

DNS : Domain Name System

Maxime Bombar

8 Janvier 2019



Introduction

- ▶ **Vers qui pointe l'adresse IP 138.231.136.1 ?**
- ▶ Vers zamok.crans.org
- ▶ Comment contacter thot.crans.org en IPv6 ?
- ▶ Comment faire le lien entre tout ça ?
- ▶ **C'est le but de ce séminaire**



Introduction

- ▶ Vers qui pointe l'adresse IP 138.231.136.1 ?
- ▶ Vers zamok.crans.org
- ▶ Comment contacter thot.crans.org en IPv6 ?
- ▶ Comment faire le lien entre tout ça ?
- ▶ C'est le but de ce séminaire



Introduction

- ▶ Vers qui pointe l'adresse IP 138.231.136.1 ?
- ▶ Vers zamok.crans.org
- ▶ Comment contacter thot.crans.org en IPv6 ?
- ▶ Comment faire le lien entre tout ça ?
- ▶ C'est le but de ce séminaire



Introduction

- ▶ Vers qui pointe l'adresse IP 138.231.136.1 ?
- ▶ Vers zamok.crans.org
- ▶ Comment contacter thot.crans.org en IPv6 ?
- ▶ Comment faire le lien entre tout ça ?
- ▶ C'est le but de ce séminaire



Introduction

- ▶ Vers qui pointe l'adresse IP 138.231.136.1 ?
- ▶ Vers zamok.crans.org
- ▶ Comment contacter thot.crans.org en IPv6 ?
- ▶ Comment faire le lien entre tout ça ?
- ▶ **C'est le but de ce séminaire**



Pour bien commencer :

Quelques paquets :

- ▶ `dnsutils`
- ▶ `ldnsutils`

et des commandes utiles :

- ▶ `dig`
- ▶ `drill`
- ▶ `host`



Table des matières

Introduction à DNS

Rentrons dans les détails

Outils en ligne de commande

DNS au Cr@ns

Discussions



Sommaire

Introduction à DNS

Architecture du DNS

Entrées DNS

Résolution directe et inverse ?

Rentrons dans les détails

Outils en ligne de commande

DNS au Cr@ns

Discussions



Des fichiers sur vos machines

- ▶ `/etc/hosts` **Consulté avant le DNS.**
 - ▶ Annuaire manuel
 - ▶ Ancêtre du DNS
 - ▶ Adresses locales
- ▶ `/etc/resolv.conf` **Les informations sur vos DNS.**



Noms de domaines

- ▶ Des labels séparées par un point (.)
- ▶ Chaque labels peut contenir des caractères alphanumériques (a-zA-Z0-9) et des tirets (-)
- ▶ Un label possède au plus 63 caractères
- ▶ Un domaine peut posséder au plus 253 caractères
- ▶ Insensible à la casse.



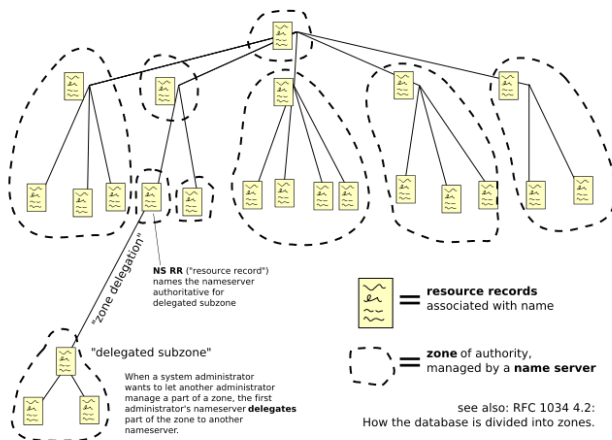
One root to rule them all...

- ▶ Système hautement hiérarchisé :
- ▶ Une racine unique (., distribuée sur plusieurs serveurs)
- ▶ Des domaines de haut niveau (TLD, Top Level Domains) distribués par l'IANA
(<http://www.iana.org/domains/root/db/>),
notamment (org., eu., fr., ...)
- ▶ Chaque TLD distribue des domaines (crans.org., ...)



Structure du DNS

Domain Name Space



Deux types de serveurs de noms

- ▶ *Autoritaires* : distribuent les entrées de zones données dont ils sont « propriétaires » (notion de délégation)
- ▶ *Récuratif* : permet la résolution de noms pour les machines clientes



Principe de fonctionnement

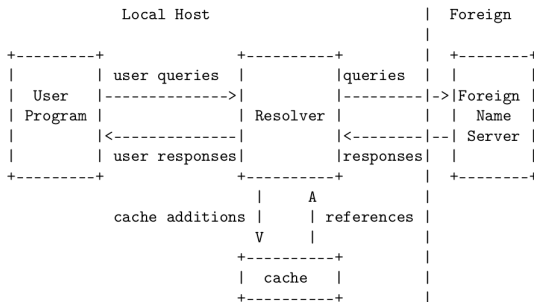


Figure 1: RFC 1035 - Novembre 1987

Format des données

- ▶ Une requête est un triplet (Classe, Type, Nom)
- ▶ La classe Internet (IN) est la plus utilisée.
- ▶ La classe Chaos (CH) peut être utilisée pour donner des informations sur le serveur DNS physique.

Vous pouvez essayer :

```
dig CH TXT hostname.bind @f.root-servers.net
```



Format de la réponse

```

+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                NAME                                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                TYPE                                |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                CLASS                               |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                TTL                                 |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                RDLENGTH                           |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                RDATA                              |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Figure 2: RFC 1035 - Réponse DNS



Différents types

- ▶ SOA : Start Of Authority - Informations sur la zone
- ▶ NS : Name Server - Serveur de noms correspondant à la zone
- ▶ MX : Mail eXchanger - Serveur d'échange d'emails
- ▶ A : Adresse IP
- ▶ AAAA : Adresse IPv6
- ▶ CNAME : Canonical Name - Redirection de nom de domaine
- ▶ DNAME : Delegation Name - Redirection d'une zone complète
- ▶ PTR : PoinTeR - Correspondance inverse
- ▶ TXT : Texte - On peut y rentrer des informations.



Comme dans l'annuaire...

- ▶ Un nom correspond à une adresse (IN A
`zamok.crans.org. → 138.231.136.1`)
- ▶ Mais il existe des zones inverses (`in-addr.arpa.` pour
l'IPv4, `ip6.arpa.` pour l'IPv6).
- ▶ Mapping inverse : IN PTR
`1.136.231.138.in-addr.arpa. →`
`zamok.crans.org.`



Sommaire

Introduction à DNS

Rentrons dans les détails

Paquet requête DNS

Quelques RR

Outils en ligne de commande

DNS au Cr@ns

Discussions



Principe du protocole

- ▶ Datagramme UDP, sur le port 53 pour les query.
- ▶ Peut utiliser TCP (par exemple synchronisation de serveurs DNS).



Datagramme et fonctionnement

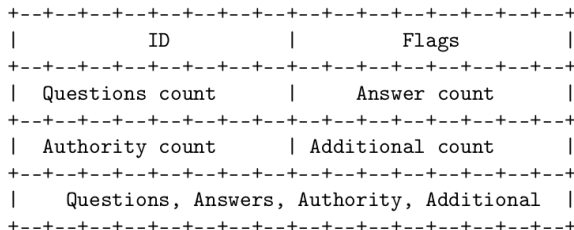


Figure 3: Datagramme DNS

Taille : Au maximum 512 octets.



- ▶ Zone, Classe, SOA
- ▶ Serveur maître pour la zone
- ▶ Adresse mail
- ▶ Numéro de série, augmenté à chaque changement.
Convention YYYYMMDDVV (RFC 1912). (On voit donc que le Crans ne respecte pas la convention).
- ▶ Refresh, Retry, Expire, TTL



CNAME, DNAME, MX records

- ▶ MX spécifie les serveurs SMTP pour la zone.
- ▶ CNAME permet de définir des alias.
- ▶ CNAME exclut tout autre record (RFC 1034, 1912)
- ▶ Impossible d'avoir un CNAME et un A record pour le même domaine.
- ▶ Impossible d'avoir un CNAME à l'apex d'une zone !
- ▶ DNAME pose des CNAME sur *.zone



Glue Record

Ce record enregistre l'adresse des DNS d'une zone dupliquée.
Exemple :

```
;; ANSWER SECTION:
```

```
crans.org. 172800 IN NS silice.crans.org.
```

```
crans.org. 172800 IN NS soyouz.crans.org.
```

```
crans.org. 172800 IN NS freebox.crans.org.
```

```
;; ADDITIONAL SECTION:
```

```
silice.crans.org. 164763 IN A 138.231.136.118
```

```
silice.crans.org. 164763 IN AAAA 2a0c:700:0:1:73:69ff:fe6c:693b
```

```
soyouz.crans.org. 167342 IN A 91.121.179.40
```

```
soyouz.crans.org. 167342 IN AAAA 2001:41d0:1:f428::1
```

```
freebox.crans.org. 156166 IN A 82.225.39.54
```



Sommaire

Introduction à DNS

Rentrons dans les détails

Outils en ligne de commande

Parcours de l'arbre DNS

La boîte à outils : la commande dig

DNS au Cr@ns

Discussions



Comment trouver `zamok.crans.org` à la main ?

- ▶ Requête du serveur autoritaire de `org.` à la racine
`dig NS org. @a.root-servers.net`
- ▶ Requête du serveur autoritaire de `crans.org.` au serveur de `org.`
`dig NS crans.org. @a0.org.afiliat-nst.info.`
- ▶ Requête de l'adresse de `zamok` au serveur autoritaire de `crans.org.`
`dig A zamok.crans.org. @silice.crans.org`



Comment trouver à qui appartient

2a0c:700:0:1:ae16:2dff:fe76:290c?

À vous de jouer.



Requête DNS simple



Pratique pour le debugging : transfert de zone complète...

```
dig AXFR crans.org.
```



Sommaire

Introduction à DNS

Rentrons dans les détails

Outils en ligne de commande

DNS au Cr@ns

Arborescence DNS au Cr@ns

Serveurs DNS et configuration

Discussions



Quelques zones directes

- ▶ crans.org
- ▶ crans.eu
- ▶ crans.fr



Et plus de zones inverses

- ▶ 76.230.185.in-addr.arpa
- ▶ ...
- ▶ 136.231.10.in-addr.arpa



Savez-vous qui sont les serveurs autoritaires du Crans ?



Savez-vous qui sont les serveurs autoritaires du Crans ?

- ▶ silice.crans.org
- ▶ soyouz.crans.org
- ▶ freebox.crans.org

On utilise `knot` pour gérer les DNS autoritaires, et un `re2o-service` se charge de remplir les zones avec les informations de la base de données.



... Et les Serveurs récursifs ?



... Et les Serveurs récursifs ?

- ▶ nem.crans.org
- ▶ odlyd.crans.org

On utilise `bind` pour gérer les récursifs.



Sommaire

Introduction à DNS

Rentrons dans les détails

Outils en ligne de commande

DNS au Cr@ns

Discussions

DNS, est-ce important ?

MITM

Peut-on s'assurer des réponses reçues ?



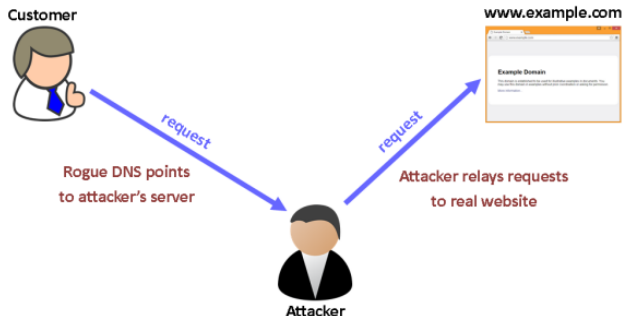
Sans DNS rien ne va plus

- ▶ Aujourd'hui 8 Janvier 2019, le DNS de BNP Paribas est tombé.
- ▶ Résultat : Plus aucune transaction bancaire autorisée dans les commerces liés de près ou de loin à BNP pendant plusieurs heure (pas encore réglé au moment de ce talk).
- ▶ Plus d'infos sur les pannes DNS :
<https://gist.github.com/bortzmeyer>



Attaque Man In The Middle

MITM Attack



DNS Menteur

- ▶ Une forme de MITM, utilisée par les FAI.
- ▶ Par exemple pour des portails captifs
- ▶ Ou pour rediriger vers une page d'aide si la requête time-out.

⇒ peut menacer la neutralité du Net !



DNS Menteur

- ▶ Une forme de MITM, utilisée par les FAI.
- ▶ Par exemple pour des portails captifs
- ▶ Ou pour rediriger vers une page d'aide si la requête time-out.

Parfois ordonné par la justice : TGI de Paris le 28 Novembre 2018 a ordonné à FREE, Orange, SFR, Bouygues de bloquer le site d'extrême droite

`www.democratieparticipative.biz`.



DNSSEC

- ▶ Le protocole `DNS` n'est pas sécurisé.
- ▶ Comment authentifier les données reçues ?
- ▶ Une extension cryptographique du protocole `DNS`
- ▶ Domain Name System Security Extensions



DNSSEC

- ▶ Signature cryptographique des zones (Asymétrique)
- ▶ Le client peut vérifier les signatures et rejeter la zone si les données sont corrompues.
- ▶ Un outil : `drill`
- ▶ Au Crans, c'est géré par le `re2o-service`
- ▶ Détails dans un séminaire ultérieur
- ▶ Limitations : Peu de providers signent leurs zones, encore moins de clients ne vérifient.
- ▶ Ils privilégient la vitesse à la sécurité.



Fin

- ▶ DNS : Un protocole majeur d'Internet
- ▶ Utilisé depuis plus de 30 ans
- ▶ Des extensions de sécurité
- ▶ A-t-on tout dit ? DNS Round-robin, DNS Caching, fonctionnement de DNSSEC, DNS over TLS etc ...



Fin

- ▶ DNS : Un protocole majeur d'Internet
- ▶ Utilisé depuis plus de 30 ans
- ▶ Des extensions de sécurité
- ▶ A-t-on tout dit ? DNS Round-robin, DNS Caching, fonctionnement de DNSSEC, DNS over TLS etc ...



Fin

- ▶ DNS : Un protocole majeur d'Internet
- ▶ Utilisé depuis plus de 30 ans
- ▶ Des extensions de sécurité
- ▶ A-t-on tout dit ? DNS Round-robin, DNS Caching, fonctionnement de DNSSEC, DNS over TLS etc ...



Fin

- ▶ DNS : Un protocole majeur d'Internet
- ▶ Utilisé depuis plus de 30 ans
- ▶ Des extensions de sécurité
- ▶ A-t-on tout dit ? DNS Round-robin, DNS Caching, fonctionnement de DNSSEC, DNS over TLS etc ...



Fin

- ▶ DNS : Un protocole majeur d'Internet
- ▶ Utilisé depuis plus de 30 ans
- ▶ Des extensions de sécurité
- ▶ A-t-on tout dit ? DNS Round-robin, DNS Caching, fonctionnement de DNSSEC, DNS over TLS etc ...

Des questions ?

