Groupe de travail Réseau
Request for Comments : 2672
Catégorie : En cours de normalisation

M. Crawford, Fermilab
août 1999
Traduction Brière de L'Isle

Renumérotage d'un sous-ensemble non terminal du DNS

1. Introduction

Le présent document définit un nouvel enregistrement de ressource du DNS appelé "DNAME", qui offre la capacité de transposer une sous-arborescence entière de l'espace de noms du DNS dans un autre domaine. Il diffère de l'enregistrement CNAME qui transpose un seul nœud de l'espace de noms.

Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", et "PEUT" du présent document doivent être interprétés tel que défini dans la [RFC2119].

2. Motifs

Cet enregistrement de ressource et ses règles de traitement ont été conçus comme une solution au problème de la conservation des transpositions d'adresse en nom dans un contexte de dénumérotation de réseau. Sans le mécanisme DNAME, un serveur DNS d'autorité pour les transpositions d'adresse en nom d'un certain réseau doit être reconfiguré lorsque ce réseau est dénuméroté. Avec DNAME, la zone peut être construite de telle sorte qu'elle n'ait besoin d'aucune renumérotation lorsque cela survient. DNAME peut aussi être utile dans d'autres situations, telles que lorsque une unité d'organisation est renommée.

3. L'enregistrement de ressource DNAME

Le RR DNAME a le mnémonique DNAME et le code de type 39 (décimal).

DNAME a le format suivant :

<propriétaire> <ttl> <classe> DNAME <cible>

Le format n'est pas sensible à la classe. Tous les champs sont exigés. Le champ de RDATA <cible> est un <nom de domaine> [RFC2065].

Le RR DNAME cause le traitement de la section additionnelle NS de type.

L'effet de l'enregistrement DNAME est la substitution de la <cible> de l'enregistrement par son <propriétaire> comme suffixe d'un nom de domaine. Une limitation "no-descendants" gouverne l'utilisation des DNAME dans un fichier de zone:

Si un RR DNAME est présent à un nœud N, il peut y avoir d'autres données à N (sauf un CNAME ou un autre DNAME), mais il NE DOIT y avoir de données chez aucun descendant de N. Cette restriction ne s'applique qu'aux enregistrements de la même classe que l'enregistrement DNAME.

Cette règle assure la prévisibilité des résultats lorsque un enregistrement DNAME est mis en antémémoire par un serveur qui n'est pas d'autorité pour la zone de l'enregistrement. Elle DOIT être mise en application lorsque des données de zone d'autorité sont chargées. Conjointement avec les règles pour l'autorité de zone DNS [RFC1035] cela implique que les enregistrements DNAME et NS ne peuvent coexister qu'au sommet d'une zone qui a seulement un nœud.

Le schéma de compression de la [RFC2065] NE DOIT PAS être appliqué à la portion RDATA d'un enregistrement DNAME sauf si le serveur qui envoie a un moyen de savoir que le receveur comprend le format d'enregistrement DNAME. La signalisation d'une telle compréhension fera l'objet de futures extensions du DNS.

Les boucles de dénomination peuvent être créées avec les enregistrements DNAME ou une combinaison d'enregistrements DNAME et CNAME, exactement comme elles peuvent l'être avec des enregistrements CNAME seuls. Les résolveurs, y compris les résolveurs incorporés dans les serveurs du DNS, DOIVENT limiter les ressources qu'ils dédient à une interrogation. Les développeurs devraient noter cependant que de très longues chaînes d'enregistrements DNAME peuvent être valides.

4. Traitement de l'interrogation

Pour exploiter le mécanisme DNAME, les algorithmes de résolution de nom de la [RFC1034] doivent être légèrement modifiés aussi bien pour les serveurs que les résolveurs.

Les deux algorithmes modifiés incorporent l'opération qui effectue une substitution sur un nom (QNAME ou SNAME) sous le contrôle d'un enregistrement DNAME. Cette opération sera appelée la "substitution DNAME".

4.1 Traitement par les serveurs

Pour un serveur qui effectue un service non récurrent, les étapes 3.c et 4 du paragraphe 4.3.2 de la [RFC1034] sont changées pour chercher un enregistrement DNAME avant de chercher une étiquette de caractère générique ("*") et retourner certains enregistrements DNAME des données de zone et de l'antémémoire.

Les clients DNS qui envoient des interrogations DNS étendues [RFC2671] avec la version 0 ou des interrogations non étendues sont supposés ne pas comprendre la sémantique de l'enregistrement DNAME, de sorte qu'un serveur qui met en œuvre la présente spécification, lorsque il répond à une interrogation non étendue, DEVRAIT synthétiser un enregistrement CNAME pour chaque enregistrement DNAME rencontré durant le traitement de l'interrogation pour aider le client à atteindre les données DNS correctes. Le comportement des clients et des serveurs sous les versions de DNS étendu supérieures à 0 sera spécifié lorsque ces versions seront définies.

Le RR CNAME synthétisé, si il est fourni, DOIT avoir la même CLASSE que la QCLASS de l'interrogation, et un TTL égal à zéro,

Un <propriétaire> égal au QNAME en effet au moment où le RR DNAME a été rencontré, et un champ RDATA contenant le nouveau QNAME formé par l'action de la substitution DNAME.

Si le serveur a la clé en ligne appropriée [RFC2065], [RFC2137], il PEUT générer et retourner un RR SIG pour le RR CNAME synthétisé.

L'algorithme révisé de serveur est :

1. Établir ou retirer la valeur de récurrence disponible dans la réponse selon que le serveur de noms veut ou non fournir le service récurrent. Si le service récurrent est disponible et demandé via le bit RD dans l'interrogation, passer à l'étape 5, autrement passer à l'étape 2.

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

3. Commencer à rechercher les correspondances, étiquette par étiquette, dans la zone. Le processus de correspondance peut se terminer de plusieurs façons :

   a. Si la correspondance du QNAME tout entier est trouvée, on a trouvé le nœud.

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

      Autrement, copier tous les RR qui correspondent au QTYPE dans la section réponse et passer à l'étape 6.

b. Si une correspondance nous faisait sortir des données d'autorité, nous avons une référence documentaire. Cela arrive lorsque on rencontre un nœud avec des RR NS qui marquent des coupures le long du fond d'une zone.

   Copier les RR NS pour la sous-zone dans la section autorité de la réponse. Mettre toute adresse disponible dans la section additionnelle, en utilisant les RR glu si les adresses ne sont pas disponibles à partir des données d'autorité ou de l'antémémoire. Passer à l'étape 4.

c. Si pour certaines étiquettes, une correspondance est impossible (c'est-à-dire, si l'étiquette correspondante n'existe pas), chercher à voir si la dernière étiquette correspondait à un enregistrement DNAME.

   Si un enregistrement DNAME existe à ce point, le copier dans la section réponse. Si la substitution de sa <cible> par son <propriétaire> dans QNAME débordait de la taille légale d'un <nom de domaine>, régler RCODE à YXDOMAIN [RFC2136] et sortir ; autrement, effectuer la substitution et continuer. Si l'interrogation n'était pas étendue [RFC2671] avec une Version indiquant la compréhension de l'enregistrement DNAME, le serveur DEVRAIT synthétiser un enregistrement CNAME comme décrit ci-dessus et l'inclure dans la section réponse. Retourner à l'étape 1.

   Si il n'y avait pas d'enregistrement DNAME, chercher à voir si l'étiquette "*" existe.

   Si l'étiquette "*" n'existe pas, vérifier si le nom recherché est le QNAME original dans l'interrogation ou si c'est un nom qui a été suivi du fait d'un CNAME. Si le nom est l'original, établir une erreur de nom d'autorité dans la réponse et sortir. Autrement, simplement sortir.

   Si l'étiquette "*" existe bien, confronter les RR de ce nœud au QTYPE. S'il en est qui correspondent, les copier dans la section réponse, mais régler le propriétaire du RR comme étant le QNAME, et non pas le nœud qui a l'étiquette "*". Passer à l'étape 6.

4. Commencer les confrontations dans l'antémémoire. Si le QNAME est trouvé dans l'antémémoire, copier tous les RR qui lui sont rattaché et qui correspondent au QTYPE dans la section réponse. Si le QNAME n'est pas trouvé dans l'antémémoire mais si un enregistrement DNAME est présent chez un ancêtre de QNAME, copier cet enregistrement DNAME dans la section réponse. Si il n'y avait pas de délégation des données d'autorité, chercher la meilleure parmi celles de l'antémémoire, et la mettre dans la section autorité. Passer à l'étape 6.

5. Utiliser le résolveur local ou une copie de son algorithme (voir au paragraphe suivant) pour répondre à l'interrogation. Mémoriser le résultat, y compris tous les CNAME et DNAME intermédiaires, dans la section réponse de la réponse.

6. En utilisant seulement les données locales, essayer d'ajouter d'autres RR qui pourraient être utiles à la section additionnelle de l'interrogation. Sortir.

Noter qu'il y aura au plus un ancêtre avec un DNAME comme décrit à l'étape 4 sauf si certaines données de la zone sont en violation de la limitation de la section 3 qui interdit leur présence chez les descendants. Une mise en œuvre peut tirer parti de cette limitation en arrêtant la recherche de l'étape 3c ou de l'étape 4 lorsque un enregistrement DNAME est rencontré.

4.2 Traitement par les résolveurs

Un résolveur, ou un serveur qui fournit le service récurrent, doit être modifié pour traiter un DNAME comme quelque chose d'analogue à un CNAME. L'algorithme de résolveur du paragraphe 5.3.3 de la [RFC1034] est modifié pour renuméroter l'étape 4.d en 4.e et insérer un nouveau 4.d. L'algorithme complet devient :

1. Voir si la réponse est dans les informations locales, et si elle l'est, la retourner au client.
2. Trouver les meilleurs serveurs à interroger.
3. Leur envoyer les interrogations jusqu'à ce que l'un d'eux retourne une réponse.
4. Analyser la réponse :
   a. si elle répond à la question ou contient une erreur de nom, mettre les données en antémémoire tout en les retournant au client ;

   b. si la réponse contient une meilleure délégation sur d'autres serveurs, mettre les informations de délégation en antémémoire, et passer à l'étape 2 ;

   c. si la réponse montre un CNAME et si ce n'est pas la réponse elle-même, mettre le CNAME en antémémoire, changer le SNAME en nom canonique dans le RR CNAME et passer à l'étape 1 ;

   d. si la réponse donne un DNAME et si ce n'est pas la réponse elle-même, mettre le DNAME en antémémoire. Si la substitution de la <cible> du DNAME par son <propriétaire> dans le SNAME débordait de la taille légale pour un <nom de domaine>, retourner une erreur dépendant de la mise en œuvre à l'application ; autrement effectuer la substitution et retourner à l'étape 1 ;

e. si la réponse montre une défaillance du serveur ou d'autres contenus bizarres, supprimer le serveur de la SLIST et retourner à l'étape 3.

Un résolveur ou serveur récurrent qui comprend les enregistrements DNAME mais envoie des interrogations non étendues DOIT augmenter l'étape 4.c en supprimant de la réponse tout enregistrement CNAME qui a un <propriétaire> qui est un sous-domaine du <propriétaire> de tout enregistrement DNAME de la réponse.

5. Exemples d'utilisation

5.1 Changement de dénomination d'une organisation

Si une organisation avec le nom de domaine FROBOZZ.EXAMPLE est incorporée dans une organisation dont le nom de domaine est ACME.EXAMPLE, cela peut faciliter la transition de placer des informations comme celles-ci dans son ancienne zone.

```
frobozz.example. DNAME      frobozz-division.acme.example.
        MX      10      mailhub.acme.example.
```

La réponse à une interrogation récurrente étendue pour www.frobozz.example contiendrait, dans la section réponse, l'enregistrement DNAME indiqué ci-dessus et les RR pertinents pour www.frobozz-division.acme.example.

5.2 Délégation sans classe de préfixes plus courts

Le schéma sans classe pour la délégation in-addr.arpa [RFC2317] peut être étendu aux préfixes plus courts que 24 bits en utilisant l'enregistrement DNAME. Par exemple, le préfixe 192.0.8.0/22 peut être délégué par les enregistrements suivants.

```
$ORIGIN     0.192.in-addr.arpa.
8/22    NS      ns.slash-22-holder.example.
8       DNAME       8.8/22
9       DNAME       9.8/22
10      DNAME       10.8/22
11      DNAME       11.8/22
```

Une entrée typique dans la zone inverse résultante pour certains hôtes à l'adresse 192.0.9.33 pourrait être

```
$ORIGIN     8/22.0.192.in-addr.arpa.
33.9    PTR     somehost.slash-22-holder.example.
```

La même remarque concernant le choix du caractère "/" s'applique ici de même que dans la [RFC2317].

5.3 Prise en charge de la dénumérotation de réseau

Si la dénumérotation des réseaux IPv4 devenait courante, la maintenance de la délégation d'espace d'adresse pourrait être simplifiée par l'utilisation des enregistrements DNAME au lieu des enregistrements NS pour déléguer.

```
$ORIGIN     new-style.in-addr.arpa.
189.190 DNAME       in-addr.example.net.

$ORIGIN     in-addr.example.net.
188     DNAME       in-addr.customer.example.

$ORIGIN     in-addr.customer.example.
1       PTR     www.customer.example.
2       PTR     mailhub.customer.example.
; etc ...
```

Cela permettrait de changer l'espace d'adresse 190.189.0.0/16 alloué au FAI "example.net" sans qu'il soit nécessaire

d'altérer les fichiers de zone qui décrivent l'utilisation de cet espace par le FAI et ses abonnés.

La dénumérotation des réseaux IPv4 est actuellement une tâche si ardue que la mise à jour du DNS est seulement une petite partie du travail, de sorte que ce schéma peut n'avoir qu'une faible valeur. Mais on espère que dans IPv6 la tâche de la dénumérotation sera assez différente et que le mécanisme DNAME pourra jouer un rôle utile.

6. Considérations relatives à l'IANA

Le présent document définit un nouveau type d'enregistrement de ressource du DNS avec le mnémonique DNAME et le code de type 39 (en décimal). L'espace de dénomination/numérotation est défini dans [RFC2065]. Ce nom et numéro a déjà été enregistré par l'IANA.

7. Considérations pour la sécurité

L'enregistrement DNAME est similaire à l'enregistrement CNAME en ce qui concerne les conséquences de l'insertion d'un enregistrement falsifié dans un serveur ou résolveur DNS. Il en diffère en ce que l'effet de DNAME couvre une sous-arborescence entière de l'espace de nom. Les facilités de la [RFC2065] sont disponibles pour authentifier ce type d'enregistrement.

8. Références

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(Information)*

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987.

[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.)*

[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.

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

[RFC2317] H. Eidnes, G. de Groot et P. Vixie, "Délégation IN-ADDR.ARPA sans classe", BCP 20, mars 1998.

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

[RFC2137] D. Eastlake 3rd, "Mise à jour dynamique sécurisée du système de noms de domaines", avril 1997. (*Obsolète, voir* RFC3007) *(MàJ* RFC1035) *(P.S.)*

9. Adresse de l'auteur

Matt Crawford
Fermilab MS 368
PO Box 500
Batavia, IL 60510
USA
téléphone : +1 630 840-3461
mél : crawdad@fnal.gov

10. Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'éditeur des RFC est actuellement fourni pat la Internet Society.