

Groupe de Travail sur les Réseaux
Requête pour Commentaires : RFC 1939 - FR
STD : 53
Remplace : RFC 1725
Catégorie : Standard

J. Myers
Carnegie Mellon
M. Rose
Dover Beach Consulting, Inc.
traduction N. Jourdan, Ecole polytechnique
de l'université de Nantes

Post Office Protocol - Version 3 Le Protocole " Bureau de Poste "

Note du traducteur

Ce document est une traduction intégrale non officielle, mais sans ajouts (excepté cette note), sans commentaires et sans omissions, du RFC 1939 tel qu'édité par ses auteurs, spécifiant le protocole Internet standard POP3. L'auteur de cette traduction décline toute responsabilité sur l'utilisation de ce document et/ou sur d'éventuelles erreurs de traduction.

Concernant les droits du traducteur : le traducteur renonce à ses droits sur la reproduction de ce document si l'ensemble de ces conditions est respecté : les reproductions doivent être **complètes** (contenant cette note), **d'un seul tenant** (un seul fichier ou un ensemble de pages physiquement reliées), **sans aucune modification** du contenu et **réalisées à partir de la dernière version** de ce document disponible gratuitement sur le site mentionné ci-après.

Dernière version du document

<http://abcdrfc.free.fr/>

Adresse du traducteur

M. Nicolas Jourdan
3, Impasse du Clos des Pins
30870 CLARENSAC
France
E-mail : njourdan@free.fr

Statut de ce Document

Ce document est une spécification d'un protocole Internet reconnu et approuvé comme un standard par la communauté Internet ; il propose une discussion sur le protocole et des suggestions pour des améliorations. Merci de se reporter à la dernière version des " Standards Officiels des Protocoles Internet " (STD 1 - " Internet Official Protocol Standards ") pour connaître l'état de standardisation et le statut de ce protocole. La distribution du RFC 1939 original (en anglais) n'est pas limitée.

Table des matières

1. Introduction	2
2. Une courte digression	3
3. Opérations de bases	3
4. L'état AUTORISATION (AUTHORIZATION)	4
QUIT	5
5. L'état TRANSACTION	5
STAT	5
LIST [msg]	6
RETR msg	7
DELE msg	7
NOOP	8
RSET	8
6. L'état MISE-A-JOUR (UPDATE)	9
QUIT	9
7. Commandes POP3 optionnelles	10
TOP msg n	10
UIDL [msg]	10
USER nom	12
PASS chaîne-de-caractères	12
APOP nom somme-de-contrôle	13
8. Considérations opérationnelles et limitatives	14
9. Résumé des commandes POP3	15
10. Exemple de session POP3	16
11. Format des messages	16
12. Références	17
13. Considérations sur la sécurité	17
14. Remerciements	18
15. Adresses des Auteurs	18
Appendice A. Différences par rapport au RFC 1725	18
Appendice B. Index des commandes	19

1. Introduction

Sur certains types de petits nœuds d'Internet, il est souvent impossible de maintenir un système de transport de message (Message Transport System). Par exemple, une station de travail peut ne pas avoir suffisamment de ressources (vitesse du processeur, espace disque) pour héberger un serveur SMTP [[RFC821](#)] et le système de distribution local de courrier associé, fonctionnant en permanence. De même, cela serait coûteux (ou impossible) de laisser un PC connecté à un réseau de type IP pendant longtemps (les nœuds manquent d'une ressource appelée " connectivité ").

Malgré cela, il est souvent très utile de pouvoir gérer du courrier sur ces petits nœuds aussi possèdent-ils souvent un logiciel spécifique (User Agent) pour accomplir les tâches de gestion de courrier. Pour résoudre ce problème, un nœud qui peut accueillir un service MTS fournit également un service de dépôt de courrier (maildrop) pour ces nœuds moins puissants. Le Protocole " Bureau de Poste " - Version 3 (POP3) a pour but de permettre à une station de travail d'accéder dynamiquement de façon pratique à un dépôt de courrier sur un hôte serveur. En général, cela signifie que le protocole POP3 est utilisé pour permettre à une station de travail de récupérer le courrier que le serveur stocke pour elle.

POP3 n'a pas pour but de fournir des opérations de manipulation de grandes quantités de courrier sur le serveur ; normalement, le courrier est téléchargé puis ensuite effacé. Un protocole plus avancé (et complexe), IMAP4, est présenté dans [\[RFC1730\]](#).

Pour la suite de ce document, le terme " hôte client " fait référence à un hôte utilisant le service POP3, alors que le terme " hôte serveur " fait référence à un hôte qui fournit le service POP3.

2. Une courte digression

Ce document ne spécifie pas comment un hôte client fait entrer un courrier à l'intérieur du système de transport, cependant une méthode compatible avec la philosophie de ce document est présentée ici :

Quand le logiciel de messagerie de l'hôte client souhaite faire entrer un message à l'intérieur du système de transport, il établit une connexion SMTP avec son hôte relais puis lui envoie tout le courrier. Cet hôte relais peut être, mais n'a pas nécessairement besoin d'être, l'hôte serveur POP3 pour l'hôte client. Bien sûr, l'hôte relais doit accepter le courrier à envoyer quelles que soient les adresses des destinataires, alors que ceci n'est pas obligatoire pour tous les serveurs SMTP.

3. Opérations de bases

D'abord, l'hôte serveur lance le service POP3 en écoutant le port TCP 110. Quand un hôte client souhaite utiliser ce service, il établit une connexion TCP avec l'hôte serveur. Quand la connexion est établie, le serveur POP3 envoie un message de bienvenue. Le client et le serveur POP3 échangent alors des commandes et des réponses (respectivement) jusqu'à ce que la connexion soit fermée ou avortée.

Les commandes POP3 sont des mot-clefs (indépendants de la casse), pouvant être suivis d'un ou plusieurs arguments. Toutes les commandes sont terminées par la séquence CRLF (Retour Chariot, Saut de Ligne ASCII). Les mot-clefs et les arguments sont formés de caractères ASCII imprimables. Les mot-clefs et les arguments sont chacun séparés par un unique caractère espace (SPACE). Les mot-clefs sont formés de trois ou quatre caractères. Chaque argument peut avoir jusqu'à 40 caractères.

Les réponses POP3 sont des indicateurs d'état et un mot-clef pouvant être suivi d'informations complémentaires. Toutes les réponses sont terminées par la séquence CRLF. Il y a actuellement deux indicateurs d'état : positif (" +OK ") et négatif (" -ERR "). Les serveurs DOIVENT envoyer " +OK " et " -ERR " en majuscules.

Certaines commandes ont une réponse sur plusieurs lignes. Dans ces cas, qui sont clairement explicités ci-après, après avoir envoyé la première ligne de la réponse et la séquence CRLF, chaque ligne complémentaire est envoyée, chacune terminée par la séquence CRLF. Lorsque toutes les lignes de la réponse ont été envoyées, une ligne finale est envoyée, formée d'un point (code ASCII décimal 046, " . ") et de la séquence CRLF. Si une des lignes de la réponse commence par un point, ce point est doublé (transmis deux fois consécutivement ou " byte-stuffed "). Ainsi une réponse sur plusieurs lignes se termine

par la séquence de cinq octets " CRLF.CRLF ". Lors de l'examen d'une réponse sur plusieurs lignes, le client examine si la ligne commence par un point. Si c'est le cas : si les deux octets suivants ne forment pas la séquence CRLF, le premier octet de la ligne (le point) est enlevé ; sinon (si CRLF suit immédiatement le point), la réponse du serveur POP se termine ici et la ligne (" .CRLF ") n'est pas considérée comme faisant parti de la réponse sur plusieurs lignes.

Une session POP3 évolue à travers un certain nombre d'états au cours de sa vie. Une fois que la connexion TCP a été ouverte et que le serveur POP3 a envoyé le message de bienvenue, la session entre dans l'état AUTORISATION (AUTHORIZATION). Dans cet état, le client doit s'authentifier auprès du serveur POP3. Une fois que le client a réussi à faire cela, le serveur acquiert les ressources associées au dépôt de courrier du client, et la session entre dans l'état TRANSACTION. Dans cet état, le client demande des actions de la part du serveur POP3. Quand le client a émis la commande QUIT (quitter), la session entre dans l'état MISE-A-JOUR (UPDATE). Dans cet état, le serveur POP3 libère les ressources acquises durant l'état TRANSACTION et dit au revoir. La connexion TCP est alors fermée.

Un serveur DOIT répondre à une commande non reconnue, non implémentée ou syntaxiquement incorrecte par l'indicateur d'état négatif. Un serveur DOIT répondre à une commande émise quand la session est dans un état incorrect en répondant avec un indicateur d'état négatif. Il n'y a pas de méthode générale pour un client pour faire la distinction entre un serveur qui ne possède pas une commande optionnelle et un serveur qui ne souhaite pas ou qui n'est pas capable de prendre en compte cette commande.

Un serveur POP3 PEUT implémenter un mécanisme afin de déconnecter les clients trop longtemps inactifs (inactivity autologout timer). Ce temps d'inactivité entraînant la déconnexion DOIT être d'au moins 10 minutes. La réception de n'importe quelle commande du client durant ce temps devrait justifier la remise à zéro de ce mécanisme. Quand ce temps expire, la session N'entre PAS dans l'état MISE-A-JOUR (UPDATE) -- le serveur devrait fermer la connexion TCP sans effacer de message et sans envoyer une réponse au client.

4. L'état AUTORISATION (AUTHORIZATION)

Une fois que la connexion TCP a été ouverte par un client POP3, le serveur POP3 émet un message de bienvenue d'une ligne. Ceci peut être n'importe quelle réponse positive. Un exemple pourrait être :

```
S : +OK POP3 server ready
```

La session POP3 est actuellement dans l'état AUTORISATION (AUTHORIZATION). Le client doit à présent s'identifier et s'authentifier auprès du serveur POP3. Deux mécanismes possibles pour faire cela sont décrits dans ce document, le couple de commande USER (utilisateur) et PASS ou la commande APOP. Ces deux mécanismes sont décrits ultérieurement dans ce document. D'autres mécanismes d'authentification sont décrits dans [\[RFC1734\]](#). Tant qu'il n'y a pas de mécanisme d'authentification unique exigé pour tous les serveurs POP3, un serveur POP3 doit naturellement supporter au moins un mécanisme d'authentification.

Une fois que le serveur POP3 a déterminé grâce à l'utilisation d'une des commandes d'authentification que le client pouvait accéder au dépôt de courrier approprié, le serveur POP3 acquiert alors un accès exclusif avec verrou sur le dépôt de courrier, nécessaire pour éviter qu'un message soit modifié ou effacé avant que la session n'entre dans l'état MISE-A-JOUR (UPDATE). Si ce verrou est réellement acquis, le serveur POP3 répond avec un indicateur d'état positif. La session POP3 entre maintenant dans l'état TRANSACTION, avec aucun message marqué comme effacé. Si le dépôt de courrier ne peut pas être ouvert pour quelque raison que ce soit (par exemple, le verrou ne peut pas être acquis, le client n'obtient pas l'accès au dépôt de courrier approprié, ou le dépôt de courrier ne peut pas être analysé), le serveur POP3 répond avec un indicateur d'état

négatif. (Si un verrou a été acquis mais que le serveur POP3 s'apprête à répondre par un indicateur d'état négatif, le serveur POP3 doit libérer le verrou avant de rejeter la commande.) Après le retour d'un indicateur d'état négatif, le serveur peut clore la connexion. Si le serveur ne clos pas la connexion, le client peut émettre soit une nouvelle commande d'authentification et recommencer, soit la commande QUIT (quitter).

Une fois que le serveur POP3 a ouvert le dépôt de courrier, il assigne à chaque message un numéro de message (`message-number`), et note la taille de chaque message en octets. Le premier message dans le dépôt de courrier reçoit le numéro de message " 1 ", le second " 2 ", et ainsi de suite, jusqu'à ce que le *n* ième message dans le dépôt de courrier reçoive le numéro de message " *n* ". Dans les commandes et les réponses POP3, tous les numéros de message et tailles de message sont exprimés en base 10 (i.e., en décimal).

Voici le résumé pour la commande QUIT (quitter) lorsqu'elle est émise dans l'état AUTORISATION (AUTHORIZATION) :

QUIT

Arguments :

aucun

Restrictions :

aucune

Réponses possibles :

+OK

Exemples :

C : QUIT

S : +OK dewey POP3 server signing off

5. L'état TRANSACTION

Une fois que le client s'est identifié avec succès auprès du serveur POP3 et que le serveur POP3 a verrouillé et ouvert le dépôt de courrier approprié, la session POP3 est à présent dans l'état TRANSACTION. Le client peut maintenant émettre plusieurs fois n'importe quelle commande POP3 suivante. Après chaque commande, le serveur POP3 émet une réponse. Eventuellement, le client émet la commande QUIT et la session POP3 entre dans l'état MISE-A-JOUR (UPDATE).

Voici les commandes POP3 valides dans l'état TRANSACTION :

STAT

Arguments :

aucun

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Le serveur POP3 émet une réponse positive avec une ligne contenant des informations sur le dépôt de courrier. Cette ligne est appelée " listing de dépôt " (" drop listing ") pour ce dépôt de courrier.

Dans le but de simplifier l'analyse, tous les serveurs POP3 doivent utiliser un certain format pour les listings de dépôt. La réponse positive est formée de " +OK " suivi par un simple espace, le nombre de message dans le dépôt de courrier, un simple espace et la taille du dépôt de courrier en octets. Ce document ne fournit aucune spécification sur ce qui suit la taille du dépôt de courrier. Les implémentations minimales peuvent simplement terminer cette ligne de réponse par la séquence CRLF. Des implémentations avancées peuvent inclure d'autres informations.

NOTE : Ce document recommande FORTEMENT aux implémentations de ne pas fournir d'informations supplémentaires dans la listing de dépôt. D'autres aménagements (optionnels) sont discutés plus loin, concernant ce qui permettrait au client d'analyser les messages dans le dépôt de courrier.

Attention, les messages marqués comme effacés ne sont comptés dans aucuns des totaux.

Réponses possibles :

+OK nn mm

Exemples :

C : STAT
S : +OK 2 320

LIST [msg]**Arguments :**

un numéro de message (optionnel), qui, s'il est présent, NE peut PAS faire référence à un message marqué comme effacé

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Si un argument a été donné et que le serveur POP3 émet une réponse positive, cette ligne contient des informations sur ce message. Cette ligne est appelée " listing de scan " (" scan listing ") pour ce message.

S'il n'y a pas d'argument et que le serveur POP3 émet une réponse positive, alors la réponse comporte plusieurs lignes. Après la séquence initiale " +OK ", pour chaque message dans le dépôt de courrier, le serveur POP3 répond par une ligne qui contient des informations sur ce message. Cette ligne est aussi appelée " listing de scan " (" scan listing ") pour ce message. S'il n'y a pas de message dans le dépôt de courrier, alors le serveur POP3 répond sans listing de scan -- il émet une réponse positive suivie par une ligne contenant un point et la séquence CRLF.

Dans le but de simplifier l'analyse, tous les serveurs POP3 doivent utiliser un certain format pour les listings de scan. Le listing de scan est formé du numéro de message du message, suivi d'un simple espace puis de la taille exacte du message en octets. Les méthodes pour calculer la taille exacte d'un message sont décrites dans la section suivante " Format d'un message ". Ce document ne fournit aucune spécification sur ce qui suit la taille du message dans le listing de scan. Les implémentations minimales peuvent simplement terminer cette ligne de réponse par la séquence CRLF. Des implémentations avancées peuvent inclure d'autres informations, obtenues à partir d'une analyse du message.

NOTE : Ce document recommande FORTEMENT aux implémentations de ne pas fournir d'informations supplémentaires dans le listing de scan. D'autres

aménagements (optionnels) sont discutés plus loin, concernant ce qui permettrait au client d'analyser les messages dans le dépôt de courrier.

Attention, les messages marqués comme effacés ne sont pas listés.

Réponses possibles :

+OK suivi d'un listing de scan
-ERR numéro de message invalide

Exemples :

```
C : LIST
S : +OK 2 messages (320 octets)
S : 1 120
S : 2 200
S : .
...
C : LIST 2
S : +OK 2 200
...
C : LIST 3
S : -ERR no such message, only 2 messages in maildrop
```

RETR msg**Arguments :**

un numéro de message (nécessaire) qui NE peut PAS faire référence à un message marqué comme effacé

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Si un serveur POP3 émet une réponse positive, alors la réponse comporte plusieurs lignes. Après la séquence initiale " +OK ", le serveur POP3 envoie le message correspondant au numéro de message donné en paramètre, en faisant attention au codage des lignes commençant par un point (comme pour toutes les réponses comportant plusieurs lignes).

Réponses possibles :

+OK suivi du message
-ERR numéro de message invalide

Exemples :

```
C : RETR 1
S : +OK 120 octets
S : <le serveur POP3 envoie le message entier ici>
S : .
```

DELE msg**Arguments :**

un numéro de message (nécessaire) qui NE peut PAS faire référence à un message marqué comme effacé

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Le serveur POP3 marque le message comme effacé. Toute future référence dans une commande POP3 au numéro de message associé à ce message marqué comme effacé générera une erreur. Le serveur POP3 n'efface pas réellement le message tant que la session POP3 n'entre pas dans l'état MISE-A-JOUR (UPDATE).

Réponses possibles :

+OK message effacé
-ERR numéro de message invalide

Exemples :

```
C : DELE 1
S : +OK message 1 deleted
...
C : DELE 2
S : -ERR message 2 already deleted
```

NOOP**Arguments :**

aucun

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Le serveur POP3 ne fait rien, il retourne simplement une réponse positive.

Réponses possibles :

+OK

Exemples :

```
C : NOOP
S : +OK
```

RSET**Arguments :**

aucun

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Si des messages ont été marqués comme effacés par Le serveur POP3, cette marque est enlevée (comme avant la commande DELE). Le serveur POP3 retourne ensuite une réponse positive.

Réponses possibles :

+OK

Exemples :

C : RSET
S : +OK maildrop has 2 messages (320 octets)

6. L'état MISE-A-JOUR (UPDATE)

Quand le client émet la commande QUIT dans l'état TRANSACTION, la session POP3 entre dans l'état MISE-A-JOUR (UPDATE). (Attention, si le client émet la commande QUIT dans l'état AUTORISATION (AUTHORIZATION), la session POP3 se termine SANS entrer dans l'état MISE-A-JOUR.)

Si une session se termine pour une autre raison que l'émission de la commande QUIT par le client, la session POP3 N'entre PAS dans l'état MISE-A-JOUR et NE DOIT PAS effacer un seul message du dépôt de courrier.

QUIT**Arguments :**

aucun

Restrictions :

aucune

Discussions :

Le serveur POP3 efface tous les messages du dépôt de courrier marqués comme effacés et retourne l'état d'accomplissement de cette opération. S'il y a une erreur, comme un problème d'allocation de ressources, rencontré durant l'effacement des messages, le dépôt de courrier peut avoir aucun ou quelques messages marqués comme effacés réellement effacés. En aucun cas le serveur peut effacer des messages qui ne sont pas marqués comme effacés.

Que l'effacement ait réussi ou non, le serveur libère le verrou et son accès exclusif au dépôt de courrier et ferme la connexion TCP.

Réponses possibles :

+OK

-ERR certains messages marqués comme effacés non effacés

Exemples :

C : QUIT
S : +OK dewey POP3 server signing off (maildrop empty)
...
C : QUIT
S : +OK dewey POP3 server signing off (2 messages left)
...
C : QUIT
S : -ERR some deleted messages not removed

7. Commandes POP3 optionnelles

Les commandes POP3 présentées ci-après doivent être supportées par toutes les implémentations minimales de serveurs POP3.

Les commandes POP3 optionnelles décrites ci-après donnent à un client POP3 une plus grande liberté de manipulation des messages, tout en préservant une implémentation simple d'un serveur POP3.

NOTE : Ce document encourage FORTEMENT les implémentations à supporter ces commandes plutôt que d'augmenter le nombre d'informations présentes dans les listings de scan et les listings de dépôt. En résumé, la philosophie de ce document est de mettre plus d'intelligence dans les clients POP3 que dans les serveurs POP3.

TOP msg n

Arguments :

un numéro de message (nécessaire) qui NE peut PAS faire référence à un message marqué comme effacé et un nombre non négatif de lignes (nécessaire)

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Si le serveur POP3 émet une réponse positive, alors la réponse est composée de plusieurs lignes. Après la séquence initiale "+OK", le serveur POP3 envoie les en-têtes du message désigné par le numéro de message, la ligne vierge séparant les en-têtes du corps du message, puis les n premières lignes demandées du corps du message, en faisant attention aux lignes commençant par un point (comme pour toutes les réponses comportant plusieurs lignes).

Il faut noter que si le nombre de lignes demandé par le client POP3 est plus grand que le nombre de lignes dans le corps du message, alors le serveur POP3 envoie le message entier.

Réponses possibles :

+OK le début du message ci-après

-ERR numéro de message invalide

Exemples :

C : TOP 1 10

S : +OK

S : <Le serveur POP3 envoie les en-têtes du message, une ligne vierge, et les 10 premières lignes du corps du message>

S : .

...

C : TOP 100 3

S : -ERR no such message

UIDL [msg]

Arguments :

un numéro de message (optionnel), qui, s'il est présent, NE peut PAS faire référence à un message marqué comme effacé

Restrictions :

ne peut être donné que dans l'état TRANSACTION

Discussion :

Si un argument a été donné et que le serveur POP3 émet une réponse positive, cette ligne contient des informations sur ce message. Cette ligne est appelée un " listing d'identificateur unique " (" unique-id listing ") pour ce message.

S'il n'y a pas d'argument et que le serveur POP3 émet une réponse positive, alors la réponse comporte plusieurs lignes. Après la séquence initiale " +OK ", pour chaque message dans le dépôt de courrier, le serveur POP3 répond par une ligne qui contient des informations sur ce message. Cette ligne est aussi appelée " listing d'identificateur unique " pour ce message.

Dans le but de simplifier l'analyse, tous les serveurs POP3 doivent utiliser un certain format pour les listings d'identificateur unique. Un listing d'identificateur unique est formé du numéro de message du message, suivi par un simple espace puis par le numéro d'identificateur unique du message. Il n'y a pas d'autre information après l'identificateur unique dans le listing d'identificateur unique.

L'identificateur unique d'un message est une chaîne de caractères arbitraire déterminée par le serveur, caractères dont la valeur ASCII est l'une des 70 valeurs de 0x21 à 0x7E, qui identifie de façon unique un message à l'intérieur d'un dépôt de courrier et qui ne change pas entre les sessions, et cela même si une session se termine sans entrer dans l'état MISE-A-JOUR (UPDATE). Le serveur ne devrait jamais réutiliser un identificateur unique dans un dépôt de courrier donné, aussi longtemps que l'entité qui se sert de cet identificateur unique existe.

Il faut noter que les messages marqués comme effacés ne sont pas listés.

Bien qu'il soit généralement préférable pour des implémentations de serveurs d'enregistrer arbitrairement les identificateurs uniques assignés dans le dépôt de courrier, cette spécification propose que les identificateurs uniques soient calculés à partir d'une partie du message. Les clients devraient être capable de gérer une situation où deux copies identiques d'un message dans un dépôt de courrier ont le même identificateur unique.

Réponses possibles :

+OK suivi du listing d'identificateur unique
-ERR numéro de message invalide

Exemples :

```
C : UIDL
S : +OK
S : 1 whqtsw000WBw418f9t5JxYwZ
S : 2 QhdPYR:00WBw1Ph7x7
...
C : UIDL 2
S : +OK 2 QhdPYR:00WBw1Ph7x7
...
C : UIDL 3
S : -ERR no such message, only 2 messages in maildrop
```

USER nom**Arguments :**

une chaîne de caractères identifiant une boîte aux lettres (nécessaire), qui a une signification UNIQUEMENT pour le serveur

Restrictions :

peut être donné uniquement dans l'état AUTORISATION (AUTHORIZATION) après le message POP3 de bienvenue ou après une commande USER ou PASS non valide

Discussion :

Pour s'authentifier en utilisant la combinaison de commandes USER et PASS, le client doit d'abord envoyer la commande USER. Si le serveur POP3 répond par un indicateur d'état positif (" +OK "), alors le client peut émettre soit la commande PASS pour terminer l'authentification, soit la commande QUIT pour terminer la session POP3. Si le serveur POP3 répond par un indicateur d'état négatif (" -ERR ") à la commande USER, alors le client peut soit émettre une nouvelle commande d'authentification, soit émettre la commande QUIT.

Le serveur peut retourner une réponse positive même s'il n'existe pas une telle boîte aux lettres. Le serveur peut retourner une réponse négative si la boîte aux lettres existe, mais n'accepte pas une authentification par mot de passe en clair (plaintext password).

Réponses possibles :

+OK le nom est une boîte aux lettres valide
-ERR ne connaît pas cette boîte aux lettres

Exemples :

```
C : USER frated
S : -ERR sorry, no mailbox for frated here
...
C : USER mrose
S : +OK mrose is a real hoopy frood
```

PASS chaîne-de-caractères**Arguments :**

un mot de passe spécifique à cette boîte aux lettres sur ce serveur (nécessaire)

Restrictions :

peut être donné uniquement dans l'état AUTORISATION (AUTHORIZATION) immédiatement après une commande USER valide

Discussion :

Quand le client émet une commande PASS, le serveur POP3 utilise les deux arguments fournis par les commandes USER et PASS pour déterminer si le client peut accéder au dépôt de courrier approprié.

Puisque la commande PASS a exactement un seul argument, un serveur POP3 peut traiter les espaces de l'argument comme faisant partis du mot de passe, plutôt que comme séparateurs d'arguments.

Réponses possibles :

+OK accès à la boîte aux lettres verrouillé et boîte aux lettres prête
 -ERR mot de passe non valide
 -ERR impossible de verrouiller l'accès à la boîte aux lettres

Exemples :

```
C : USER mrose
S : +OK mrose is a real hoopy frood
C : PASS secret
S : -ERR maildrop already locked

...

C : USER mrose
S : +OK mrose is a real hoopy frood
C : PASS secret
S : -OK mrose's maildrop has 2 messages (320 octets)
```

APOP nom somme-de-contrôle**Arguments :**

une chaîne de caractères identifiant une boîte aux lettres et une somme de contrôle (digest) de type MD5 (tous les deux nécessaires)

Restrictions :

peut être donné uniquement dans l'état AUTORISATION (AUTHORIZATION) après le message POP3 de bienvenue ou après une commande USER ou PASS non valide

Discussion :

Normalement, chaque session POP3 commence par un échange USER/PASS. De cela résulte que le mot de passe spécifique à l'utilisateur sur le serveur sera transmis en clair sur le réseau. Pour une utilisation intermittente de POP3, cela peut ne pas introduire un risque très important. Cependant, un grand nombre d'implémentations de client POP3 se connecte au serveur POP3 périodiquement -- pour savoir si du courrier est arrivé. L'intervalle de temps entre les sessions peut même parfois être de l'ordre de cinq minutes. Aussi, le risque d'interception du mot de passe est fortement augmenté.

Une autre méthode d'authentification est nécessaire, permettant à la fois d'authentifier l'origine et de protéger les réponses, mais qui n'implique pas l'envoi du mot de passe en clair sur le réseau. La commande APOP fournit cette fonctionnalité.

Un serveur POP3 qui implémente la commande APOP mettra un timbre-à-date (timestamp) dans son message de bienvenue. La syntaxe de ce timbre-à-date respecte les spécifications des identificateurs de message (msg-id) du [\[RFC822\]](#), et DOIT être différent chaque fois qu'un serveur POP3 émet un message de bienvenue. Par exemple, pour une implémentation UNIX dans laquelle un processus UNIX séparé est utilisé pour chaque instance de serveur POP3, la syntaxe d'un timbre-à-date pourrait être :

```
<identificateur-de-processus.heure@nom-de-l'hôte>
```

où l'identificateur de processus est la valeur décimale du PID du processus, l'heure est la valeur décimale de l'heure système et le nom de l'hôte est le nom complet du nom de domaine correspondant à l'hôte sur lequel tourne le serveur POP3.

Le client POP3 prend note du timbre-à-date et émet la commande APOP. Le paramètre " nom " a exactement le même sens que le paramètre " nom " de la commande USER. Le paramètre " somme de contrôle " est calculé en appliquant l'algorithme MD5 du [\[RFC1321\]](#) à la chaîne de caractères formée du timbre-à-

date (incluant les symboles <>) suivi du secret partagé. Le secret partagé est une chaîne de caractères connue uniquement par le client et le serveur POP3. Certaines précautions devraient être prises afin que le secret ne soit pas dévoilé, car chacun a conscience qu'il permet à n'importe qui de prendre l'identité de l'utilisateur " nom " sur le serveur. Le paramètre " somme de contrôle " lui-même est une valeur de 16 octets envoyée dans un format hexadécimal, en utilisant les caractères ASCII minuscules.

Quand le serveur POP3 reçoit la commande APOP, il vérifie la somme de contrôle donnée en paramètre. Si la somme de contrôle est correcte, le serveur POP3 émet une réponse positive et la session POP3 entre dans l'état TRANSACTION. Sinon, une réponse négative est émise et la session POP3 reste dans l'état AUTORISATION (AUTHORIZATION).

Il faut noter que lorsque la longueur du secret partagé augmente, la difficulté de trouver ce secret à partir de sommes de contrôle augmente d'autant. Aussi, les secrets partagés devraient être de longues chaînes de caractères (beaucoup plus longues que l'exemple de 8 caractères ci-après).

Réponses possibles :

```
+OK accès à la boîte aux lettres verrouillé et boîte aux lettres prête
-ERR permission non accordée
```

Exemples :

```
S : +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C : APOP mrose c4c9334bac560ecc979e58001b3e22fb
S : +OK maildrop has 1 message (369 octets)
```

Dans cet exemple, le secret partagé est la chaîne de caractères " tanstaaf ". Aussi, l'algorithme MD5 est appliqué à la chaîne " <1896.697170952@dbc.mtview.ca.us>tanstaaf " qui produit la somme de contrôle " c4c9334bac560ecc979e58001b3e22fb ".

8. Considérations opérationnelles et limitatives

Depuis que certaines des caractéristiques optionnelles décrites précédemment ont été ajoutées au protocole POP3, une certaine habitude s'est répandue de les utiliser pour les opérations à l'intérieur des bureaux de poste commerciaux à grande échelle, où la plupart des utilisateurs n'ont aucuns contacts entre eux. Dans ces situations et d'autres, les utilisateurs et les vendeurs de clients POP3 ont découvert que l'utilisation de la commande UIDL sans émettre de commande DELE pouvait fournir une version simplifiée de la fonctionnalité de " dépôt de courrier comme dépôt quasi-permanent " normalement associée avec IMAP. Bien sûr les autres possibilités d'IMAP, comme celle de scruter dans une connexion existante l'arrivée de nouveaux messages et le support de plusieurs dossiers sur le serveur, ne sont pas présentes dans POP3.

Quand ces fonctionnalités sont utilisées de cette façon par des utilisateurs peu soucieux, il y a une tendance à ce que les messages déjà lus s'accumulent sans limite sur le serveur. Ceci est clairement un type de comportement indésirable du point de vue de l'administrateur du serveur. Cette situation est aggravée par le fait que les possibilités limitées de POP3 ne permettent pas une gestion efficace des boîtes aux lettres qui ont des centaines voire des milliers de messages.

Par conséquent, il est recommandé que les administrateurs de gros serveurs ayant beaucoup d'utilisateurs, surtout sur ceux où les utilisateurs ont uniquement accès au dépôt de courrier via POP3, envisagent les options suivantes :

- * **Imposer un quota de stockage identique ou personnalisé pour chaque utilisateur**

Un inconvénient de cette option est que l'accumulation de messages peut entraîner l'impossibilité pour l'utilisateur de recevoir de nouveaux messages dans le dépôt de courrier. Les sites qui choisissent cette option devraient assurer l'information de l'utilisateur concernant un imminent ou actuel épuisement de son quota, peut-être en insérant un message approprié à l'intérieur de son dépôt de courrier.

*** Imposer un règlement à propos de la rétention de courrier sur le serveur**

Les sites sont libre d'établir un règlement à propos de l'utilisation des ressources informatiques comme l'espace de stockage ou la rétention de messages sur le serveur, qu'ils soient lus ou non lus. Par exemple, un site pourrait effacer les messages non-lus sur le serveur après 60 jours et effacer les messages lus après 7 jours. Ces effacements de messages sont en dehors du cadre du protocole POP3 et ne sont pas considérés comme une violation du protocole.

Les administrateurs de serveur imposant des règles d'effacement de messages devraient penser à informer tous les utilisateurs de l'existence des règles appliquées.

Les clients ne devraient pas supposer que des règles d'effacement des messages sont automatiquement appliquées et devraient continuer à effacer explicitement les messages en utilisant la commande DELE de façon appropriée.

Il devrait être noté qu'imposer des règles d'effacement de messages sur un serveur peut être déroutant pour la communauté des utilisateurs, car leurs clients POP3 peuvent être configurés pour laisser le courrier sur le serveur alors que cela n'est pas totalement supporté par le serveur.

Une façon spéciale de régler l'utilisation du serveur est d'imposer que les messages ne puissent être téléchargés qu'une seule fois à partir du serveur, puis sont effacés lorsque cela a été accompli. Cela pourrait être implémenté au niveau du logiciel du serveur POP3 par le mécanisme suivant : " lorsque le client POP3 est entré à l'intérieur du système et qu'il en est ressorti par un QUIT, effacer tous les messages téléchargés avec la commande RETR pendant la session ". Il est important de ne pas effacer les messages lors d'une fin anormale de la connexion (i.e., s'il n'y a pas eu de QUIT reçu de la part du client) car le client peut ne pas avoir bien reçu et enregistré les messages. Les serveurs qui imposent cette règle d' " effacement après téléchargement " peuvent aussi souhaiter désactiver ou limiter la commande optionnelle TOP, puisqu'elle pourrait être utilisée comme un mécanisme de substitution au téléchargement de messages entiers.

9. Résumé des commandes POP3

Commandes POP3 minimales :

Valides dans l'état AUTORISATION (AUTHORIZATION)

USER nom
PASS mot-de-passe
QUIT

Valides dans l'état TRANSACTION

STAT
LIST [msg]
RETR msg
DELE msg
NOOP

RSET

QUIT

Commandes POP3 optionnelles :

Valides dans l'état AUTORISATION (AUTHORIZATION)

APOP nom somme-de-contrôle

Valides dans l'état TRANSACTION

TOP msg n

UIDL [msg]

Réponses POP3 :

+OK

-ERR

Il faut noter qu'à l'exception des commandes STAT, LIST et UIDL, la réponse donnée par le serveur POP3 à toute commande est significative avec seulement "+OK " et "-ERR ". Tout texte apparaissant après ces réponses peut être ignoré par le client.

10. Exemple de session POP3

```
S : <Attend une connexion TCP sur le port 110>
C : <ouvre une connexion sur ce port>
S : +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C : APOP mrose c4c9334bac560ecc979e58001b3e22fb
S : +OK mrose's maildrop has 2 messages (320 octets)
C : STAT
S : +OK 2 320
C : LIST
S : +OK 2 messages (320 octets)
S : 1 120
S : 2 200
S : .
C : RETR 1
S : +OK 120 octets
S : <le serveur POP3 envoie le message 1>
S : .
C : DELE 1
S : +OK message 1 deleted
C : RETR 2
S : +OK 200 octets
S : <le serveur POP3 envoie le message 2>
S : .
C : DELE 2
S : +OK message 2 deleted
C : QUIT
S : +OK dewey POP3 server signing off (maildrop empty)
C : <ferme la connexion>
S : <attend une connexion suivante>
```

11. Format des messages

Tous les messages transmis durant une session POP3 sont supposés être conformes au standard pour le format des messages texte d'Internet [[RFC822](#)].

Il est important de noter que la taille du message en octet sur l'hôte serveur peut être différente de la taille allouée pour ce message à cause des conventions locales de représentation des fins de ligne (end-of-line). Habituellement, lorsque la session est dans l'état AUTORISATION, le serveur POP3 peut calculer la taille de chaque message en octets quand il ouvre le dépôt de courrier. Par exemple, si l'hôte serveur POP3 représente en interne une fin de ligne par un simple octet, alors le serveur POP3 compte simplement chaque occurrence de ce caractère dans le message comme deux octets. Il faut noter qu'il n'est pas nécessaire (et qu'il ne faut pas) compter deux fois le point initial des lignes du message qui commencent par un point, puisque le client POP3 enlèvera tous les premiers points nécessaires à l'encodage des réponses sur plusieurs lignes reçues.

12. Références

[RFC821] J. Postel, " Protocole Simple de Transfert de Courrier "
(" Simple Mail Transfer Protocol "), STD 10, RFC 821, USC/Institut des
Sciences de l'Information, août 1982.

[RFC822] D. Crocker, " Standard pour le Format des Messages Texte de
l'ARPA-Internet " (" Standard for the Format of ARPA-Internet Text
Messages "), STD 11, RFC 822, Université de Delaware, août 1982.

[RFC1321] R. Rivest, " L'algorithme MD5 pour les sommes de contrôle "
(" The MD5 Message-Digest Algorithm "), RFC 1321, Laboratoire
d'Informatique MIT, avril 1992.

[RFC1730] M. Crispin, " Protocole d'Accès aux Messages Internet -
Version 4 " (" Internet Message Access Protocol - Version 4 "),
RFC 1730, Université de Washington, décembre 1994.

[RFC1734] J. Myers, " Commande POP3 d'authentification " (" POP3
AUTHentication command "), RFC 1734, Carnegie Mellon, décembre 1994.

13. Considérations sur la sécurité

Il est admis que l'utilisation de la commande APOP permet une authentification de l'origine et une protection des réponses lors d'une session POP3. Par conséquent, un serveur POP3 qui implémente les deux commandes PASS et APOP ne devrait pas autoriser les deux méthodes d'accès pour un utilisateur donné ; c'est, pour une boîte aux lettres donnée, soit la séquence de commande USER/PASS, soit la commande APOP qui est autorisée, mais pas les deux.

De plus, il faut noter que lorsque la longueur du secret partagé augmente, la difficulté de trouver ce secret à partir de sommes de contrôle augmente d'autant.

Les serveurs qui répondent par -ERR à la commande USER peuvent permettre à d'éventuels pirates informatiques de trouver quels sont les noms d'utilisateur valides.

L'utilisation de la commande PASS envoie les mots de passe en clair à travers le réseau.

L'utilisation des commandes RETR et TOP envoie le courrier en clair à travers le réseau.

A part ces considérations, les problèmes de sécurité ne sont pas discutés dans ce document.

14. Remerciements

La famille des protocoles POP a eu une longue histoire mouvementée. Quoique principalement présenté comme une révision mineure du RFC 1460, POP3 s'est basé sur les idées présentées dans les RFC 918, 937 et 1081.

De plus, Alfred Grimstad, Keith Mac Cloghrie et Neil Ostroff ont donné des commentaires significatifs sur la commande APOP.

15. Adresses des Auteurs

John G. Myers
Carnegie-Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213
E-mail : jgm+@cmu.edu

Marshall T. Rose
Dover Beach Consulting, Inc.
420 Whisman Court
Mountain View, CA 94043-2186
E-mail : mrose@dbc.mtview.ca.us

Appendice A. Différences par rapport au RFC 1725

Ce document est la révision du RFC 1725, un premier essai de définition d'un Standard. Il propose les modifications suivantes par rapport à ce document :

- il clarifie le fait que les mot-clefs des commandes ne sont pas sensibles à une écriture majuscule ou minuscule.
- il spécifie que les serveurs doivent envoyer " +OK " et " -ERR " en majuscules
- il spécifie que le message de bienvenue initial est une réponse positive, plutôt que toute chaîne de caractères pouvant être éventuellement une réponse positive.
- il clarifie le comportement vis-à-vis des commandes non implémentées
- il rend les commandes USER et PASS optionnelles
- il clarifie l'ensemble des réponses possibles à la commande USER
- il inverse l'ordre des exemples des commandes USER et PASS, pour diminuer les confusions
- il clarifie le fait que la commande PASS ne peut qu'uniquement être donnée immédiatement après une commande USER ayant réussi
- il clarifie l'obligation de persistance des identificateurs utilisateur (UIDs) et ajoute quelques suggestions d'implémentation
- il spécifie les limites de la longueur d'un identificateur utilisateur entre 1 et 70 octets
- il spécifie la longueur maximale d'un indicateur d'état à 512 octets, y compris le CRLF
- il clarifie le fait que LIST sans argument sur une boîte aux lettres vide retourne un indicateur d'état positif
- il ajoute une référence à la section " Format des Messages " dans le paragraphe sur la commande LIST.

- il clarifie le comportement de QUIT lorsqu'il y a un problème important
- il clarifie la section " Considérations sur la sécurité " à propos de la recommandation de ne pas utiliser la commande USER avec la commande APOP
- il ajoute les références aux RFC 1730 et 1734
- il clarifie la méthode que peut utiliser un logiciel de messagerie pour faire entrer un courrier à l'intérieur du système de transport.
- il clarifie le fait que le second argument de la commande TOP est un nombre de lignes
- il modifie la suggestion pour un serveur de ne pas accepter à la fois PASS et APOP pour un utilisateur donné, dans la section " Considérations sur la sécurité ", passant de la suggestion " il ne doit pas " à " il ne devrait pas "
- il ajoute une section " Considérations opérationnelles et limitatives "

Appendice B. Index des commandes

<u>APOP</u>	13
<u>DELE</u>	7
<u>LIST</u>	6
<u>NOOP</u>	8
<u>PASS</u>	12
<u>QUIT</u>	5
<u>QUIT</u>	9
<u>RETR</u>	7
<u>RSET</u>	8
<u>STAT</u>	5
<u>TOP</u>	10
<u>UIDL</u>	10
<u>USER</u>	11