

Domain Name System

Stéphane Bortzmeyer
stephane+cnam@bortzmeyer.org

CNAM, 11 mai 2017

Domain Name System

Stéphane Bortzmeyer
stephane+cnam@bortzmeyer.org

CNAM, 11 mai 2017

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Généralités

- Des noms uniques et mémorissables,
- Un vecteur d'identité,
- Un nommage arborescent : racine, puis TLD puis domaine de deuxième niveau, de troisième niveau et ainsi de suite,
- Le nombre de composants dans un nom est quelconque (2, 3, 4...)

Les noms

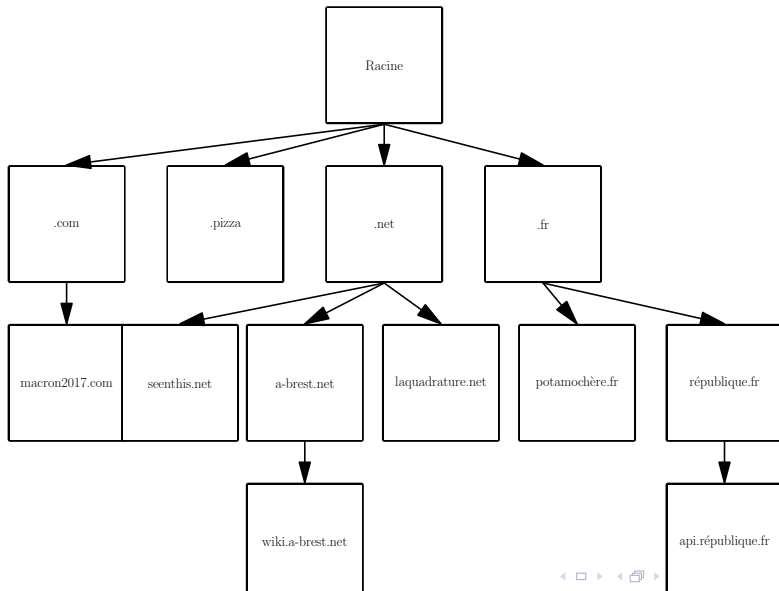
Les noms

- Exemples de noms de domaines : `wiki.a-brest.net`,
`www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`,
`www.st-cyr.terre.defense.gouv.fr`, `re`,
`_sipfederationtls._tcp.en-marche.fr`,
`fr.wikipedia.org`, `mamot.fr...`

Les noms

- Exemples de noms de domaines : `wiki.a-brest.net`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `www.st-cyr.terre.defense.gouv.fr`, `re_sipfederationtls_tcp.en-marche.fr`, `fr.wikipedia.org`, `mamot.fr`...
- `nca.x.gsi.gov.uk` a cinq composants. Le nom le plus général, le **TLD** (*Top-Level Domain*, ici `uk`) est à la fin.

L'arbre du DNS



Délégation

Des noms peuvent être **délegués** et on change alors d'organisme responsable. Par exemple `uk.com` est délégué depuis `com` et délègue à son tour.

Rien dans le nom n'indique où est la frontière de délégation : il faut utiliser le DNS.

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS**
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Nommage et protocole

- Les **noms de domaine** : des identificateurs
- Le **DNS** : un protocole réseau pour résoudre ces noms en données

Le DNS n'est qu'une des techniques possibles. Les noms de domaine lui survivront sans doute.

Un peu de technique

Un peu de technique

- Les machines sont identifiées par une **adresse** comme
2001:4b98:dc2:45:216:3eff:fe4b:8c5b,

Un peu de technique

- Les machines sont identifiées par une **adresse** comme 2001:4b98:dc2:45:216:3eff:fe4b:8c5b,
- L'adresse dépend de votre connexion, de votre FAI, vous en changez parfois,

Le DNS

DNS = *Domain Name System*

Le DNS

DNS = *Domain Name System*

- Les adresses IP ne sont pas stables (et ont d'autres limites),

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

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),

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.

La résolution DNS

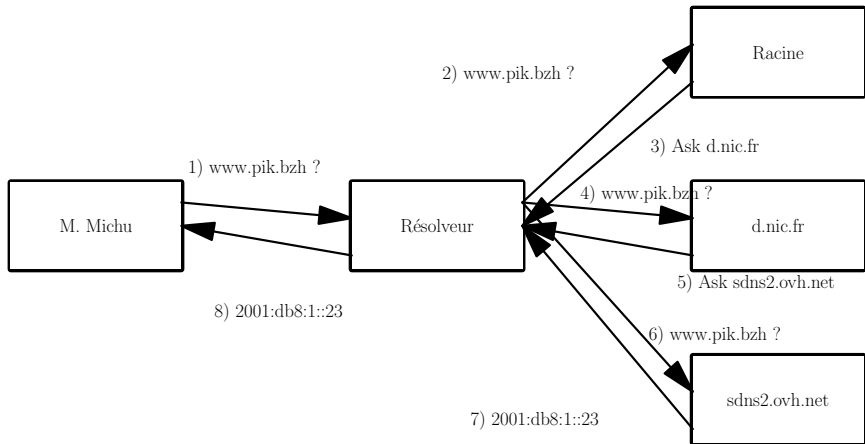
Résolution : demander aux serveurs DNS les informations associées à un nom de domaine (par exemple les adresses IP)

Il y a les serveurs **résolveurs** (typiquement fournis par le FAI) et les serveurs **faisant autorité** (ceux des titulaires de noms ou d'un hébergeur DNS).

Vocabulaire important

- **Résolveur** (ou serveur récursif) : serveur DNS qui ne connaît rien mais pose des questions aux serveurs faisant autorité et mémorise les réponses. Chez le FAI, ou sur le réseau local ou chez Google.
- **Serveur faisant autorité** : serveur DNS qui connaît le contenu d'un domaine. Exemple : les serveurs de l'AFNIC qui connaissent ce qu'il y a dans `.fr` et peuvent répondre. Ou les serveurs de `lacantine.org` (chez Bearstech)

Résolution de noms, ou le protocole DNS en action



Avec le client DNS dig

```
% dig AAAA www.bortzmeyer.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11397
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1
...
;; ANSWER SECTION:
www.bortzmeyer.org. 10791 IN AAAA 2605:4500:2:245b::42
...
;; Query time: 2937 msec
;; SERVER: 192.168.10.110#53(192.168.10.110)
;; WHEN: Wed Aug 14 17:46:47 2013
;; MSG SIZE rcvd: 164
```

Types de données

- AAAA : adresses IP
- NS : serveurs de noms faisant autorité
- SOA : *Start Of Authority*, diverses méta-données sur la zone, dont un numéro de série, versionnant la zone
- A : adresses de l'ancien protocole IP (IPv4)
- SRV : serveurs du domaine pour une application donnée (par exemple XMPP)

Avec le client check-soa

```
% check-soa -i mr
censvrns0001.ird.fr.
    91.203.32.147: OK: 2017050701 (14 ms)
ns.univ-nkc.mr.
    82.151.64.1: OK: 2017050701 (149 ms)
ns1.nic.mr.
    41.188.65.193: OK: 2017050701 (104 ms)
ns3.nic.fr.
    192.134.0.49: OK: 2017050701 (6 ms)
    2001:660:3006:1::1:1: OK: 2017050701 (6 ms)
```

Les champs d'une requête DNS

Vus par tshark

```
User Datagram Protocol, Src Port: 38590 (38590), Dst Port: domain (53)  
Domain Name System (query)
```

```
Transaction ID: 0xcc27
```

```
Flags: 0x0100 Standard query
```

```
0... .. = Response: Message is a query
```

```
.000 0... .. = Opcode: Standard query (0)
```

```
.... ..0. .... = Truncated: Message is not truncated
```

```
.... ...1 .... = Recursion desired: Do query recursively
```

```
.... .... .0.. .... = Z: reserved (0)
```

```
.... .... ...0 .... = Non-authenticated data: Unacceptable
```

```
Questions: 1
```

```
Answer RRs: 0
```

```
Authority RRs: 0
```

```
Additional RRs: 0
```

```
Queries
```

```
www.cnam.fr: type AAAA, class IN
```

```
Name: www.cnam.fr
```

```
Type: AAAA (IPv6 Address) (28)
```

Les champs d'une réponse DNS

```
% dig AAAA mamot.fr

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17124
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; ANSWER SECTION:
mamot.fr.                86400 IN AAAA 2a00:99a0:0:1000::7

;; AUTHORITY SECTION:
mamot.fr.                86400 IN NS  secondary.heberge.info.
mamot.fr.                86400 IN NS  primary.heberge.info.

;; Query time: 215 msec
;; SERVER:  ::1#53(::1)
;; WHEN: Thu May 11 06:17:27 UTC 2017
;; MSG SIZE  rcvd: 123
```

Dans la réponse

- Le code de retour (*status*) : NOERROR, NXDOMAIN, SERVFAIL
- Les *flags*
- Plusieurs sections, dont une pour la réponse
- Dans les enregistrements (RR, *Resource Record*), notez le TTL (*Time To Live*).

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel**
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Les problèmes

```
% check-soa -i bf
censvrns0001.ird.fr.
    91.203.32.147: OK: 2015092800 (2 ms)
nahouri.onatel.bf.
    206.82.130.196: OK: 2015092800 (130 ms)
nahouri1.onatel.bf.
    206.82.130.203: ERROR: read udp 206.82.130.203:53: i/o timeout
nahouri2.onatel.bf.
    206.82.130.204: ERROR: read udp 206.82.130.204:53: i/o timeout
ns1.as6453.net.
    66.198.145.55: OK: 2015092800 (27 ms)
    2001:5a0:d00:ffff::42c6:9137: OK: 2015092800 (118 ms)
ns2.as6453.net.
    66.198.145.99: OK: 2015092800 (26 ms)
    2001:5a0:d00:ffff::42c6:9163: OK: 2015092800 (211 ms)
```

Exemple de surveillance continue

bortzmeyer.org.

Edit

UDP



<https://atlas.ripe.net/domainmon/>

Robustesse

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :
- Le domaine `.ht` était sur six serveurs dont deux à Port-au-Prince,

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :
- Le domaine `.ht` était sur six serveurs dont deux à Port-au-Prince,
- Évidemment, les serveurs en Haïti ont stoppé,

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :
- Le domaine `.ht` était sur six serveurs dont deux à Port-au-Prince,
- Évidemment, les serveurs en Haïti ont stoppé,
- Les serveurs extérieurs ont continué, `.ht` n'a jamais stoppé,

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :
- Le domaine `.ht` était sur six serveurs dont deux à Port-au-Prince,
- Évidemment, les serveurs en Haïti ont stoppé,
- Les serveurs extérieurs ont continué, `.ht` n'a jamais stoppé,
- En se concertant, les gérants des serveurs extérieurs ont pu prolonger le service (aucun contact avec les gérants haïtiens).

Robustesse

- Exemple du tremblement de terre à Haïti en 2010 :
- Le domaine `.ht` était sur six serveurs dont deux à Port-au-Prince,
- Évidemment, les serveurs en Haïti ont stoppé,
- Les serveurs extérieurs ont continué, `.ht` n'a jamais stoppé,
- En se concertant, les gérants des serveurs extérieurs ont pu prolonger le service (aucun contact avec les gérants haïtiens).
- Leçons : la coopération marche mieux que les règles et les processus.

Mesures depuis plusieurs points

Mesures depuis plusieurs points

- Le résultat peut dépendre d'où on est (problème de routage, censure nationale...)

Mesures depuis plusieurs points

- Le résultat peut dépendre d'où on est (problème de routage, censure nationale...)
- Il faut donc mesurer depuis plusieurs points

Mesures depuis plusieurs points

- Le résultat peut dépendre d'où on est (problème de routage, censure nationale...)
- Il faut donc mesurer depuis plusieurs points
- Les sondes RIPE Atlas sont de petits boîtiers que les volontaires installent chez eux et qui effectuent des mesures actives

Autre exemple de panne

Panne DNS de “impots.gouv.fr” en Avril 2016 (serveurs accessibles depuis certains réseaux seulement)

```
% atlas-resolve -r 500 -c FR impots.gouv.fr  
[ERROR: SERVFAIL] : 177 occurrences  
[145.242.11.48] : 213 occurrences  
[TIMEOUT(S)] : 107 occurrences  
Test #3645793 done at 2016-04-05T10:01:16Z
```

Panne Cedexis le 10 mai

```
% check-soa -i cedexis.net
flipa.cedexis.net.
  68.232.43.4: ERROR: read udp 10.10.86.133:53036->68.232.43.4:53: i/o
flipd.cedexis.net.
  69.28.180.4: OK: 1494424929 (4 ms)
flipg.cedexis.net.
  204.48.34.10: ERROR: read udp 10.10.86.133:59627->204.48.34.10:53: i
flipm.cedexis.net.
  204.48.34.10: ERROR: read udp 10.10.86.133:35249->204.48.34.10:53: i

% atlas-resolve -c FR -r 100 www.sudouest.fr
[195.154.181.181] : 10 occurrences
[ERROR: SERVFAIL] : 50 occurrences
[TIMEOUT(S)] : 33 occurrences
[37.187.142.180] : 5 occurrences
[62.210.93.5] : 2 occurrences
Test #8681136 done at 2017-05-10T13:23:15Z
```

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs**
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Quels logiciels utiliser et comment les configurer ?

Quels logiciels utiliser et comment les configurer ?

- Certains logiciels font à la fois résolveur et serveur faisant autorité (mauvaise idée),

Quels logiciels utiliser et comment les configurer ?

- Certains logiciels font à la fois résolveur et serveur faisant autorité (mauvaise idée),
- Résolveur : Unbound, Knot Resolver (kres), PowerDNS Recursor, BIND

Quels logiciels utiliser et comment les configurer ?

- Certains logiciels font à la fois résolveur et serveur faisant autorité (mauvaise idée),
- Résolveur : Unbound, Knot Resolver (kres), PowerDNS Recursor, BIND
- Serveur faisant autorité : NSD, Knot, BIND

BIND

- Sans doute le serveur DNS le plus répandu (mais pas le meilleur, de loin),
- Peut faire serveur faisant autorité **ou** résolveur.

Configuration de BIND en résolveur simple

```
acl me {  
    2001:db8:43::/48;  
};  
options {  
    recursion yes;  
    allow-recursion { me; };  
    allow-query-cache { me; };  
    allow-query { me; };  
};
```

Configuration de BIND en serveur faisant autorité

Pour le TLD .example

```
options {  
    recursion no;  
};  
zone "example" {  
    type master;  
    file "example";  
};
```

Et le fichier example contient les données.

Les données (« fichier de zone »)

```
@      IN      SOA      ns1.nic root@nic (
        2013071800          ; Serial
        7200                ; Refresh
        1800                ; Retry
        2419200             ; Expire
        600 ) ; Negative Cache TTL

@      IN      NS      ns1.nic.example.
@      IN      NS      ns1.pch.net.

www    IN      AAAA    2001:db8::bad:dcaf
```

Configuration NSD

Serveur faisant autorité pour plusieurs gros TLD (et la racine)

```
zone:  
  name: "example"  
  zonefile: "example"
```

Configuration Unbound

Résolveur

server:

```
interface: ::0
```

```
interface: 0.0.0.0
```

```
access-control: 2001:db8:43::/48 allow
```

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement**
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).
- Dans certains cas, l'enregistrement ne se fait pas en direct mais via un troisième acteur, le **bureau d'enregistrement** (BE, *registrar*). C'est le système RRR (*registry-registrar-registrant*). Par exemple Gandi, OVH...

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).
- Dans certains cas, l'enregistrement ne se fait pas en direct mais via un troisième acteur, le **bureau d'enregistrement** (BE, *registrar*). C'est le système RRR (*registry-registrar-registrant*). Par exemple Gandi, OVH...
- Les serveurs faisant autorité pour le nom sont parfois gérés par le titulaire, parfois par le BE, parfois par un hébergeur DNS.

Interroger les bases sociales

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)
- Rappel : les bases sont purement déclaratives et leur valeur varie...

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)
- Rappel : les bases sont purement déclaratives et leur valeur varie...
- whois remplacé dans le futur ? Par RDAP ?

Démo whois

```
% whois cecyf.fr
...
%% This is the AFNIC Whois server.
...
status:      ACTIVE
holder-c:    C30672-FRNIC
...
nic-hdl:    C30672-FRNIC
type:       ORGANIZATION
address:    C/ centre de recherches de l'Eogn
address:    49, rue de Babylone
```

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance**
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Les acteurs

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :
 - Registres de noms de domaines,

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :
 - Registres de noms de domaines,
 - Gérants de résolveurs DNS (FAI, votre service informatique, GAFA...)

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :
 - Registres de noms de domaines,
 - Gérants de résolveurs DNS
 - Hébergeurs DNS (OVH, Gandi, Linode...)

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :
 - Registres de noms de domaines,
 - Gérants de résolveurs DNS
 - Hébergeurs DNS (OVH, Gandi, Linode. . .)
 - BE (Bureaux d'Enregistrement, *registrars*)

Les acteurs

- Qui gère toutes ces machines, les achète, les remplace, paie les techniciens ?
- Rappel : il n'y a pas de président de l'Internet, en charge de s'assurer que tout est fait.
- Il y a donc **des tas** d'acteurs :
 - Registres de noms de domaines,
 - Gérants de résolveurs DNS
 - Hébergeurs DNS (OVH, Gandi, Linode. . .)
 - BE (Bureaux d'Enregistrement, *registrars*)

Il est fréquent qu'un acteur ait plusieurs rôles.

Les acteurs, suite

Les acteurs, suite

- Qui décide, qui organise, qui établit les normes techniques ?

Les acteurs, suite

- Qui décide, qui organise, qui établit les normes techniques ?
- Ce n'est pas toujours clair. (Et c'est une très bonne chose.)

Les acteurs, suite

- Qui décide, qui organise, qui établit les normes techniques ?
- Ce n'est pas toujours clair. (Et c'est une très bonne chose.)
- Règles d'enregistrement dans un domaine : le registre du domaine. Pour la racine, c'est l'ICANN (mais pas toute seule).

Les acteurs, suite

- Qui décide, qui organise, qui établit les normes techniques ?
- Ce n'est pas toujours clair. (Et c'est une très bonne chose.)
- Règles d'enregistrement dans un domaine : le registre du domaine.
- Politique du résolveur (« DNS menteur », qui fausse les réponses) : le gérant du résolveur, la justice locale, la loi locale.

Les acteurs, suite

- Qui décide, qui organise, qui établit les normes techniques ?
- Ce n'est pas toujours clair. (Et c'est une très bonne chose.)
- Règles d'enregistrement dans un domaine : le registre du domaine.
- Politique du résolveur (« DNS menteur », qui fausse les réponses) : le gérant du résolveur, la justice locale, la loi locale.
- Normes techniques : l'IETF, via ses normes (notamment les document nommés RFC).

Étude de cas : qui décide de la racine unique ?

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS, sinon, un nom pourrait signifier des choses différentes - RFC 2826

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS
- Mais qui décide de laquelle ?

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS
- Mais qui décide de laquelle ?
- Le gérant du résolveur DNS choisit la racine qu'il interroge

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS
- Mais qui décide de laquelle ?
- Le gérant du résolveur DNS choisit la racine qu'il interroge
- Il peut en changer (« racine alternative »)

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS
- Mais qui décide de laquelle ?
- Le gérant du résolveur DNS choisit la racine qu'il interroge
- Il peut en changer (« racine alternative »)
- En pratique, presque tout le monde utilise la même : intérêt commun

Étude de cas : qui décide de la racine unique ?

- Il faut une racine unique du DNS
- Mais qui décide de laquelle ?
- Le gérant du résolveur DNS choisit la racine qu'il interroge
- Il peut en changer (« racine alternative »)
- En pratique, presque tout le monde utilise la même : intérêt commun, même des gouvernements chinois et russes

Organisation de la coopération

Pas de chef ne veut pas dire pas d'ordre ! L'an-archie n'est pas la jungle.

Organisation de la coopération

Pas de chef ne veut pas dire pas d'ordre ! L'an-archie n'est pas la jungle.

- Du plus informel (administrateurs système qui se parlent en IRC),

Organisation de la coopération

Pas de chef ne veut pas dire pas d'ordre ! L'an-archie n'est pas la jungle.

- Du plus informel (administrateurs système qui se parlent en IRC),
- Au plus formel (organisations professionnelles comme DNS-OARC),

Organisation de la coopération

Pas de chef ne veut pas dire pas d'ordre ! L'an-archie n'est pas la jungle.

- Du plus informel (administrateurs système qui se parlent en IRC),
- Au plus formel (organisations professionnelles comme DNS-OARC),
- En passant par diverses formules ad-hoc (liste de diffusion dns-fr, groupe de travail dnsop ou dns-privacy à l'IETF, forum ServerFault. . .).

Organisation de la coopération

Pas de chef ne veut pas dire pas d'ordre ! L'an-archie n'est pas la jungle.

- Du plus informel (administrateurs système qui se parlent en IRC),
- Au plus formel (organisations professionnelles comme DNS-OARC),
- En passant par diverses formules ad-hoc (liste de diffusion dns-fr, groupe de travail dnsop ou dns-privacy à l'IETF, forum ServerFault. . .).
- Beaucoup d'échanges d'informations. *Share what you know, learn what you don't.*

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité**
- 8 Alternatives
- 9 Conclusion

SécuritéS

Il n'y a pas **la** sécurité. Il y a **plusieurs** services de sécurité, parfois contradictoires, entre autres :

- 1 La disponibilité (le service fonctionne)
- 2 L'intégrité (le service n'a pas été modifié subrepticement)
- 3 La confidentialité (le service ne laisse pas fuir des informations)

Disponibilité et intégrité s'entendent souvent mal.

Au secours, je suis attaqué par les cyberguerriers !

Au secours, je suis attaqué par les cyberguerriers !

- Les attaques par déni de service (DoS = *Denial of Service*) sont une plaie de l'Internet

Au secours, je suis attaqué par les cyberguerriers !

- Les attaques par déni de service sont une plaie de l'Internet
- « Tout écosystème réel a des parasites » (Cory Doctorow)

Au secours, je suis attaqué par les cyberguerriers !

- Les attaques par déni de service sont une plaie de l'Internet
- « Tout écosystème réel a des parasites » (Cory Doctorow)
- Le DNS en est aussi victime (voire est utilisé pour ces attaques)

Au secours, je suis attaqué par les cyberguerriers !

- Les attaques par déni de service sont une plaie de l'Internet
- « Tout écosystème réel a des parasites » (Cory Doctorow)
- Le DNS en est aussi victime
- La défense : redondance, réactivité, coopération, créativité

Attaque contre la racine de juin 2016, vue par DNSmon

» DNSMON > root

DNSMON

DNS responses for

Protocol: Servers:



La censure, et comment la contourner

La censure, et comment la contourner

- En France, plusieurs sources de censure frappent le DNS :
ARJEL, ministère de l'Intérieur (la Main Rouge), tribunaux...

La censure, et comment la contourner

- En France, plusieurs sources de censure frappent le DNS : ARJEL, ministère de l'Intérieur, tribunaux. . .
- Le mécanisme ? Les résolveurs DNS mentent pour les noms censurés,

La censure, et comment la contourner

- En France, plusieurs sources de censure frappent le DNS : ARJEL, ministère de l'Intérieur, tribunaux. . .
- Le mécanisme ? Les résolveurs DNS mentent pour les noms censurés,
- Seuls les gros FAI français le font, les réseaux locaux, les petits FAI ou les étrangers ignorent cette règle,

Exemple de censure en France, vu par les sondes Atlas

```
% atlas-resolve --country FR -r 500 thepiratebay.se
Measurement #2420872 for thepiratebay.se/A uses 500 probes
[141.101.118.194 141.101.118.195] : 239 occurrences
[ERROR: NXDOMAIN] : 21 occurrences
[146.112.61.106] : 2 occurrences
[ERROR: SERVFAIL] : 31 occurrences
[127.0.0.1] : 184 occurrences
Test done at 2015-09-16T07:43:43Z
```

Détournement de nom de domaine

(*Hijacking*) : prendre le contrôle d'un nom par

Détournement de nom de domaine

(*Hijacking*) : prendre le contrôle d'un nom par

- Ingénierie sociale

Détournement de nom de domaine

(*Hijacking*) : prendre le contrôle d'un nom par

- Ingénierie sociale
- Craquage de mot de passe

Détournement de nom de domaine

(*Hijacking*) : prendre le contrôle d'un nom par

- Ingénierie sociale
- Craquage de mot de passe
- Procédures (par exemple de transfert) insuffisamment sécurisées

Analyse d'un détournement, a posteriori, avec DNSDB

NORMALEMENT

```
;; bailiwick: fr.  
;;  
count: 116142  
;; first seen: 2012-11-26 10:28:11 -0000  
;; last seen: 2016-09-01 13:04:31 -0000  
meteofrance.fr. IN NS vivaldi.meteo.fr.  
meteofrance.fr. IN NS cadillac.meteo.fr.
```

PENDANT LE DÉTOURNEMENT

```
;; bailiwick: fr.  
;;  
count: 57  
;; first seen: 2016-05-23 22:33:49 -0000  
;; last seen: 2016-05-24 08:00:57 -0000  
meteofrance.fr. IN NS ns1.hostinger.fr.  
meteofrance.fr. IN NS ns2.hostinger.fr.  
meteofrance.fr. IN NS ns3.hostinger.fr.  
meteofrance.fr. IN NS ns4.hostinger.fr.
```


Vie privée

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs
- Et elles sont en clair, donc écoutables

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs
- Et elles sont en clair, donc écoutables
- La NSA a un programme d'espionnage du DNS (MoreCowBell) mais elle n'est pas la seule

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs
- Et elles sont en clair, donc écoutables
- La NSA a un programme d'espionnage du DNS (MoreCowBell) mais elle n'est pas la seule
- Projet « *DNS privacy* » à l'IETF, solution en deux approches

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs
- Et elles sont en clair, donc écoutables
- La NSA a un programme d'espionnage du DNS (MoreCowBell) mais elle n'est pas la seule
- Projet « *DNS privacy* » à l'IETF, solution en deux approches
- 1) Minimiser les données (ne plus envoyer le nom complet dans la requête)

Vie privée

- Sans le savoir, vous envoyez des requêtes DNS à plein d'acteurs
- Et elles sont en clair, donc écoutables
- La NSA a un programme d'espionnage du DNS (MoreCowBell) mais elle n'est pas la seule
- Projet « *DNS privacy* » à l'IETF, solution en deux approches
- 1) Minimiser les données (ne plus envoyer le nom complet dans la requête)
- 2) Chiffrer (DNS sur TLS)

Quel résolveur ?

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ?
Google ? Cisco ?

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ?
Google ? Cisco ?
- Risques pour la vie privée

Quel résolveur ?

- Contre la censure et les pannes, passer à un autre résolveur ?
Google ? Cisco ?
- Risques pour la vie privée
- Pas d'authentification : parlez-vous vraiment à Google ?

DNSSEC

- On peut **empoisonner** la mémoire d'un résolveur, en répondant avant le vrai serveur faisant autorité,

DNSSEC

- On peut **empoisonner** la mémoire d'un résolveur, en répondant avant le vrai serveur faisant autorité,
- DNSSEC signe cryptographiquement les enregistrements DNS, pour détecter toute modification,

DNSSEC

- On peut **empoisonner** la mémoire d'un résolveur, en répondant avant le vrai serveur faisant autorité,
- DNSSEC signe cryptographiquement les enregistrements DNS, pour détecter toute modification,
- Si le menteur transforme le code en NXDOMAIN, pas trop de changement (SERVFAIL au lieu de NXDOMAIN, le déni de service fonctionne),

DNSSEC

- On peut **empoisonner** la mémoire d'un résolveur, en répondant avant le vrai serveur faisant autorité,
- DNSSEC signe cryptographiquement les enregistrements DNS, pour détecter toute modification,
- Si le menteur transforme le code en NXDOMAIN, pas trop de changement (SERVFAIL au lieu de NXDOMAIN, le déni de service fonctionne),
- Permet d'empêcher les détournements,

DNSSEC

- On peut **empoisonner** la mémoire d'un résolveur, en répondant avant le vrai serveur faisant autorité,
- DNSSEC signe cryptographiquement les enregistrements DNS, pour détecter toute modification,
- Si le menteur transforme le code en NXDOMAIN, pas trop de changement (SERVFAIL au lieu de NXDOMAIN, le déni de service fonctionne),
- Permet d'empêcher les détournements,
- En supposant qu'on valide en aval du résolveur menteur. . .

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives**
- 9 Conclusion

« Nous vous rappelons qu'il existe d'autres possibilités »

Mais pas de miracles : les alternatives ont aussi leurs inconvénients

- Identificateurs fondés sur le contenu comme les magnets de BitTorrent
- Identificateurs fondés sur la cryptographie (BitMessage, .onion, Namecoin - chaîne de blocs, GNUnet)

Plan du tutoriel

- 1 Les noms de domaine
- 2 Le protocole DNS
- 3 Opérationnel
- 4 Configurer les serveurs
- 5 Avitaillement
- 6 Gouvernance
- 7 Sécurité
- 8 Alternatives
- 9 Conclusion

Avenir

Avenir

- Les noms de domaine ne sont pas qu'une solution technique :
c'est aussi un vecteur d'identité

Avenir

- Les noms de domaine ne sont pas qu'une solution technique : c'est aussi un vecteur d'identité
- Cela ne durera pas forcément toujours. Tout le monde sur Facebook ?

Avenir

- Les noms de domaine ne sont pas qu'une solution technique : c'est aussi un vecteur d'identité
- Cela ne durera pas forcément toujours. Tout le monde sur Facebook ?
- Mais la base installée est énorme

Avenir

- Les noms de domaine ne sont pas qu'une solution technique : c'est aussi un vecteur d'identité
- Cela ne durera pas forcément toujours. Tout le monde sur Facebook ?
- Mais la base installée est énorme
- Le DNS peut être remplacé, même si on garde les noms de domaine

Avenir

- Les noms de domaine ne sont pas qu'une solution technique : c'est aussi un vecteur d'identité
- Cela ne durera pas forcément toujours. Tout le monde sur Facebook ?
- Mais la base installée est énorme
- Le DNS peut être remplacé, même si on garde les noms de domaine
- Mais là aussi, la base installée est énorme