

Groupe de travail Réseau
Request for Comments : 3361
Catégorie : En cours de normalisation

H. Schulzrinne, Columbia University
août 2002
Traduction Claude Brière de L'Isle

Option du protocole de configuration dynamique d'hôte (DHCPv4) pour les serveurs du protocole d'initialisation de session (SIP)

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de 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 (2002). Tous droits réservés

Résumé

Le présent document définit une option du protocole de configuration dynamique d'hôte (DHCPv4, *Dynamic Host Configuration Protocol for IPv4*) qui contient une liste de noms de domaines ou d'adresses IPv4 qui peuvent être transposés en un ou plusieurs serveurs mandataires de sortie du protocole d'initialisation de session (SIP, *Session Initiation Protocol*). C'est une des nombreuses méthodes que peut utiliser un client SIP pour obtenir les adresses d'un tel serveur SIP local.

1. Terminologie

Client DHCP : selon la [RFC2131] c'est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration tels qu'une adresse réseau.

Serveur DHCP : c'est un hôte Internet qui retourne les paramètres de configuration aux clients DHCP.

Serveur SIP : comme défini dans la [RFC3261]. Ce serveur DOIT être un serveur mandataire de sortie, comme défini dans la [RFC3263]. Dans le contexte de ce document, un serveur SIP se réfère à l'hôte sur lequel fonctionne le serveur SIP.

Client SIP : comme défini dans la [RFC3261]. Le client peut être un client d'agent d'utilisateur ou la portion client d'un serveur mandataire. Dans le contexte de ce document, un client SIP se réfère à l'hôte sur lequel fonctionne le client SIP.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Introduction

Le protocole d'initialisation de session (SIP) [RFC3261] est un protocole de contrôle de couche application qui peut établir, modifier et terminer des sessions ou appels multimédia. Un système SIP a un certain nombre de composants logiques : agents d'utilisateur, serveurs mandataires, serveurs de redirection et registraires. Les agents d'utilisateur PEUVENT contenir des clients SIP, les serveurs mandataires en contiennent toujours. Le présent document spécifie une option DHCP [RFC1035], [RFC3396] qui permet aux clients SIP de localiser un serveur SIP local qui est à utiliser pour toutes les demandes SIP sortantes, ce qu'on appelle un serveur mandataire de sortie. (Les clients SIP PEUVENT contacter directement l'adresse identifiée dans l'URL SIP, sans impliquer de serveur SIP local. Cependant, dans certaines circonstances, par exemple, lorsque des pare-feu sont présents, les clients SIP ont besoin d'utiliser un serveur local pour les demandes sortantes.) C'est une des nombreuses solutions possibles pour localiser le serveur SIP sortant ; la configuration manuelle en est un autre exemple.

3. Option DHCP de serveur SIP

L'option DHCP de serveur SIP porte soit une adresse (binaire) IPv4 de 32 bits, soit, de préférence, un nom de domaine DNS ([RFC1035]) pleinement qualifié à utiliser par le client SIP pour localiser un serveur SIP.

L'option a deux codages, spécifiés par l'octet de codage ('enc') qui suit l'octet de code. Si l'octet de codage a la valeur 0, il est suivi par une liste de noms de domaines, comme décrit ci-dessous (paragraphe 3.1). Si l'octet de codage a la valeur 1, il est suivi par une ou plusieurs adresses IPv4 (paragraphe 3.2). Toutes les mises en œuvre DOIVENT prendre en charge les deux codages. Le champ 'Longueur' indique le nombre total d'octets de l'option qui suit le champ 'Longueur', incluant l'octet de codage.

Un serveur DHCP NE DOIT PAS mélanger les deux codages dans le même message DHCP, même si il envoie deux différentes instances de la même option. Toute tentative de le faire résulterait en un comportement incorrect du client car les règles du traitement de DHCP imposent l'enchaînement de plusieurs instances d'une option dans une seule option avant de traiter l'option [RFC3396].

Le code pour cette option est 120.

3.1 Liste de noms de domaines

Si l'octet 'enc' a une valeur de 0, l'octet de codage est suivi par une séquence d'étiquettes, codées selon le paragraphe 3.1 de la [RFC1035], citée ci-après : "Les noms de domaines dans les messages sont exprimés en termes de séquence d'étiquettes. Chaque étiquette est représentée par un champ de longueur d'un octet suivi par ce nombre d'octets. Comme chaque nom de domaine se termine par l'étiquette nulle de la racine, un nom de domaine se termine par un octet longueur de zéro. Les deux bits de poids fort de chaque octet de longueur doivent être à zéro, et les six bits restants du champ longueur limitent l'étiquette à 63 octets ou moins. Pour simplifier la mise en œuvre, la longueur totale d'un nom de domaine (c'est-à-dire, octets d'étiquette et octets de longueur d'étiquette) est restreinte à 255 octets ou moins.

Le codage de la [RFC1035] a été choisi pour s'accommoder des futurs mécanismes d'internationalisation des noms de domaine.

La longueur minimale de ce codage est 3.

L'option PEUT contenir plusieurs noms de domaines, mais ils DEVRAIENT se référer à des enregistrements NAPTR différents, plutôt qu'à des enregistrements A différents. Le client DOIT essayer les enregistrements dans l'ordre dans lequel ils sont donnés, en appliquant le mécanisme décrit au paragraphe 4.1 de la [RFC3263] à chacun. Le client ne résout les noms de domaine suivants que si le premier qu'il tente de contacter échoue ou ne donne pas de protocole de transport commun entre le client et le serveur ou note un domaine interdit administrativement par la politique du client.

L'utilisation de plusieurs noms de domaine n'est pas destinée à remplacer les enregistrements NAPTR et SRV, mais plutôt à permettre à un seul serveur DHCP d'indiquer les serveurs mandataires de sortie gérés par les divers opérateurs.

Les clients DOIVENT prendre en charge la compression conformément au codage du paragraphe 4.1.4 de la [RFC1035] "Noms de domaines – mise en œuvre et spécification".

Cependant, comme les noms de domaines sont supposés être de domaines différents, la compression aura vraisemblablement peu d'effet.

Si la longueur de la liste des domaines excède le maximum permis avec une seule option (254 octets) la liste de domaines DOIT être représentée dans le message DHCP comme spécifié dans la [RFC3396].

L'option DHCP pour ce codage a le format suivant :

```

Code Long. Code  Nom DNS du serveur SIP
+-----+-----+-----+-----+-----+-----+-----+-----+
| 120 |  n  |  0  |  s1 |  s2 |  s3 |  s4 |  s5 |  ...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Par exemple, considérons le cas où le serveur veut offrir deux serveurs mandataires de sortie, "example.com" et "example.net". Ils seraient codés comme suit :

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|120|27| |0| |7| |'e'|'x'|'a'|'m'|'p'|'l'|'e'| |3| |'c'|'o'|'m'| |0| |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|'e'|'x'|'a'|'m'|'p'|'l'|'e'| |3| |'n'|'e'|'t'| |0| | +-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

3.2 Liste d'adresses IPv4

Si l'octet 'enc' a une valeur de 1, l'octet codeur est suivi par une liste d'adresses IPv4 qui indiquent les serveurs mandataires sortant SIP disponibles pour le client. Les serveurs DOIVENT être énumérés dans l'ordre de préférence.

Sa longueur minimum est 5, et la longueur DOIT être un multiple de 4 plus un. L'option DHCP pour ce codage a le format suivant :

Code	Long.	Code	Adresse 1				Adresse 2		
120	n	1	a1	a2	a3	a4	a1	...	

4. Considérations pour la sécurité

Les considérations pour la sécurité des [RFC2131], [RFC3261] et [RFC3263] s'appliquent. Si un adversaire s'arrange pour modifier la réponse d'un serveur DHCP ou pour insérer sa propre réponse, un agent d'utilisateur SIP pourrait être conduit à contacter un serveur SIP pirate, qui pourrait éventuellement intercepter alors les demandes d'appel ou dénier le service. Une réponse DHCP modifiée pourrait aussi omettre les noms d'hôte qui traduisent en des serveurs SIP fondés sur TLS, facilitant ainsi l'interception.

5. Considérations relatives à l'IANA

L'IANA a alloué le numéro d'option DHCP de 120 pour l'option DHCP de serveur SIP définie dans le présent document.

6. Remerciements

Ralph Droms, Robert Elz, Wenyu Jiang, Peter Koch, Gautam Nair, Thomas Narten, Erik Nordmark, Jonathan Rosenberg, Kundan Singh, Sven Ubik, Bernie Volz et Dean Willis ont fourni des retours utiles tout au long de l'évolution de ce document.

7. Bibliographie

- [RFC1035] P. Mockapetris, "Noms de domaines – [Mise en œuvre](#) et spécification", STD 13, novembre 1987. (*MàJ par la RFC6604*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2131] R. Droms, "Protocole de [configuration dynamique d'hôte](#)", mars 1997. (*Mise à jour par les RFC 3396 et 4361*)
- [RFC2132] S. Alexander et R. Droms, "Options DHCP et [Extensions de fabricant BOOTP](#)", mars 1997.
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (*Mise à jour par RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665*)
- [RFC3263] J. Rosenberg, H. Schulzrinne, "Protocole d'initialisation de session (SIP) : [Localisation des serveurs SIP](#)", juin 2002. (*Remplace RFC2543*) (P.S.)

[RFC3396] T. Lemon et S. Cheshire, "[Codage d'options longues](#) dans le protocole de configuration dynamique d'hôte (DHCPv4)", novembre 2002.

8. Adresse de l'auteur

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA
mél : schulzrinne@cs.columbia.edu

9. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2002). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations y 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.

Remerciement

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