Groupe de travail Réseau
Request for Comments : 2645
Catégorie : En cours de normalisation

R. Gellens, Qualcomm
août 1999
Traduction Claude Brière de L'Isle

Relais de messagerie à la demande (ODMR) pour SMTP avec adresses IP dynamiques

Table des Matières

1. Résumé

Avec la diffusion de systèmes informatiques bon marché et de la connexité Internet, la demande de serveurs de messagerie locaux s'est mise à augmenter. De nombreuses personnes veulent maintenant avoir un serveur de messagerie sur un système qui a une connexion seulement intermittente avec un fournisseur de service. Si le système a une adresse IP statique, la commande ESMTP ETRN [RFC1985] peut être utilisée. Cependant, les systèmes avec des adresses IP dynamiques (qui sont très courants sur les connexions bon marché) n'ont pas de solution largement répandue.

Le présent mémoire propose un nouveau service, le relais de messagerie à la demande (ODMR, *On-Demand Mail Relay*) qui est un profil de SMTP [RFC0821], [RFC1869], qui fournit une approche du problème sûre, extensible, et facile à mettre en œuvre.

2. Conventions utilisées dans le document

Comme les rôles de client et de serveur s'inversent durant la session, pour éviter la confusion, les termes "consommateur" et "fournisseur" seront utilisés à la place de "client" et "serveur", quoique, bien sûr, ce protocole puisse être utile dans des cas autres que celui des fournisseurs et consommateurs de service commercial.

Dans les exemples, "P:" est utilisé pour indiquer les lignes envoyées par le fournisseur, et "C:" indique celles envoyées par le consommateur. Les sauts de lignes au sein d'une commande ne sont que pour faciliter la lecture.

Les mots-clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", et "PEUT" dans ce document sont à interpréter comme défini dans la [RFC2119].

Les exemples utilisent 'exemple.net' pour le fournisseur, et 'exemple.org' et ' exemple.com' pour les consommateurs.

3. Commentaires

Les commentaires privés devraient être envoyés à l'auteur. Les commentaires publics peuvent être envoyés à la liste de diffusion SMTP déconnectée de l'IETF, <ietf-disconn-smtp@imc.org>. Pour s'y inscrire, envoyer un message à <ietf-disconn-smtp-request@imc.org> contenant le mot SUBSCRIBE comme corps de message.

4. Description

Le relais de messagerie à la demande est un profil restreint de SMTP [RFC0821], [RFC1869]. L'accès 366 est réservé au relais de messagerie à la demande. Les rôles de client et serveur initial sont d'une durée limitée, car l'objectif est de permettre à l'hôte connecté de façon intermittente de demander la messagerie détenue pour lui par un fournisseur de service.

Le consommateur initie une connexion avec le fournisseur, s'authentifie, et demande ses messages. Les rôles de client et de serveur s'inversent alors, et un SMTP normal [RFC0821], [RFC1869] s'effectue.

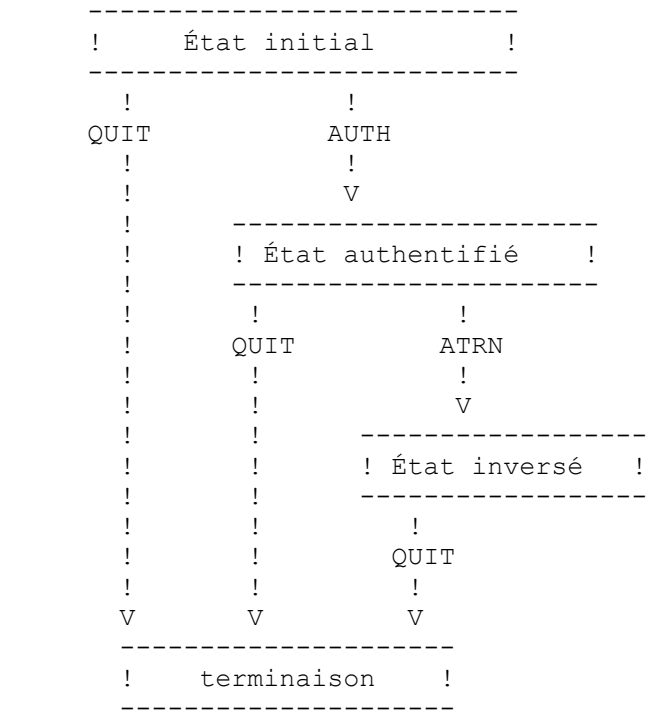
Le fournisseur a un processus d'écoute du relais de messagerie à la demande des connexions sur l'accès ODMR. Ce processus n'a pas besoin d'être un plein serveur SMTP. Il n'a pas besoin d'être un client SMTP avec accès aux files d'attentes de messagerie sortante, et en tant que serveur met en œuvre les commandes EHLO, AUTH, ATRN, et QUIT.

Un MTA a normalement un composant de client de messagerie qui traite les files d'attentes de messagerie sortante, tentant d'envoyer des messages à des domaines particuliers, sur la base du temps ou des événements (comme les nouveaux messages placés dans la file d'attente, ou la réception d'une commande ETRN par le composant de serveur SMTP). Le service de relais de messagerie à la demande ne traite pas la file d'attente sortante comme un temporisateur ou une création de nouveau message, mais à la demande.

Le côté fournisseur a les responsabilités normales d'un serveur SMTP [RFC0821], incluant de générer des notices d'échec de livraison, etc., en tant que de besoin.

8. États

Le service de relais de messagerie à la demande a trois états : un état initial, un état authentifié, et un état inversé. La progression des états est illustrée par le diagramme suivant :



(Noter que dans l'état inversé, les commandes sont envoyées par le fournisseur, et non par le consommateur.)

5.1 État initial

Dans l'état initial, le fournisseur est le serveur et le consommateur est le client. Trois commandes sont valides : EHLO, AUTH, et QUIT.

5.1.1 EHLO

La commande EHLO est la même que dans la [RFC1869]. La réponse DOIT inclure AUTH et ATRN.

5.1.2 AUTH

La commande AUTH est spécifiée dans la [RFC2554]. La commande AUTH utilise un mécanisme de la [RFC2222] pour authentifier la session. La session n'est pas considérée comme authentifiée jusqu'à ce qu'une réponse de succès à AUTH ait été envoyée.

Pour l'interopérabilité, les mises en œuvre DOIVENT prendre en charge le mécanisme CRAM-MD5 [RFC2195]. D'autres mécanismes SASL peuvent être pris en charge. Un site PEUT désactiver la prise en charge de CRAM-MD5 si il utilise des méthodes plus sûres. Le mécanisme EXTERNAL de la [RFC2222] peut être utile dans certains cas, par exemple, si le fournisseur a déjà authentifié le client, comme durant une connexion PPP.

5.1.3 QUIT

La commande QUIT est la même que dans la [RFC0821].

5.2 État authentifié

L'état authentifié est acquis après la réussite d'une commande AUTH. Deux commandes sont valides dans l'état authentifié : ATRN et QUIT.

5.2.1 ATRN (TURN authentifié)

À la différence de la commande TURN dans la [RFC0821], la commande ATRN prend facultativement un ou plusieurs domaines comme paramètre. La commande ATRN DOIT être rejetée si la session n'a pas été authentifiée. Le code de réponse 530 [RFC2554] est utilisé pour cela.

La temporisation pour cette commande DOIT être d'au moins 10 minutes pour donner au fournisseur le temps de traiter sa file d'attente de messages.

Une commande ATRN envoyée sans domaine est équivalente à une commande ATRN qui spécifie tous les domaines auxquels le consommateur a accès.

Si l'authentification utilisée par le consommateur ne fournit pas l'accès à tous les domaines spécifiés dans l'ATRN, le fournisseur NE DOIT envoyer de messages pour aucun domaine au consommateur ; le fournisseur DOIT rejeter la commande ATRN avec un code 550.

Si le consommateur a accès à tous les domaines spécifiés, mais si aucun d'eux n'a de message en file d'attente, le fournisseur rejette normalement la commande ATRN avec un code de réponse de 453. Le fournisseur PEUT à la place produire un code de réussite de 250, et après que les rôles sont inversés, envoyer un QUIT suivant le EHLO.

Le fournisseur PEUT aussi rejeter la commande ATRN avec une réponse 450 pour indiquer le refus d'accepter plusieurs demandes produites dans un certaine intervalle de temps.

Si le consommateur a accepté tous les domaines spécifiés et si il existe des messages dans au moins un d'eux, le fournisseur produit un code de succès de 250.

Si le serveur est dans l'incapacité de vérifier l'accès aux domaines demandés (par exemple, une base de données de transposition est temporairement indisponible) il envoie le code de réponse 451.

ABNF pour ATRN :
atrn = « ATRN » [SP domaine *(« , » domaine)]
domaine = sous-domaine 1*(« . » sous-domains)
sous-domains = (ALPHA / CHIFFRE) *(ldh-str)
ldh-str = *(ALPHA / CHIFFRE / « -«) (ALPHA / CHIFFRE)

5.3 État inversé

Après que le fournisseur a envoyé une réponse de succès à la commande ATRN, les rôles s'inversent, le consommateur devient le serveur, et le fournisseur devient le client.

Après avoir reçu la réponse de succès à ATRN, le consommateur envoie une ligne standard d'accueil initial SMTP. À ce point, les commandes normales SMTP [RFC0821], [RFC1869] sont utilisées. Normalement, le fournisseur envoie un EHLO après avoir vu l'accueil du consommateur, qui sera suivi d'un MAIL FROM et ainsi de suite.

5.4 Autres commandes

Le fournisseur PEUT rejeter toutes les commandes autres que EHLO, AUTH, ATRN, et QUIT, avec le code de réponse 502.

8. Exemple de session de relais de messagerie à la demande

P : 220 serveur EXEMPLE.NET de relais de messagerie à la demande prêt
C : EHLO exemple.org
P : 250-EXEMPLE.NET
P : 250-AUTH CRAM-MD5 EXTERNAL
P : 250 ATRN
C : AUTH CRAM-MD5
P : 334 MTg5Ni42OtcxNzA5NTJASVNQLkNPTQo=
C : Zm9vYmFyLm5ldCBiOTEzYTYwMmM3ZWRhN2E0OTViNGU2ZTczMzRkMzg5Mao=
P : 235 maintenant authentifié comme exemple.org
C : ATRN exemple.org,exemple.com
P : 250 OK inversant maintenant la connexion
C : 220 exemple.org prêt à recevoir des messages électroniques
P : EHLO EXEMPLE.NET
C : 250-exemple.org
C : 250 SIZE
P : MAIL FROM : <Lester.Tester@dot.foo.bar>
C : 250 OK
P : RCPT TO : <l.eva.msg@exemple.com>
C : 250 OK, receveur accepté
...
P : QUIT
C : 221 exemple.org clôt la connexion

7. Codes de réponse

Les codes de réponse utilisés dans le présent document sont :
250 Action de messagerie demandée acceptée, terminée
450 Demande ATRN refusée
451 Incapable de traiter maintenant la demande ATRN
453 Vous n'avez pas de message
502 Commande non mise en œuvre
530 Authentification exigée [RFC2554]

8. Considérations pour la sécurité

Parce que l'accès au serveur de relais de messagerie à la demande n'est utile que sur accord préalable entre les parties (de sorte que le fournisseur est la cible des enregistrements MX pour les domaines du consommateur et a donc de la messagerie à relayer) il peut être utile pour le fournisseur de restreindre l'accès au relais de messagerie à la demande. Par exemple, le serveur ODMR pourrait être configurable, ou un enveloppeur TCP ou un pare-feu pourrait être utilisé, pour bloquer l'accès au port 366 sauf au sein du réseau du fournisseur. Cela peut être utile quand le fournisseur est le FAI du consommateur. L'utilisation de tels mécanismes ne réduit pas cependant le besoin de la commande AUTH, mais peut augmenter la sécurité qu'elle fournit.

L'utilisation de SASL dans la commande AUTH permet la substitution à l'avenir de plus de mécanismes sûrs d'authentification.

Voir les paragraphes 5.1.2 et 5.2.1 pour plus de détails sur la sécurité.

9. Remerciements

Le présent mémoire a été développé en partie sur la base des commentaires et discussions qui ont eu lieu sur la liste de diffusion IETF-disconn-smtp. Des remerciements particuliers à Chris Newman et Ned Freed pour leurs commentaires.

10. Références

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

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

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

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

[RFC2195] J. Klensin et autres, "Extension IMAP/POP AUTHorize pour mise au défi/réponse simple", septembre 1997. *(P.S.)*

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

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

[RFC2554] J. Myers, "Extension de service SMTP pour l'authentification", mars 1999. (*Obsolète, voir* RFC4954) *(P.S.)*

11. Adresse de l'auteur

Randall Gellens
QUALCOMM Incorporated
5775 Morehouse Dr.
San Diego, CA 92121-2779
U.S.A.

téléphone : +1.619.651.5115
mél : randy@qualcomm.com

12. Déclaration complète de droits de reproduction

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