Internet Engineering Task Force (IETF)
Request for Comments : 6891
STD : 75
RFC rendues obsolètes : 2671, 2673
Catégorie : Sur la voie de la normalisation
ISSN : 2070-1721

J. Damas, Bond Internet Systems
M. Graff
P. Vixie, Internet Systems Consortium
avril 2013

Traduction Claude Brière de L'Isle

Mécanismes d'extension pour le DNS (EDNS(0))

Résumé
Le protocole réseau du système des noms de domaines inclut un certain nombre de champs fixes dont la gamme est ou va être prochainement épuisée et ne permet pas aux demandeurs d'annoncer leurs capacités aux répondeurs. Le présent document décrit des mécanismes rétro-compatibles pour permettre la croissance du protocole.

Le présent document met à jour la spécification des mécanismes d'extension pour le DNS (EDNS(0)) (et rend obsolète la RFC 2671) sur la base des retours de l'expérience du déploiement dans plusieurs mises en œuvre. Il rend aussi obsolète la RFC 2673 ("Étiquettes binaires dans le système des noms de domaine") et ajoute des considérations sur l'utilisation des étiquettes étendues dans le DNS.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc6891

Table des matières

1. Introduction

Le DNS [RFC1035] spécifie un format de message, et dans ces messages il y a des formats standard pour les options de codage, les erreurs, et la compression des noms. La taille maximale admise pour un message DNS sur UDP n'utilisant pas les extensions décrites dans ce document est de 512 octets. Beaucoup des limites de protocole du DNS, comme la taille maximum de message sur UDP, sont trop petites pour prendre en charge efficacement les informations supplémentaires qui peuvent être convoyées dans le DNS (par exemple, plusieurs adresses IPv6 ou signatures de la sécurité du DNS (DNSSEC)). Finalement, la RFC 1035 ne définit aucun moyen pour que les mises en œuvre annoncent leurs capacités aux autres acteurs avec lesquels elles interagissent.

La [RFC2671] a ajouté un mécanisme d'extension au DNS. Ces mécanismes sont largement pris en charge, et un certain nombre de nouvelles utilisations du DNS et extensions du protocole dépendent de la présence de ces extensions. Le présent mémoire précise et rend obsolète la [RFC2671].

Les agents non étendus ne vont pas savoir comment interpréter les extensions de protocole définies dans la [RFC2671] et déclarées à nouveau ici. Les agents étendus doivent être prêts à traiter les interactions avec des clients non étendus en face de nouveaux éléments de protocole et à revenir en douceur au DNS non étendu.

EDNS est une extension bond par bond au DNS. Cela signifie que l'utilisation de EDNS est négociée entre chaque paire d'hôtes dans un processus de résolution DNS, par exemple, le résolveur de bout communiquant avec le résolveur récurrent ou le résolveur récurrent communiquant avec un serveur d'autorité.

La [RFC2671] a spécifié des types d'étiquettes étendus. La seule de ces étiquettes proposées était dans la [RFC2673] pour un type d'étiquette appelé "étiquette de chaîne binaire" ou "étiquettes binaires", ce dernier terme étant le plus couramment utilisé. Pour diverses raisons, l'introduction d'un nouveau type d'étiquette s'est révélé extrêmement difficile, et la [RFC2673] a été classée comme Expérimentale. Le présent document rend obsolète la [RFC2673] et déconseille les étiquettes binaires. Les étiquettes étendues restent définies, mais leur utilisation est déconseillée du fait des difficultés pratiques de leur déploiement ; leur utilisation à l'avenir DEVRAIT seulement être envisagée après une évaluation attentive des obstacles à leur déploiement.

2. Terminologie

"Demandeur" se réfère au côté qui envoie une demande. "Répondeur" se réfère à un composant DNS d'autorité, résolveur récurrent ou autre qui répond aux questions. Le reste de la terminologie utilisée ici est comme défini dans les RFC citées dans ce document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Exigences de la prise en charge de EDNS

EDNS fournit un mécanisme pour améliorer l'adaptabilité du DNS lorsque ses utilisations deviennent plus diversifiées dans l'Internet. Il le fait en permettant l'utilisation du transport UDP pour les messages DNS avec des tailles au delà des limites spécifiées dans la [RFC1035] ainsi qu'en fournissant un espace de données supplémentaire pour de nouveaux fanions et codes de retour (RCODE). Cependant, l'expérience de la mise en œuvre indique que l'ajout de nouveaux RCODE devrait être évitée à cause de la difficulté de mettre à niveau la base installée. Les fanions DEVRAIENT n'être utilisés que quand nécessaire pour que la résolution du DNS fonctionne.

Pour de nombreux usages, un code d'option EDNS peut être préférable.

Au fil du temps, certaines applications du DNS ont fait de EDNS une exigence de leur déploiement. Par exemple, DNSSEC utilise l'espace de fanions supplémentaire introduit dans EDNS pour signaler la demande d'inclure des données DNSSEC dans une réponse DNS.

Étant donnée l'augmentation de la taille des réponse du DNS quand on inclut de plus grands éléments de données comme les enregistrements AAAA, des informations DNSSEC (par exemple, RRSIG ou DNSKEY) ou de grands enregistrements TXT, les capacités supplémentaires de charge utile UDP fournies par EDNS peuvent aider à améliorer l'adaptabilité du DNS en évitant une large utilisation de TCP pour le transport DNS.

4. Changements au message DNS

4.1 En-tête de message

Le second mot complet de 16 bits de l'en-tête de message DNS est divisé en un OPCODE de 4 bits, un RCODE de 4 bits, et un certain nombre de fanions de 1 bit (voir le paragraphe 4.1.1 de la [RFC1035]). Certaines de ces valeurs de fanions ont été marquées "pour utilisation future", et la plupart ont été allouées depuis. Aussi, la plupart des valeurs de RCODE sont maintenant utilisées. Le pseudo-RR OPT spécifié ci-dessous contient des extensions au champ binaire RCODE ainsi que des bits de fanion supplémentaires.

4.2 Types d'étiquettes

Les deux premiers bits d'une étiquette de domaine au format du réseau sont utilisés pour noter le type de l'étiquette. La [RFC1035] alloue deux des quatre types possibles et réserve les deux autres. Plus de types d'étiquettes étaient définis dans la [RFC2671]. L'utilisation de la combinaison de deux bits définie dans la [RFC2671] pour identifier les types d'étiquette étendus reste valide. Cependant, il a été remarqué que le déploiement de nouveaux types d'étiquettes présente des difficultés notables et n'est donc recommandé qu'après une évaluation attentive des solutions de remplacement et du besoin du déploiement.

4.3 Taille de message UDP

Les messages DNS traditionnels sont limités à 512 octets en envoi sur UDP [RFC1035]. Faire tenir la quantité croissante de données qui doivent être transportées dans le DNS dans cette limite de 512 octets devient plus difficile. Par exemple, l'inclusion d'enregistrements DNSSEC exige fréquemment une réponse bien plus grande que ce qu'un message de 512 octets peut contenir.

EDNS(0) spécifie un moyen pour annoncer des caractéristiques supplémentaires comme une plus grande capacité de taille, qui est destinée à aider à éviter de tronquer les réponses UDP, ce qui à son tour cause de nouveaux essais sur TCP. Il fournit donc la prise en charge du transport de plus grandes tailles de paquet sans avoir besoin de recourir à TCP pour le transport.

5. Types d'étiquettes étendues

Le premier octet dans la représentation du réseau d'une étiquette DNS spécifie le type d'étiquette ; la spécification DNS de base [RFC1035] dédie les deux bits de poids fort de cet octet à cette fin.

La [RFC2671] définissait le type d'étiquette DNS 0b01 comme indication des types d'étiquette étendus. Un type spécifique d'étiquette a été choisi comme les six bits de plus fort poids du premier octet. Donc, les types d'étiquette étendus étaient indiqués par les valeurs 64 à 127 (0b01xxxxxx) dans le premier octet de l'étiquette.

Les types d'étiquette étendus sont extrêmement difficiles à déployer du fait du manque de prise en charge par les clients et les passerelles intermédiaires, comme décrit dans la [RFC3363], qui a placé la [RFC2673] au statut Expérimental, et dans la [RFC3364], qui décrit les pour et les contre. À ce titre, les propositions qui envisagent des étiquettes étendues DEVRAIENT mettre en balance le coût de ce déploiement avec la possibilité de mettre en œuvre la fonction par d'autres moyens.

Finalement, les mises en œuvre NE DOIVENT PAS générer ou passer des étiquettes binaires dans leurs communications, car elles sont maintenant déconseillées.

6. Pseudo-RR OPT

6.1 Définition d'enregistrement OPT

6.1.1 Éléments de base

Un pseudo-RR OPT (parfois appelé un méta-RR) PEUT être ajouté à la section des données supplémentaires d'une demande.

Le RR OPT a le type de RR 41.

Si un enregistrement OPT est présent dans une demande reçue, les répondeurs conformes DOIVENT inclure un enregistrement OPT dans leurs réponses respectives.

Un enregistrement OPT ne porte aucune donnée du DNS. Il est seulement utilisé pour contenir des informations de contrôle relevant de la séquence de questions/réponses d'une transaction spécifique. Les RR OPT NE DOIVENT PAS être mis en antémémoire, transmis, ou mémorisés ou chargés des fichiers maîtres.

Le RR OPT PEUT être placé n'importe où dans la section des données supplémentaires. Quans un RR OPT est inclus dans un message DNS, il DOIT être le seul RR OPT de ce message. Si un message d'interrogation avec plus d'un RR OPT est reçu, une FORMERR (RCODE=1) DOIT être retournée. La souplesse de placement pour le RR OPT ne supprime pas le besoin que le RR TSIG ou SIG(0) soit le dernier de la section supplémentaire chaque fois qu'il est présent.

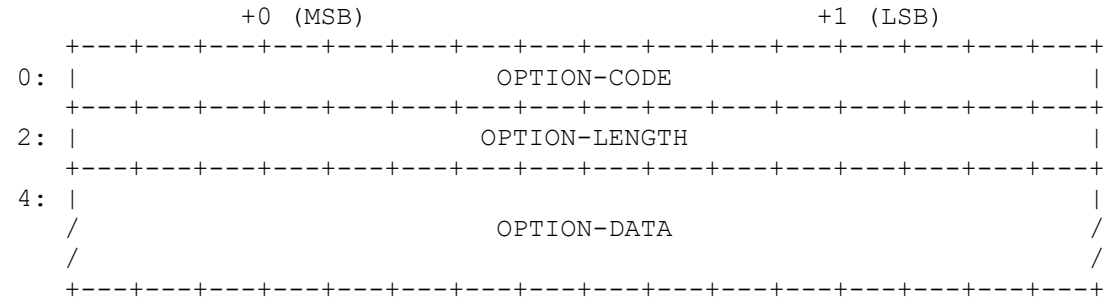
6.1.2 Format sur le réseau

Un RR OPT a une partie fixe et un ensemble variable d'options exprimées comme paires de{attribut, valeur}. La partie fixe contient des métadonnées DNS, et aussi une petite collection d'éléments d'extension de base dont on s'attend à ce qu'ils soient courants et ce serait un gaspillage de l'espace réseau de les coder comme des paires {attribut, valeur}.

La partie fixe d'un RR OPT est structurée comme suit :

Nom du champ	Type du champ	Description
NAME	nom de domaine	DOIT être 0 (domaine racine)
TYPE	u_int16_t	OPT (41)
CLASS	u_int16_t	taille de la charge utile UDP du demandeur
TTL	u_int32_t	RCODE étendu et fanions
RDLEN	u_int16_t	longueur de toutes les RDATA
RDATA	flux d'octets	paires{attribut,valeur}

Format RR OPT : la partie variable d'un RR OPT peut contenir zéro, une ou plusieurs options dans le RDATA. Chaque option DOIT être traitée comme un champ de bits. Chaque option est codée comme :



OPTION-CODE : alloué par le processus de revue d'expert comme défini par le groupe de travail DNSEXT et l'IESG.

OPTION-LENGTH : taille (en octets) de OPTION-DATA.

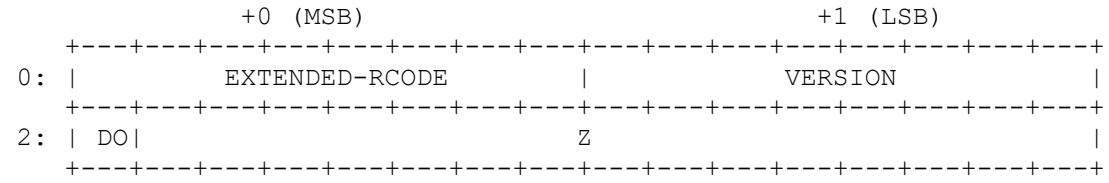
OPTION-DATA : varie selon le OPTION-CODE. DOIT être traité comme un champ de bits.

L'ordre d'apparition des couples d'option n'est pas défini. Si une option modifie le comportement d'une ou plusieurs autres ou si plusieurs options sont relatives à une autre d'une certaine façon, elles ont le même effet sans considération de leur ordre dans le codage réseau du RDATA.

Toute valeur de OPTION-CODE non comprise par un répondeur ou demandeur DOIT être ignorée. Les spécifications de telles options pourraient souhaiter inclure une sorte d'accusé de réception signalé. Par exemple, une spécification d'option pourrait dire que si un répondeur voit et prend en charge l'option XYZ, il DOIT inclure l'option XYZ dans sa réponse.

6.1.3 Utilisation du champ TTL de l'enregistrement OPT

Le RCODE étendu et les fanions, que OPT mémorise dans le champ Durée de vie (TTL, *Time to Live*) du RR, sont structurés comme suit :



EXTENDED-RCODE : forme les 8 bits de poids fort du RCODE étendu de 12 bits (avec les quatre bits définis dans la [RFC1035]. Noter que la valeur de EXTENDED-RCODE de 0 indique qu'un RCODE non étendu est utilisé (valeurs de 0 à 15).

VERSION : indique le niveau de mise en œuvre. La pleine conformité à la présente spécification est indiquée par la version "0". Les demandeurs sont invités à régler cela au plus bas niveau de mise en œuvre capable d'exprimer une transaction, pour minimiser la charge du répondeur et du réseau pour découvrir le plus grand niveau commun de mise en œuvre entre demandeur et répondeur. Une stratégie de numérotation de version d'un demandeur PEUT idéalement être une option de configuration au démarrage. Si un répondeur ne met pas en œuvre le niveau de VERSION de la demande, il DOIT alors répondre avec RCODE=BADVERS. Toutes les réponses DOIVENT être limitées en format au niveau de VERSION de la demande, mais la VERSION de chaque réponse DEVRAIT être le plus haut niveau de mise en œuvre du répondeur. De cette façon, un demandeur va apprendre le niveau de mise en œuvre d'un répondeur comme effet collatéral de chaque réponse, y compris des réponses d'erreur et les RCODE=BADVERS.

6.1.4 Fanions

DO : bit DNSSEC OK comme défini par la [RFC3225].

Z : réglé à zéro par l'envoyeur et ignoré du receveur, sauf si c'est modifié dans une spécification ultérieure.

6.2 Comportement

6.2.1 Comportement d'antémémoire

L'enregistrement OPT NE DOIT PAS être mis en antémémoire.

6.2.2. Repli

Si un demandeur détecte que l'extrémité distante ne prend pas en charge EDNS(0), il PEUT produire des interrogations sans un enregistrement OPT. Il PEUT mettre en antémémoire ces informations pour un bref instant afin d'éviter des délais de repli à l'avenir. Cependant, si DNSSEC ou une future option utilisant EDNS est requise, aucun repli ne devrait être effectué, car ces options sont seulement signalées par EDNS. Si une mise en œuvre détecte que certains serveurs pour la zone prennent en charge EDNS(0) alors que d'autres vont forcer l'utilisation de TCP pour aller chercher toutes les données, la préférence PEUT être donnée aux serveurs qui prennent en charge EDNS(0). Les mises en œuvre DEVRAIENT analyser ce choix et l'impact sur les deux points d'extrémité.

6.2.3 Taille de la charge utile du demandeur

La taille de la charge utile UDP du demandeur (codée dans le champ CLASS du RR) est le nombre d'octets de la plus grande charge utile UDP qui peut être réassemblée et livrée dans la pile réseau du demandeur. Noter que la MTU du chemin, avec ou sans fragmentation, pourrait être plus petite que cela.

Les valeurs inférieures à 512 DOIVENT être traitées comme égales à 512.

Le demandeur DEVRAIT placer dans ce champ une valeur qu'il puisse réellement recevoir. Par exemple, si un demandeur est derrière un pare-feu qui va bloquer les paquets IP fragmentés, un demandeur NE DEVRAIT PAS choisir une valeur qui va causer la fragmentation. Faire ainsi va empêcher de grandes réponses d'être reçues et peut causer un repli. Cette connaissance peut être auto-détectée par la mise en œuvre ou fournie par un administrateur humain.

Noter qu'une charge utile UDP de 512 octets exige une mémoire tampon de réassemblage IP de 576 octets. Choisir entre 1280 et 1410 octets pour IP (v4 ou v6) sur Ethernet serait raisonnable.

Lorsque la fragmentation n'est pas un problème, utiliser de plus grandes valeurs DEVRAIT être envisagé par les mises en œuvre. Les mises en œuvre DEVRAIENT utiliser leurs plus grande valeurs configurées ou utilisées comme point de départ dans une transaction EDNS en l'absence de connaissance préalable sur le serveur de destination.

Choisir une très grande valeur va garantir la fragmentation à la couche IP, et peut empêcher que les réponses soient reçues à cause de la perte d'un seul fragment ou de pare-feu mal configurés.

La taille maximum de la charge utile du demandeur peut changer dans le temps. Elle NE DOIT PAS être mise en antémémoire pour l'utiliser au delà de la transaction dans laquelle elle est annoncée.

6.2.4 Taille de la charge utile de celui qui répond

La taille maximum de la charge utile du répondeur peut changer dans le temps mais on peut raisonnablement s'attendre à ce qu'elle reste constante entre deux transactions se suivant dans un bref délai, par exemple, une QUERY arbitraire utilisée comme sonde pour découvrir la taille maximum de la charge utile UDP du répondeur, suivie immédiatement par un UPDATE qui tire parti de cette taille. Ceci est considéré comme préférable à l'utilisation directe de TCP pour les demandes de grande taille, si il y a des raisons de soupçonner que celui qui répond met en œuvre EDNS, et si une demande ne va pas tenir dans la limite par défaut de 512 octets de taille de charge utile.

6.2.5 Choix de la taille de charge utile

Du fait des frais généraux de transaction, il n'est pas recommandé d'annoncer une limite architecturale comme taille maximum de charge utile UDP. Même sur des piles systèmes capables de réassembler des datagrammes de 64 k octets, l'usage de la mémoire à de faibles niveaux dans le système va poser problème. Un bon compromis peut être d'utiliser une taille maximum de charge utile EDNS de 4096 octets comme point de départ.

Un demandeur PEUT choisir de mettre en œuvre un repli sur des tailles annoncées plus petites pour contourner les limitations de pare-feu ou du réseau. Un demandeur DEVRAIT choisir d'utiliser un mécanisme de repli qui commence par une grande taille, comme 4096. Si cela échoue, un repli autour de la gamme de 1280-1410 octets DEVRAIT être essayé, car elle a des chances raisonnables de tenir dans une seule trame Ethernet. À défaut de cela, un demandeur PEUT choisir un paquet de 512 octets, qui avec de grandes réponses peut causer un réessai TCP.

Les valeurs de moins de 512 octets DOIVENT être traitées comme égales à 512 octets.

6.2.6 Prise en charge des boîtiers de médiation

Dans un réseau qui porte du trafic du DNS, il peut y avoir des équipements actifs autres que ceux participant directement au processus de résolution du DNS (résolveurs de bout et de mise en antémémoire, serveurs d'autorité) qui affectent la transmission des messages DNS (par exemple, les pare-feu, les équilibreurs de charge, les mandataires, etc.) appelés ici des "boîtiers de médiation" *(middlebox)*.

Les boîtiers de médiation conformes NE DOIVENT PAS limiter les messages DNS sur UDP à 512 octets.

Les boîtiers de médiation qui transmettent simplement les demandes à un résolveur récurrent NE DOIVENT PAS modifier et NE DOIVENT PAS supprimer le contenu de l'enregistrement OPT dans l'une ou l'autre direction.

Les boîtiers de médiation qui ont des fonctions supplémentaires, comme de répondre aux questions ou d'agir comme des transmetteurs intelligents, DEVRAIENT être capables de traiter les enregistrements OPT et d'agir sur la base de leur contenu. Ces boîtiers de médiation DOIVENT considérer la demande entrante et toute demande sortante comme des transactions séparées si les caractéristiques des messages sont différentes.

Une discussion plus approfondie de ce type d'équipement et des autres considérations concernant leur interaction avec le trafic DNS se trouve dans la [RFC5625].

7. Considérations sur le transport

La présence d'un pseudo-RR OPT dans une demande devrait être prise comme l'indication que le demandeur met pleinement en œuvre la version donnée d'EDNS et peut correctement comprendre toute réponse qui se conforme à la spécification de cette caractéristique.

L'absence d'un enregistrement OPT dans une demande DOIT être prise comme l'indication que le demandeur ne met en œuvre aucune partie de la présente spécification et que le répondeur NE DOIT PAS inclure d'enregistrement OPT dans sa réponse.

Les agents étendus DOIVENT être prêts à traiter les interactions avec des clients non étendus en face d'éléments du nouveau protocole et se replier en douceur sur le DNS non étendu quand nécessaire.

Les répondeurs qui choisissent de ne pas mettre en œuvre les extensions de protocole définies dans ce document DOIVENT répondre avec un code de retour (RCODE) de FORMERR aux messages qui contiennent un enregistrement OPT dans la section supplémentaire et NE DOIVENT PAS inclure d'enregistrement OPT dans la réponse.

Si il y a un problème avec le traitement de l'enregistrement OPT lui-même, comme une valeur d'option mal formatée ou qui inclut des valeurs hors gamme, une FORMERR DOIT être retournée. Si cela arrive, la réponse DOIT inclure un enregistrement OPT. Ceci est destiné à permettre au demandeur de distinguer entre serveurs qui ne mettent pas en œuvre EDNS et les erreurs de format au sein de EDNS.

La réponse minimale DOIT être l'en-tête DNS, la section de question, et un enregistrement OPT. Cela DOIT aussi se produire quand une réponse tronquée (utilisant le bit TC de l'en-tête DNS) est retournée.

8. Considérations sur la sécurité

La spécification côté demandeur de la taille maximum de mémoire tampon ouvre la possibilité d'une attaque de déni de

service contre le DNS si les répondeurs peuvent être conduits à envoyer des messages trop grands pour que les passerelles intermédiaires les transmettent, conduisant ainsi à une tempête ICMP potentielle entre passerelles et répondeurs.

Annoncer de très grandes tailles de mémoire tampon UDP peut résulter en l'élimination de messages DNS par des boîtiers de médiation (voir le paragraphe 6.2.6). Cela pourrait causer des retransmissions sans espoir de succès. Certains appareils se sont trouvés rejeter des paquets UDP fragmentés.

L'annonce de tailles de mémoire tampon UDP trop petites peut résulter en un repli sur TCP avec un impact de charge correspondant sur les serveurs du DNS. Ceci est particulièrement important avec DNSSEC, où les réponses sont bien plus grandes.

9. Considérations relatives à l'IANA

L'IANA a alloué le code de type de RR 41 pour OPT.

La [RFC2671] a spécifié un certain nombre de sous registres de l'IANA au sein des "Paramètres du système des noms de domaine" :
- Options DNS EDNS(0)
- Numéro de version EDNS
- Fanions d'en-tête EDNS

De plus, deux entrées ont été générée dans les registres existants :
- Type d'étiquette EDNS étendue dans le registre des types d'étiquette DNS
- Mauvaise version OPT dans le registre des RCODES DNS

L'IANA a mis à jour les références à la [RFC2671] dans ces entrées et sous registres au présent document.

La [RFC2671] a créé le registre des types d'étiquette DNS. Ce registre reste ouvert.

La procédure d'enregistrement pour le registre des types d'étiquette DNS est Action de normalisation.

Le présent document alloue le code d'option 65535 dans le registre des options DNS EDNS0 à "Réservé pour future expansion".

Le statut actuel du registre de l'IANA pour les codes d'option EDNS au moment de la publication du présent document est
- 0 à 4 : alloués, pour des références dans le registre
- 5 à 65000 : disponible pour allocation, non alloués
- 65001 à 65534 : utilisation locale/expérimentale
- 65535 : réservé pour une future expansion

La [RFC2671] étend l'espace de RCODE de 4 bits à 12 bits. Cela permet plus que les 16 valeurs distinctes de RCODE permises dans la [RFC1035]. La revue de l'IETF est requise pour l'ajout de nouvel RCODE.

Le présent document alloue le RCODE EDNS étendu de 16 à "BADVERS" dans le registre des RCODES DNS.

La [RFC2671] demandait l'enregistrement des allocations des types d'étiquettes étendues 0bxx111111 comme "Réservé pour de futurs types d'étiquettes étendues" ; le registre IANA contient actuellement "Réservé pour une future expansion". Cette demande implique, pour l'instant, une demande d'ouvrir un nouveau registre pour des types d'étiquettes étendues, mais du fait d'une possible ambiguïté, de nouveaux enregistrements de texte ont plutôt été faits au sein du registre général des types d'étiquette DNS, qui enregistre aussi les entrées définies à l'origine par la [RFC1035]. Il n'y a donc pas de registre des types d'étiquette étendues, avec tous les types d'étiquette enregistrés dans le registre des types d'étiquette DNS.

Le présent document déconseille les étiquettes binaires. Donc, le statut de l'enregistrement du type d'étiquette DNS "Binary Labels" est maintenant "Historique".

Une action de normalisation de l'IETF est requise pour les allocations de nouveaux fanions EDNS(0). Les fanions DEVRAIENT être utilisés seulement quand nécessaire pour que la résolution du DNS fonctionne. Pour de nombreuses utilisations, un code d'option EDNS peut être préféré.

Une action de normalisation de l'IETF est requise pour créer de nouvelles entrées dans le registre des numéros de version EDNS. Dans l'espace de codes d'option, la revue d'expert est requise pour l'allocation d'un code d'option EDNS. Selon le présent document, l'IANA tient un registre pour l'espace de codes d'option EDNS.

9.1 Procédure d'allocation de code d'option OPT

Les codes d'option OPT sont alloués par revue d'expert.

L'allocation des codes d'option devrait être libérale, mais la duplication de fonctions devrait être évitée.

10. Références

10.1 Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.) (Remplacée par* RFC6891)

[RFC3225] D. Conrad, "Indication de la prise en charge de DNSSEC par le résolveur", décembre 2001. (*MàJ par* RFC4033, RFC4034, RFC4035) *(P.S.)*

10.2 Références pour information

[RFC2673] M. Crawford, "Étiquettes binaires dans le système des noms de domaine", août 1999. *(Remplacée par* RFC6891)

[RFC3363] R. Bush, A. Durand, B. Fink, O. Gudmundsson et T. Hain, "Représentation des adresses du protocole Internet version 6 (IPv6) dans le système des noms de domaine (DNS)", août 2002. (*MàJ par la* RFC6672)

[RFC3364] R. Austein, "Compromis pour la prise en charge de IPv6 par le système des noms de domaine (DNS)", août 2002. *(Info.)*

[RFC5625] R. Bellis, "Lignes directrices pour la mise en œuvre de mandataire du DNS", BCP0152, août 2009.

Appendice A. Changements par rapport aux RFC 2671 et 2673

Une liste des changements majeurs aux RFC 2671 et 2673 est donnée ci-après.

- La prise en charge de l'enregistrement OPT est maintenant obligatoire.
- Les types d'étiquettes étendues restent disponibles, mais leur utilisation est déconseillée comme solution générale du fait des difficultés observées dans leur déploiement dans l'Internet, comme illustré par le travail sur le type "étiquettes binaires".
- La RFC 2673, qui définissait le type "étiquettes binaires" et est actuellement expérimentale, est passée au statut de Historique.
- Des changements sur la façon dont les tailles de mémoire tampon EDNS sont choisies, et des recommandations sur la

façon de les choisir, ont été introduits.

Adresse des auteurs

Joao Damas
Bond Internet Systems
Av Albufera 14
S.S. Reyes, Madrid 28701
ES
téléphone : +1 650.423.1312
mél : joao@bondis.org

Michael Graff
mél : explorer@flame.org

Paul Vixie
Internet Systems Consortium
950 Charter Street
Redwood City, California 94063
US
téléphone : +1 650.423.1301
mél : vixie@isc.org