RFC 8375 : Special-Use Domain 'home.arpa.'

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mai 2018

Date de publication du RFC : Mai 2018

https://www.bortzmeyer.org/8375.html

Ce nouveau RFC a l'air compliqué comme cela, mais en fait il ne fait qu'une chose : remplacer, dans le protocole Homenet/HNCP ("*Home Networking Control Protocol*"), le nom de domaine `.home` par `home.arpa`.

`home.arpa` est désormais enregistré dans la liste officielle des noms de domaine spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>, ceux qui ne passent pas par les mécanismes habituels d'enregistrement de noms de domaine, et/ou les mécanismes habituels de résolution DNS. (Cette liste a été créée par le RFC 6761 [1], et critiquée par le RFC 8244. `home.arpa` n'étant pas un TLD, il pose moins de problèmes politiciens.)

Quelle est l'utilité de ce nom `home.arpa` ? La série de protocoles Homenet (l'architecture de Homenet est décrite dans le RFC 7368) vise à doter la maison de l'utilisateur normal (pas participant à l'IETF) d'un ensemble de réseaux IPv6 qui marchent automatiquement, sans intervention humaine. Parmi les protocoles Homenet, HNCP, normalisé dans le protocole RFC 7788 est le protocole de configuration. Il utilise un suffixe pour les noms de domaines comme `nas.SUFFIXE` ou `printer.SUFFIX`. C'est ce `home.arpa` qui va désormais servir de suffixe.

Mais quel était le problème avec le suffixe `.home` du RFC 7788 ? D'abord, le RFC 7788 avait commis une grosse erreur, enregistrée sous le numéro 4677 <https://www.rfc-editor.org/errata_search.php?rfc=7788&eid=4677> : il ne tenait pas compte des règles du RFC 6761, et réservait ce TLD `.home` sans suivre les procédures du RFC 6761. Notamment, il ne listait pas les particularités qui font que ce domaine est spécial (pour `home.arpa`, notre nouveau RFC 8375 le fait dans sa section 5), et il ne demandait pas à l'IANA de le mettre dans le registre des noms de domaine spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6761.txt`

Cela avait des conséquences pratiques comme le fait que ce .home ne pouvait pas marcher à travers un résolveur DNS validant (puisque ce nom n'existait pas du tout dans la racine). Un bon article sur ce choix et sur les problèmes qu'il posait était « "*Homenet, and the hunt for a name*" <https://blog.apnic.net/2017/03/30/ietf-98-chicago-homenet-hunt-name/> ».

On peut aussi ajouter que le risque de « collision » entre deux noms de domaine était élevé puisque pas mal de réseaux locaux sont nommés sous .home et que ce nom est un de ceux qui « fuitent » souvent vers les serveurs racines (voir par exemple les statistiques du serveur racine L <http://stats.dns.icann.org/plotcache/L-Root/qtype_vs_othertld/2017-11-19T00:00-2017-11-19T23:59-all.html>.). On peut consulter à ce sujet les documents de l'ICANN « "*New gTLD Collision Risk Mitigation*" <https://www.icann.org/en/system/files/files/new-gtld-collision-mitigation-05pdf> » et « "*New gTLD Collision Occurence Management*" <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf> ». Notons qu'il y avait eu plusieurs candidatures <https://icannwiki.org/.home> (finalement rejetées en février 2018 <https://www.icann.org/resources/board-material/resolutions-2018-02-04-en#2.c>) pour un .home en cours auprès de l'ICANN. "*Exit*", donc, .home, plus convivial mais trop convoité. Demander à l'ICANN de déléguer un .home pour l'IETF (ce qui aurait été nécessaire pour faire une délégation DNSSEC non signée, cf. RFC 4035, section 4.3) aurait pris dix ou quinze ans.

À la place, voici home.arpa, qui profite du RFC 3172, et du caractère décentralisé du DNS, qui permet de déléguer des noms sous .arpa.

L'utilisation de home.arpa n'est pas limitée à HNCP, tous les protocoles visant le même genre d'usage domestique peuvent s'en servir. Il n'a évidemment qu'une signification locale.

La section 3 décrit le comportement général attendu avec home.arpa. Ce n'est pas un nom de domaine comme les autres. Sa signification est purement locale. printer.home.arpa désignera une machine à un endroit et une autre machine dans une autre maison. Les serveurs DNS globaux ne peuvent pas être utilisés pour résoudre les noms sous home.arpa. Tous les noms se terminant par ce suffixe doivent être traités uniquement par les résolveurs locaux, et jamais transmis à l'extérieur.

Notez que, la plupart du temps, les utilisateurs ne verront pas le suffixe home.arpa, l'interface des applications « "*Homenet*" » leur masquera cette partie du nom. Néanmoins, dans certains cas, le nom sera sans doute visible, et il déroutera sans doute certains utilisateurs, soit à cause du suffixe arpa qui n'a pas de signification pour eux, soit parce qu'ils ne sont pas anglophones et qu'ils ne comprennent pas le home. Il n'y a pas de solution miracle à ce problème.

La section 4 est le formulaire d'enregistrement dans le registre des noms spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>, suivant les formalités du RFC 6761, section 5. (Ce sont ces formalités qui manquaient au RFC 7788 et qui expliquent l'errata <https://www.rfc-editor.org/errata_search.php?rfc=7788&eid=4677>.) Prenons-les dans l'ordre (relisez bien la section 5 du RFC 6761) :

— Les humains et les applications qu'ils utilisent n'ont pas à faire quelque chose de particulier, ces noms, pour eux, sont des noms comme les autres.
— Les bibliothèques de résolution de noms (par exemple, sur Mint, la GNU libc) ne devraient pas non plus appliquer un traitement spécial aux noms en home.arpa. Elles devraient passer par le mécanisme de résolution normal. Une exception : si la machine a été configurée pour utiliser un autre résolveur DNS que celui de la maison (un résolveur public <https://www.bortzmeyer.org/dns-resolveurs-publics.html>, par exemple, qui ne connaîtra pas **votre** home.arpa), il peut être nécessaire de mettre une règle particulière pour faire résoudre ces noms par un résolveur local.

— Les résolveurs locaux (à la maison), eux, **doivent** traiter ces noms à part, comme étant des « zones locales » à l'image de celles décrites dans le RFC 6303. Bref, le résolveur ne doit pas transmettre ces requêtes aux serveurs publics faisant autorité (il y a une exception pour le cas particulier des enregistrements DS). Ils doivent transmettre ces requêtes aux serveurs locaux qui font autorité pour ces noms (cf. section 7).
— Les serveurs publics faisant autorité n'ont pas besoin d'un comportement particulier. Par exemple, ceux qui font autorité pour `.arpa` retournent une délégation normale.

Voici la délégation :

```
% dig @a.root-servers.net ANY home.arpa

; <<>> DiG 9.10.3-P4-Debian <<>> @a.root-servers.net ANY home.arpa
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48503
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;home.arpa. IN ANY

;; AUTHORITY SECTION:
home.arpa. 172800 IN NS blackhole-1.iana.org.
home.arpa. 172800 IN NS blackhole-2.iana.org.
home.arpa. 86400 IN NSEC in-addr.arpa. NS RRSIG NSEC
home.arpa. 86400 IN RRSIG NSEC 8 2 86400 (
20180429000000 20180415230000 56191 arpa.
K4+fNoY6SXQ+VtHsO5/F0oYrRjZdNSG0MSMaeDSQ78aC
NHko4uqNAzoQzoM8a2joFeP4wOL6kVQ72UJ5zqd/iZJD
0ZSh/57lCUVxjYK8sL0dWy/3xr7kbaqi58tNVTLkp8GD
TfyQf5pW1rtRB/1pGzbmTZkK1jXw4ThG3e9kLHk= )

;; Query time: 24 msec
;; SERVER: 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30)
;; WHEN: Mon Apr 16 09:35:35 CEST 2018
;; MSG SIZE  rcvd: 296
```

La section 5 rassemble les changements dans la norme HNCP (RFC 7788. C'est juste un remplacement de `.home` par `home.arpa`.

Quelques petits trucs de sécurité (section 6). D'abord, il ne faut pas s'imaginer que ces noms locaux en `home.arpa` sont plus sûrs que n'importe quel autre nom. Ce n'est pas parce qu'il y a `home` dedans qu'on peut leur faire confiance. D'autant plus qu'il y a, par construction, plusieurs `home.arpa`, et aucun moyen, lorsqu'on se déplace de l'un à l'autre, de les différencier. (Des travaux ont lieu pour concevoir un mécanisme qui pourrait permettre d'avertir l'utilisateur « ce n'est pas le `home.arpa` que vous pensez » mais ils n'ont pas encore abouti.)

`home.arpa` n'est pas sécurisé par DNSSEC. Il ne serait pas possible de mettre un enregistrement DS dans `.arpa` puisqu'un tel enregistrement est un condensat de la clé publique de la zone et que chaque `home.arpa` qui serait signé aurait sa propre clé. Une solution possible aurait été de ne **pas** déléguer `home.arpa`. `.arpa` étant signé, une telle non-délégation aurait pu être validée par DNSSEC (« *"denial of existence"* »). La réponse DNS aurait été (commande tapée avant la délégation de `home.arpa`) :

```
% dig A printer.home.arpa
...
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37887
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
...
;; AUTHORITY SECTION:
arpa. 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
2017112001 ; serial
1800       ; refresh (30 minutes)
900        ; retry (15 minutes)
604800     ; expire (1 week)
86400      ; minimum (1 day)
)
arpa. 10800 IN RRSIG SOA 8 1 86400 (
20171203120000 20171120110000 36264 arpa.
QqiRv85fb6YO/79ZdtQ8Ke5FmZHF2asjLrNejjcivAAo...
arpa. 10800 IN RRSIG NSEC 8 1 86400 (
20171203120000 20171120110000 36264 arpa.
dci8Yr95yQtL9nEBFL3dpdMVTK3Z2cOq+xCujeLsUm+W...
arpa. 10800 IN NSEC as112.arpa. NS SOA RRSIG NSEC DNSKEY
e164.arpa. 10800 IN RRSIG NSEC 8 2 86400 (
20171203120000 20171120110000 36264 arpa.
jfJS6QuBEFHWgc4hhtvdfR0Q7FCCgvGNIoc6169lsxz7...
e164.arpa. 10800 IN NSEC in-addr.arpa. NS DS RRSIG NSEC

;; Query time: 187 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Nov 20 20:28:27 CET 2017
;; MSG SIZE  rcvd: 686
```

Ici, on reçoit un NXDOMAIN (ce domaine n'existe pas), et les enregistrements NSEC qui prouvent que `home.arpa` n'existe pas non plus (rien entre `e164.arpa` et `in-addr.arpa`). Mais cela aurait nécessité un traitement spécial de `home.arpa` par le résolveur validant (par exemple, sur Unbound, `domain-insecure: "home.arpa"`). Finalement, le choix fait a été celui d'une délégation non sécurisée (section 7 du RFC), vers les serveurs `blackhole-1.iana.org` et `blackhole-2.iana.org` :

```
% dig NS home.arpa

; <<>> DiG 9.10.3-P4-Debian <<>> NS home.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64059
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;home.arpa. IN NS

;; ANSWER SECTION:
home.arpa. 190 IN NS blackhole-1.iana.org.
home.arpa. 190 IN NS blackhole-2.iana.org.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Apr 16 09:36:25 CEST 2018
;; MSG SIZE  rcvd: 98
```

Cette délégation a été faite le 15 mars 2018.

Le domaine home.arpa a été ajouté dans le registre des noms de domaine spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml> ainsi que dans celui des noms servis localement <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xml>.

En testant avec les sondes RIPE Atlas <https://atlas.ripe.net/>, on voit que tous les résolveurs ne voient pas la même chose, ce qui est normal, chaque maison pouvant avoir son home.arpa local :

```
% blaeu-resolve -r 1000 -q SOA home.arpa
[prisoner.iana.org. hostmaster.root-servers.org. 1 604800 60 604800 604800] : 548 occurrences
[prisoner.iana.org. hostmaster.root-servers.org. 1 1800 900 604800 604800] : 11 occurrences
[prisoner.iana.org. hostmaster.root-servers.org. 1 1800 900 604800 15] : 33 occurrences
[prisoner.iana.org. hostmaster.root-servers.org. 2002040800 1800 900 604800 60480] : 229 occurrences
[ERROR: FORMERR] : 1 occurrences
[ERROR: SERVFAIL] : 132 occurrences
[] : 4 occurrences
[prisoner.iana.org. hostmaster.root-servers.org. 1 604800 60 604800 3600] : 11 occurrences
[prisoner.iana.org. hostmaster.trex.fi. 1 604800 86400 2419200 86400] : 4 occurrences
[prisoner.iana.org. ops.inx.net.za. 1513082668 10800 3600 604800 3600] : 2 occurrences
[TIMEOUT(S)] : 19 occurrences
Test #12177308 done at 2018-04-16T07:38:32Z
```

On voit sur ce premier test que la grande majorité des sondes voient le vrai SOA (numéro de série 1 ou 2002040800 ; curieusement, les serveurs faisant autorité envoient des numéros différents). Certaines voient un tout autre SOA (par exemple celle où l'adresse du responsable est en Afrique du Sud ou bien en Finlande), et le numéro de série très différent. Ce n'est pas un problème ou un piratage : le principe de home.arpa est que chacun peut avoir le sien.

Pour une autre description de ce home.arpa, voyez l'article de John Shaft <https://www.shaftinc.fr/unbound-domaine-local.html> (où il utilise Unbound) et (en anglais), regardez celui de Daniel Aleksandersen <https://www.ctrl.blog/entry/homenet-domain-name.html>.

À l'heure actuelle, toutes les mises en œuvre en logiciel libre que j'ai regardées utilisent encore .home, mais elles semblent souvent non maintenues.