Groupe de travail Réseau
Request for Comments: 4592
RFC mises à jour : 1034, 2672
Catégorie : Sur la voie de la normalisation

E. Lewis
NeuStar

juillet 2006
Traduction Claude Brière de L'Isle

Rôle des caractères génériques dans le système des noms de domaine

Résumé
Ceci est une mise à jour de la définition du caractère générique de la RFC 1034. L'interaction entre caractères génériques et CNAME est changée, une condition d'erreur est supprimée, et les mots qui définissennt certains concepts centraux des caractères génériques sont changés. L'objectif global n'est pas de changer les caractères génériques, mais de préciser la définition de la RFC 1034.

Table des matières

1. Introduction

Dans la [RFC1034], les paragraphes 4.3.2 et 4.3.3 décrivent la synthèse des réponses provenant d'enregistrements de ressource spéciaux (RR, *resource record*) appelés des caractères génériques. La définition de la RFC 1034 est incomplète

et s'est révélée confuse. Le présent document décrit la synthèse de caractère générique en ajoutant à la discussion et en faisant des modifications limitées. Les modifications sont faites pour résoudre des incohérences qui ont conduit à des problèmes d'interopérabilité. Cette description ne s'étend pas sur le service prévu par la définition d'origine.

En restant dans l'esprit et le style des documents d'origine, le présent document évite de spécifier des règles pour les mises en œuvre du DNS concernant les caractères génériques. L'intention est seulement de décrire ce qui est nécessaire pour l'interopérabilité, et pas de restreindre les choix de mise en œuvre. De plus, on a veillé à minimiser tous les problèmes de rétro compatibilité avec les mises en œuvre qui se conforment à la définition de la RFC 1034.

Le présent document se concentre sur le concept de caractère générique tel que défini dans la RFC 1034. Rien n'est impliqué en ce qui concerne d'autres moyens de synthétiser les ensembles d'enregistrement de ressource (RRSet, *resource record set*) et ces autres moyens ne sont pas discutés.

1.1 Motivation

De nombreuses mises en œuvre du DNS divergent, de différentes façons, de la définition d'origine du caractère générique. Bien qu'il y ait un clair besoin de préciser les documents d'origine à la lumière de ce seul point, l'impulsion du présent document se trouve dans la préparation des extensions de sécurité du DNS [RFC4033]. Avec une définition obscure des caractères génériques, la conception des refus authentifiés devenait difficile.

Le présent document est destiné à limiter ses changements, en documentant seulement ceux réputés nécessaires sur la base de l'expérience de la mise en œuvre, et de rester aussi proche que possible du document d'origine. Pour renforcer le fait que le présent document est destiné à préciser et ajuster et non de redéfinir les caractères génériques, les paragraphes pertinents de la RFC 1034 sont répétés mot à mot pour faciliter la comparaison du texte ancien et nouveau.

1.2 Définition d'origine

La définition du concept de caractère générique est comprise dans la documentation de l'algorithme par lequel un serveur de noms prépare une réponse (au paragraphe 4.3.2 de la RFC 1034) et de la façon dont un enregistrement (ou ensemble de) de ressource est identifié comme étant une source de données synthétiques (paragraphe 4.3.3).

Voici la définition du terme "caractère générique" *(wildcard)* comme elle apparaît au paragraphe 4.3.3 de la RFC 1034.
"Dans l'algorithme précédent, un traitement particulier est appliqué aux RR dont les noms de propriétaire commencent par l'étiquette "*". De tels RR sont appelés à caractère générique. Les RR à caractères générique peuvent être vus comme des instructions pour synthétiser les RR. Quand les conditions appropriées sont satisfaites, le serveur de noms crée des RR avec un nom de propriétaire égal au nom et contenu de l'interrogation tirés des RR à caractères génériques."

Ce passage suit l'algorithme dans lequel le terme de caractère générique est utilisé pour la première fois. Dans cette définition, caractère générique se réfère aux enregistrements de ressources. Dans un autre usage, caractère générique se réfère aux noms de domaines, et il a été utilisé pour décrire la pratique opérationnelle de s'appuyer sur des caractères génériques pour générer des réponses. Il est clair d'après cela qu'il y a un besoin de définir clairement et sans ambiguïté la terminologie dans le processus de discussion des caractères génériques.

La mention de l'utilisation des caractères génériques dans la préparation d'une réponse est contenue dans l'étape 3, partie 'c' du paragraphe 4.3.2 de la RFC 1034, intitulée "Algorithme". Noter que "caractère générique" n'apparaît pas dans l'algorithme, des références sont à la place faites à l'étiquette "*". La portion de l'algorithme relative aux caractères génériques est déconstruite en détails à la Section 3 du présent document ; c'est le début de la portion pertinente de "Algorithme".

"c. si à une certaine étiquette, une correspondance est impossible (c'est-à-dire, si l'étiquette correspondante n'existe pas) regarder si [...] l'étiquette "*" existe."

La portée du présent document est la définition de la RFC 1034 des caractères génériques et des implications des mises à jour à des documents comme “Sécurité du DNS“ (DNSSEC). D'autres schémas pour des réponses synthétiques ne sont pas pris en compte. (Noter qu'il n'est pas cité de référence. Aucun document connu ne décrit d'autre schéma, bien qu'il en soit fait mention dans les listes de diffusion.)

1.3 Objectifs du présent document

Le présent document réalise les trois tâches suivantes.

- o Il définit de nouveaux termes
- o Il fait des changements mineurs pour éviter des conflits de concepts
- o Il décrit les actions de certains enregistrements de ressource comme des caractères génériques

1.3.1 Nouveaux termes

Pour aider à discuter quels enregistrements de ressource sont des caractères génériques, deux termes seront définis : "étiquette astérisque" et "nom de domaine à caractères génériques". Ils sont définis au paragraphe 2.1.1.

Pour aider à préciser le rôle des caractères génériques dans l'algorithme de serveur de noms du paragraphe 4.3.2 de la RFC 1034, "source de synthèse" et "plus proche enrobant" sont définis. Ces définitions sont au paragraphe 3.3.1. "Correspondance d'étiquette" est défini au paragraphe 3.2.

Les nouveaux termes sont utilisés pour rendre plus claire la discussions des caractères génériques. La terminologie n'a pas d'impact direct sur la mise en œuvre.

1.3.2 Changements de texte

La définition de "existence" est changée superficiellement. Ce changement ne sera pas apparent aux mises en œuvre ; il est nécessaire pour rendre les descriptions plus précises. Le changement apparaît au paragraphe 2.2.3.

Le paragraphe 4.3.3 de la RFC 1034 semble interdire d'avoir deux étiquettes astérisque dans un nom de propriétaire à caractères génériques. Dans le présent document, cette restriction est entièrement supprimée. Ce changement et ses implications sont au paragraphe 2.1.3.

Les actions quand une source de synthèse possède un RR CNAME sont changées pour refléter les actions si une correspondance exacte de nom possède un RR CNAME. Ceci s'ajoute aux mots de la partie “c” de l'étape 3 du paragraphe 4.3.2 de la RFC 1034. Cette discussion est au paragraphe 3.3.3.

Seul ce dernier changement représente un impact sur les mises en œuvre. La définition de “existence” n'a pas d'impact sur le protocole. Le changement à la restriction sur les noms n'aura probablement pas d'impact, car la RFC 1034 ne contenait pas de spécification de quand et comment appliquer la restriction.

1.3.3 Considérations sur les types particuliers

Le présent document décrit la sémantique des RRSet à caractère générique pour les types "intéressants" ainsi que pour les caractères génériques non terminaux vides. La compréhension de ces situations dans le contexte des caractères génériques a été obscurcie parce que ces types subissent un traitement particulier si il sont le résultat d'une correspondance exacte. Cette discussion est à la Section 4.

Ces discussions n'ont pas d'impact de mise en œuvre ; elles couvrent la connaissance existante des types, mais avec un niveau de détail supérieur.

1.4 Terminologie standard

Le présent document n'utilise pas les termes définis dans "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigences" [RFC2119].

Les citations de la RFC 1034 sont notées par un "#" au début de la ligne. Les références au pargraphe "4.3.2" sont supposées se référer au paragraphe 4.3.2 de la RFC 1034, simplement intitulée "Algorithme".

2. Syntaxe de caractère générique

La syntaxe d'un caractère générique est la même que dans tout autre enregistrement de ressource du DNS, sur toutes les classes et types. La seule caractéristique significative est le nom de propriétaire.

Parce que les caractères génériques sont codés comme des enregistrements de ressource avec des noms spéciaux, ils sont inclus dans des transferts de zone et des transferts de zone incrémentaires [RFC1995] juste comme le sont des

enregistrements de ressource qui ne sont pas à caractère générique. Cette caractéristique a été sous appréciée jusqu'aux discussions sur les autres approches des caractères génériques qui sont apparues sur les listes de diffusion.

2.1 Identification d'un caractère générique

Pour donner une description plus précise des caractères génériques, la définition doit commencer par une discussion des noms de domaines qui apparaissent comme propriétaires. Deux nouveaux termes sont nécessaires, "étiquette astérisque" et "nom de domaine à caractères génériques".

2.1.1 Nom de domaine à caractère générique et étiquette astérisque

Un "nom de domaine à caractères génériques" est défini comme ayant son étiquette initiale (c'est-à-dire, la plus à gauche ou de moindre poids) qui est, en format binaire : 0000 0001 0010 1010 (binaire) = 0x01 0x2a (hexadécimal)

Le premier octet est le type normal d'étiquette et la longueur pour une étiquette de un octet, et le second octet est la représentation ASCII [RFC20] du caractère '*'.

Un nom descriptif d'une étiquette égale à cette valeur est une "étiquette astérique".

La définition de la RFC 1034 du caractère générique serait "un enregistrement de ressource possédé par un nom de domaine à caractères génériques".

2.1.2 Astérisques et autres caractères

Aucune valeur d'étiquette autre que celle du paragraphe 2.1.1 n'est une étiquette astérisque, donc les noms qui commencent par d'autres étiquettes ne sont jamais des noms de domaine à caractère générique. Des étiquettes comme “le *” et “**” ne sont pas des étiquettes astérisques, de sorte que ces étiqueettes ne commencent pas des noms de domaine à caractères génériques.

2.1.3 Noms de domaine à caractère générique non terminal

Le paragraphe 4.3.3 déclare :

…..... Le nom de propriétaire des RR à caractères génériques est de la forme "*.<toutdomaine>", où #<toutdomaine> est tout nom de domaine. <toutdomaine> ne devrait pas contenir d'autre étiquette *.

Cette restriction est maintenant supprimée. Sa documentation d'origine est incomplète et la restriction ne sert à rien au vu de l'expérience de plusieurs années de fonctionnement.

Il y avait trois raisons possibles pour la mise en place de la restriction, mais aucune des trois n'a tenu au fil du temps. Une est que la restriction signifiait qu'il n'y aurait jamais de sous domaines des noms de domaine à caractère générique, mais la restriction telle que déclarée permettait quand même, par exemple "exemple.*.exemple.". Une autre est que les noms de domaine à caractères génériques ne sont pas destinés à être des non terminaux vides, mais cette situation n'interrompt pas l'algorithme de 4.3.2. Finalement, les noms de domaine à caractère générique "incorporés" ne sont pas ambigus une fois que le concept du plus proche enrobant a été documenté.

Un nom de domaine à caractères génériques peut avoir des sous domaines. Il n'est pas besoin d'inspecter les sous domaines pour voir si il y a une autre étiquette astérisque dans un sous domaine.

Un nom de domaine à caractères génériques peut être un non terminal vide. (Voir les paragraphes à venir sur les non terminaux vides.) Dans ce cas, toute recherche qui le rencontre va se terminer comme le ferait toute correspondance de non terminal vide.

2.2 Règles d'existence

La notion qu'un nom de domaine “existe” est mentionnée dans la définition des caractères génériques. Au paragraphe 4.3.3 de la RFC 1034 :
Les RR à caractères génériques ne s'appliquent pas :
...

- Quand le nom d'interrogation ou un nom entre le domaine à caractères génériques et le nom d'interrogation est connu
pour exister.

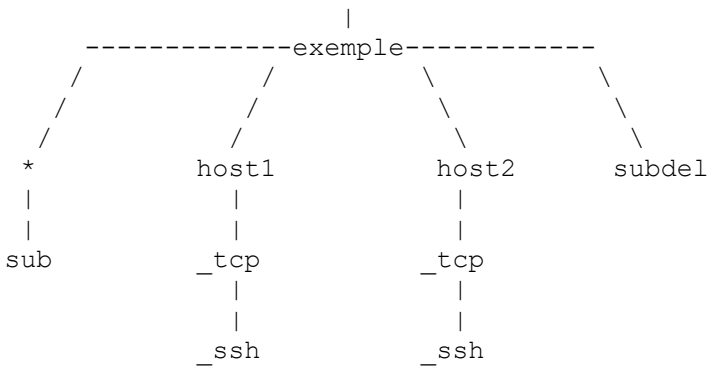
"Existence" est donc un important concept pour comprendre les caractères génériques. Malheureusement, la définition de ce qui existe, dans la RFC 1034, n'est pas clair. Donc, dans les paragraphes 2.2.2. et 2.2.3, un autre regard est porté sur la définition de “existence”.

2.2.1 Exemple

Pour illustrer ce qu'on entend par “existence”, considérons cette zone complète :

```
$ORIGIN exemple.
exemple.              3600 IN  SOA   <SOA RDATA>
exemple.              3600     NS    ns.exemple.com.
exemple.              3600     NS    ns.exemple.net.
*.exemple.            3600     TXT   "ceci est un caractère générique"
*.exemple.            3600     MX    10 host1.exemple.
sub.*.exemple.        3600     TXT   "ceci n'est pas un caractère générique"
host1.exemple.        3600     A     192.0.2.1
_ssh._tcp.host1.exemple. 3600  SRV   <SRV RDATA>
_ssh._tcp.host2.exemple. 3600  SRV   <SRV RDATA>
subdel.exemple.       3600     NS    ns.exemple.com.
subdel.exemple.       3600     NS    ns.exemple.net.
```

On s'aidera d'une streucture arborescente des noms de domaines :



Les réponses suivantes vont être synthétisée à partir d'un des caractères génériques dans la zone :

QNAME=host3.exemple. QTYPE=MX, QCLASS=IN
la réponse va être un "host3.exemple. IN MX ..."

QNAME=host3.exemple. QTYPE=A, QCLASS=IN
la réponse va refléter "pas d'erreur, mais pas de données" parce que il n'y a pas de RRSet A à “*.exemple.”

QNAME=foo.bar.exemple. QTYPE=TXT, QCLASS=IN
la réponse va être "foo.bar.exemple. IN TXT ..." parce que bar.exemple. n'existe pas, mais le caractère générique existe.

Les réponses suivantes ne vont être synthétisée à partir d'aucun caractère générique dans la zone:

QNAME=host1.exemple., QTYPE=MX, QCLASS=IN
parce que host1.exemple. existe

QNAME=sub.*.exemple., QTYPE=MX, QCLASS=IN
parce que sub.*.exemple. existe

QNAME=_telnet._tcp.host1.exemple., QTYPE=SRV, QCLASS=IN
parce que _tcp.host1.exemple. existe (sans données)

QNAME=host.subdel.exemple., QTYPE=A, QCLASS=IN
parce que subdel.exemple. existe (et est une coupure de zone)

QNAME=ghost.*.exemple., QTYPE=MX, QCLASS=IN
parce que *.exemple. existe

L'exemple final souligne une erreur de conception courante sur les caractères génériques. Un caractère générique "se bloque lui-même" en ce sens qu'un caractère générique ne correspond pas à ses propres sous domaines. C'est-à-dire, "*.exemple." ne correspond pas à tous les noms dans la zone "exemple." ; il échoue à correspondre aux noms en-dessous de "*.exemple.". Pour couvrir les noms en dessous de "*.exemple.", un autre nom de domaine à caractères génériques est nécessaire --"*.*.exemple."-- qui couvre tous les sous domaines sauf le sien propre.

2.2.2 Non terminaux vides

Les non terminaux vides (paragraphe 7.16 de la [RFC2136]) sont des noms de domaines qui ne possèdent pas d'enregistrements de ressource mais ont des sous domaines qui en possèdent. Au paragraphe 2.2.1, "_tcp.host1.exemple." est un exemple de nom de non terminal vide. Les non terminaux vides sont introduits par ce texte au paragraphe 3.1 de la RFC 1034 :

L'espace de nom de domaine est une structure arborescente. Chaque nœud et feuille sur l'arborescence correspond à un
ensemble de ressources (qui peut être vide). Le système des domaines ne fait pas de distinction entr les utilisations des
nœuds et feuilles intérieurs, et le présent mémoire utilise le terme de "nœud" pour se référer aux deux.

Le "qui peut être vide" entre parenthèses spécifie que des non terminaux vides sont explicitement reconnus et que des non terminaux vides "existent".

Un lecture pédante du paragraphe ci-dessus peut conduire à une interprétation que tous les domaines possibles existent – jusqu'à la limite suggérée de 255 octets pour un nom de domaine [RFC1035]. Par exemple, www.exemple. peut avoir un RR A, et pour autant que la pratique soit concernée, est une feuille de l'arborescence des domaines. Mais la définition peut être prise comme signifiant qu'un “sub.www.exemple.” existe aussi, quoique sans données. Par extension, tous les domaines possibles existent, de la racine à l'extrémité.

Comme la RFC 1034 définit aussi "une erreur de nom d'autorité qui indique que le nom n'existe pas" au paragraphe 4.3.1, ce n'est apparemment pas l'intention de la définition d'origine, justifiant le besoin d'une mise à jour de la définition au paragraphe suivant.

2.2.3 Autre définition de "existence"

La formulation de la RFC 1034 est corrigée par le paragraphe qui suit :

L'espace de nom de domaine est une structure arborescente. Les nœuds de l'arborescence possèdent au moins un RRSet et/ou ont des descendants qui possèdent collectivement au moins un RRSet. Il ne peut exister un nœud sans RRSet que si il a des descendants qui en ont ; ce nœud est un non terminal vide.

Un nœud sans descendant est un nœud feuille. Il n'existe pas de nœud feuille vide.

Noter qu'à une frontière de zone, le nom de domaine possède des données, incluant le RRSet NS. Dans la zone déléguante, le RRSet NS n'est pas d'autorité, mais c'est sans conséquence ici. Le nom de domaine possède des donnes ; donc il existe.

2.3 Quand un nom de domaine à caractère générique est il non spécial ?

Quand un nom de domaine à caractères génériques apparaît dans la section interrogation d'un message, aucun traitement spécial ne survient. Une étiquette astérisque dans un nom d'interrogation correspond seulement à une seule étiquette astérisque correspondante dans l'arborescence de la zone existante quand l'algorithme du paragraphe 4.3.2 est suivi.

Quand un nom de domaine à caractères génériques apparaît dans les données de ressource d'un enregistrement, aucun traitement spécial ne survient. Une étiquette astérisque dans ce contexte signifie littéralement juste un astérisque.

3. Impact d'un nom de domaine à caractère générique sur une réponse

La descritption de la RFC 1034 de comment les caractères génériques impactent la génération de la réponse est dans son paragraphe 4.3.2. Ce passage contient l'algorithme suivi par un serveur pour construire une réponse. Au sein de cet algorithme, l'étape 3, partie 'c' définit le comportement du caractère générique.

L'algorithme du paragraphe 4.3.2 n'est pas destiné à être du pseudo-code ; c'est-à-dire, ses étapes ne sont pas destinées à être suivies dans un ordre strict. L'algorithme est un moyen suggéré pour mettre en œuvre les exigences. À ce titre, dans l'étape 3, les parties 'a', 'b', et 'c' n'ont pas à être mises en œuvre dans cet ordre, pourvu que le résultat du code mis en œuvre soit conforme à la spécification du protocole.

3.1 Étape 2

L'étape 2 du paragraphe 4.3.2 dit :

2. Chercher les zones disponibles pour la zone qui est le plus proche ancêtre du QNAME. Si une telle zone est trouvée,
passer à l'étape 3, autrement, passer à l'étape 4.

Dans cette étape, la zone la plus appropriée pour la réponse est choisie. La signification de cette étape est que toute l'étape 3 est effectuée au sein d'une zone. Cela a un sens quand on examine si un RR SOA peut ou non être utilisé pour la synthèse.

3.2 Étape 3

L'étape 3 est dominée par trois parties, marquées 'a', 'b', et 'c'. Mais le début de l'étape est important et mérite des explications.

3. Commencer la recherche de correspondance dans la zone, étiquette par étiquette. Le processus de confrontation peut
s'achever de plusieurs manières :

Le mot “correspondance”'se réfère à la correspondance d'étiquettes. Le concept se fonde sur l'idée de la zone comme arborescence des noms existants. Le nom d'interrogation est considéré comme étant une séquence ordonnée d'étiquettes – comme si le nom était un chemin de la racine au propriétaire des données désirées (ce qu'il est – 3ème alinéa du paragraphe 3.1 de la RFC 1034).

Le processus de correspondance d'étiquette d'un nom d'interrogation termine exactement un des trois choix, les parties 'a', 'b', et 'c'. Soit le nom est trouvé, le nom est en dessous d'un point de coupure, soit le nom n'est pas trouvé.

Une fois choisie une des parties, les autres parties ne sont pas considérées (par exemple, on n'exécute pas la partie 'c' pour ensuite changer le chemin d'exécution poiur finir dans la partie 'b'). Le processus de correspondance d'étiquette est aussi fait indépendamment du type d'interrogation (QTYPE).

Les parties 'a' et 'b' ne posent pas de problème pour ces clarifications car elles n'ont pas de rapport avec la synthèse d'enregistrements. La partie 'a' est une correspondance exacte qui résulte en une réponse ; la partie 'b' est un référant.

3.3 Partie 'c'

Le contexte de la partie 'c' est que le processus de correspondance d'étiquettes sur les étiquettes du nom d'interrogation a résulté en une situation où il n'y a pas d'étiquette correspondante dans l'arborescence. C'est comme si la recherche était "tombée de l'arbre".

c. Si à une certaine étiquette, une correspondance est impossible (c'est-à-dire, l'étiquette correspondante n'existe pas)
chercher si [...] l'étiquette "*" existe.

Pour aider à décrire le processus de recherche “pour voir si [...] l'étiquette "*" existe”, un terme a été inventé pour décrire le dernier domaine (nœud) qui correspondait. Ce terme est "plus proche enrobant".

3.3.1 Plus proche enrobant et source de synthèse

Le plus proche enrobant est le nœud qui dans l'arborescence des noms de domaine existants de la zone a le plus d'étiquettes correspondant au nom d'interrogation (consécutivement, en comptant à partir de l'étiquette racine). Chaque correspondance est une "correspondance d'étiquette" et l'ordre des étiquettes est le même.

Le plus proche enrobant est, par définition, un nom existant dans la zone. Le plus proche enrobant peut être un non terminal vide ou même être lui-même un nom de domaine à caractères génériques. En aucune circonstance le plus proche enrobant ne va être utilisé pour synthétiser des enregistremens pour l'interrogation en cours.

La source de synthèse est définie dans le contexte d'un processus d'interrogation comme le nom de domaine à caractères génériques qui descend immédiatement du plus proche enrobant, pourvu que ce nom de domaine à caractères génériques existe. "Qui descend immédiatement" signifie que la source de synthèse a un nom de forme <étiquette astérisque>.<plus proche enrobant>.

Une source de synthèse ne garantit pas d'avoir un RRSet à utiliser pour la synthèse. La source de synthèse pourrait être un non terminal vide.

Si la source de synthèse n'existe pas (n'est pas dans l'arborescence du domaine) il n'y aura pas de synthèse de caractère générique. Il n'y a pas de recherche pour une solution de remplacement.

Le concept important est que pour tout processus de recherche donné, il y a au plus un endroit où l'enregistrement synthétique de caractère générique peut être obtenu. Si la source de synthèse n'existe pas, la recherche se termine, et ne cherche pas d'autres enregistrements à caractère générique.

3.3.2 Exemples de plus proche enrobant et source de synthèse

Pour illustrer, en utilisant l'exemple de zone du paragraphe 2.2.1 du présent document, le diagramme suivant montre les QNAME et les plus proches enrobants.

QNAME	Plus proche enrobant	Source de synthèse
host3.exemple.	exemple.	*.exemple.
_telnet._tcp.host1.exemple.	_tcp.host1.exemple.	pas de source
_dns._udp.host2.exemple.	host2.exemple.	pas de source
_telnet._tcp.host3.exemple.	exemple.	*.exemple.
_chat._udp.host3.exemple.	exemple.	*.exemple.
foobar.*.exemple.	*.exemple.	pas de source

3.3.3 Correspondance de type

La RFC 1034 conclut la partie 'c' avec :

Si l'étiquette "*" n'existe pas, vérifier si le nom recherché est le QNAME original dans l'interrogation ou un nom qui a
été suivi à cause d'un CNAME. Si le nom est original, établir une erreur de nom d'autorité dans la réponse et sortir.
Autrement, juste sortir.
#
Si l'étiquette "*" n'existe pas, confronter les RR à ce nœud au QTYPE. Si il en est qui correspondent, les copier dans la
section réponse, mais régler le propriétaire du RR à être le QNAME, et non le nœud avec l'étiquette "*". Passer à
l'étape 6.

Le paragraphe final couvre le rôle du QTYPE dans le processus de recherche.

Sur la base des retours et similarités de mise en œuvre entre la partie 'a' et la partie 'c', un changement a été fait à ce passage.

Le changement est d'ajouter le texte qui suit à la partie 'c' avant l'instruction "Passer à l'étape 6":

Si les données de la source de synthèse sont un CNAME, et si le QTYPE ne correspond pas au CNAME, copier le RR CNAME dans la section Réponse de la réponse en changeant le nom de propriétaire en le QNAME, changer le QNAME en le nom canonique dans le RR CNAME, et revenir à l'étape 1.

C'est essentiellement le même texte que dans la partie 'a' qui couvre le traitement des RRSet CNAME.

4. Considérations sur les types spéciaux

Les Sections 2 et 3 du présent document discutent de la synthèse de caractères génériques par raport au noms dans l'arborescence des domaines et ignorent l'impact des types. Dans cette section, les implication des caractères génériques de types spécifiques sont discutées. Les types couverts sont ceux qui se sont révélés être les plus difficiles à comprendre. Les types sont SOA, NS, CNAME, DNAME, SRV, DS, NSEC, RRSIG, et "none", c'est-à-dire, les noms de domaine à caractères génériques non terminal vide.

4.1 RRSet SOA à un nom de domaine avec caractère générique

Un nom de domaine à caractères génériques qui possède un RRSet SOA signifie que le domaine est à la racine de la zone (apex). Le domaine ne peut pas être une source de synthèse parce que c'est, par définition, un nœud descendant (du plus proche enrobant) et un apex de zone est au sommet de la zone.

Bien qu'un nom de domaine à caractères génériques possédant un RRSet SOA ne puisse jamais être une source de synthèse, il n'y a pas de raison d'interdire la possession d'un RRSet SOA.

Par exemple, dans cette zone :

```
$ORIGIN *.exemple.
@           3600 IN  SOA   <SOA RDATA>
            3600     NS    ns1.exemple.com.
            3600     NS    ns1.exemple.net.
www         3600     TXT   "the www txt record"
```

Une interrogation sur l'enregistrement TXT de www.*.exemple. va tout de même trouver la réponse "the www txt record". L'étiquette astérisque ne devient significative que quand le paragraphe 4.3.2, étape 3, partie 'c' entre en jeu.

Bien sûr, il faut qu'il y a ait une délégation dans la zone parente, "exemple." pour que cela fonctionne. Ceci est couvert par le paragraphe suivant.

4.2 RRSet NS à un nom de domaine avec caractère générique

Avec la définition du DNSSEC [RFC4033], [RFC4034], RFC4035] qui est maintenant en place, la sémantique d'un nom de domaine à caractères génériques possédant un RRSet NS se trouve être défectueuse. Le dilemme se rapporte à un conflit entre les règles pour la synthèse dans la partie 'c' et le fait que la synthèse résultante génère un enregistrement pour lequel la zone n'est pas d'autorité. Dans une zone DNSSEC signée, les mécanismes de gestion de signature (génération et inclusion dans un message) sont devenus peu clairs.

Les points saillants de la discussion du groupe de travail sur ce sujet sont résumés au paragraphe 4.2.1.

Par suite de ces discussions, aucune définition n'est donnée pour les noms de domaine à caractère générique possédant un RRSet NS. La sémantique est laissée indéfinie jusqu'à ce qu'il y ait un besoin clair d'avoir un ensemble défini et qu'il y ait une direction claire à suivre. L'inclusion de RRSet NS à caractères génériques dans une zone est déconseillée, mais pas interdite.

4.2.1 Notions éliminées

Avant l'arrivée de DNSSEC, un nom de domaine à caractères génériques possédant un RRSet NS apparaissait comme gérable, et il y a des instances dans lesquelles on en trouve dans des déploiements qui utilisent des mises en œuvre qui prennent cela en charge. Continuer de permettre cela dans la spécification n'est pas tenable avec DNSSEC. La raison en est que la synthèse du RRSet NS est faite dans une zone qui a délégué la responsabilité de ce nom. Cette synthèse "non autorisée" n'est pas un problème pour le protocole DNS de base, mais le DNSSEC expose le problème en affirmant le modèle d'autorisation pour le DNS.

Une interdiction radicale de caractères génériques de type NS est aussi intenable car le protocole DNS ne définit pas comment traiter les données "illégales". Les mises en œuvre peuvent choisir de ne pas charger une zone, mais il n'y a pas de définition dans le protocole. Ce manque de définition est compliqué par le besoin de couvrir la mise à jour dynamique [RFC2136] et les transferts de zone, ainsi que le chargement du serveur maître. Le cas d'un client (résolveur, serveur de mise en antémémoire) qui reçoit un type de NS à caractère générique dans une réponse devrait aussi être considéré.

Étant donné le défi d'une définition complète de la façon d'interdire de tels enregistrements, traiter les mises en œuvre existantes qui permettent aujourd'hui ces enregistrements est une complication supplémentaire. Il ya des utilisations de nom de domaine à caractères génériques possédant des RRSet NS.

Un compromis proposé serait de redéfinir les caractères génériques de type NS comme n'étant pas utilisés dans la synthèse, ce compromis ne tient pas parce que il aurait exigé des ajouts significatifs au travail de signature et validation de DNSSEC. (Là encore, DNSSEC attrape les données non autorisées.)

Comme il ne s'est pas formé de clair consensus sur la solution de ce dilemme, et que la réalité est que des caractères génériques de type NS sont une rareté dans les opérations, le mieux est de laisser la question ouverte jusqu'à ce que cela "paraisse important".

4.3 RRSet CNAME à un nom de domaine avec caractère générique

La question d'un RRSet CNAME possédé par un nom de domaine à caractères génériques a invité au changement suggéré au dernier paragraphe de l'étape 3c de l'algorithme du 4.3.2. Le texte changé apparaît au paragrahe.3.3 du présent document.

4.4 RRSet DNAME à un nom de domaine avec caractère générique

La propriété d'un RRSet DNAME [RFC2672] par un nom de domaine à caractères génériques représente une menace pour la cohérence du DNS et doit être évitée ou radicalement rejetée. Un tel RRSet DNAME représente une synthèse non déterministe des règles alimentées aux différentes antémémoires. Comme les antémémoires sont alimentées avec les différentes règles (d'une façon non prévisible) les antémémoires cessent d'être cohérentes. ("Comme les antémémoires sont alimentées" se réfère à la mémorisation dans une antémémoire d'enregistrements obtenus dans les réponses par les serveurs récurrents ou itératifs.)

Par exemple, supposons qu'une antémémoire, répondant à une demande récurrente, obtienne l'enregistrement suivant : "a.b.exemple. DNAME foo.bar.exemple.net."

et qu'une autre antémémoire obtienne : "b.exemple. DNAME foo.bar.exemple.net."

toutes deux générées à partir de l'enregistrement : "*.exemple. DNAME foo.bar.exemple.net."

par un serveur d'autorité.

La spécification de DNAME n'est pas claire sur le point de savoir si les enregistrements DNAME dans une antémémoire sont utilisées pour réécrire les interrogations. Dans certaines interprétations, la réécriture survient, dans d'autres, non. En permettant l'occurrence de reécriture, les interrogations pour "sub.a.b.exemple. A" peuvent être reécrites comme "sub.foo.bar.tld. A" par l'ancien serveur qui met en antémémoire et peuvent être reécrites comme "sub.a.foo.bar.tld. A" par le dernier. La cohérence est perdue, et un fonctionnement cauchemardesque s'ensuit.

Un autre justification de la recommandation d'éviter d'utiliser des enregistrements DNAME à caractères génériques est l'observation qu'un tel enregistrement pourrait synthétiser un DNAME possédé par "sub.foo.bar.exemple." et "foo.bar.exemple.". Il y a une restriction dans la définition de DNAME qu'aucun domaine n'existe en dessous d'un domaine possédant un DNAME ; donc, le DNAME à caractère générique est à éviter.

4.5 RRSet SRV à un nom de domaine avec caractère générique

La définition du RRSet SRV est dans la [RFC2782]. Dans la définition de l'enregistrement, il y a une certaine confusion sur le terme "Nom". La définition se lit comme suit :

Le format du RR SRV
...

```
#    _Service._Proto.Name TTL Class SRV Priority Weight Port Target

# Nom
# C'est le domaine auquel ce RR se réfère. Le RR SRV est unique en ce que le nom qu'on recherche n'est pas ce nom ;
# l'exemple près de la fin le montre clairement.
```

Ne pas confondre la définition de "Npm" avec le nom du propriétaire. C'est-à-dire, une fois retirées les étiquettes _Service et _Proto du nom du propriétaire du RRSet SRV, ce qui reste pourrait être un nom de domaine à caractères génériques mais ceci est immatériel pour le RRSet SRV.

Par exemple, si un enregistrement SRV est le suivant :

```
_foo._udp.*.exemple. 10800 IN SRV 0 1 9 old-slow-box.exemple.
```

.exemple est un nom de domaine à caractères génériques et bien qu'il soit le Nom du RR SRV, il n'est pas le propriétaire (nom de domaine). Le nom de domaine propriétaire est "_foo._udp..exemple.", qui n'est pas un nom de domaine à caractères génériques.

Une interrogation pour le RRSet SRV de "_foo._udp.bar.exemple." (classe IN) va résulter en une correspondance du nom "*.exemple." (en supposant qu'il n'y a pas de bar.exemple.) et aucune correspondance de l'enregistrement SRV montré. Si il n'y a pas de RRSet SRV à "*.exemple.", la section réponse va refléter cela (être vide ou un RRSet CNAME).

La confusion est probablement fondée sur le mélange de la spécification du RR SRV RR et de la description d'un "cas d'utilisation".

4.6 RRSet DS à un nom de domaine avec caractère générique

Un RRSet DS possédé par un nom de domaine à caractères génériques est sans signification et sans dommage. Cette déclaration est faite dans le contexte où un RRSet NS à un nom de domaine à caractères génériques est indéfini. À un point de non délégation, un RRSet DS n'a pas de valeur (aucun RRSet DNSKEY correspondant ne va être utilisé dans la validation DNSSEC). Si il y a un RRSet DS synthétisé, lui seul ne sera pas très utile car il existe dans le contexte d'un point de délégation.

4.7 RRSet NSEC à un nom de domaine avec caractère générique

Les noms de domaine à caractères génériques dans les zones DNSSEC signées vont avoir un RRSet NSEC. La synthèse de ces enregistrement ne va se produire que quand l'interrogation correspond exactement à l'enregistrement. Les RR NSEC synthétisés ne sont pas dommageables car ils ne vont jamais être utilisés dans une mise en antémémoire négative ou pour générer une réponse négative [RFC2308].

4.8 RRSIG à un nom de domaine avec caractère générique

Les enregistrements RRSIG vont être présents à un nom de domaine à caractères génériques dans une zone signée et vont être synthétisés avec les données recherchées dans l'interrogation. Le fait que le nom de propriétaire soit synthétisé n'est pas un problème car le compte d'étiquettes dans le RRSIG va dire au code de vérification de l'ignorer.

4.9 Nom de domaine avec caractère générique non terminal vide

Si une source de synthèse est un non terminal vide, alors la réponse va être soit pas d'erreur dans le code de retour soit pas de RRSet dans la section réponse.

5. Considérations sur la sécurité

Le présent document précise les spécifications pour rendre plus probable que la sécurité puisse être ajoutée au DNS. Aucun ajout fonctionnel n'est fait, et on précise seulement ce qui est considéré comme approprié pour permettre que le DNS, la sécurité du DNS, et les extensions au DNS, soient plus prévisibles.

6 Références

6.1 Références normatives

[RFC0020] V. Cerf, "Format ASCII pour les échanges sur les réseaux", octobre 1969. (STD80)

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[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)

[RFC1995] M. Ohta, "Transferts de zone par incréments dans le DNS", RFC 1995, août 1996.

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

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par les RFC* 4033, 4034, 4035, 6604, 8020) *(P.S.)*

[RFC2672] M. Crawford, "Renumérotage d'un sous-ensemble non terminal du DNS", août 1999. (*MàJ par* RFC4592, RFC6604)) (*Remplacée par la* RFC6672) *(P.S.)*

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198

6.2 Références pour information

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

7. Autres contributeurs à ce document

Le présent document représente les efforts d'un grand groupe de travail. L'éditeur a simplement collecté ses connaisances collectives.

Les commentaires sur le présent document peuvent être envoyés à l'éditeur sur la liste de diffusion du groupe de travail DNSEXT à namedroppers@ops.ietf.org .

Adresse de l'éditeur

Edward Lewis
NeuStar
46000 Center Oak Plaza
Sterling, VA
20166, US

téléphone : +1-571-434-5468
mél : ed.lewis@neustar.biz

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif (IASA) de l'IETF.