

Groupe de travail Réseau
Request for Comments : 3203
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

Y. T'Joens & C. Hublet, Alcatel
P. De Schrijver, Mind
décembre 2001

Extension DHCP Reconfigure

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 (2001). Tous droits réservés.

Résumé

Le présent document définit des extensions à DHCP (protocole de configuration dynamique d'hôte) pour permettre la reconfiguration dynamique d'un seul hôte déclenchée par le serveur DHCP (par exemple, une nouvelle adresse IP et/ou des paramètres locaux de configuration). Cela est réalisé par l'introduction d'un message FORCERENEW en envoi individuel qui force le client à l'état RENEW. Le comportement pour les hôtes qui utilisent le message DHCP INFORM pour obtenir des informations de configuration est aussi décrit.

1. Introduction

Les procédures décrites dans le présent document permettent la reconfiguration dynamique des hôtes individuels.

1.1 Conventions

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT" et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Renouvellement forcé DHCP

La présente section décrit l'extension de message FORCERENEW.

2.1 Terminologie

Client DHCP : c'est l'hôte à reconfigurer en utilisant DHCP.

Serveur DHCP : c'est le serveur qui configure le client DHCP.

2.2 Procédures de renouvellement forcé

Le serveur DHCP envoie un message FORCERENEW en envoi individuel au client. À réception du message FORCERENEW en envoi individuel, le client va changer son état en état RENEW, et va ensuite essayer de renouveler son bail selon les procédures DHCP normales. Si le serveur veut allouer une nouvelle adresse IP au client, il va répondre au message DHCP REQUEST par un DHCP NAK. Le client va alors revenir à l'état init et diffuser un message DHCP DISCOVER. Le serveur peut maintenant allouer une nouvelle adresse IP au client en répondant par un DHCP OFFER. Si le message FORCERENEW est perdu, le serveur DHCP ne va pas recevoir une DHCP REQUEST du client et il devrait retransmettre le message FORCERENEW en utilisant un algorithme de retard exponentiel. Selon la bande passante du réseau entre le serveur et le client, le serveur devrait choisir un délai. Ce délai augmente de façon exponentielle lors d'un échec de retransmission. Le nombre des retransmissions devrait être limité.

Les procédures décrites ci-dessus supposent que le serveur envoie un message FORCERENEW en envoi individuel au client. La réception d'un message FORCERENEW en diffusion groupée devrait être éliminée en silence par le client.

Il se peut qu'un client ait obtenu une adresse réseau par d'autres moyens (par exemple, par configuration manuelle) et ait utilisé une demande DHCP INFORM pour obtenir d'autres paramètres locaux de configuration. De tels clients devraient répondre à la réception d'un message FORCERENEW en envoi individuel par une nouvelle demande DHCP INFORM de façon à obtenir un éventuel ensemble nouveau de paramètres locaux de configuration. Noter que l'usage de ces procédures est limité à l'ensemble d'options qui sont éligibles pour configuration par DHCP et ne devrait pas subroger les paramètres configurés manuellement.

Noter de plus que l'usage du message FORCERENEW pour reconfigurer une adresse de client ou des paramètres locaux de configuration peut conduire à l'interruption de sessions actives, et qu'à ce titre, ces procédures devraient être utilisées dans des circonstances bien contrôlées.

2.3 Exemple d'utilisation

2.3.1 Clients DHCP incorporés

L'autoconfiguration de passerelles locales (plus généralement un équipement de terminaison de réseau) pour les besoins du réseautage public peut être réalisée au moyen de DHCP, comme décrit dans la [RFC2131]. Afin de permettre des changements de service ou une interruption de service, le message FORCERENEW peut déclencher la prise de contact du serveur DHCP par la passerelle locale, avant l'arrivée à expiration du prêt.

2.3.2 Scénario de service d'hospitalité

Dans les réseaux auto provisionnés, par exemple, des chambres d'hôtel, le serveur DHCP possédé par l'hôtel peut permettre une utilisation limitée des adresses IP, ce qui autorise l'usager à consommer des services locaux ou à choisir des services externes à partir d'une interface de navigateur de la Toile. Afin de permettre des services externes par d'autres fournisseurs de services, par exemple, des services de l'Internet mondial ou des services de VPN d'entreprise, le serveur DHCP peut faire que le client demande une nouvelle session d'initialisation DHCP de façon à obtenir, par exemple, une adresse IP à acheminement mondial.

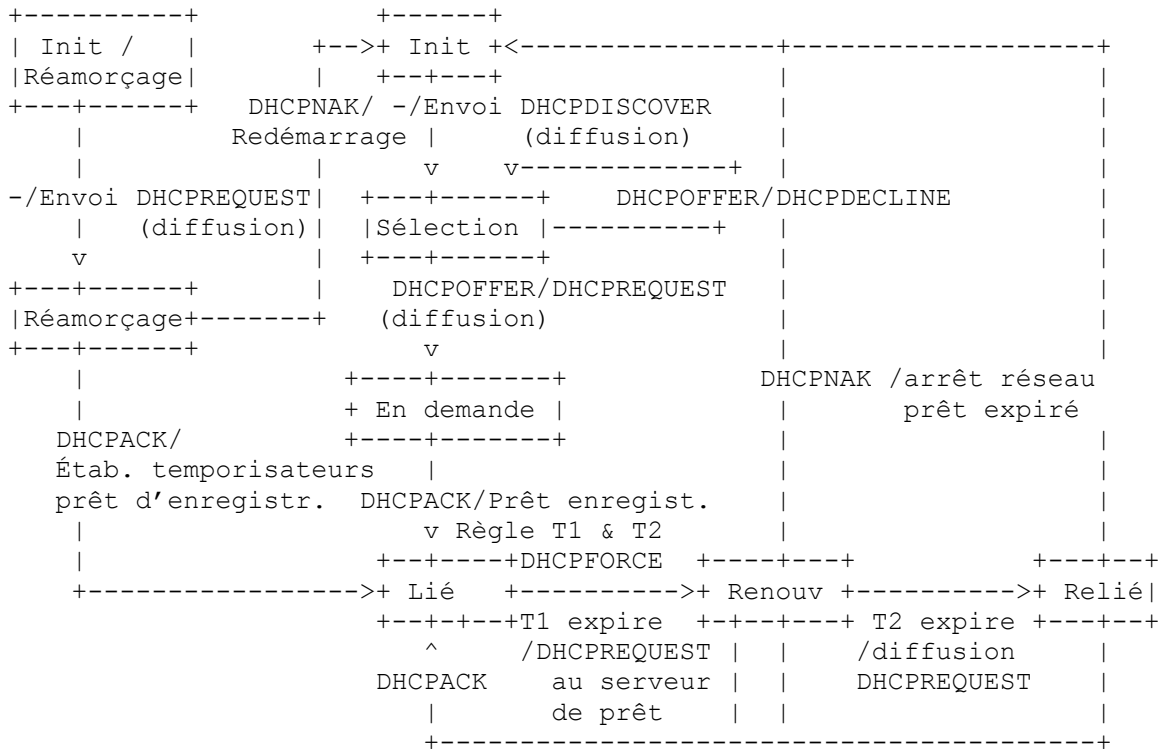
2.3.3 Dénomérotation de réseau

Dans des conditions étroitement contrôlées, les procédures FORCERENEW peuvent être utilisées pour passer en force la dénomérotation de sous-réseaux entiers, client par client, sous le contrôle d'un serveur DHCP.

2.4 Raisons

L'approche, telle que décrite dans le présent document, a un certain nombre d'avantages. Elle n'exige pas d'ajouter de nouveaux états à la mise en œuvre du client DHCP. Cela minimise la quantité de code à changer. Cela permet aussi que le renouvellement (RENEWAL) du prêt soit piloté par le serveur, ce qui peut être utilisé pour optimiser l'usage du réseau ou de la charge du serveur DHCP.

3. Diagramme d'état étendu de DHCP



4. Disposition du message

Le message FORCERENEW utilise la disposition normale de message DHCP avec l'introduction d'un nouveau type de message DHCP. L'option DHCP 53 (type de message DHCP) est étendue avec une nouvelle valeur : DHCPFORCERENEW (9)

5. Considérations relatives à l'IANA

La nouvelle valeur pour l'option DHCP 53 (type de message DHCP) pour indiquer un message DHCPFORCERENEW est 9.

6. Considérations sur la sécurité

Comme dans certains environnements de réseau, FORCERENEW peut être utilisé pour espionner et falsifier le trafic, le message FORCERENEW DOIT être authentifié en utilisant les procédures décrites dans la [RFC3118]. Les messages FORCERENEW qui échouent à l'authentification devraient être éliminés en silence par le client.

6.1 Faiblesses du protocole

Le mécanisme décrit dans le présent document est vulnérable à une attaque de déni de service par l'inondation d'un client avec des messages FORCERENEW bogués. Les calculs impliqués dans l'authentification des messages FORECERENEW bogués peut submerger l'appareil sur lequel fonctionne le client.

7. Références

[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](#)*)

[RFC3118] R. Droms et W. Arbaugh, "[Authentification des messages](#) DHCP", juin 2001.

[DSL_autoconf] Technical Report TR-044, "Auto-Configuration for Basic Internet (IP-based) Services", DSL Forum, novembre 2001

8. Remerciements

Les auteurs tiennent à remercier David Allan, de Nortel, de ses commentaires constructifs sur ces procédures.

9. Adresse des auteurs

Yves T'joens
Alcatel Network Strategy Group
Francis Wellesplein 1,
2018 Antwerp, Belgium
téléphone : +32 3 240 7890
mél : yves.tjoens@alcatel.be

Peter De Schrijver
Mind NV
Vaartkom 11
3000 Leuven
mél : p2@mind.be

Christian Hublet
Alcatel Broadband Networking Division
Veldkant 33b,
2550 Kontich, Belgium
téléphone : +32 3 450 3322
mél : Christian.Hublet@alcatel.be

10. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2001). 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 copyright ci-dessus et le présent et 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 copyright 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 copyright 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 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.