DNS

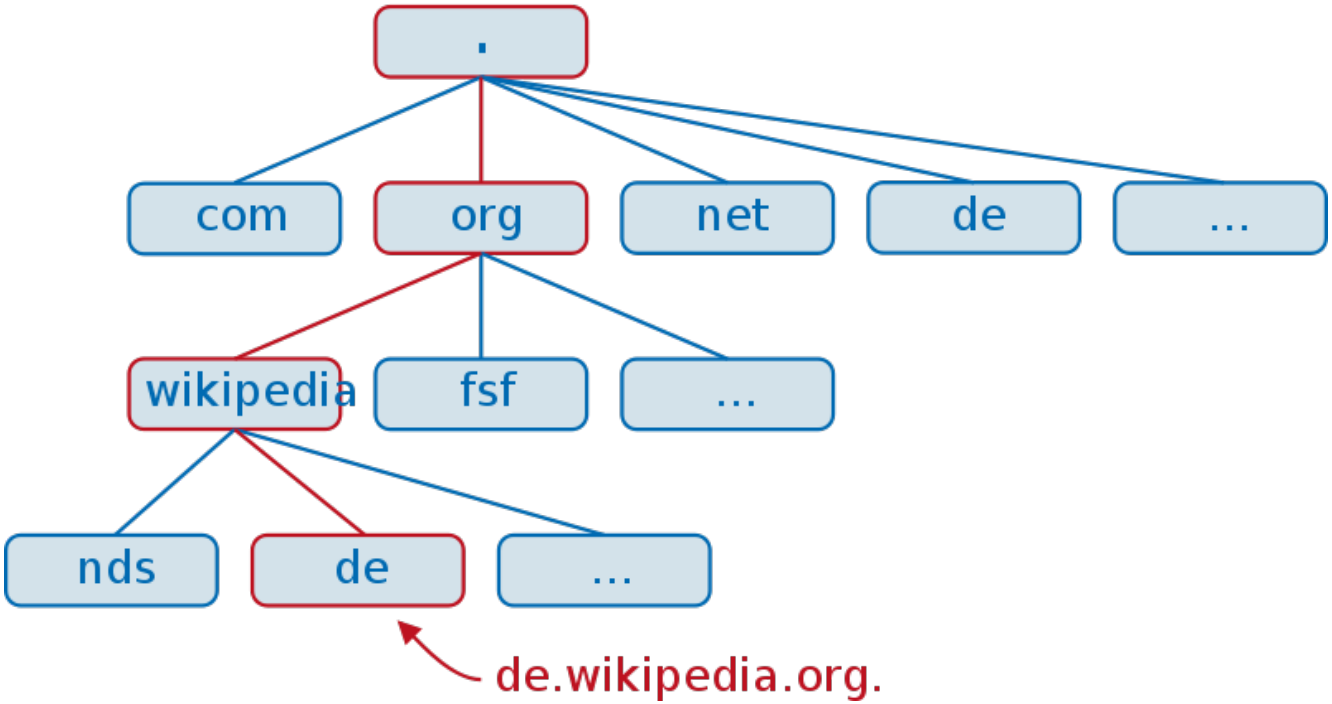
Vincent Guiraud

CRANS

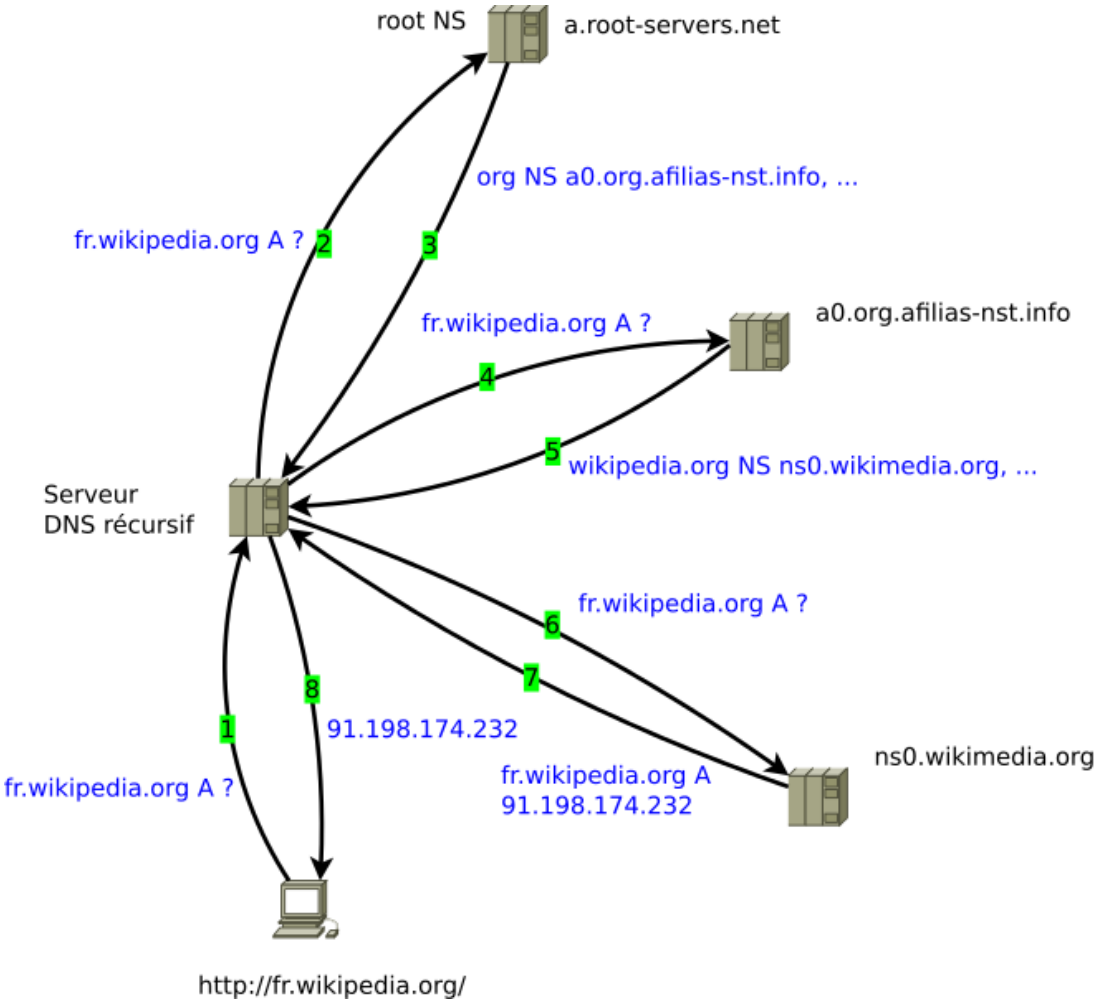
28 mai 2013

- Savoir qui est 2a01 :240 :fe3d :4 :21f :29ff :fe08 :a4ae
- Savoir qui est 173.194.45.68
- Savoir quelle est l'IP de zamok.crans.org

- fichiers Hosts à mettre à jour manuellement
- Un fichier Host centralisé que tout le monde copie pour se mettre a jour.



Liste des serveurs racines sur http ://root-servers.org/



Fonctionnement récursif des DNS

- Serveurs de nom autoritaires qui distribuent la responsabilité de sous-zones d'une zone dont ils sont «propriétaires»
- Serveurs de nom récursifs qui permettent la résolution de nom pour les machines clientes

- A : Donne l'adresse IPv4 du nom d'hôte donné
- AAAA : id mais en IPv6
- NS : Donne le serveur de nom ayant autorité sur la zone

Exemple : le domaine crans.org

dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

dig zamok.crans.org

- CNAME : alias d'un nom de domaine vers un autre. Exemple : smtp.crans.org
- MX : Donne les serveurs d'emails du domaine, associés de priorités
- SOA : donne des informations sur la zone (quel est le serveur ayant autorité, quel est l'adresse email du contact technique ?)

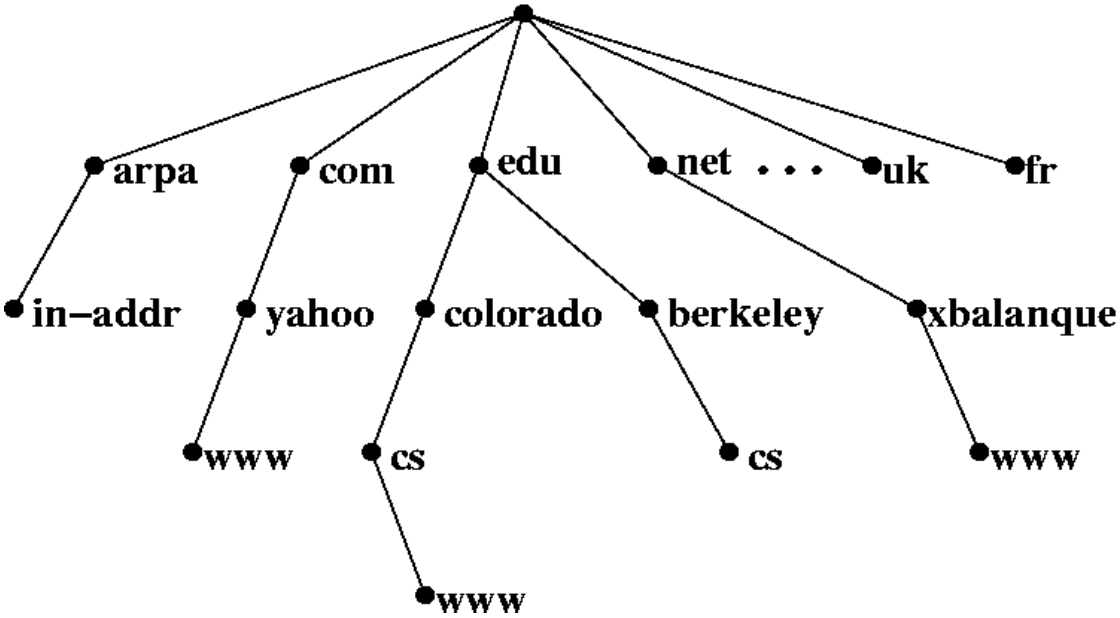
Passer d'une adresse ip à un nom de domaine ?

Adresse ip : 138.231.136.39 manière simple : dig -x 138.231.136.39
De même, en IPv6 : Adresse IP :
2a01 :240 :fe3d :4 :21f :29ff :fe08 :a4ae
dig -x 2a01 :240 :fe3d :4 :21f :29ff :fe08 :a4ae

Et en plus compliqué : Adresse ip : 138.231.136.39 Pour avoir le nom du domaine : dig 39.136.231.138.in-addr.arpa

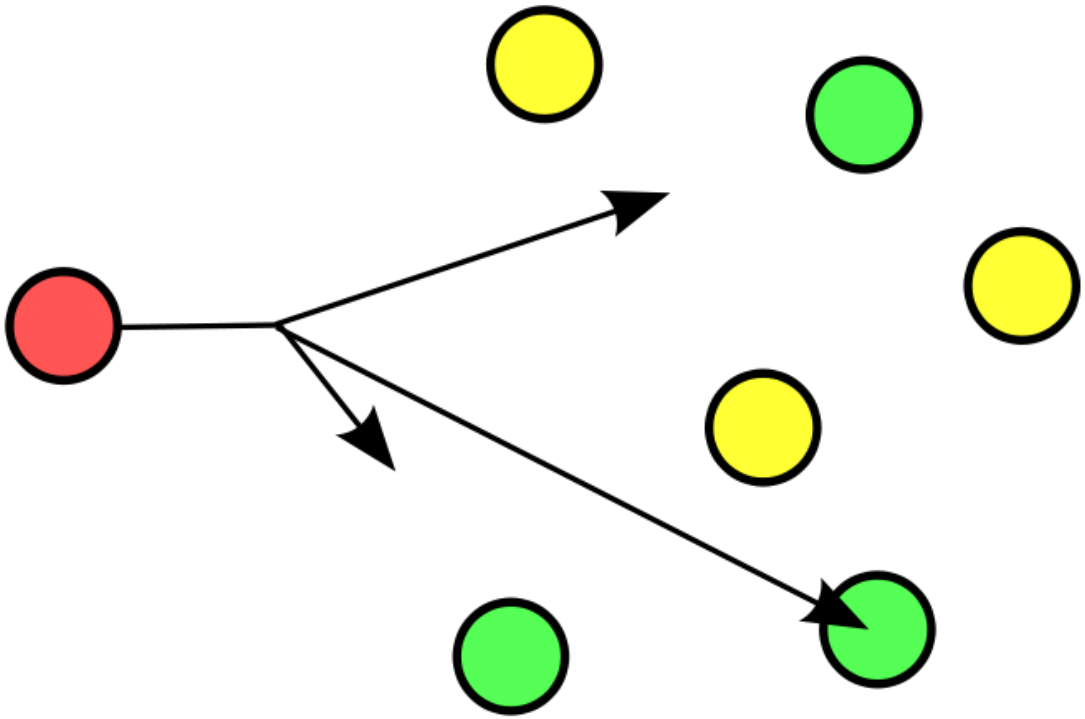
- Cache DNS, fichiers Hosts modifiables facilement
- Réponses DNS non signées
- Messages DNS limités à 512 octets en UDP
- Si les serveurs . sautent, on est foutu

Domain Name System Security Extensions (2005) Signature par clefs, on bâtit une chaine de confiance depuis la racine jusqu'au nom de domaine



Permet de fiabiliser les caches des serveurs DNS Pb : Taille de la réponse DNS trop grande ⇒ Extension mechanisms for DNS (EDNS) qui permet d'avoir des signatures tout en conservant une rétro compatibilité.

Fragilité des serveurs racines ?



L'anycast

Les zones directes :

- crans.org
- crans.eu (redirige wiki)
- crans.fr (redirige wiki)
- crans.ens-cachan.fr (redirige crans.org)

Les zones inverses :

- 136-151 .231.138.in-addr.arpa
- 136.231.10.in-addr.arpa (IP locales au réseau)

Les serveurs DNS du crans sont :

- sable
- ovh
- freebox

Servent tous comme serveurs autoritaires

- charybde
- gordon
- nem

Serveurs DNS récursifs

config BIND9 dans /etc/bind/

FIN !