent être générés de façon sensée.)

La présente spécification ne traite pas plus des questions d'authentification associées à SMTP autrement que pour plaider qu'une founctionnlité utile ne doit pas être désactivée dans l'espoir de fournir une petite marge de protection contre un utilisateur qui essaye de falsifier des messages.

7.2. Copies "aveugles"

Les adresses qui n'apparaissent pas dans la section d'en-tête du message peuvent apparaître dans la commande RCPT à un serveur SMTP pour un certain nombre de raisons. Les deux plus courantes impliquent l'utilisation d'une adresse de messagerie comme "exploseur de liste" (une seule adresse qui se résout en plusieurs adresses) et l'apparition de "copies aveugles". En particulier quand plus d'une commande RCPT est présente, et afin d'éviter d'aller contre l'objet de ces mécanismes, les clients et serveurs SMTP NE DEVRAIENT PAS copier tout l'ensemble des arguments de commande RCPT dans la section d'en-tête, soit au titre des champs d'en-tête de trace, soit comme champs d'en-tête d'information ou d'extension privée. Comme cette règle est souvent violée en pratique, et qu'elle ne peut pas être appliquée, les systèmes SMTP envoyeurs qui ont la capacité d'utiliser "bcc" PEUVENT trouver utile d'envoyer chaque copie aveugle comme transaction de message séparé contenant une seule commande RCPT.

Il n'y a pas de relation inhérente entre les adresses "reverse" (des commandes MAIL, SAML, etc.,) ou "forward" (RCPT) dans la transaction SMTP ("envelope") et les adresses dans la section d'en-tête. Les systèmes receveurs NE DEVRAIENT PAS tenter de déduire de telles relations et les utiliser pour altérer la section d'en-tête du message pour le livrer. Le champ d'en-tête populaire "Apparently-to" est une violation de ce principe ainsi qu'une source courante de divulgation involontaire d'informations et NE DEVRAIT PAS être utilisé.

7.3 VRFY, EXPN, et sécurité

Comme expliqué au paragraphe 3.5, des sites individuels peuvent vouloir désactiver VRFY ou EXPN, les deux pour des raisons de sécurité (voir ci-dessous). Comme corollaire de ceci, les mises en œuvre qui permettent cela NE DOIVENT PAS apparaître comme ayant vérifié des adresses qui ne sont en fait pas 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.

Retourner un code de réponse 250 avec l'adresse mentionnée dans la commande VRFY après l'avoir vérifiée sur la seule syntaxe viole cette règle. Bien sûr, une mise en œuvre qui "prend en charge" VRFY en retournant toutjours 550 que l'adresse soit ou non valide est également non conforme.

Dans l'Internet public, le contenu des listes de diffusion est devenu une source d'information d'adresses pour les envoyeurs de "pourriels."

L'utilisation de EXPN pour "récolter" des adresses a augmenté quand les administrateurs de listes ont installé des protections contre l'utilisation inappropriée des listes elles-mêmes. Cependant, VRFY et EXPN sont toujours utiles pour les utilisateurs authentifiés et au sein d'un domaine administratif. Par exemple, VRFY et EXPN sont utiles pour effectuer des audits internes sur la façon dont est acheminée la messagerie électronique pour vérifier et s'assurer que personne ne transmet automatiquement des messages sensibles en dehors de l'organisation. Les sites qui mettent en œuvre l'authentification SMTP peuvent choisir de ne rendre VRFY et EXPN disponibles qu'aux demandeurs authentifiés. Les mises en œuvre DEVRAIENT quand même prendre en charge EXPN, mais les sites DEVRAIENT évaluer avec soin le pour et le contre.

Savoir si la désactivation de VRFY assure un réel gain marginal de sécurité dépend d'une série d'autres conditions. Souvent, les commandes RCPT peuvent être utilisées pour obtenir les mêmes information sur la validité d'une adresse. Par ailleurs, en particulier dans des situations où la détermination de la validité des adresses pour les commandes RCPT est diférée jusqu'à la réception de la commande DATA, RCPT peut ne retourner aucune information, tandis que VRFY est supposé faire une tentative sérieuse pour déterminer la validité avant de générer un code de réponse (voir la discussion ci-dessus).

7.4 Réacheminement de messagerie fondée sur les codes de réponse 251 et 551

Avant qu'un client utilise les codes de réponse 251 ou 551 provenant d'une commande RCPT pour mettre automatiquement à jour son comportement futur (par exemple, mettre à jour le carnet d'adresses de l'utilisateur) il devrait être certain de l'authenticité du serveur. Si il ne le fait pas, il peut être soumis à une attaque par interposition.

7.5 Divulgation d'informations dans les annonces

Un débat a lieu sur le pour et le contre des avantages du déboguage de l'annonce du type et la version du serveur (et, parfois même du nom de domaine du serveur) dans la réponse à l'accueil ou dans la réponse à la commande HELP et les inconvénients d'exposer des informations qui pourraient être utiles dans une potentielle attaque hostile. L'utilité des informations de déboguage ne fait pas de doute. Ceux qui plaident en faveur de sa disponibilité soulignent qu'il est bien préférable de sécuriser réellement un serveur SMTP plutôt que d'espérer qu'essayer de cacher des vulnérabilités connues en cachant l'identité précise du serveur va fournir plus de protection. Les sites sont encouragés à évaluer le pour et le contre en

pensant à ce problème ; les mises en œuvre DEVRAIENT au minimum rendre disponibles les informations de type et de version d'une façon ou d'une autre aux autres hôtes du réseau.

7.6 Divulgation d'informations dans les champs Trace

Dans certaines circonstances, comme quand les messages ont leur origine à l'intérieur d'un LAN dont les hôtes ne sont pas directement sur l'Internet public, les champs d'en-tête de trace ("Received") produits conformément à la présente spécification peuvent divulguer les noms des hôtes et des informations similaires qui ne seraient normalement pas disponibles. Cela ne pose ordinairement pas de problème, mais des sites avec un souci particulier de non divulgation des noms devraient en avoir conscience. Aussi, la clause facultative FOR devrait être fournie avec prudence, ou pas du tout, quand plusieurs receveurs sont impliqués, de risque d'une divulgation par inadvertence des identités des receveurs en "copie aveugle" aux autres receveurs.

7.7 Divulgation d'informations dans la transmission des messages

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

7.8 Résistance aux attaques

Dans les années récentes, il y a eu un accroissement des attaques contre les serveurs SMTP, soit en conjonction avec des tentatives pour découvrir des adresses pour envoyer des messages non sollicités, soit simplement pour rendre les serveurs inaccessibles aux autres (c'est-à-dire, comme une attaque de déni de service de niveau application). Bien que les moyens de le faire sortent du domaine d'application de la présente norme, un comportement de fonctionnement rationnel exige qu'il soit permis aux serveurs de détecter de telles attaques et de prendre des actions pour se défendre. Par exemple, si un serveur détermine qu'un grand nombre de commandes RCPT TO sont envoyées, dont la plupart ou toutes ont des adresses invalides, il serait raisonnable, au titre d'une telle attaque, que le serveur close la connexion après avoir généré un certain nombre approprié de réponses 5yz (normalement 550).

7.9 Portée du fonctionnement des serveurs SMTP

Il est un principe bien établi qu'un serveur SMTP peut refuser d'accepter de la messagerie pour toute raison de fonctionnement ou technique qui a un sens pour le site qui fournit le serveur. Cependant, la coopération entre les sites et les installations rend l'Internet possible. Si les sites tirent un parti excessif du droit de rejeter du trafic, cala menace l'ubiquité de la disponibilité de la messagerie électroniquey (une des forces de l'Internet) ; un soin considérable devrait être pris et un équilibre conservé si 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 arbitraires a été utilisée au titre d'effots hostiles pour cacher les origines réelles des messages. Certains sites ont décidé de limiter l'utilisation de la fonction de relais aux sources connues ou identifiables, et les mises en œuvre DEVRAIENT fournir la capacité d'effectuer ce type de filtrage. Quand des messages sont rejetés pour cette raison de politique ou d'autres, un code 550 DEVRAIT être utilisé en réponse au EHLO (ou HELO), MAIL, ou RCPT comme approprié.

8. Considérations relatives à l'IANA

L'IANA tient trois registres pour la prise en charge de la présente spécification, qui ont tous été créés pour la RFC 2821 ou plus tôt. Le présent document étend le troisième comme spécifié ci-dessous. Les références de registre citées sont celle du moment de la publication ; l'IANA ne garantit pas les localisations associées aux URL. Les registres sont comme suit :

- Le premier, "Extensions de service du protocole simple de transfert de messagerie (SMTP)" [IANA-MP], comporte les extensions de service SMTP avec les mots-clés associés, et, quand nécessaire, les paramètres et verbes. Comme spécifié au paragraphe 2.2.2, aucune entrée qui commence par un "X" ne peut être faite dans ce registre. Les entrées ne peuvent être faites que pour les extensions de service (et les mots-clés, paramètres ou verbes associés) qui sont définis dans des RFC sur la voie de la normalisation ou expérimentales spécifiquement approuvées par l'IESG dans ce but.

- Le second registre, "Étiquettes d'adresses littérales" [IANA-ALT], consiste en "étiquettes" qui identifient des formes de domaines littéraux autres que ceux des adresses IPv4 (spécifiées dans la RFC 821 et dans le présent document). L'entrée initiale dans ce registre est pour les adresses IPv6 (spécifiée dans le présent document). Des types de littéraux supplémentaires exigent la normalisation avant d'être utilisés ; aucun n'est prévu pour l'instant.

- Le troisième "Types de transmission de messagerie" [IANA-MP], établi par la RFC 821 et renouvelé par la présente specification, est un registre d'identifiants de liaisons et protocoles à utiliser avec les sous clauses "via" et "with" de l'horodatage (champ d'en-tête "Received:") décrites au paragraphe 4.4. Les identifiants de liaison et de protocole en plus de ceux spécifiés dans le présent document ne peuvent être enregistrés que par normalisation ou au moyen d'une extension de protocole expérimentale documentée dans une RFC, appouvée par l'IESG. Cet espace de noms est pour l'identification et n'est pas limité en taille : l'IESG est invité à approuver sur la base d'une documentation claire et d'une méthode distincte plutôt que de préférences sur les propriétés de la méthode elle-même.

Un paragraphe additionnel a été ajouté aux paragraphes "types de liaisons VIA" et "types de protocoles WITH" de ce registre pour contenir les enregistrements des "clauses enregistrées additionnelles" comme décrit ci-dessus. Le registre va contenir les noms de clauses, une description, un sommaire de la syntaxe de la chaîne associée, et une référence. Lorsque de nouvelles clauses sont définies, elles peuvent, en principe, spécifier la création de leurs propres registres si les chaînes consistent en termes ou mots-clés réservés plutôt que des chaînes moins restreintes. Comme avec les identifiants de liaisons et protocoles, des clauses additionnelles ne peuvent être enregistrées que par normalisation ou au moyen d'une d'une extension de protocole expérimentale documentée dans une RFC, appouvée par l'IESG. L'espace de noms de clause additionnelle est pour l'identification et n'est pas limité en taille : l'IESG est invité à approuver sur la base d'une documentation claire, de l'utilisation réelle ou de signes forts que la clause va être utilisée, et une exigence distincte plutôt que des préférences sur les propriétés de la clause elle-même.

De plus, si des champs d'en-tête de trace supplémentaires (c'est-à-dire, en plus de Return-path et Received) sont créés, ces champs de trace DOIVENT être ajoutés au registre IANA établi par le BCP 90 [RFC3864] à utiliser avec la [RFC5322].

9. Remerciements

De nombreuses personnes ont contribué au développement de la RFC 2821. Ce document devrait être consulté pour ses remerciements. Pour le présent document, l'éditeur et la communauté se doivent de remercier Dawn Mann et Tony Hansen qui ont aidé au processus très pénible d'édition et de conversion du format interne du document d'un système à l'autre.

Ni le présent document ni la RFC 2821 n'auraient été possibles sans les nombreuses contributions et conseils du regreté Jon Postel. Ces contributions incluent bien sûr la spécification originale de SMTP dans la RFC 821. Une quantité considérable du texte de la RFC 821 apparaît dans le présent document ainsi que plusieurs exemples originaux de Jon qui n'ont été mis à jour que lorsque nécessaire pour refleter d'autres changements de la spécification.

De nombreuses personnes ont fait des commentaires ou suggestions sur les listes de diffusion ou dans des notes à l'auteur. Des corrections ou précisions importantes ont été suggérées par plusieurs personnes, incluant Matti Aarnio, Glenn Anderson, Derek J. Balling, Alex van den Bogaerdt, Stephane Bortzmeyer, Vint Cerf, Jutta Degener, Steve Dorner, Lisa Dusseault, Frank Ellerman, Ned Freed, Randy Gellens, Sabahattin Gucukoglu, Philip Guenther, Arnt Gulbrandsen, Eric Hall, Richard O. Hammer, Tony Hansen, Peter J. Holzer, Kari Hurtta, Bryon Roche Kain, Valdis Kletnieks, Mathias Koerber, John Leslie, Bruce Lilly, Jeff Macdonald, Mark E. Mallett, Mark Martinec, S. Moonesamy, Lyndon Nerenberg, Chris Newman, Douglas Otis, Pete Resnick, Robert A. Rosenberg, Vince Sabio, Hector Santos, David F. Skoll, Paul Smith, et Brett Watson.

Les efforts des directeurs de zone -- Lisa Dusseault, Ted Hardie, et Chris Newman – pour obtenir le redémarrage de cet effort et le garder actif, et d'un comité ad hoc avec le même objet, sont à souligner. Les membres de ce comité étaient (par ordre alphabétique) Dave Crocker, Cyrus Daboo, Tony Finch, Ned Freed, Randall Gellens, Tony Hansen, l'auteur, et Alexey Melnikov. Tony Hansen a aussi agi comme président ad hoc sur la liste de diffusion de relecture de ce document ; sans ses efforts, son sens de l'équité et du compromis, et sa patience, cela n'aurait clairement pas été possible.

10. Références

10.1 Références normatives

[ANSI-X3.4] American National Standards Institute (ANSI), "USA Code for Information Interchange", ANSI X3.4-1968, 1968. ANSI X3.4-1968 a été remplacée par de nouvelles versions avec des modifications légères; mais la version 1968 reste la version de référence pour l'Internet.

[RFC0821] J. Postel, "Protocole simple de transfert de messagerie", STD 10, août 1982.

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

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC1870] J. Klensin, N. Freed, K. Moore, "Extensions de service à SMTP pour déclaration de taille de message", novembre 1995. (STD0010)

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

[RFC3848] C. Newman, "Enregistrement des types de transmission ESMTP et LMTP", juillet 2004. *(P.S.)*

[RFC3864] G. Klyne, M. Nottingham, J. Mogul, "Procédures d'enregistrement pour les champs d'en-tête de message", septembre 2004. (BCP0090)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*Remplace* RFC3513) *(D.S.)*

[RFC5234] D. Crocker, éd., P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

[RFC5322] P. Resnick, éd., "Format du message Internet", octobre 2008. (*Remplace* RFC2822) (*MàJ* RFC4021) *(D.S.)*

10.2 Références pour information

[IANA-MP] Internet Assigned Number Authority (IANA), "IANA Mail Parameters", 2007, <http://www.iana.org/assignments/mail-parameters >.

[IANA-ALT] Internet Assigned Number Authority (IANA), "Address Literal Tags", 2007, <http://www.iana.org/assignments/address-literal-tags >.

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

[RFC0937] M. Butler, J. Postel, D. Chase, J. Goldberger et J. Reynolds, "Protocole Post Office version 2", février 1985. *(Historique)*

[RFC0959] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", STD 9, octobre 1985.

[RFC0974] C. Partridge, "L'acheminement de la messagerie et le système des domaines", janvier 1986. *(Obsolète, voir la RFC 2821)*

[RFC1047] C. Partridge, "Message dupliqué et SMTP", février 1988.

[RFC1056] M. Lambert, "PCMAIL : un système de messagerie réparti pour les ordinateurs individuels", juin 1988.

[RFC1176] M. Crispin , "Protocole d'accès à la messagerie interactive", août 1990. *(Exp)*

[RFC1652] J. Klensin et autres, "Extensions de service SMTP pour transport MIME sur 8 bits", juillet 1994. *(D.S.)*

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC1869] J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker, "Extensions de service à SMTP", novembre 1995. (*Obsolète, voir* RFC5321, STD0010)

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, RFC2449) (STD0053)

[RFC1985] J. De Winter, "Extension de service SMTP pour débuter la file d'attente de messages distants", août 1996. *(P.S.)*

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

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

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

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

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

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

[RFC2920] N. Freed, "Extension de service SMTP pour le traitement de commandes en parallèle", septembre 2000. (STD0060)

[RFC2979] N. Freed, "Exigences de comportement pour les pare-feu Internet", octobre 2000. *(Information)*

[RFC3030] G. Vaudreuil, "Extensions de service SMTP pour la transmission de grands messages MIME binaires", décembre 2000. *(P.S.)*

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

[RFC3463] G. Vaudreuil, "Codes d'état améliorés du système de messagerie", janvier 2003. (*MàJ par* RFC3886, RFC4468, RFC4865, RFC4954, RFC5248) *(D.S.)*

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

[RFC3501] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", mars 2003. (*MàJ par* RFC4466, RFC4469, RFC4551, RFC5032, RFC5182) *(P.S.)*

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

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Remplacée par* RFC5751)

[RFC3974] M. Nakamura, J. Hagino, "Expérience de fonctionnement de SMTP dans des environnements mixtes IPv4/v6", janvier 2005. *(Information)*

[RFC4408] M. Wong, W. Schlitt, "Cadre de la politique de l'expéditeur (SPF) pour l'autorisation d'utilisation des domaines dans la messagerie électronique, version 1", avril 2006. *(Expérimentale)*

[RFC4409] R. Gellens, J. Klensin, "Soumission du message de messagerie électronique", avril 2006. (*Remplace* RFC2476) *(D.S.)*

[RFC4686] J. Fenton, "Analyse des menaces qui motivent la messagerie identifiée par DomainKeys (DKIM)", septembre 2006. *(Info.)*

[RFC4871] E. Allman et autres, "Signatures de messagerie identifiées par DomainKeys (DKIM)", mai 2007. *(Remplace* RFC4870 *Màj par RFC 5672) (P.S.)*

[RFC4880] J. Callas et autres, "Format de message OpenPGP", novembre 2007. (*Remplace* RFC1991, RFC2440) *(P.S.)*

[RFC5248] T. Hansen, J. Klensin, "Registre des codes d'état de système de messagerie améliorée pour SMTP", juin 2008. (BCP0138)

Appendice 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 de 7 bits. Chaque caractère est transmis comme un octet de 8 bits avec le bit de poids fort réglé à zéro. Des extensions de service peuvent modifier cette règle pour permettre la transmission d'octets de données de 8 bits complets au titre du corps de message, ou, si elles sont spécifiquement conçues pour le faire, des commandes ou réponses SMTP.

Appendice B Générer des commandes SMTP à partir de champs d'en-tête de la RFC0822

Certains systèmes utilisent une section d'en-tête (seulement) RFC 822 dans un protocole de soumission de messages, ou par ailleurs génèrent des commandes SMTP à partir des champs d'en-tête de la RFC0822 quand un tel message est passé d'un UA à un MTA. Bien que le protocole MTA-UA soit une affaire privée, non couverte par une norme de l'Internet, cette approche pose des problèmes. Par exemple, il y a eu des problèmes répétés avec le traitement approprié des copiés "bcc" et des listes de redistribution quand des informations qui conceptuellement appartiennent à l'enveloppe de message ne sont pas séparées précocement dans le traitement des informations de champ d'en-tête (et gardées séparées).

Il est recommandé que l'UA fournisse à son MTA initial ("client de soumission") une enveloppe séparée du message lui-même. Cependant, si l'enveloppe n'est pas fournie, les commandes SMTP DEVRAIT être générées comme suit :

1. Chaque adresse de receveur provenant d'un champ d'en-tête TO, CC, ou BCC DEVRAIT être copiée dans une commande RCPT (générant plusieurs copies de message si c'est exigé pour la mise en file d'attente ou la livraison). Cela inclut toutes les adresses mentionnées dans un "groupe" de la RFC0822. Tous les champs d'en-tête BCC DEVRAIENT alors être retirés de la section d'en-tête. Une fois ce processus achevé, les champs d'en-tête restants DEVRAIENT être vérifiés pour voir si au moins un champ d'en-tête TO, CC, ou BCC reste. Si il n'y en a plus, alors un champ d'en-tête BCC sans information supplémentaire DEVRAIT être inséré comme spécifié dans la [RFC5322].

2. L'adresse de retour dans la commande MAIL DEVRAIT, si possible, être déduite de l'identité du système pour l'utilisateur soumetteur (local) et le champ d'en-tête "From:" autrement. 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 dans le champ d'en-tête From. (Tout champ d'en-tête Sender qui est déjà présent DEVRAIT être retiré.) Les systèmes peuvent fournir un moyen pour que les soumettants outrepassent l'adresse de retour de l'enveloppe, mais peuvent vouloir restreindre son utilisation à des utilisateurs privilégiés. Cela ne va pas empêcher les falsifications de messagerie, mais peut diminuer leur incidence ; voir au paragraphe 7.1.

Quand 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 validité, et de traitement (ou retour) des messages qui ne sont pas valides au moment de l'arrivée, font partie de l'interface MUA-MTA et ne sont pas couverts par la présente spécification.

Un protocole de soumission fondé sur les informations standard de la RFC 822 seules NE DOIT PAS être utilisé pour passer un message d'un système de messagerie étranger (non SMTP) dans un environnement SMTP. Les informations supplémentaires pour construire une enveloppe doivent venir d'une source dans l'autre environnement, que ce soient des champs d'en-tête supplémentaires ou l'enveloppe du système étranger.

Les tentatives de 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 comportement néfastes pour le bon fonctionnement de l'environnement de messagerie de l'Internet. Ces problèmes ont été particulièrement courants quand le message a pour origine une liste de diffusion Internet et est distribué dans l'environnement étranger en utilisant les informations de l'enveloppe. Quand ces messages sont alors traités par un messageur de section d'en-tête seule, des boucles de retour dans l'environnement Internet (et la liste de diffusion) sont presque inévitables.

Appendice C Chemins de source

Historiquement, le <chemin inverse> était une liste des hôtes sur le chemin inverse vers la source et une boîte aux lettres source. Le premier hôte dans le <chemin inverse> était historiquement l'hôte envoyeur de la commande MAIL ; aujourd'hui, les routes de source NE DEVRAIENT PAS apparaître dans le chemin inverse. De même, le <chemin de transmission> peut être une liste des hôtes de l'acheminement vers la source 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 noms de domaine pour fournir si nécessaire les informations d'acheminement. L'utilisation des routes de source est déconseillée (voir l'Appendice F.2) ; alors que les serveurs DOIVENT être prêts à les recevoir et les traiter comme expliqué au paragraphe 3.3 et à l'Appendice F.2, les clients NE DEVRAIENT PAS les

transmettre et cette section n'est incluse dans la spécification actuelle que pour fournir le contexte. Il a été un peu modifié par rapport au matériel de la RFC 821 pour empêcher des actions des serveurs qui pourraient perturber les clients ou les serveurs suivants qui n'attendent pas une pleine mise en œuvre de route de source.

Pour les besoins de 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 (ici, JOE@TROIS) est une adresse absolue, et la route est les informations sur la façon d'y arriver. On ne devrait pas confondre les deux concepts.

Si les routes de source sont utilisées, la RFC 821 et le texte qui suit devraient être consultés sur les mécanismes pour construire et mettre à jour le chemin de transmission. Un serveur qui est joint au moyen d'une route de source (par exemple, son nom de domaine apparaît en premier dans la liste du chemin de transmission) DOIT retirer son nom de domaine de tout chemin de transmission dans lequel ce nom de domaine apparaît avant de transmettre le message et PEUT retirer toutes les autres informations d'acheminement de source. Le chemin inverse NE DEVRAIT PAS être mis à jour par les serveurs qui se conforment à la présente spécification.

Noter que le chemin de transmission et le chemin inverse apparaissent dans les commandes et réponses SMTP, mais pas nécessairement dans le message. C'est-à-dire qu'il n'est aucun besoin que ces chemins et en particulier cette syntaxe apparaissent dans les champs "To:" , "From:", "CC:", etc. de la section d'en-tête du message. À l'inverse, les serveurs SMTP NE DOIVENT PAS déduire les informations finales d'acheminement du message des champs d'en-tête du message.

Quand la liste des hôtes est présente en dépit des recommandations ci-dessus, c'est une route de source "inverse" et elle indique que le message a été relayé par chaque hôte de la liste (le premier hôte de la liste est le relais le plus récent). Cette liste est utilisée comme route de source pour retourner des notifications de non livraison à l'envoyeur. Si, contrairement à ce qui est recommandé ici, un hôte relais s'ajoute au début de la liste, il DOIT utiliser son nom tel que connu dans l'environnement de transport auquel il relaye le message plutôt que dans l'environnement de transport d'où vient le message (si ils sont différents). Noter qu'une situation pourrait survenir dans laquelle des hôtes relais ajoutent leur nom à la route de source inverse et d'autres ne le font pas, générant des discontinuités dans la liste d'acheminement. C'est une raison de plus pour que les serveurs qui ont beson de retourner un message DEVRAIENT ignorer entièrement la route de source et simplement utiliser le domaine spécifié dans la boîte aux lettres.

Appendice 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 normale

Cet exemple SMTP montre un message envoyé par Smith à l'hôte bar.com, et 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 l'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 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.

C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

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 No such user here
C: RSET
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

D.3 Scénario de messagerie relayée

Étape 1 – Hôte source à hôte relais
L'hôte source effectue une recherche DNS sur XYZ.COM (l'adresse de destination) et trouve des enregistrements DNS MX qui spécifient xyz.com comme meilleure préférence et foo.com comme moindre préférence. Il tente d'ouvrir une connexion avec xyz.com et échoue. Il ouvre alors une connexion sur foo.com, avec le dialogue suivant :

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:<Jones@XYZ.COM>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Date: Thu, 21 May 1998 05:33:29 -0700
C: From: John Q. Public <JQP@bar.com>
C: Subject: Prochaine réunion du bureau
C: To: Jones@xyz.com
C:
C: Bill:
C: La prochaine réunion du bureau des directeurs sera mardi
C: John.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

Étape 2 – De l'hôte relais à l'hôte de destination
foo.com, ayant reçu le message, fait maintenant une recherche DNS sur xyz.com. Il trouve le même ensemble d'enregistrements MX, mais ne peut pas utiliser celui qui pointe sur lui-même (ou sur tout autre hôte comme plus mauvaise préférence). Il essaye d'ouvrir une connexion sur xyz.com lui-même et réussit. On a alors :

S: 220 xyz.com Simple Mail Transfer Service Ready
C: EHLO foo.com
S: 250 xyz.com est sur le réseau
C: MAIL FROM:<JQP@bar.com>
S: 250 OK
C: RCPT TO:<Jones@XYZ.COM>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <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: Subject: Prochaine réunion du bureau
C: To: Jones@xyz.com
C:
C: Bill:
C: La prochaine réunion du bureau des directeurs sera mardi
C: John.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

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: MAIL FROM:<EAK@bar.com>
S: 250 OK
C: RCPT TO:<Admin.MRC@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input ; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

Appendice E Autres problèmes de passerelles

En général, les passerelles entre l'Internet et les autres systèmes de messagerie DEVRAIENT tenter de préserver toute la sémantique de mise en couche à travers les frontières entre les deux systèmes de messagerie impliqués. L'approche de traduction de passerelle qui tente de prendre des raccourcis en transposant (comme la transposition des informations d'enveloppe d'un système à la section d'en-tête ou corps de message d'un autre) s'est généralement révélée être inadéquate de façon importante. Les systèmes qui traduisent entre des environnements qui ne prennent pas en charge à la fois les enveloppes et une section d'en-tête et la messagerie Internet doivent être écrits en sachant qu'une certaine perte d'informations est presque inévitable.

Appendice F Caractéristiques déconseillées de la RFC0821

Quelques caractéristiques de la RFC 821 se sont révélées problématiques et NE DEVRAIENT PAS être utilisées dans la messagerie Internet.

F.1 TURN

Cette commande, décrite dans la RFC 821, soulève d'importantes questions de sécurité car, en l'absence d'une forte authentification de l'hôte quand le client et le serveur échangent leurs rôles, elle peut facilement être utilisée pour détourner des messages de leur destination correcte. Son utilisation est déconseillée ; les systèmes SMTP NE DEVRAIENT PAS l'utiliser sauf si le serveur peut authentifier le client.

F.2 Acheminement de source

La RFC 821 utilisait le concept d'acheminement de source explicite pour obtenir que les messages allant d'un hôte à un autre passent via une série de relais. L'exigence d'utiliser les routes de source dans le trafic de messagerie régulier a été éliminé par l'introduction de l'enregistrement "MX" du système de noms de domaines et leur dernière justification significative a été éliminée par l'introduction, dans la RFC 1123, d'une exigence claire que les adresses suivant un "@" doivent toutes être des noms de domaine pleinement qualifiés. Par conséquent, la seule justification restante pour l'utilisation de routes de source est la prise en charge de trèx vieux clients ou MUA SMTP et pour le débogage du système de messagerie. Elle peut, cependant, être encore utile dans ces dernières circonstances et pour achenminer des messages en cas de problèmes sérieux, mais temporaires, comme des problèmes avec les enregistrements pertinents du DNS.

Les serveurs SMTP DOIVENT continuer d'accepter la syntaxe de route de source comme spécifiée dans le corps principal du présent document et dans la RFC 1123. Ils PEUVENT, si nécessaire, ignorer les routes et utiliser seulement le domaine cible dans l'adresse. Si ils utilisent la route de source, le message DOIT être envoyé dans le premier domaine montré dans l'adresse. En particulier, un serveur NE DOIT PAS deviner des raccourcis au sein de la route de source.

Les clients NE DEVRAIENT PAS utiliser l'acheminement de source explicite sauf dans des circonstances inhabituelles, comme le débogage ou potentiellement contourner des erreurs de configuration de pare-feu ou de système de messagerie.

F.3 HELO

Comme expliqué aux paragraphes 3.1 et 4.1.1, EHLO DEVRAIT être utilisé plutôt que HELO quand le serveur accepte le premier. Les serveurs DOIVENT continuer d'accepter et traiter le HELO afin de prendre en charge les anciens clients.

F.4 #-literals

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

F.5 Dates et années

Quand des dates sont insérées dans les messages par les clients ou serveurs SMTP (par exemple, dans les champs d'en-tête de trace) les quatre chiffres de l'année DOIVENT être utilisés. Les années à deux chiffres sont déconseillées ; les années à trois chiffres n'ont jamais été permises dans le système de messagerie de l'Internet.

F.6. Envoi direct et envoi comme message

En plus de spécifier un mécanisme pour livrer les messages aux boîtes aux lettres des utilisateurs, la RFC 821 fournissait des commandes facultatives supplémentaires pour livrer les messages directement sur l'écran du terminal de l'utilisateur. Ces commandes (SEND, SAML, SOML) ont rarement été mises en œuvre, et les changements de la technologie des stations de travail et l'introduction d'autres protocoles peuvent les avoir rendues obsolètes même lorsque elles sont mises en œuvre.

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

Adresse de l'auteur

John C. Klensin
1770 Massachusetts Ave, Suite 322
Cambridge, MA 02140
USA
mél : john+smtp@jck.com

Déclaration complète de droits de reproduction

Propriété intellectuelle