Gérer son DNS

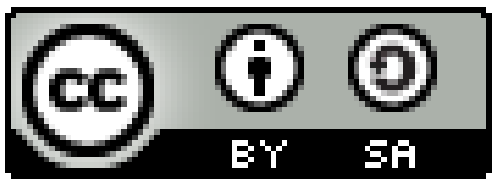
Matthieu Herrb

tetaneutral.net

Atelier Tetaneutral.net, 10 février 2015

`http://homepages.laas.fr/matthieu/talks/ttnn-dns.pdf`

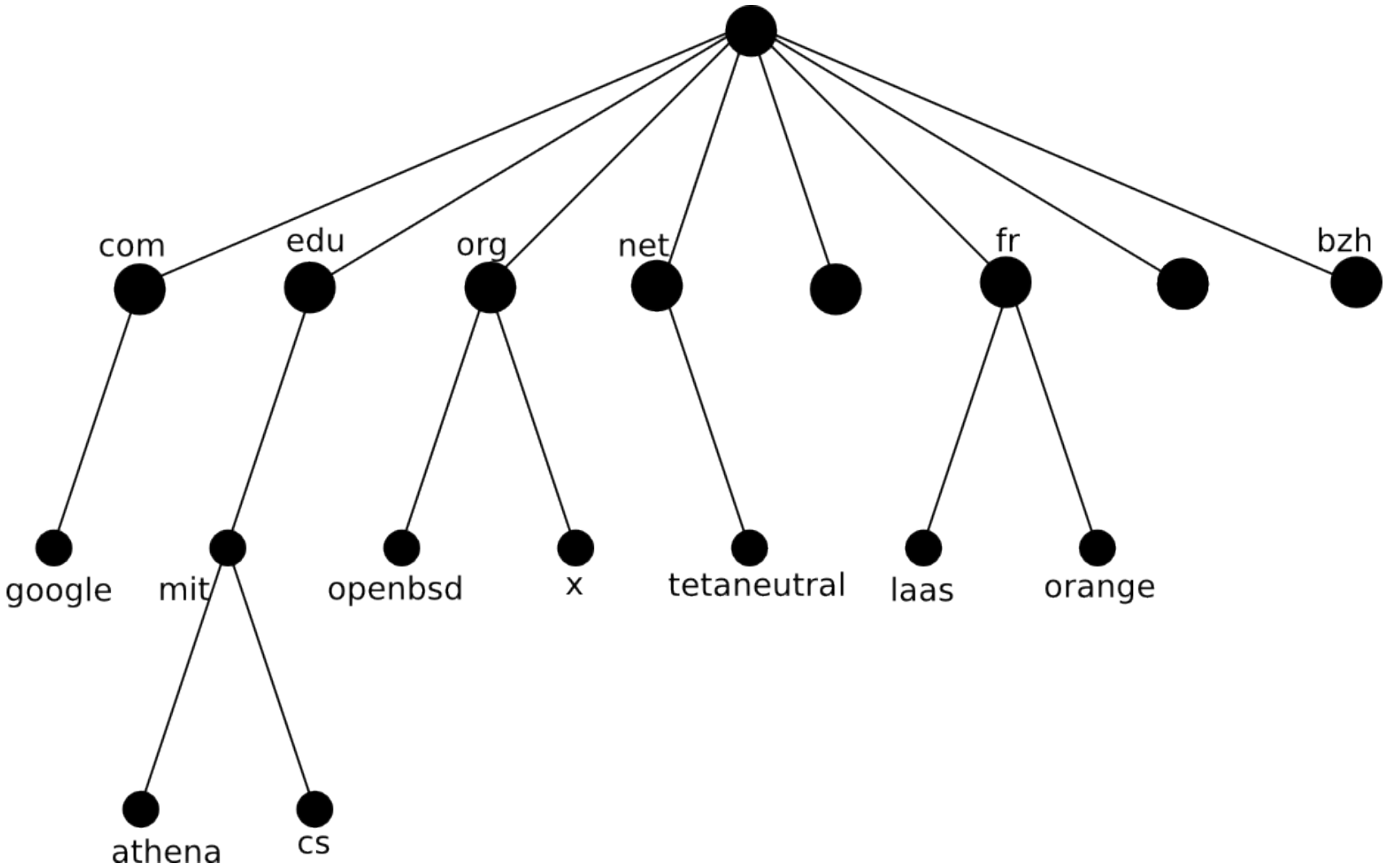
Licence



Introduction

- Nommage dans les internets
  - Nom de machine $\rightarrow$ adresse IP
  - Espace hiérarchique / domaines
  - Gère aussi d'autres informations
  - Infrastructure quasi-indispensable
- Base de données distribuée
- Business des noms de domaines
  ICANN / bureaux d'enregistrement

Arborescence de domaines



Vocabulaire

domaine : un sous-arbre de l'arbre complet;

zone : un ensemble de feuilles gérées par un même serveur;

resource record : (RR) un enregistrement dans la base de données.

resolver : un client qui intérroge un serveur DNS

TTL : *Time To Live* durée de vie d'une information

Types de serveurs :

autoritaire : « maître » de l'information d'une zone

- *primaire* copie de référence des zones
- *secondaire* copies de secours des zones

caching : interroge d'autres serveurs pour fournir les infos aux resolveurs

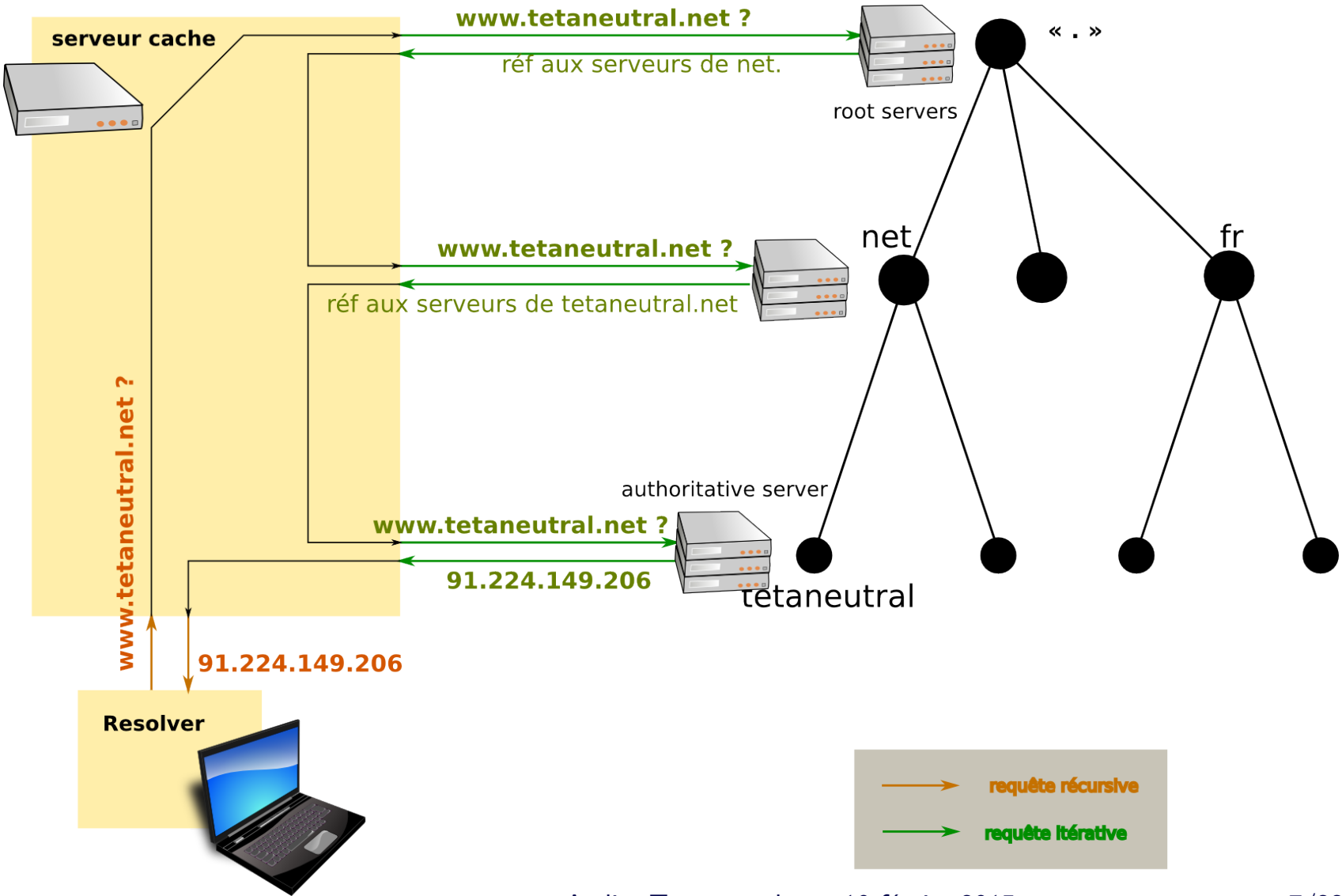
Requêtes DNS

Types de requêtes :

recursive : utilisées par les résolveurs :
le serveur va chercher l'info et la retourne au resolver

iterative : utilisées par les serveurs intermédiaires :
le serveur retourne une référence (liste d'adresses) de serveurs qui pourront répondre.

Cheminement d'une requête DNS



Types d'enregistrements

- **SOA** *Start of Authority* Infos admin sur une zone (serveur autoritaire)
- **A** adresse IPv4
- **AAAA** adresse IPv6
- **CNAME** *Canonical Name* alias
- **NS** nom d'un serveur DNS
- **MX** nom d'un serveur de messagerie
- **PTR** pointeur vers un nom (reverse)
- **SRV** nom du serveur pour un service donné (XMPP)
- **TXT** données diverses format texte *(SPF, DKIM,..)*

Registres DNS

- **Registres de 1er niveau :**
  - Gèrent les domaine de 1er niveau.
  - Désignés par l'ICANN.
- **Autres**
  - Organismes habilités à vendre des noms de domaine
  - Opérateurs pour un ensemble de zones
  - Définissent leur politique tarifaire
  - Proposent souvent d'héberger les domaines achetés
  - Exemple : Gandi (`http://www.gandi.net/`)

DNS reverse

Correspondance adresse IP $\rightarrow$ nom

- Réalisé via des enregistrements **PTR** dans une zone dédiée.
- Utilise les adresses IP *inversées* :
  `12.31.168.192.in-addr.arpa.` ou
  `f.e.d.c.b.a.9.8.7.6.5.4.3.2.1.0.4.0.0.0.2.0.6.6.0.6.6.0.1.0.0.2.ip6.arpa.`
- Mécanisme de délégation mis en place par LIR qui a attribué les adresses IP
- Nombreux problèmes (adresses dynamiques,...)
- Souvent utilisé à tord comme contrôle de sécurité

Serveur autoritaire en pratique...

- Achat d'un nom de domaine
- Installation d'un logiciel serveur (Bind, NSD,...)
- Création fichier(s) de zone(s)
- Création de serveurs secondaires
- Déclaration des `glue records`

Exemple de fichier de zone

```
$TTL 1d
@     IN SOA    ns1.example.com. root.example.com. (
                      2015021001 ; serial
                      12h        ; refresh
                      1h         ; retry
                      1w         ; expire
                      6h )       ; negative TTL
      IN NS     ns1.example.com.
      IN NS     ns2.example.com.
      IN MX 10  mail.example.com.
      IN MX 20  mail.other.com.
      IN A      192.0.2.1
      IN AAAA   2001:db8:1234:5678::1
www   IN CNAME  example.com.
ns1   IN A      192.0.2.10
      IN AAAA   2001:db8:1234:5678::a
ns2   IN A      192.0.2.20
mail  IN A      192.0.2.21
```

Serveur secondaire (esclave)

- Augmente la résilience de la zone
- Si possible sur un réseau (AS) différent
- Limiter les transferts de zone
- Utiliser TSIG pour sécuriser les transferts de zone si possible

Configuration d'un serveur cache

- Pour un site qui n'a pas son propre domaine mais veut éviter de dépendre de son FAI
- Pour gérer une zone reverse de ses adresses RFC1918 (NAT)
- Pour un FAI qui propose le service DNS à ses abonnés.
- Chaque serveur cache augmente un peu la charge sur les serveurs racine
- Mécanisme de *forwarder* pour utiliser un autre serveur récursif plutôt que de parler directement aux serveurs racine
- Logiciel : unbound ou bind

Configuration d'un resolver

- `/etc/resolv.conf` sur systèmes Unix-like
- Souvent géré automatiquement → pas d'édition directe
- Renseigné par client DHCP ou SLAAC IPv6.
- Utilise le serveur récursif du site ou du FAI
- Gère un domaine de recherche par défaut pour noms pas entièrement qualifiés.
- Mécanisme pour privilégier une famille d'adresse `gai.conf` sur linux.

Outils

- `dig`
- `host`
- `whois`
- zonecheck
- netmagis
- DynDNS & Co

Sécurité

- Utilise le protocole UDP sur le port 53
- Fuites d'informations par transfert de zone
- Par défaut, pas d'authentification ni de signature des données
- $\rightarrow$ nombreuses attaques possible pour falsifier les résultats
- Attaques DDOS par amplification DNS sur serveurs récursifs

Solutions

- Limiter les transferts de zone
- Désactiver le mode récursif sauf pour requêtes locales
- Installer des serveurs récursif et autoritaire séparés (Unbound + NSD)
- DNSSEC...

DNSSEC

- Ensemble d'extensions pour sécuriser le protocole DNS
- Signature numérique des zones
- Permet d'utiliser des enregistrements DNS pour diffuser des clés publiques pour d'autres applis (SSH, IPSec,...)
- Indispensable mais très **lourd** à déployer
- Outils : OpenDNSSEC

Détournements du DNS

- DNS menteur : moyen de censure
- Observation du trafic DNS : collecte d'informations
- Tunnels IP over DNS (contournement portail captif)
- ...

Autres fonctions

- IDN (Internationalized Domain Names) - noms en UTF8
- DANE - gestion de clés publiques / signatures
- RBL - real time black lists
- Mises à jour dynamiques ; utilisées par AD (Microsoft)
- ...

Systemes alternatifs

Contestation du rôle centralisateur de l'ICANN
Gouvernance de l'internet
...

- open-root (Louis Pouzin)
- Namecoin

Ateliers

- Configuration du résolveur unbound
- Achat et configuration d'un domaine auprès d'un bureau d'enregistrement
- Configuration d'un serveur autoritaire nsd
- Configuration d'un serveur mixte bind
- Configuration d'un serveur secondaire