Infrastructure DNS et bien commun

Stéphane Bortzmeyer
stephane+bc@bortzmeyer.org

Le Temps des Communs, Brest, 5 octobre 2015

Infrastructure DNS et bien commun

Stéphane Bortzmeyer
stephane+bc@bortzmeyer.org

Le Temps des Communs, Brest, 5 octobre 2015

Les dirigeants d'Internet

IMPRIMER

23 avril 2015 - Actualité

Lutte contre la propagande terroriste : le Gouvernement mobilise les dirigeants d'internet

[Source : Numérama]

Introduction

Introduction

- Structure de l'Internet : pas de hiérarchie, pas de Président de l'Internet,

Introduction

- Structure de l'Internet : pas de hiérarchie, pas de Président de l'Internet,
- Personne ne peut donner d'ordres à **tous** les acteurs « Arrêtez d'utiliser le protocole SSLv3 », « Mettez au moins deux serveurs par zone », « Bloquez tous les noms commençant par `thepiratebay` », « Mettez à jour vos logiciels pour gérer les adresses en Unicode »,

Introduction

- Structure de l'Internet : pas de hiérarchie, pas de Président de l'Internet,
- Personne ne peut donner d'ordres à **tous** les acteurs,
- Très difficile à comprendre pour les ministres d'un pays monarchique comme la France. (Et pour la plupart des journalistes.)

Bien commun

Bien commun

- Infrastructure commune,

Bien commun

- Infrastructure commune,
- Qui ne marche pas toute seule,

Bien commun

- Infrastructure commune,
- Qui ne marche pas toute seule,
- Mais dont tout le monde a intérêt à ce que ça marche.

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,

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,
- Dans les messages échangés, chaque machine indique l'adresse source et l'adresse destination, ce qui permet au destinataire de répondre,

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,
- Dans les messages échangés, chaque machine indique l'adresse source et l'adresse destination, ce qui permet au destinataire de répondre,
- Un mécanisme non décrit ici permet aux messages d'arriver à l'adresse de destination (allocation d'adresses par les RIR, routage, BGP...).

Difficile d'agir ensemble

Difficile d'agir ensemble

- Exemple : filtrage à la source des adresses IP usurpées,

Difficile d'agir ensemble

- Exemple : filtrage à la source des adresses IP usurpées,
- Tout le monde y a intérêt,

Difficile d'agir ensemble

- Exemple : filtrage à la source des adresses IP usurpées,
- Tout le monde y a intérêt,
- Mais les premiers qui le font supportent les coûts et n'ont pas de bénéfices,

Difficile d'agir ensemble

- Exemple : filtrage à la source des adresses IP usurpées,
- Tout le monde y a intérêt,
- Mais les premiers qui le font supportent les coûts et n'ont pas de bénéfices,
- Et aucun Dictateur de l'Internet ne peut l'imposer,

Difficile d'agir ensemble

- Exemple : filtrage à la source des adresses IP usurpées,
- Tout le monde y a intérêt,
- Mais les premiers qui le font supportent les coûts et n'ont pas de bénéfices,
- Et aucun Dictateur de l'Internet ne peut l'imposer,
- **Comme souvent en écologie, la somme des intérêts individuels ne fait pas l'intérêt collectif**.

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.

Les noms DNS

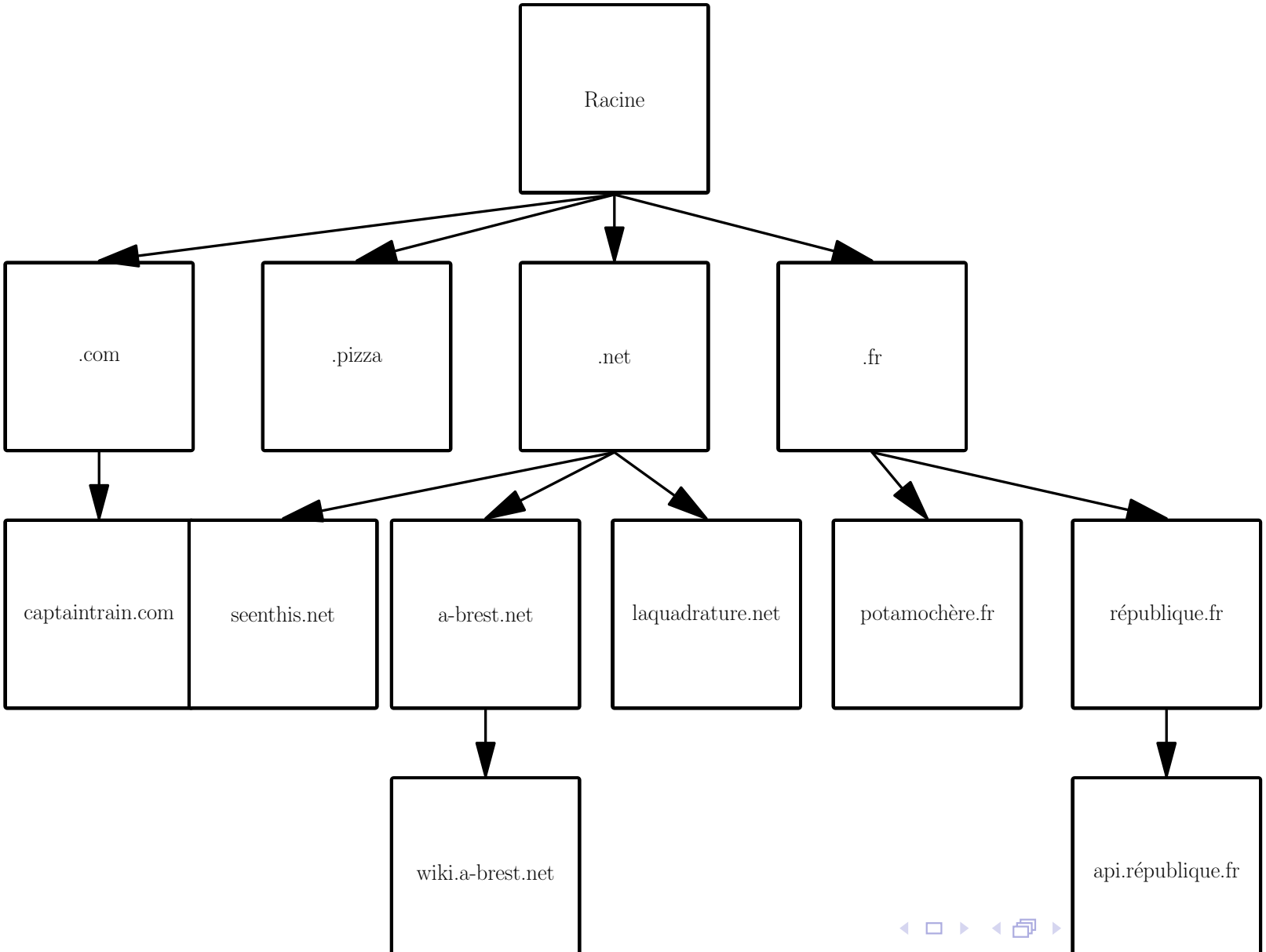
Les noms DNS

- Exemples de noms de domaines : `wiki.a-brest.net`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `fr.wikipedia.org`...

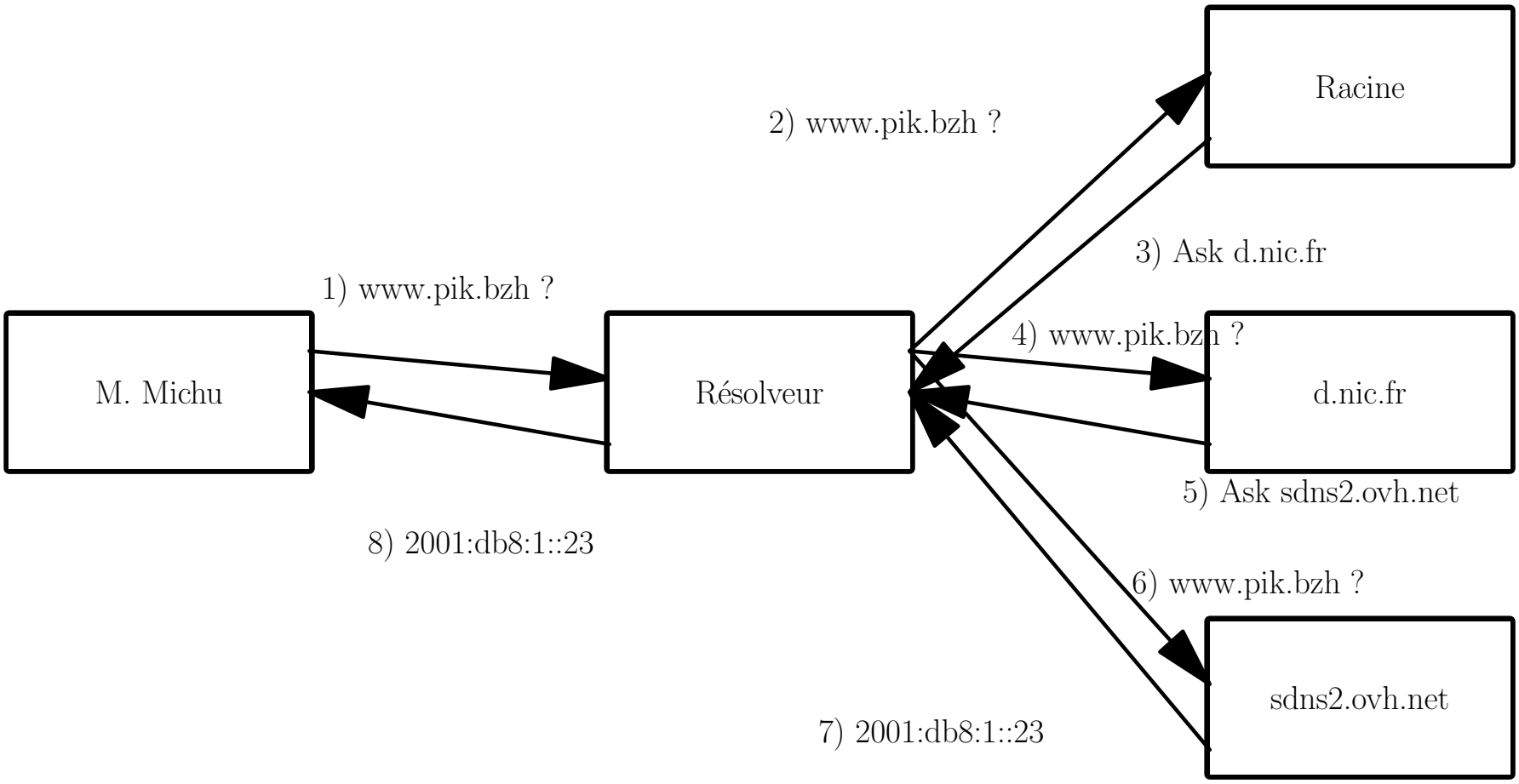
Les noms DNS

- Exemples de noms de domaines : `wiki.a-brest.net`, `www.phy.cam.ac.uk`, `www.potamochère.fr`, `gmail.com`, `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



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.

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 le gouvernement des États-Unis, caché derrière l'ICANN.
- 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).

Les méchants

Les méchants

- Hackers russes et chinois ?

Les méchants

- Hackers russes et chinois ?
- Pédophiles djihadistes radicalisés ?

Les méchants

- Hackers russes et chinois ?
- Pédophiles djihadistes radicalisés ?
- NSA et DGSE ?

Les méchants

- Hackers russes et chinois ?
- Pédophiles djihadistes radicalisés ?
- NSA et DGSE ?
- Industrie du divertissement ou bien du jeu ?

Les méchants

- Hackers russes et chinois ?
- Pédophiles djihadistes radicalisés ?
- NSA et DGSE ?
- Industrie du divertissement ou bien du jeu ?
- Lycéen dans son garage ?

Les négligents

Les négligents

- Bien plus nombreux que les méchants

Les négligents

- Bien plus nombreux que les méchants
- Manque de temps, de compétences. . .

Les négligents

- Bien plus nombreux que les méchants
- Manque de temps, de compétences. . .
- Beaucoup de gens largués, ou irresponsables.

Les négligents

- Bien plus nombreux que les méchants
- Manque de temps, de compétences. . .
- Beaucoup de gens largués, ou irresponsables. Exemple : correction des logiciels pour une faille de sécurité. Ça prend un temps fou.

Les négligents

- Bien plus nombreux que les méchants
- Manque de temps, de compétences...
- Beaucoup de gens largués, ou irresponsables.
- Longues campagnes collectives nécessaires, avec test des serveurs `https://ednscomp.isc.org/compliance/tld-report.html`

Déploiement d'une nouveauté

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).
- Peu de changements logiciels nécessaires dans l'infrastructure

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).
- Peu de changements logiciels nécessaires dans l'infrastructure
- Changements dans les logiciels utilisateur

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).
- Peu de changements logiciels nécessaires dans l'infrastructure
- Changements dans les logiciels utilisateur
- Norme technique finie en 2003

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).
- Peu de changements logiciels nécessaires dans l'infrastructure
- Changements dans les logiciels utilisateur
- Norme technique finie en 2003
- Autorisés dans la racine en 2009

Déploiement d'une nouveauté

- Exemple des IDN (noms de domaine en Unicode comme `république-numérique.fr`).
- Peu de changements logiciels nécessaires dans l'infrastructure
- Changements dans les logiciels utilisateur
- Norme technique finie en 2003
- Autorisés dans la racine en 2009
- Toujours pas compris par certains hébergeurs, certains logiciels

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)
```

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.

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,

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,
- S'il y avait vraiment un Chef de l'Internet, la censure serait réellement appliquée.

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.*

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

Conclusion

Conclusion

- Le DNS est un bien commun : pas de chef, mais tout le monde est partie prenante,

Conclusion

- Le DNS est un bien commun : pas de chef, mais tout le monde est partie prenante,
- Sa gouvernance est donc compliquée mais très robuste.

Conclusion

- Le DNS est un bien commun : pas de chef, mais tout le monde est partie prenante,
- Sa gouvernance est donc compliquée mais très robuste.
- S'il y avait un chef du DNS, certains problèmes seraient résolus plus vite mais les catastrophes seraient pires.