

Groupe de travail Réseau

G. Vaudreuil, Lucent Technologies

Request for Comments : 4238

Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

octobre 2005

Service d'acheminement de messagerie vocale

Statut de ce mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

La messagerie vocale est traditionnellement traitée en utilisant l'adresse du numéro de téléphone. Le présent document décrit deux techniques pour acheminer les messages vocaux sur la base d'un numéro de téléphone. Le service complet utilise le service de répertoire de profil vocal pour la messagerie Internet (VPIM, *Voice Profile for Internet Mail*) pour chercher une adresse de messagerie électronique VPIM avec un numéro de téléphone et confirmer que l'adresse est à la fois valide et associée au destinataire prévu. Cependant, à court terme, ce service va prendre du temps pour se déployer rapidement. Le présent document décrit aussi un service de base d'envoi " au petit bonheur" qui achemine et livre les messages en utilisant seulement le service de résolution de numéro de téléphone ENUM et les facilités existantes d'acheminement de la messagerie du DNS.

Table des matières

1. Objectifs de conception.....	1
2. Service complet.....	2
2.1 Spécification du service "E2U+VPIM:LDAP".....	2
2.2 Découverte de répertoire VPIM.....	2
2.3 Interrogation d'adresse.....	3
3. Service de base.....	3
3.1 Spécification du service "E2U+VPIM:Mailto:".....	3
3.2 Construction d'adresse.....	3
3.3 Acheminement de message interdomaine.....	3
3.4 Acheminement de message intradomaine.....	3
4. Considérations sur la sécurité.....	4
4.1 Messagerie non sollicitée.....	4
4.2 Attaques fondées sur le DNS.....	4
5. Considérations relatives à l'IANA.....	4
6. Références.....	4
6.1 Références normatives.....	4
6.2 Références pour information.....	5
Remerciements.....	5
Adresse de l'auteur.....	5
Déclaration complète de droits de reproduction.....	5

1. Objectifs de conception

Ce profil est destiné à fournir une gamme de capacités fonctionnelles pour l'acheminement des messages sur la base d'un de deux mécanismes. Le service le plus complet devrait utiliser le service de résolution d'adresse ENUM pour déterminer le répertoire VPIM, et ensuite utiliser LDAP pour restituer l'adresse de messagerie électronique spécifique de VPIM qui sera utilisée pour l'acheminement de message.

Le service plus basique d'envoi au petit bonheur utilise seulement le service ENUM et des enregistrements MX pour acheminer le message au domaine du receveur prévu. L'intelligence pour finir l'acheminement du message au receveur prévu est placée au sein du système d'acheminement de message du domaine du receveur.

Le mécanisme de base peut être utilisé même quand il y a un service de répertoire VPIM disponible. Le service de base est utile quand les interrogations de LDAP ne sont pas disponibles, comme ce peut être le cas pour des terminaux mobiles déconnectés ou à cause de pare-feu ou de politiques de sécurité de l'information.

Le mécanisme de base devrait faciliter l'acheminement des messages VPIM à une destination interne convenable avec un minimum de configuration. Un but important est d'éviter qu'un traitement de contenu détermine la nature du message et sa destination interne. Au minimum, il devrait être possible d'établir une simple règle de transmission de messagerie qui envoie tous les messages VPIM entrants à un système désigné, tout en facilitant l'acheminement des télécopies, messages courts, et autres messages à adresse téléphonique aux autres systèmes potentiellement différents.

Le but est que les mécanismes décrits dans le présent document soient extensibles pour tous les services de messagerie à livraison différée avec des adresses de numéro de téléphone.

Un objectif est que les étapes de découverte de répertoire VPIM et d'interrogation du répertoire VPIM se produisent dans les contraintes de délai prévues pour les interfaces d'utilisateur dans le réseau téléphonique public commuté. 95 % du temps, cette contrainte peut être une réponse en deux secondes.

2. Service complet

Pour le service complet d'acheminement de message VPIM, le client envoyeur DEVRAIT interroger le répertoire VPIM sur l'adresse de messagerie électronique spécifique de VPIM. Le client DEVRAIT utiliser le service ENUM pour restituer l'identité du répertoire VPIM à interroger. Le client devrait ensuite interroger ce serveur sur l'adresse de messagerie électronique et sur tous les attributs supplémentaires désirés.

2.1 Spécification du service "E2U+VPIM:LDAP"

- * Nom du service : E.164 to VPIM LDAP URL
- * Type d'URI : "LDAP:"
- * Type : VPIM
- * Sous type : LDAP
- * Spécification fonctionnelle : voir les paragraphes 3.2 et 3.3
- * Usage prévu : COMMUN
- * Auteur : Greg Vaudreuil (gregv@ieee.org)
- * Considérations de sécurité :
 - o Redirection malveillante : un des dangers fondamentaux relatifs à tout service comme celui-ci est celui d'une entrée malveillante dans la base de données d'un résolveur qui va conduire les clients à résoudre le E.164 en un mauvais URL LDAP. L'intention possible peut être de causer la connexion du client à un serveur LDAP félon et la restitution (ou l'échec à restituer) une ressource contenant des informations frauduleuses ou dommageables.
 - o Dénier de service : en supprimant l'URL auquel transpose le E.164, un intrus malveillant peut supprimer la capacité du client à accéder au serveur d'adresses LDAP.

2.2 Découverte de répertoire VPIM

Le serveur de répertoire VPIM est trouvé en utilisant le protocole ENUM et en interrogeant le service VPIMDIR associé au numéro de téléphone du receveur.

Le nom d'interrogation DNS est créé comme décrit dans la [RFC3761]. Le numéro de téléphone utilisé pour la localisation du répertoire PEUT contenir des informations de sous adresse supplémentaires avec des chiffres supplémentaires.

Exemple :

Interrogation : 2.1.2.1.5.5.3.1.6.1.e164.arpa

Réponses :

```
IN NAPTR 10 10 "U" "E2U+VPIM:LDAP" \ "!^.*$!ldap://vdir1.Zcorp.com/telephoneNumber=\1!" .
IN NAPTR 10 20 "U" "E2U+VPIM:LDAP" \ "!^.*$!ldap://vdir2.Zcorp.com/telephoneNumber=\1!" .
```

Il est recommandé que les serveurs VPIMDIR soient déployés dans une configuration redondante. Les champs de poids NAPTR permettent de donner des poids différents à deux enregistrements indiquant les mêmes services et préférences. Le

même poids peut être spécifié pour une distribution aléatoire entre les deux serveurs. Voir les [RFC3401], [RFC3402], [RFC3403], [RFC3404]

2.3 Interrogation d'adresse

Une fois le répertoire VPIM découvert, le client DEVRAIT produire une interrogation LDAP pour vPIMrFC822Mailbox, c'est-à-dire, l'adresse qui DEVRAIT être utilisée comme valeur pour le champ RFC 822 To: et pour la commande SMTP RCPT. Voir la [RFC4237].

3. Service de base

Le service de base s'appuie sur les règles de réécriture NAPTR pour construire mécaniquement une adresse valide de messagerie électronique spécifique de VPIM. Dans le domaine du receveur, l'adresse construite peut être encore acheminée en utilisant des techniques d'acheminement de messagerie intra domaine.

Pour faciliter une pleine gamme d'options d'acheminement intra domaine, l'adresse de messagerie électronique construite indique que le message est un message VPIM. Pour faciliter le traitement dans le système d'acheminement de messagerie intra domaine du receveur, l'indication que le message est un message VPIM DEVRAIT être dans la portion "nom de domaine".

Noter qu'il n'est pas garanti que l'adresse construite soit valide, ni que l'adresse construite corresponde au receveur prévu. Comme aucune information de capacité n'est fournie sur le receveur, les messages envoyés avec ce mécanisme DEVRAIENT être envoyés en utilisant seulement les types de support et de contenu du profil VPIM v2.

3.1 Spécification du service "E2U+VPIM:Mailto:"

- * Nom du service : E.164 to VPIM MailTo: URL
- * Type d'URI : "Mailto:"
- * Type : VPIM
- * Sous type : MAILTO
- * Spécification fonctionnelle : voir les paragraphes 4.2 à 4.4
- * Usage prévu : COMMUN
- * Auteur : Greg Vaudreuil (gregv@ieee.org)
- * Conditions d'erreur :
 - o le numéro E.164 n'est pas dans le plan de numérotage
 - o le numéro E.164 est dans le plan de numérotage, mais aucun URL n'existe pour ce numéro
 - o service E2U+VPIM:Mailto indisponible
- * Considérations de sécurité :
 - o Redirection malveillante : un des dangers fondamentaux relatifs à tous les services comme celui-ci est qu'une entrée malveillante dans la base de données d'un résolveur va amener les clients à résoudre le E.164 en un mauvais URL de messagerie électronique. L'intention possible peut être d'amener le client à envoyer les informations à une destination incorrecte.
 - o Déni de service : en supprimant l'URL auquel transpose le E.164, un intrus malveillant peut supprimer la capacité du client à accéder à la ressource.
 - o Messagerie non sollicitée : l'exposition des adresses de messagerie à travers le service ENUM fournit un accès pour l'émission de messages en masse à de grands nombres d'adresses de messagerie électronique dont seul le numéro de téléphone était d'abord connu.

3.2 Construction d'adresse

Construire une adresse de messagerie électronique VPIM en utilisant les règles de réécriture d'adresse des enregistrements NAPTR associés au service VPIM.

3.3 Acheminement de message interdomaine

L'acheminement inter domaine d'une adresse construite avec VPIM est mécaniquement indistinguable de l'acheminement de messagerie électronique existant. Aucun changement de l'infrastructure n'est requis. Le système expéditeur consulte le système des noms de domaines sur un enregistrement MX correspondant au nom de domaine et transmet le message au système indiqué.

3.4 Acheminement de message intradomaine

Au sein du domaine du receveur, le message peut encore être acheminé au système de messagerie approprié. Deux mécanismes généraux peuvent être utilisés pour poursuivre l'acheminement du message au système prévu au sein d'un réseau.

Note : ce paragraphe est strictement informatif. Les mécanismes pour l'acheminement intra domaine sont une affaire interne du domaine et n'affectent pas le protocole. Il est seulement nécessaire que les adresses créées par les règles de réécriture de NAPTR aient une signification pour le domaine qui les annonce. Cependant, une convention pour la création et l'utilisation de telles adresses peut être utile.

3.4.1 Acheminement à capacité de répertoire

Divers mécanismes de répertoire propriétaires fournissent des moyens pour qu'un routeur de messagerie entrante du domaine du receveur envoie un message à l'hôte de messagerie interne approprié. Dans de nombreux cas, la partie locale de l'adresse est utilisée pour interroger sur une adresse de messagerie interne. Cette adresse de messagerie interne est substituée à l'adresse RCPT SMTP et utilisée pour livrer le message à la boîte aux lettres du receveur. Noter que la boîte aux lettres n'a pas besoin d'avoir connaissance de l'adresse construite mécaniquement sur la base du numéro de téléphone.

Exemple d'adresse : +12145551212@sp.net

3.4.2 Acheminement de messagerie fondé sur le service

Autrement, une passerelle de messagerie peut simplement envoyer tous les messages vocaux dans un système de messagerie séparé. Ce système peut être un seul serveur de messagerie vocale ou une passerelle spécifique du service dans un plus grand réseau de messagerie vocale fondé sur le numéro de téléphone.

Une telle passerelle de messagerie peut être provisionnée avec une simple règle ou un petit ensemble de règles pour transmettre tous les messages d'un certain type de service à un serveur prédéfini. Cette règle vérifierait que le nom de service "VPIM" a un préfixe pour le nom de domaine construit pour réacheminer les messages.

Exemple d'adresse : +12145551212@VPIM.sp.net

4. Considérations sur la sécurité

Il y a peu d'informations divulguées à l'expéditeur du message qui ne soient déjà divulguées en utilisant les protocoles standard de messagerie électronique. La capacité d'utiliser ce protocole pour sonder les adresses valides est identique à l'envoi de messages d'essai et l'attente d'une notification de non livraison en retour.

4.1 Messagerie non sollicitée

Cependant, l'utilisation d'enregistrements ENUM pour créer des adresses de messagerie électronique acheminables à partir de numéros de téléphone fournit aux émetteurs de messages en masse la capacité d'envoyer de la messagerie à un grand ensemble de receveurs dont seul le numéro de téléphone est connu et où les numéros de téléphone sont devinés au hasard.

4.2 Attaques fondées sur le DNS

Les deux services, complet et de base s'appuient sur le DNS pour fournir les informations nécessaires pour valider un receveur ou envoyer un message. L'expéditeur de message est un utilisateur occasionnel, non authentifié des serveurs indiqués, et il s'appuie sur le DNS pour des informations précises. Si le DNS est compromis, un attaquant peut rediriger les messages en fournissant une adresse de messagerie électronique malveillante ou en indiquant un répertoire félon avec des URL LDAP malveillants. L'utilisation des protocoles de sécurité du DNS [RFC4033] réduit substantiellement le risque qu'un domaine soit pris en otage. Si la zone E.164 est sécurisée avec DNSSEC, l'attaque est alors empêchée si le client peut faire confiance à la clé utilisée pour signer la zone. La sécurité du DNS ne protège pas contre la compromission indépendante du service LDAP. Une discussion plus approfondie du risque pour ce service LDAP est fournie dans la [RFC4237].

5. Considérations relatives à l'IANA

La présente spécification enregistre les services E2U+VPIM:LDAP et E2U+VPIM:Mailto conformément aux spécifications et lignes directrices de la [RFC3761] et aux définitions du présent document.

6 Références

6.1 Références normatives

- [RFC3401] M. Mealling, "[Système de découverte dynamique de délégation](#) (DDDS) Partie I : DDDS complet", octobre 2002. (*Info.*)
- [RFC3402] M. Mealling, "Système de découverte dynamique de délégation ([DDDS](#)) [Partie II : l'algorithme](#)", octobre 2002. (*P.S.*)
- [RFC3403] M. Mealling, "Système de découverte dynamique de délégation ([DDDS](#)) [Partie III : base de données du système](#) de noms de domaines (DNS)", octobre 2002. (*P.S.*)
- [RFC3404] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie IV : [Identifiants de ressource uniformes](#) (URI)", octobre 2002. (*P.S.*)
- [RFC3761] P. Faltstrom, M. Mealling, "Application de E.164 au système de découverte dynamique de délégation (DDDS) d'identifiants de ressource uniformes (URI) (ENUM)", avril 2004. (*P.S.*) (*Obsolète, voir la RFC6116*)
- [RFC4237] G. Vaudreuil, "[Service d'annuaire de messagerie vocale](#)", octobre 2005. (*P.S.*)

6.2 Références pour information

- [RFC3801] G. Vaudreuil, G. Parsons, "[Profil vocal pour la messagerie Internet](#) - version 2 (VPIMv2)", juin 2004. (*D.S.*)
- [RFC4033] R. Arends, et autres, "Introduction et [exigences pour la sécurité du DNS](#)", mars 2005.

Remerciements

Le présent schéma de répertoire s'appuie sur un travail antérieur de Carl Malamud et Marshall Rose dans leur expérience d'impression à distance et sur le travail conduit par Anne Brown au titre de l'essai sur les répertoires du comité pour la messagerie vocale de l'EMA. Anne Brown a assuré la direction et était co-auteur de la version originale du présent document.

Bernhard Elliot, travaillant avec le TMIA, a fourni la plus grande partie de l'impulsion organisationnelle pour faire avancer ce projet, ce qui était une tâche substantielle étant donnée la nature parfois lente et bureaucratique de l'industrie de la messagerie vocale et de l'environnement réglementaire.

Merci à Dave Dudley et à l'Alliance pour la messagerie (TMA, *The Messaging Alliance*) pour leurs travaux de pionniers sur un service partagé de répertoires pour la messagerie vocale et pour leurs efforts soutenus à la poursuite de ce travail.

Greg White et Jeff Bouis, de Lucent Technologies, ont fourni une assistance précieuse de relecture et de vérification. D'innombrables erreurs et incohérences ont été corrigées grâce à leur relecture attentive.

Comme président du groupe de travail VPIM, Glenn Parsons a fourni un soutien essentiel pendant les nombreuses années où ce document a été en développement.

Adresse de l'auteur

Prière d'envoyer les commentaires sur ce document à la liste de diffusion du groupe de travail VPIM à <vpim@ietf.org>.

Gregory M. Vaudreuil
Lucent Technologies
9489 Bartgis Ct
Frederick, MD 21702
US
mél : GregV@ieec.org

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

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

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

Propriété intellectuelle

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

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

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

Remerciement

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