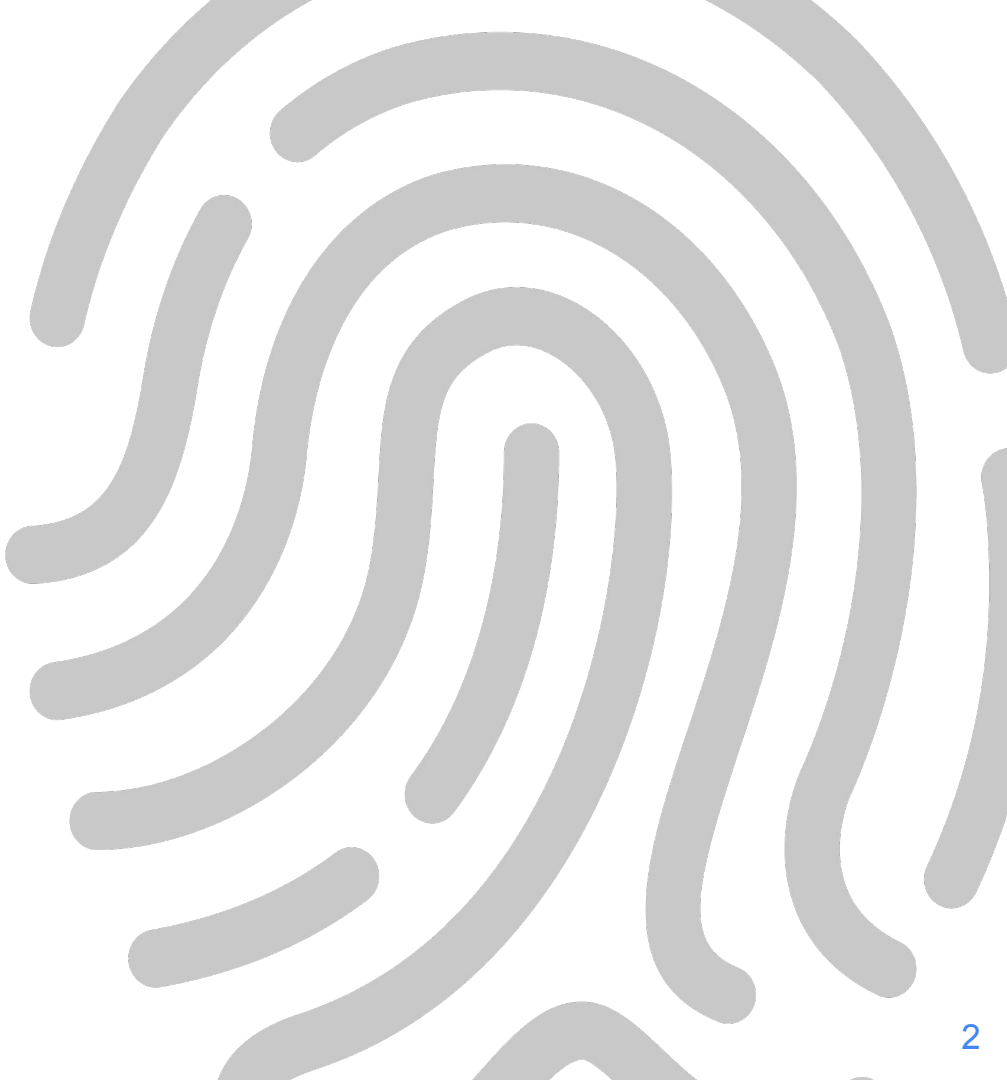
WILD CODE SCHOOL

Domain Name System

DNS

- Ça sert à quoi ?
- Comment ça marche ?



Plan

WILD CODE SCHOOL

Introduction

Humain vs ordinateur

Pour pouvoir communiquer sur un réseau (IP), il est nécessaire de connaître l'adresse IP du destinataire d'un message.

Les adresses IP sont des séquences binaires (32 ou 128 bits).
Elles disposent d'une notation standard les rendant plus facile à manipuler…

… Néanmoins, il reste difficile de les manipuler au quotidien et surtout de s'en souvenir.

En revanche, il est aisé de retenir des noms textuels

Un système de correspondances

Pour pouvoir utiliser des noms à la place des adresses
=> système de correspondances

Ce système doit pouvoir faire correspondre à des noms d'hôtes (*hostname*) leur adresse IP

Ce système est apparu très tôt dans l'histoire d'Internet et était historiquement géré à la main !

HOSTS.TXT

Dès les débuts du réseau qui deviendra internet, un fichier texte contenant des adresses IP et les noms de machine correspondants est apparu.

Il est standardisé par la RFC 608 de 1974.

Ce fichier était maintenu par le NIC (*Network Information Center*) et copié sur chaque machine via transfert de fichier (FTP).

L'augmentation rapide du nombre d'hôtes sur ce qui allait devenir Internet a rendu cette gestion obsolète

DNS

Le système des noms de domaine (*Domain Name System* - DNS) a vu le jour au NIC pour permettre de répondre à cet enjeu majeur.

Il a été standardisé dans les RFC 882 et 883 en 1983 par Paul V. Mockapetris

Aujourd'hui, il s'appuie sur les RFC 1034 et 1035, toujours valables à ce jour, mais complétées de nombreuses autres

Idée générale

DNS est :

- une base de données répartie et décentralisée
  => robustesse et passage à l'échelle
- une technologie d'infrastructure
  => invisible pour l'utilisateur
- un ensemble de noms de domaine auxquels sont associées des données

WILD CODE SCHOOL

Les noms de domaine

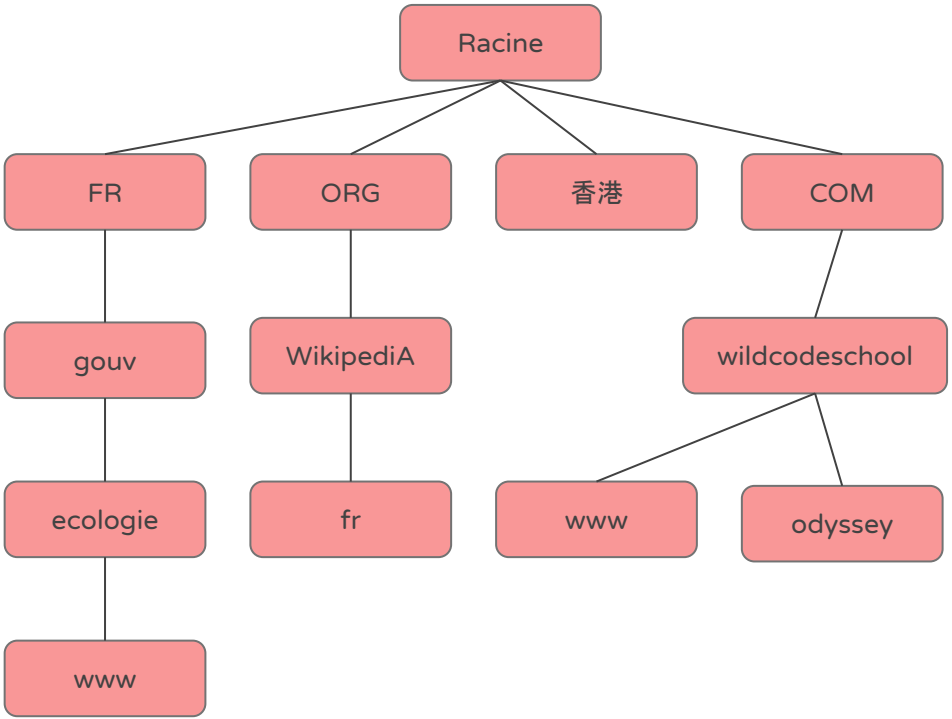
Une définition

Un nom de domaine est :

- Un identifiant (unique) textuel non sensible à la casse
- Composite suivant une structure hiérarchique arborescente
  - Un domaine peut contenir des sous-domaines
  - Chaque domaine appartient à un domaine parent sauf la racine
- Désigne un ensemble de ressources Internet
- Assimilable à l'identité d'une personne/structure/ressource sur Internet
  - Plus stable que les adresses
  - Au choix => vecteur d'image

Arborescence

- Racine appelée point .
- TLD (*Top Level Domain*)
- et ainsi de suite
- séparé par des points .
- FQDN (*Fully Qualified Domain Name*)
- point final souvent omis



Les composants

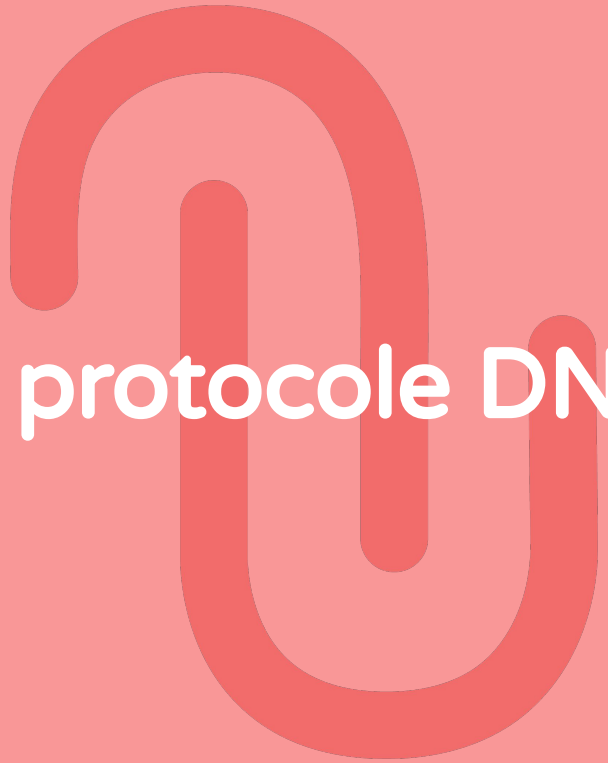
Les composants d'un nom de domaine (*label*)

- En nombre quelconque (mais en avoir un seul est compliqué - TLD - donc en général au moins 2)
- peuvent utiliser un jeu de caractères étendus - Internationalized domain name (IDN)
- 63 caractères max - l'ensemble d'un nom de domaine : 255 max

Des exemples

- odyssey.wildcodeschool.com.
- www.wildcodeschool.com
- fr.wikipedia.org
- नेपाल.icom.museum
- ietf.org
- dany.wilder.name.fr
- tssr.pro

WILD CODE SCHOOL



Le protocole DNS

La communication DNS

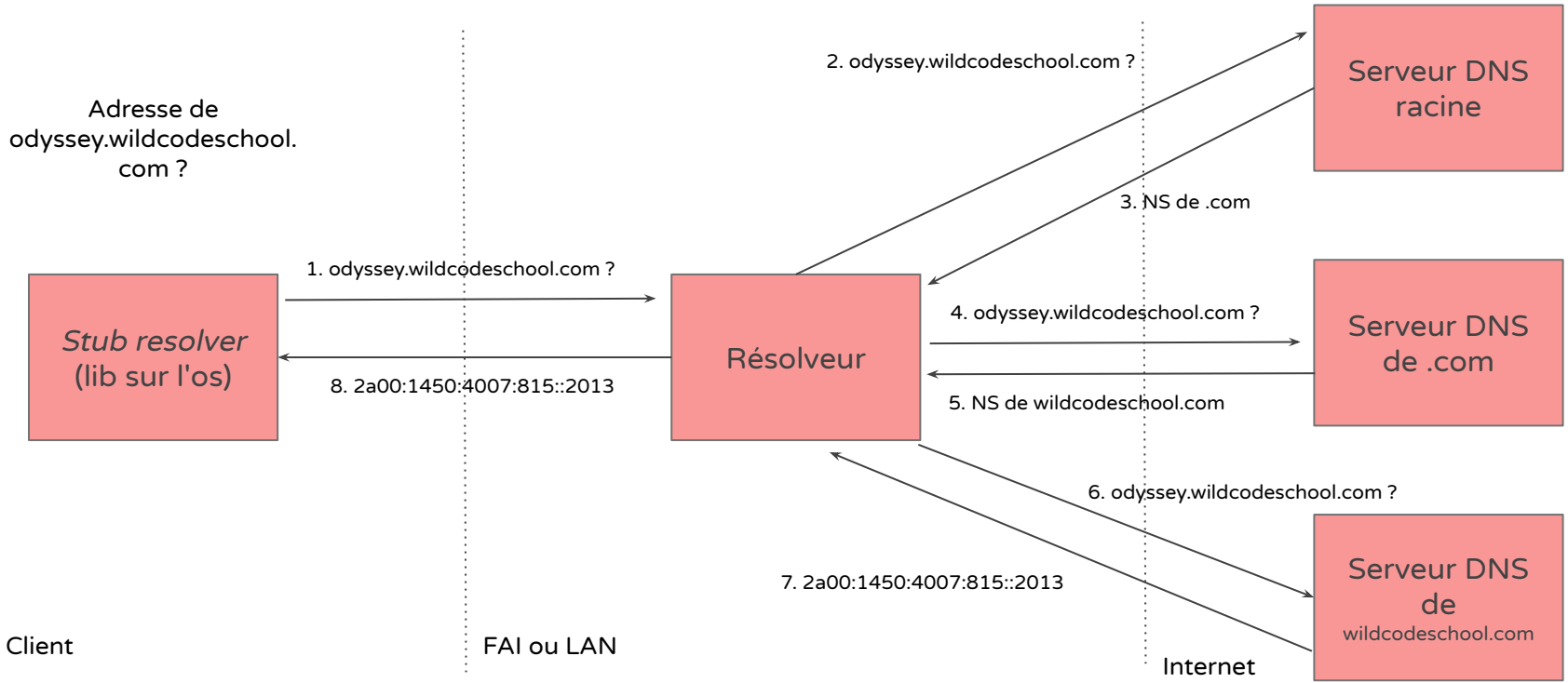
DNS est un protocole client-serveur de niveau applicatif (couche 7)

- UDP (en général) ou TCP - port 53 (DNS over TLS : port 853)
- En général : une requête, une réponse puis fin de communication

Différents types de serveurs :

- Serveurs faisant autorité (*authoritative server*)
- Résolveurs (*resolver*) ou serveur DNS récursif (“serveur de cache DNS”)

La résolution de nom



Les serveurs faisant autorité

Serveur faisant autorité :

- Serveur contenant les informations pour une (ou plusieurs) zone(s)
  - zone = partie de l'arborescence des noms de domaine
- En général plusieurs serveurs pour une même zone (tolérance de panne)
  - Primaire et secondaires
  - Synchronisation (Transfert de zone) via DNS
- Plusieurs solutions logicielles : NSD, Knot, BIND, PowerDNS, Microsoft DNS

Les serveurs racines

La racine est gérée par l'ICANN et est hébergée sur 13 domaines administrés par 12 organisations (dont le RIPE NCC - K et l'ICANN directement - L)

<*lettre*>.root-servers.net ou <*lettre*> = [a-m]

Ils gèrent une zone contenant les TLD et sont censés être connus par tous les résolveurs (leurs adresses IP).

En réalité il y a bien plus de 13 serveurs, notamment via anycast, réparti sur l'ensemble de la planète (+ de 130 sites)

Plus d'info : Serveur racine du DNS (WikipediA)

Les résolveurs

Ces serveurs ne contiennent à l'initialisation que les 13 root-servers
Ces serveurs récursifs interrogent les serveurs faisant autorité pour obtenir l'information demandée par le client.
En général, ils mettent en place du cache (enregistrement des réponses)
Ces informations doivent être temporaire (TTL - *Time To Live*)

Ce sont ces serveurs que les clients interrogent.
Ils sont en général chez les FAI ou sur un réseau privé et dédiés à un usage interne.
Logiciels serveur récursif : Unbound, BIND, PowerDNS, Microsoft DNS

Les résolveurs publiques

Certains résolveurs ne sont pas privés et sont accessibles à tous.

Quelques exemples :

- quad9 (Suisse) : 9.9.9.9 ou 149.112.112.112 / 2620:fe::fe ou 2620:fe::9
- Cloudflare (US) : 1.1.1.1 ou 1.0.0.1 / 2606:4700:4700::1111 ou 2606:4700:4700::1001
- Google (US) : 8.8.8.8 ou 8.8.4.4 / 2001:4860:4860::8888 ou 2001:4860:4860::8844
- FDN (FR) : 80.67.169.12 ou 80.67.169.40 / 2001:910:800::12 ou 2001:910:800::40

Stub resolver (DNS local)

Un résolveur minimum (*stub resolver*) :

- ne gère pas la partie récursive des requêtes consistant à demander successivement à différents serveurs faisant autorité en commençant par la racine
- gère (en général) un cache pour économiser les requêtes
- doit connaître l'adresse d'au moins un résolveur récursif pour transmettre les requêtes
- est en général intégré au système d'exploitation (ex. : systemd-resolved)

Configuration DNS d'un hôte

La configuration réseau d'une machine indique au moins une (mais en général plusieurs) adresse(s) de résolveur(s) DNS.
Ces informations sont en général fournies par DHCP

Quand une application veut accéder à une information DNS (par exemple récupérer l'adresse via le nom)

- Elle questionne le stub resolver du système (la libc, par exemple)
- Regarde dans son cache et dans le fichier hosts (/etc/hosts sous Unix)
- Si absent s'adresse à un résolveur récursif de sa config (puis un autre jusqu'à obtenir une réponse)

WILD CODE SCHOOL

Les enregistrements

Les enregistrements DNS

DNS associe à un nom de domaine des *Resource Record* (RR)

Il existe de nombreux types d'enregistrements (une liste sur WikipediA).

Par exemple :

- A : une ou plusieurs adresses IPv4
- AAAA : une ou plusieurs adresses IPv6
- NS : serveur faisant autorité sur ce domaine
- CNAME : le nom canonique d'un alias
- SOA : serveur primaire d'une zone
- PTR : pour la résolution inverse
- MX : nom du serveur de courrier du domaine

Ces RR ont un TTL (*Time To Live*) : temps maximum de validité dans un cache

La résolution inverse

Pour récupérer le nom de domaine d'une adresse IP :

- Résolution inverse
- Pseudo domain .in-addr.arpa (IPv4) ou ip6.arpa (IPv6)
  - Inversant le sens de l'adresse IP (sens d'un nom de domaine)
  - Découpe par octet et notation décimal (v4)
  - Découpe par chiffre hexa (v6)
- Nécessaire pour les adresses publiques
- Stockée dans des enregistrements PTR

Ex : `155.146.67.172.in-addr.arpa`

`b.9.2.9.3.4.C.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.3.0.2.3.0.0.7.4.6.0.6.2.ip6.arpa`

DNS round-robin

On peut associer plusieurs adresses à un nom de domaine

- Technique de partage de charge
- À chaque requête : la réponse est différente
- Le serveur fait tourner les adresses

WILD CODE SCHOOL

Enregistrer un nom de domaine

Racine et TLD

La racine DNS est gérée par l'ICANN (via sa composante IANA)
C'est à la racine qu'on doit enregistrer les TLD.

Longtemps la liste des TLD a été très limitée :

- Domaines de premier niveau nationaux (ccTLD - *Country Code Top Level Domain*)
- Quelques domaines génériques ouverts (gTLD) : com, org, net, info
- Domaines commandités, réservé à des activitées particulières : edu, gov, mil
- Le domaine technique spécial .arpa (zone de résolution inverse) et quelques domaines réservés : example, invalid, localhost, test

Depuis 2012 de nombreux autres TLD ont vu le jour et sont enregistré à l'iana

Registre de noms de domaine

Un registre de nom de domaine désigne :

- la base des informations sur un domaine (*domain name registry*)
- l'organisme en charge de sa gestion (*registry operator*) parfois aussi appelé un NIC (*Network Information Center*)

L'IANA gère la racine et délègue la gestion des sous domaines (par exemple les TLD) à d'autres organismes : registre pour ce domaine

Par exemple : l'AFNIC est le registre de .fr. (mais aussi .pm. .re. .tf. .wf. et .yt.)

Bureau d'enregistrement

Un bureau d'enregistrement est chargé par un registre de la relation avec les clients voulant réserver un nom de domaine.

Parfois, le bureau d'enregistrement peut aussi héberger votre zone DNS sur ses serveurs (Hébergeur DNS).
Sinon, il doit indiquer l'adresse de vos serveurs (NS) pour le domaine que vous réserver

Ex : OVH, Gandi… (383 accrédités par l'AFNIC)

WILD CODE SCHOOL

Outils

dig

dig (*Domain Information Groper*) est une commande Unix pour interroger des serveurs DNS qui fait partie de la suite BIND

dig est en général préféré à **nslookup** ou **host** car offrant plus de fonctionnalité

Sur Windows seul **nslookup** est disponible par défaut

Conclusion

- Fonctionnement général de DNS
- Nom de domaine
- Serveur faisant autorité
- Résolveur DNS
- Resource Records