Groupe de travail Réseau
Request for Comments : 2181
RFC mises à jour : 1034, 1035, 1123
Catégorie : En cours de normalisation

R. Elz, University of Melbourne
R. Bush, RGnet, Inc.
juillet 1997
Traduction Claude Brière de L'Isle

Clarifications pour la spécification du DNS

1. Résumé

Le présent document examine certains domaines qui ont été identifiés comme posant problème dans la spécification du système des noms de domaines, et propose des remèdes pour les défauts identifiés. Huit questions distinctes ont été considérées :
+ l'usage de l'adresse de l'en-tête du paquet IP provenant de serveurs multi rattachements,
+ les TTL dans les ensembles d'enregistrement avec le même nom, classe, et type,
+ le traitement correct des coupures de zone,
+ trois problèmes mineurs concernant les enregistrements SOA et leur utilisation,
+ la définition précise de la durée de vie (TTL, *Time to Live*)
+ l'utilisation du bit d'en-tête TC (tronqué),
+ la question de ce qui est nom d'autorité ou canonique,
+ et la question de ce qui rend valide une étiquette DNS.

Les six premières sont des domaines où le comportement correct a été un peu obscur,et on cherche à rectifier cela. Les deux autres sont déjà spécifiées de façon adéquate, mais les spécifications semblent un peu ignorées. On cherche à renforcer les spécifications existantes.

Table des Matières

2. Introduction

Plusieurs domaines de problèmes de la spécification du système des noms de domaines [RFC1034], [RFC1035] ont été notés au fil du temps [RFC1123]. Le présent document vise plusieurs domaines de problèmes supplémentaires. Les questions soulevées ici sont indépendantes. Ce sont la question de savoir quelle adresse de source un serveur DNS multi rattachements devrait utiliser lorsque il répond à une interrogation, la question de TTL différents pour des enregistrements DNS avec les mêmes étiquettes, classes et types, et la question des noms canoniques, ce qu'ils sont, comment les enregistrements CNAME sont en rapports, quels noms sont légaux dans quelles parties du DNS, et quelle est la syntaxe valide d'un nom DNS.

Le présent mémoire apporte de éclaircissements aux spécification du DNS pour éviter ces problèmes. Une ambiguïté mineure de la RFC1034 concernant les enregistrements SOA est aussi corrigée, comme l'est une de la définition de la durée de vie (TTL, *Time To Live*) et une possible confusion sur l'utilisation du bit TC.

3. Terminologie

Le présent mémoire n'utilise pas les expressions DOIT, DEVRAIT, PEUT, ou leur forme négative. Dans certains paragraphes, il peut sembler qu'une spécification est formulée d'une façon douce, et donc certains pourraient en déduire que la spécification est facultative. Il n'en est rien. Partout où le présent mémoire suggère qu'une action devrait être réalisée, ou doit être réalisée, ou qu'un certain comportement est acceptable, ou non, cela doit être considéré comme un aspect fondamental de la présente spécification, sans considération de la formulation spécifique utilisée. Si un certain comportement ou action est vraiment facultatif, cela sera clairement spécifié par le texte.

4. Choix de l'adresse de source du serveur de réponse

La plupart, sinon tous, les clients DNS s'attendent à ce que l'adresse de laquelle une réponse est reçue soit la même que celle à laquelle l'interrogation qui déclanche la réponse a été envoyée. Cela est vrai pour les serveurs qui agissent comme clients pour les besoins de la résolution d'interrogation récurrente, ainsi que comme simples clients résolveurs. L'adresse avec l'identifiant (ID) dans la réponse est utilisée pour ôter toute ambiguïté aux réponses, et filtrer les réponses parasites. Cela peut, ou non, avoir été l'intention lors de la conception du DNS, mais c'est maintenant un fait qu'on ne peut ignorer.

Certains hôtes multi rattachements qui hébergent des serveurs du DNS génèrent une réponse qui utilise une adresse de source qui n'est pas la même que l'adresse de destination du paquet de demande provenant du client. De telles réponses seront éliminées par le client parce que l'adresse de source de la réponse ne correspond pas à celle de l'hôte auquel le client a envoyé la demande d'origine. C'est-à-dire qu'elle paraît être une réponse non sollicitée.

4.1 Choix de l'adresse de source avec UDP

Pour éviter ces problèmes, les serveurs doivent causer l'envoi de la réponse aux interrogations qui utilisent UDP avec le champ Adresse de source dans l'en-tête IP réglé à l'adresse qui était dans le champ Adresse de destination de l'en-tête IP du paquet contenant l'interrogation qui cause la réponse. Si cela causerait l'envoi de la réponse à partir d'une adresse IP qui n'est pas permise pour cela, la réponse peut alors être envoyée à partir de toute adresse IP légale allouée au serveur. Cette adresse devrait être choisie de façon à maximiser les possibilités que le client soit capable de l'utiliser pour les interrogations ultérieures. Les serveurs configurés d'une telle façon que toutes leurs adresses ne sont pas également accessibles de tous les clients potentiels doivent y apporter un soin particulier lorsque ils répondent aux interrogations envoyées à des adresses d'envoi à la cantonade, de diffusion groupée, ou similaires.

4.2 Choix du numéro d'accès

Les réponses à toutes les interrogations doivent être dirigées sur l'accès à partir duquel elles ont été envoyées. Lorsque des

interrogations sont reçues via TCP, c'est une partie inhérente du protocole de transport. Pour les interrogations reçue par UDP, le serveur doit noter l'accès de source et l'utiliser comme accès de destination dans la réponse. Les réponses devraient toujours être envoyées de l'accès sur lequel l'interrogation était dirigée. Sauf circonstances extraordinaires, ce sera l'accès bien connu alloué aux interrogations du DNS [RFC1700].

5. Ensembles d'enregistrements de ressources

Chaque enregistrement de ressource (RR, *Resource Record*) du DNS a une étiquette *(label)*, une classe, un type, et des données. Il serait absurde que deux enregistrements aient des étiquettes, classe, type et données toutes égales – les serveurs devraient supprimer de tels dupliqués si ils en rencontrent. Il est cependant possible pour la plupart des types d'enregistrements d'exister avec la même étiquette, classe et type, mais avec des données différentes. Un tel groupe d'enregistrements est ici défini comme étant un ensemble d'enregistrements de ressources (RRset, *Resource Record Set*).

5.1 Envoi des RR à partir d'un RRset

Une interrogation pour une étiquette, classe, et type spécifiques (ou non spécifiques) va toujours retourner tous les enregistrements qui sont dans le RRset associé – qu'il y ait un ou plusieurs RR. La réponse doit être marquée comme "tronquée" si le RRset entier ne tient pas dans la réponse.

5.2 TTL des RR dans un RRset

Les enregistrements de ressource ont aussi une durée de vie (TTL, *Time To Live*). Il est possible que des RR dans un RRset aient des TTL différents. On n'a rien trouvé pour cela qui ne soit mieux accompli d'autres façons. Ceci peut, cependant, causer des réponses partielles (non marquées "tronquée") provenant d'un serveur qui met en antémémoire, où les TTL pour certains des RR du RRset, mais pas tous, sont arrivés à expiration.

Par conséquent, l'utilisation de TTL différents dans un RRset est ici déconseillée, les TTL de tous les RR d'un RRset doivent être les mêmes.

Si un client reçoit une réponse contenant des RR avec des TTL différents provenant d'un même RRset, il devrait traiter cela comme une erreur. Si le RRset concerné provient d'une source qui n'est pas d'autorité pour ces données, le client devrait simplement ignorer le RRset, et si les valeurs sont exigées, chercher à les acquérir d'une source d'autorité. Les clients qui sont configurés à envoyer toutes les interrogations à un, ou plusieurs, serveurs particuliers devraient traiter ces serveurs comme d'autorité à cette fin. Si une source d'autorité devait envoyer un tel RRset mal formé, le client devrait traiter les RR pour tout objet comme si tous les TTL du RRset avaient été réglés à la valeur du plus petit TTL dans le RRset. En aucun cas un serveur ne peut envoyer un RRset avec des TTL qui ne sont pas tous égaux.

5.3 Cas particuliers de DNSSEC

Deux des types d'enregistrement ajoutés par la sécurité du DNS (DNSSEC) [RFC2065] exigent une attention particulière lorsque on considère la formation des ensembles d'enregistrements de ressource. Ce sont les enregistrements SIG et NXT. On devrait noter que la sécurité du DNS est encore très récente, et qu'il n'y a pour l'instant que peu d'expérience sur elle. Le lecteur devrait être prêt à ce que les informations relatives à DNSSEC contenues dans le présent document soient dépassées lorsque la spécification de la sécurité du DNS aura mûri.

5.3.1 Enregistrements SIG et RRset

Un enregistrement SIG fournit des données de signature (validation) pour un autre RRset dans le DNS. Lorsque une zone a été signée, chaque RRset dans la zone va avoir un enregistrement SIG associé. Le type de données du RRset est inclus dans les données du RR SIG, pour indiquer avec quel RRset particulier cet enregistrement SIG est associé. Si les règles ci-dessus étaient appliquées, chaque fois q'un enregistrement SIG serait inclus avec une réponse pour valider cette réponse, les enregistrements SIG pour tous les autres RRset associés au nœud approprié auraient aussi besoin d'être inclus. Dans certains cas, cela pourrait faire un très grand nombre d'enregistrements, empiré par le fait que ce sont d'assez gros RR.

Donc, il est spécifiquement permis que la section Autorité ne contienne que les RR SIG qui ont le champ "type couvert" égal au champ Type d'une réponse qui est retournée. Cependant, lorsque les enregistrements SIG sont retournés dans la section Réponse, en réponse à une interrogation sur des enregistrements SIG, ou à une interrogation pour tous les enregistrements associés à un nom (type=ANY) le RRset SIG entier doit être inclus, comme pour tout autre type de RR.

Les serveurs qui reçoivent des réponses contenant des enregistrements SIG dans la section Autorité, ou (probablement par erreur) comme données additionnelles, doivent comprendre que le RRset entier n'a presque certainement pas été inclus. Donc, ils ne doivent pas mettre en antémémoire l'enregistrement SIG d'une manière qui permettrait d'être retourné si une interrogation pour des enregistrements SIG était reçue à ce serveur. La RFC2065 exige en fait que les interrogations SIG ne soient dirigées que sur les serveurs d'autorité pour éviter les problèmes que cela pourrait causer, et tant qu'il existera des serveurs qui ne comprennent pas les propriétés particulières des enregistrements SIG, cela restera nécessaire. Cependant, un traitement bien conçu des enregistrements SIG dans les nouvelles mises en œuvre devrait permettre que cette restriction soit relâchée à l'avenir, de sorte que les résolveurs n'aient pas besoin de traiter les interrogations d'enregistrements SIG d'une façon particulière.

Il a été déclaré occasionnellement qu'une demande reçue pour un enregistrement SIG devrait être transmise à un serveur d'autorité, plutôt que répondue à partir des données conservées dans l'antémémoire. Ceci n'est pas nécessaire - un serveur qui a connaissance qu'un SIG est un cas particulier de traitement va s'efforcer de mettre correctement en antémémoire les enregistrements SIG, en prenant en compte leurs caractéristiques. Le serveur peut alors déterminer quand il est sûr de répondre à partir de l'antémémoire, et quand la réponse n'est pas disponible et que l'interrogation doit être transmise.

5.3.2 RR NXT

Les enregistrements de ressource NXT *(prochain enregistrement de ressource)* sont encore plus particuliers. Il n'y aura jamais d'un seul enregistrement NXT dans une zone pour une certaine étiquette, donc superficiellement, le problème du RRset est trivial. Cependant, à une coupure de zone, la zone parente et la zone fille (super zone et sous zone dans la terminologie de la RFC2065) vont avoir des enregistrements NXT pour le même nom. Ces deux enregistrements NXT ne forment pas un RRset, même lorsque les deux zones sont hébergées dans le même serveur. Les RRset NXT contiennent toujours un seul RR. Lorsque les deux enregistrements NXT sont visibles, deux RRset existent. Cependant, les serveurs ne sont pas obligés de traiter cela comme un cas particulier lorsque ils reçoivent des enregistrements NXT dans une réponse. Ils peuvent choisir de remarquer l'existence de deux RRset NXT différents, et de traiter cela comme ils l'auraient fait pour deux RRset différents de n'importe quel autre type. C'est-à-dire, en mettre un en antémémoire, et ignorer l'autre. Les serveurs à capacités de sécurité auront donc besoin de traiter correctement l'enregistrement NXT dans la réponse reçue.

5.4 Réception des RRset

Les serveurs ne doivent jamais fusionner des RR provenant d'une réponse avec des RR qui sont en antémémoire pour former un RRset. Si une réponse contient des données qui formeraient un RRset avec des données qui sont dans l'antémémoire d'un serveur, celui-ci doit soit ignorer les RR de la réponse, soit éliminer en entier le RRset qui est actuellement dans l'antémémoire, comme approprié. Par conséquent, la question des TTL qui varient entre l'antémémoire et une réponse ne cause pas de souci : une sera ignorée. C'est-à-dire qu'un des ensembles de données est toujours incorrect si les données provenant d'une réponse diffèrent des données qui sont dans l'antémémoire. Le défi pour le serveur est de déterminer quel ensemble de données est correct, si il en est un, et de conserver l'un tout en ignorant l'autre. Noter que si un serveur reçoit une réponse contenant un RRset qui est identique à celui de l'antémémoire, à l'exception possible de la valeur du TTL, il peut, facultativement, mettre à jour le TTL dans son antémémoire avec celui de la réponse reçue. Il devrait faire cela si la réponse reçue était considérée comme plus d'autorité (comme discuté au paragraphe suivant) que la réponse précédemment mise en antémémoire.

5.4.1 Données de rang

Lorsque il examine si il faut accepter un RRset dans une réponse, ou plutôt conserver un RRset déjà dans son antémémoire, un serveur devrait considérer la confiance relative probable des diverses données. Une réponse d'autorité provenant d'une réponse devrait remplacer les données en antémémoire qui avaient été obtenues d'informations additionnelles dans une réponse antérieure. Cependant les informations additionnelles provenant d'une réponse seront ignorées si l'antémémoire contient des données provenant d'une réponse ou d'un fichier de zone d'autorité.

La pertinence des données disponibles est supposée de par leur source. La confiance devra être accordée, en ordre décroissant, du plus digne de confiance au moins digne de confiance :
+ aux données provenant d'un fichier de zone principale, autres que des données glu,
+ aux données provenant d'un transfert de zone, autres que des données glu,
+ aux données d'autorité incluses dans la section Réponse d'une réponse d'autorité,
+ aux données provenant de la section Autorité d'une réponse d'autorité,
+ aux données glu provenant d'une zone principale, ou d'un transfert de zone,
+ aux données provenant de la section Réponse d'une réponse qui n'est pas d'autorité, et de données non d'autorité provenant de la section Réponse de réponses d'autorité,
+ aux informations additionnelles d'une réponse d'autorité,

+ aux données provenant de la section Autorité d'une réponse non d'autorité,
+ aux informations additionnelles provenant de réponses non d'autorité.

Noter que la section Réponse d'une réponse d'autorité contient normalement seulement des données d'autorité. Cependant lorsque le nom cherché est un alias (voir au paragraphe 10.1.1) seul l'enregistrement qui décrit cet alias est nécessairement d'autorité. Les clients devraient supposer que les autres enregistrements ont pu venir de l'antémémoire du serveur. Lorsque des réponses d'autorité sont requises, le client devrait interroger à nouveau, en utilisant le nom canonique associé à l'alias.

Les RR non authentifiés reçus et mis en antémémoire provenant du moins digne de confiance de ces groupements, c'est-à-dire les données provenant de la section Données additionnelles, et les données provenant de la section Autorité d'une réponse non d'autorité, ne devraient pas être mises en antémémoire d'une façon telle qu'elle ne puissent jamais être retournées comme des réponses à une interrogation reçue. Elles peuvent être retournées comme informations additionnelles lorsque approprié. Ignorer cela permettrait de transformer en données de confiances des données relativement peu fiables, sans cause ni excuse.

Lorsque la sécurité du DNS [RFC2065] est en vigueur, et qu'une réponse authentifiée a été reçue et vérifiée, les données ainsi authentifiées doivent être considérées comme plus dignes de confiance que des données non authentifiées du même type. Noter que tout au long du présent document, "d'autorité" signifie une réponse avec le bit AA établi *(à 1)*. Le DNSSEC utilise des chaînes de confiance d'enregistrements SIG et KEY pour déterminer l'authenticité des données, le bit AA est presque non pertinent. Cependant les serveurs à capacité DNSSEC doivent quand même régler correctement le bit AA dans les réponses pour permettre un fonctionnement correct avec les serveurs qui n'ont pas de capacités de sécurité (actuellement presque tous).

Noter que, glu exclu, il est impossible que les données provenant de deux fichiers de zone primaire correctement configurés, deux zones secondaires correctement configurées (données provenant de transferts de zone) ou les données provenant de zones primaires et secondaires correctement configurées entrent jamais en conflit. Lorsque il existe des données glu pour le même nom dans plusieurs zones, et qu'elles diffèrent en valeur, le serveur de noms devrait choisir les données provenant du fichier de zone primaire de préférence au secondaire, mais autrement peut choisir tout ensemble de telles données. Choisir celles qui paraissent venir d'une source plus proche de la source des données d'autorité peut avoir un sens lorsque on peut le déterminer. Choisir des données primaires plutôt que secondaires permet de découvrir plus directement la source de données glu incorrectes, lorsque un problème se pose avec de telles données. Lorsque un serveur peut détecter à partir de deux fichiers de zone que un ou plusieurs sont configurés de façon incorrecte, ce qui pourrait générer des conflits, il devrait refuser de charger les zones dont il a déterminé qu'elles sont erronées, et produire les diagnostics qui conviennent.

"Glu" ci-dessus inclut tous les enregistrements dans un fichier de zone qui ne font pas à proprement parler partie de cette zone, incluant les enregistrements de serveur de noms des sous zones déléguées (enregistrements NS) les enregistrements d'adresse qui accompagnent ces enregistrements NS (A, AAAA, etc.) et toutes autres données diverses qui peuvent apparaître.

5.5 Envoi des RRset (reprise)

Un ensemble d'enregistrements de ressource ne devrait être inclus qu'une seule fois dans toute réponse DNS. Il peut survenir dans toutes section Réponse, Autorité, ou Informations additionnelles, comme nécessaire. Cependant il ne devrait pas être répété dans la même section, ou dans aucune autre, sauf lorsque explicitement exigé par une spécification. Par exemple, une réponse AXFR exige que l'enregistrement SOA (toujours un RRset contenant un seul RR) soit à la fois le premier et le dernier enregistrement de la réponse. Lorsque des dupliqués sont exigés de cette façon, le TTL transmis dans chaque cas doit être le même.

6. Coupures de zone

L'arborescence du DNS est divisée en "zones", qui sont des collections de domaines traitées comme une unité pour certains besoins de gestion. Les zones sont délimitées par des "coupures de zone". Chaque coupure de zone sépare une zone "fille" (en dessous de la coupure) d'une zone "parente" (au dessus de la coupure). Le nom de domaine qui apparaît au sommet d'une zone (juste en dessous de la coupure qui sépare la zone de sa parente) est appelée "origine" de la zone. Le nom de la zone est le même que celui du domaine à l'origine de la zone. Chaque zone comprend le sous ensemble de l'arborescence du DNS qui est à, ou en dessous de l'origine de la zone, et qui est au dessus des coupures qui séparent la zone de ses filles (si il en est). L'existence d'une coupure de zone est indiquée dans la zone parente par l'existence d'enregistrements NS qui spécifient l'origine de la zone fille. Une zone fille ne contient aucune référence explicite à sa parente.

6.1 Autorité de zone

Les serveurs d'autorité pour une zone sont énumérés dans les enregistrements NS pour l'origine de la zone, qui, avec l'enregistrement de début d'autorité (SOA, *Start Of Authority*) sont les enregistrements obligatoires de chaque zone. Un tel serveur est d'autorité pour tous les enregistrements de ressource dans une zone qui ne sont pas dans une autre zone. Les enregistrements NS qui indiquent une coupure de zone sont la propriété de la zone fille créée, comme le sont tous les autres enregistrements pour l'origine de cette zone fille, ou tous ses sous domaines. Un serveur pour une zone ne devrait pas retourner de réponses d'autorité pour des interrogations qui se rapportent à des noms dans une autre zone, ce qui inclut les enregistrements NS, et peut-être A, à une coupure de zone, sauf si il est aussi un serveur pour l'autre zone.

En dehors des cas de DNSSEC mentionnés immédiatement ci-dessous, les serveurs devraient ignorer les données autres que les enregistrements NS, et les enregistrements A nécessaires pour localiser les serveurs mentionnés dans les enregistrements NS, qui peuvent se trouver être configurés dans une zone à une coupure de zone.

6.2 Problèmes relatifs à DNSSEC

Les mécanismes de sécurité du DNS de la [RFC2065] compliquent un peu cela, car certains des nouveaux types d'enregistrement de ressource ajoutés sont très inhabituels comparés aux autres RR du DNS. En particulier, le type de RR NXT ("prochain RR") contient des informations sur les noms qui existent dans une zone, et donc ceux qui n'y existent pas, et doit donc nécessairement se rapporter à la zone dans laquelle ils existent. Le même nom de domaine peut avoir différents enregistrements NXT dans la zone parente et dans la zone fille, et tous deux sont valides, et ne sont pas un RRset. Voir aussi au paragraphe 5.3.2.

Comme les enregistrements NXT sont destinés à être générés automatiquement, plutôt que configurés par les opérateurs du DNS, les serveurs peuvent, mais sans y être obligés, conserver tous les différents enregistrements NXT qu'ils reçoivent, sans considération des règles du paragraphe 5.4.

Pour qu'une zone parente sûre indique en toute sécurité qu'une sous zone n'est pas sûre, DNSSEC exige qu'un RR KEY indique que la sous zone n'est pas sûre, et que les RR SIG qui authentifient la zone parente soient présents dans la zone parente, car par définition ils ne peuvent pas être dans la sous zone. Lorsque une sous zone est sûre, les enregistrements KEY et SIG seront présents, et d'autorité, dans cette zone, mais devraient aussi toujours être présents dans la zone parente (si elle est sûre).

Noter que dans aucun de ces cas un serveur pour la zone parente, n'étant pas aussi un serveur pour la sous zone, n'établit le bit AA dans une réponse pour une étiquette à la coupure de zone.

7. RR SOA

Trois questions mineures concernant l'enregistrement de ressource Début de zone d'autorité (SOA, *Start Of zone of Authority*) doivent être précisées.

7.1 Placement des RR SOA dans les réponses d'autorité

Le paragraphe 3.7 de la RFC1034 indique que la section Autorité d'une réponse d'autorité peut contenir l'enregistrement SOA pour la zone à partir de laquelle la réponse a été obtenue. Lorsqu'elle parle de mise en antémémoire négative, le paragraphe 4.3.4 de la RFC1034 se réfère à cette technique mais mentionne la section Additionnelle de la réponse. La première est correcte, car c'est impliqué par l'exemple montré au paragraphe 6.2.5 de la RFC1034. Les enregistrements SOA, si ils sont ajoutés, sont à placer dans la section Autorité.

7.2 TTL sur les RR SOA

On peut observer au paragraphe 3.2.1 de la RFC1035, qui définit le format d'un enregistrement de ressource, que la définition du champ TTL contient une ligne séparée qui déclare que le TTL d'un enregistrement SOA devrait toujours être envoyé à zéro pour empêcher la mise en antémémoire. Ceci n'est mentionné nulle part ailleurs, et n' a généralement pas été mis en œuvre. Les mises en œuvre ne devraient pas supposer que les enregistrements SOA auront un TTL de zéro, ni qu'il est exigé que les enregistrements SOA soient envoyés avec un TTL de zéro.

7.3 Champ SOA.MNAME

Il est assez clair dans les spécifications, mais semble avoir été largement ignoré, que le champ MNAME de l'enregistrement SOA devrait contenir le nom du serveur principal (maître) pour la zone identifiée par le SOA. Il ne devrait pas contenir le nom de la zone elle-même. Cette information serait sans usage, car pour la découvrir, on aurait besoin de commencer par le nom de domaine de l'enregistrement SOA – qui est le nom de la zone.

8. Durée de vie

La définition des valeurs appropriées pour le champ TTL (TTL, *Time to Live*) dans le STD 13 n'est pas aussi clair qu'il pourrait l'être, par rapport au nombre de bits significatifs qui existent, et si la valeur est un entier signé ou non. On spécifie ici qu'une valeur de TTL est un entier non signé, avec une valeur minimum de 0, et une valeur maximum de 2 147 483 647. C'est-à-dire, un maximum de 2^31 - 1. À l'émission, cette valeur doit être codée dans les 31 bits de moindre poids du champ TTL de 32 bit, avec le bit de poids fort, ou signe, réglé à zéro.

Les mises en œuvre devraient traiter les valeurs de TTL reçues avec le bit de poids fort établi comme si la valeur entière reçue était zéro.

Les mises en œuvre ont toujours la liberté de fixer une limite supérieure à tout TTL reçu, et de traiter toute valeur supérieure comme si elle était à cette limite supérieure. Le TTL spécifie une durée maximum de vie, non une durée de vie obligatoire.

9. Bit d'en-tête TC (tronqué)

Le bit TC devrait être établi *(à 1)* dans les réponses seulement lorsque un RRset est demandé au titre de la réponse, mais n'a pas pu être inclus dans sa totalité. Le bit TC ne devrait pas être établi simplement parce que des informations supplémentaires n'ont pas pu être incluses, mais que l'espace était insuffisant. Cela inclut les résultats du traitement de la section Additionnelle. Dans un tel cas, le RRset entier qui ne va pas tenir dans la réponse devrait être omis, et la réponse envoyée telle quelle, avec le bit TC à zéro. Si le receveur de la réponse a besoin des données omises, il peut construire une interrogation pour ces données et l'envoyer séparément.

Lorsque TC est établi, le RRset partiel qui ne peut pas complètement tenir peut être laissé dans la réponse. Lorsque un client DNS reçoit une réponse avec le bit TC établi, il devrait ignorer cette réponse, et interroger à nouveau, en utilisant un mécanisme, comme une connexion TCP, qui va permettre de plus grandes réponses.

10. Questions de dénomination

Il a parfois été déduit de certains paragraphes de la spécification du DNS [RFC1034], [RFC1035] qu'il est permis à un hôte, ou peut-être une interface d'un hôte, exactement un seul nom d'autorité, ou nom officiel, appelé le nom canonique. Cette exigence n'existe pas dans le DNS.

10.1 Enregistrements de ressource CNAME

L'enregistrement DNS CNAME ("nom canonique") existe pour fournir le nom canonique associé à un alias. Il peut y avoir seulement un tel nom canonique pour tout alias. Ce nom devrait généralement être un nom qui existe ailleurs dans le DNS, bien qu'il y ait quelques rares demandes pour un alias avec le nom canonique accompagnant qui reste indéfini dans le DNS. Un alias (étiquette d'un enregistrement CNAME) peut, si DNSSEC est utilisé, avoir des RR SIG, NXT, et KEY, mais peut n'avoir pas d'autres données. C'est-à-dire, pour toute étiquette dans le DNS (tout nom de domaine) exactement une de conditions suivantes est vraie :
+ un enregistrement CNAME existe, facultativement accompagné de RR SIG, NXT, et KEY,
+ un ou plusieurs enregistrements existent, aucun n'étant un enregistrement CNAME,
+ le nom existe, mais n'est associé à aucun RR d'aucun type,
+ le nom n'existe pas du tout.

10.1.1 Terminologie de CNAME

On s'est traditionnellement référé à l'étiquette d'un enregistrement CNAME comme à "un CNAME". C'est malencontreux, car "CNAME" est l'abréviation de "nom canonique", et que l'étiquette d'un enregistrement CNAME n'est très certainement

pas un nom canonique. C'est cependant un usage bien arrêté. Il faut donc faire attention d'être très clair sur ce qu'on désigne, l'étiquette, ou la valeur (le nom canonique) d'un enregistrement de ressource CNAME. Dans le présent document, l'étiquette d'un enregistrement de ressource CNAME sera toujours mentionnée comme un alias.

10.2 Enregistrements PTR

La confusion sur les noms canoniques a conduit à la croyance qu'un enregistrement PTR devrait avoir exactement un RR dans son RRset. C'est incorrect ; la section pertinente de la RFC1034 (paragraphe 3.6.2) indique que la valeur d'un enregistrement PTR devrait être un nom canonique. C'est-à-dire qu'il devrait être un alias. Il n'est nullement impliqué dans ce paragraphe que seul un enregistrement PTR serait permis pour un nom. On ne devrait pas déduire une telle restriction.

Noter que tandis que la valeur d'un enregistrement PTR ne doit pas être un alias, il n'est pas exigé que le processus de résolution d'un enregistrement PTR ne rencontre aucun alias. L'étiquette qui est recherchée pour une valeur de PTR peut avoir un enregistrement de CNAME. C'est-à-dire qu'il peut être un alias. La valeur de ce RR CNAME, si elle n'est pas un autre alias, ce qu'elle ne devrait pas être, va donner la localisation de l'enregistrement PTR. Cet enregistrement donne le résultat de la recherche du type de PTR. Ce résultat final, la valeur du RR PTR, est l'étiquette qui ne doit pas être un alias.

10.3 Enregistrements MX et NS

Le nom de domaine utilisé comme valeur d'un enregistrement de ressource NS, ou d'une partie de la valeur d'un enregistrement de ressource MX ne doit pas être un alias. Non seulement la spécification est claire sur ce point, mais utiliser un alias dans une de ces positions ne fonctionne pas aussi bien qu'on pourrait l'espérer, ni ne satisfait l'ambition qui peut avoir conduit à cette approche. Ce nom de domaine doit avoir comme valeur un ou plusieurs enregistrements d'adresse. Ce sera actuellement un enregistrement A, cependant à l'avenir d'autres types d'enregistrements donnant des informations d'adresse pourront être acceptables. Il peut aussi y avoir d'autres RR, mais jamais un RR CNAME.

Chercher des enregistrements NS ou MX cause un "traitement de la section additionnelle" dans lequel les enregistrements d'adresse associés à la valeur de l'enregistrement recherché sont ajoutées à la réponse. Cela aide à éviter d'inutiles interrogations supplémentaires qui sont facilement anticipées lorsque la première a été faite.

Le traitement de la section Additionnelle n'inclut pas les enregistrements CNAME, mis à part les enregistrements d'adresse qui peuvent être associés au nom canonique déduit de l'alias. Donc, si un alias est utilisé comme valeur d'un enregistrement NS ou MX, aucune adresse ne sera retournée avec la valeur de NS ou MX. Cela peut causer des interrogations supplémentaires, et une charge supplémentaire pour le réseau, sur chaque interrogation. Il est trivial pour l'administrateur du DNS d'éviter cela en résolvant l'alias et en plaçant le nom canonique directement dans l'enregistrement affecté juste une fois quand il est mis à jour ou installé. Dans certains cas particuliers difficiles, le manque des enregistrements d'adresse de la section Additionnelle dans les résultats d'une recherche de NS peut causer l'échec de la demande.

11. Syntaxe du nom

Il est supposé occasionnellement que le système des noms de domaines ne sert qu'aux besoins de transposition des noms d'hôtes Internet en données, et de transposition des adresses Internet en noms d'hôtes. Ce n'est pas exact, le DNS est une base de données générale (mais un peu limitée) hiérarchique, qui peut mémoriser presque toutes sortes de données, pour presque tous les objets.

Le DNS lui-même ne fait qu'une restriction sur les étiquettes particulières qui peuvent être utilisées pour identifier les enregistrements de ressource. Cette restriction est relative à la longueur de l'étiquette et du nom complet. La longueur de toute étiquette est limitée entre 1 et 63 octets. Un nom de domaine complet est limité à 255 octets (incluant les séparateurs). Le nom complet de longueur zéro est défini comme représentant la racine de l'arborescence du DNS, et est normalement écrite et affichée comme ".". Ces restrictions mises à part, toute chaîne binaire quelle qu'elle soit peut être utilisée comme étiquette de tout enregistrement de ressource. De même, toute chaîne binaire peut servir de valeur à tout enregistrement qui comporte un nom de domaine comme sa valeur ou une de ses parties (SOA, NS, MX, PTR, CNAME, et tous les autres qui pourraient y être ajoutées). Les mises en œuvre des protocoles du DNS ne doivent pas faire de restriction sur les étiquettes qui peuvent être utilisées. En particulier, les serveurs du DNS ne doivent pas refuser de servir une zone parce qu'elle contient des étiquettes qui pourraient n'être pas acceptables pour certains programmes de clients DNS. Un serveur DNS peut être configurable à produire des avertissements lors du chargement, ou même refuser de charger, une zone primaire contenant des étiquettes qui pourraient être considérées comme discutables, toutefois, ceci ne devrait pas arriver par défaut.

Noter cependant, que les diverses applications qui utilisent les données du DNS peuvent avoir des restrictions imposées sur l'acceptabilité de valeurs particulières dans leur environnement. Par exemple, que toute étiquette binaire puisse avoir un

enregistrement MX n'implique pas que tout nom binaire puisse être utilisé comme partie hôte d'une adresse de messagerie électronique. Les clients du DNS peuvent imposer toutes les restrictions appropriées à leurs circonstances sur les valeurs qu'ils utilisent comme clés pour leurs demandes de recherche sur le DNS, et sur les valeurs retournées par le DNS. Si le client a de telles restrictions, il est seul responsable de la validation des données provenant du DNS pour s'assurer qu'elles sont conformes avant qu'il fasse usage de ces données. Voir aussi au paragraphe 6.1.3.5 de la [RFC1123].

12. Considérations sur la sécurité

Le présent document ne traite pas de sécurité. En particulier, rien dans la Section 4 ne se rapporte, ni n'est utile, pour aucune question en rapport avec la sécurité.

Le paragraphe 5.4.1 ne se rapporte pas non plus à la sécurité. La sécurité des données du DNS sera obtenue par le DNS sûr [RFC2065], qui est essentiellement orthogonal au présent mémoire.

On estime que rien dans le présent document n'ajoute à aucune question de sécurité qui pourrait exister pour le DNS, ni rien qui pourrait nécessairement les diminuer. Une mise en œuvre correcte des précisions du présent document pourrait jouer un petit rôle dans la limitation du développement de mauvaises données non malveillantes dans le DNS, mais seul DNSSEC peut aider contre les tentatives délibérées de subvertir les données du DNS.

13 Références

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 2065, RFC 2181, RFC 2308, RFC 2535, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 4035, RFC 4592, RFC 5936, RFC 8020)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 2673, RFC 2845, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966, RFC 6604, RFC 7766)

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org))*

[RFC2065] D. Eastlake 3rd, C. Kaufman, "Extensions de sécurité du système de noms de domaines", janvier 1997. (*Obsolète, voir* RFC2535) (*MàJ* RFC1034, RFC1035) *(P.S.)*

14. Remerciements

Le présent mémoire est issu de discussions au sein du groupe de travail DNSIND de l'IETF en 1995 et 1996, les membres de ce groupe de travail sont largement responsables des idées proposées ici. Des remerciements particuliers vont à Donald E. Eastlake, 3rd, et Olafur Gudmundsson, qui ont aidé sur les questions du DNSSEC dans le présent document, et à John Gilmore qui a relevé où les clarifications n'étaient pas nécessairement claires. Bob Halley a suggéré de préciser le placement des enregistrements SOA dans les réponses d'autorité, et fourni les références. Michael Patton, comme d'habitude, et Mark Andrews, Alan Barrett et Stan Barber ont fourni leur assistance sur beaucoup de détails. Josh Littlefield a aidé à s'assurer que les éclaircissements ne causaient pas problèmes dans certains cas marginaux irritants.

15. Adresse des auteurs

Robert Elz
Computer Science
University of Melbourne
Parkville, Victoria, 3052
Australia.
mél : kre@munnari.OZ.AU

Randy Bush
RGnet, Inc.
5147 Crystal Springs Drive NE
Bainbridge Island, Washington, 98110
United States.
mél : randy@psg.com