Choisir son résolveur DNS, pas si facile (1/12)

Stéphane Bortzmeyer
stephane+ubuntuparty@bortzmeyer.org

Ubuntu Party, Paris, 26 novembre 2017

Le DNS

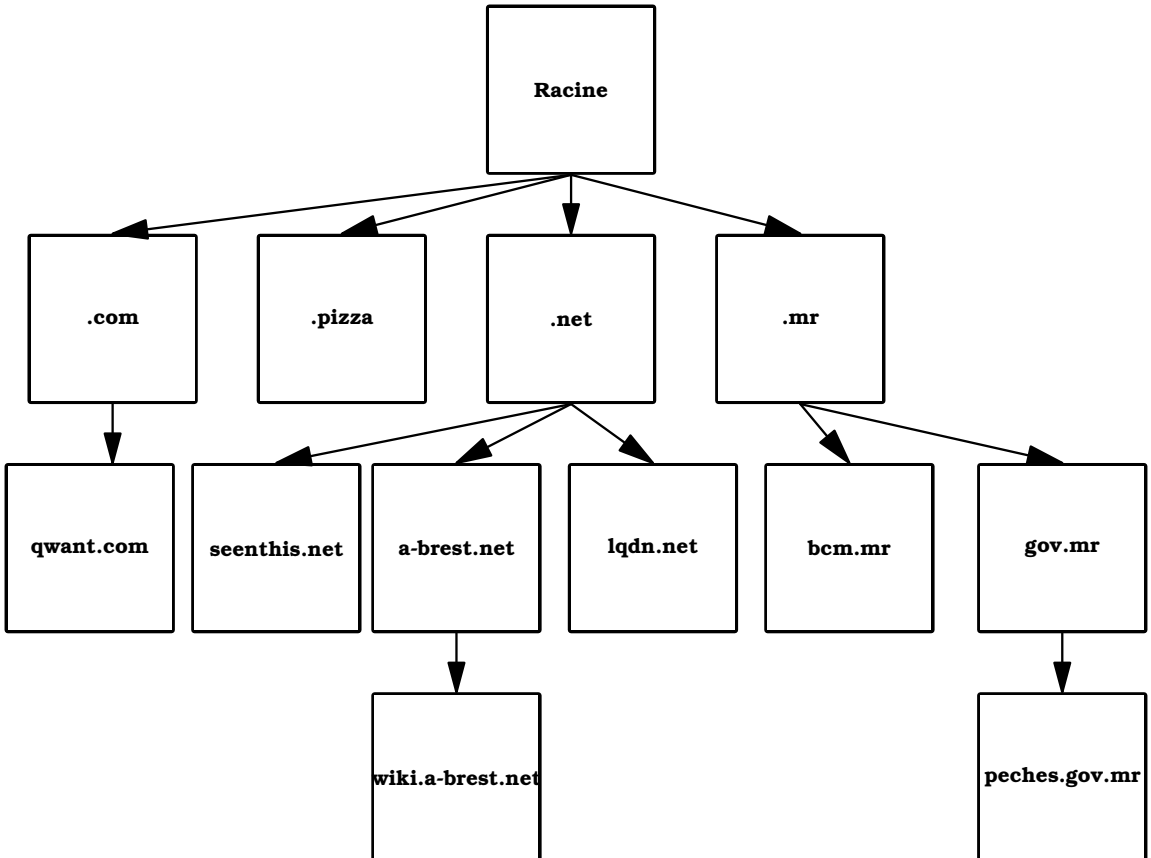
DNS = *Domain Name System*

- Les adresses IP ne sont pas stables (et ont d'autres limites),
- On utilise donc plutôt des **noms** qui, eux, sont stables,
- Le DNS est une base de données qui associe à ces noms des informations (comme les adresses IP),
- C'est une technologie d'**infrastructure** comme l'eau ou l'électricité : tant qu'elle marche, personne ne la voit. Le DNS reste donc peu connu et peu discuté.

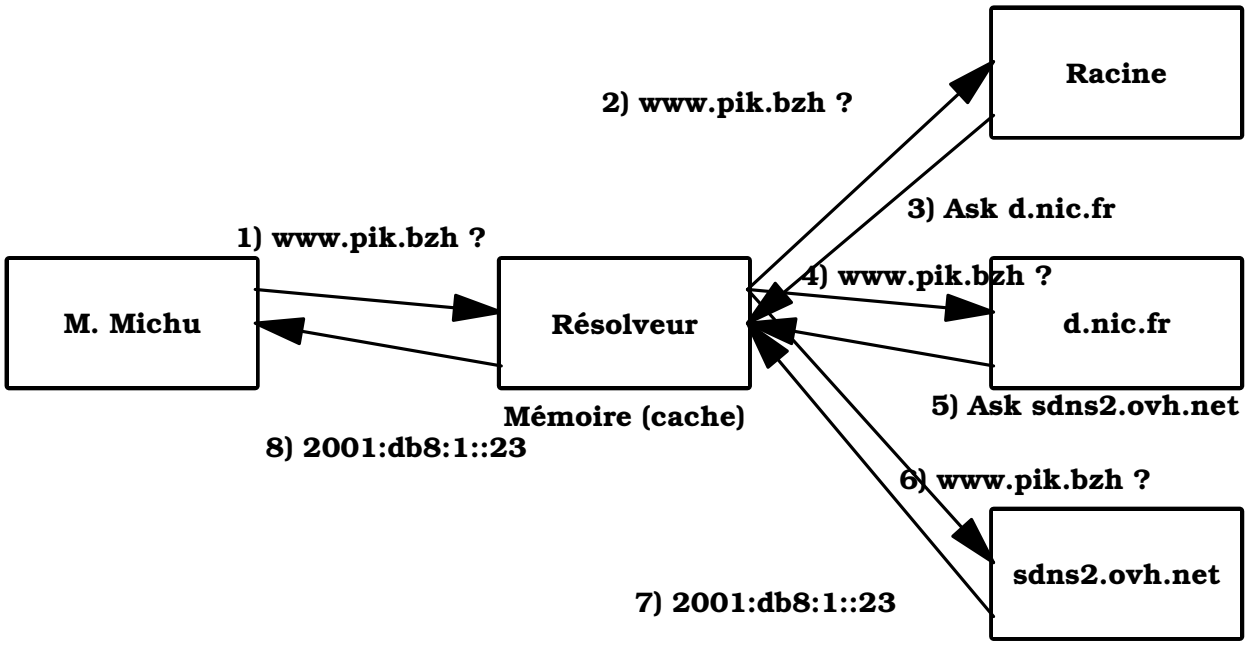
Les noms DNS

- Exemples de noms de domaines : `ubuntu-paris.org`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `www.st-cyr.terre.defense.gouv.fr`, `fr.wikipedia.org`...
- Le nom le plus général (TLD *Top-Level Domain* ou domaine de tête), à la fin.

L'arbre du DNS



Résolution de noms, ou le protocole DNS en action



Le pouvoir du résolveur DNS

1. Si le résolveur est en panne $\longrightarrow$ plus de DNS $\longrightarrow$ plus d'Internet,
2. Le résolveur peut être lent,
3. Le résolveur peut mentir (cas de la Main Rouge en France, décret n° 2015-125 du 5 février 2015),
4. Le résolveur peut enregistrer vos requêtes (vous avez consulté `www.djihad.sa`, `pornhub.com` et `alcooliques-anonymes.fr`),
5. Le trafic peut être lu avant ou après le résolveur (amont ou aval),
6. **Qui contrôle votre résolveur DNS contrôle tout votre usage de l'Internet**.

Comment je trouve mon résolveur DNS ?

1. Par défaut, indiqué à votre machine par le serveur DHCP,
2. Ce serveur DHCP peut être contrôlé par votre FAI / votre service informatique, ou bien cela peut être un engin à vous (100 % libre avec OpenWRT ; cf. Turris Omnia),
3. On peut souvent surmonter cette décision et indiquer le résolveur qu'on veut.

Critères de choix d'un résolveur DNS

1. Fiabilité,
2. Performance (**attention**, c'est vraiment difficile à mesurer, notamment cache chaud vs. cache froid),
3. Non-mensonger, ou alors seulement les mensonges que j'approuve,
4. Authentifié,
5. Protégé contre l'écoute, en amont et en aval.

Résolveur du FAI / service informatique

1. Souvent rapide (car proche),
2. Fiabilité variable (Orange se trompant et redirigeant vers la Main Rouge le 17 octobre 2016),
3. Souvent menteur (Deutsche Telekom ment sur les domaines non existants, les gros FAI français mentent sur ordre de la justice, de l'ARJEL, de la police...),
4. Que font-ils des données ?
5. Écoute difficile en amont (mais, en aval, aucun ne fait de *QNAME minimisation*).

Résolveur public

(Comme Cisco OpenDNS, LDN, Google Public DNS, Quad9, FDN...)

1. Parfois lointain, donc lent,
2. Fiabilité variable (être joignable 24x7 est difficile),
3. Parfois menteur (Cisco OpenDNS, Quad9),
4. Que font-ils des données ? Le RGPD protège t-il, pour des acteurs étrangers ?,
5. Rarement chiffré (sauf Cisco OpenDNS, LDN et Quad9) donc vulnérable à l'écoute en amont. En aval, on est « protégé » par le nombre de requêtes.

Son propre résolveur

Peut être sur un PC (Ubuntu, bien sûr !) ou sur une « *box* » qu'on contrôle (brique Internet ?).

1. Proche, donc rapide, lorsque le cache est chaud,
2. Aussi fiable que le reste du réseau local,
3. Menteur uniquement si on le veut (`googleanalytics.com`),
4. Aucune capture des données (si logiciel libre),
5. Vie privée : bonne protection des requêtes amont mais très mauvais pour les requêtes aval (pensez à la *QNAME minimisation*).

Conclusion

- On peut aussi combiner des solutions (résolveur local faisant suivre au résolveur public),
- Il n'y a pas de solution DNS idéale,
- Les autres techniques de résolution de noms (Namecoin, GNUnet) sont plutôt expérimentales, peu déployées, ont leurs propres défauts.