

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Introduction

- ★ DNS, *Domain Name System* (Système de Nom de Domaine), mis en place en 1988, recouvre deux notions :
 - ★ Une **base de données répartie**, grâce à un grand nombre de serveurs de noms qui communiquent entre eux.
 - ★ Un **protocole**, de niveau application :
 - ★ Il utilise UDP pour le transport
 - ★ Le port 53 est utilisé par convention.
- ★ *Domain Name System* sert notamment à traduire un nom de domaine en adresse IP, ou en d'informations d'autres types.
- ★ Voir [STD 13](#), RFC 1034 (*Domain names - concepts and facilities*), RFC 1035 (*Domain names - implementation and specification*), etc.

★ Service de noms

- ★ Un service de noms permet aux utilisateurs d'accéder à une ressource en la désignant par son nom, plutôt que par son adresse.
- ★ DNS est un service de nommage standard sur internet (RFC 1033 à 1035).
- ★ Un des objectifs est donc de retrouver **l'adresse IP** d'une machine à partir de **son nom de domaine**.

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Nom de domaine

- ★ Il résulte d'un système hiérarchique :

- ★ Domaine de haut-niveau (TLD, *Top Level Domain*) ou domaine de premier niveau

- ★ **Générique** : gTLD ; *generic TLD*

- Ex. : .com, .net, .org, .mil, .gov, .biz, .info, .name, .pro, .aero, .coop, .xxx, .museum...

Depuis 2014, des milliers de nouveaux gTLD (nommés nTLD pour **News TLD**) peuvent être demandés, avec priorité aux propriétaires de marques déposées.

Ex. : .paris, .bzh, .guru...

- ★ **National** : ccTLD ; *country code TLD*

- Ex. : .fr, .uk, .nl, .it, .jp, .eu, .us...

- ★ Sous-domaine ou *label* : chaque sous-domaine est enregistré auprès du domaine supérieur.

Il faut donc :

- ★ la validation du domaine supérieur

- ★ ajouter un enregistrement dans les serveurs de noms du domaine supérieur.

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Nom de domaine

- ★ Les TLD sont gérés par l'[ICANN](#) (Internet Corporation for Assigned Names and Numbers) ; l'ICANN délègue la gestion de chaque TLD à un organisme appelé registre de haut-niveau (*registry*).
- ★ L' [AFNIC](#) (l' Association Française pour le Nommage Internet en Coopération) est le registry pour la France. Elle gère les ccTDL .fr, .re, .yt, .wf, .tf et .pm
- ★ [VeriSign](#) est le *registry* qui gère les .com, .net, .org...
- ★ Exemple 1

simon.info.arcep.fr

fr = ccTLD pour la France ; géré par l'AFNIC

arcep = Domaine de 2^d niveau, enregistré et validé par l'AFNIC (propriétaire : l'Autorité de Régulation des Communications Electroniques et des Postes)

info = Service informatique enregistré pour l'ARCEP.

simon = Nom d'une machine (celle de Simon) au sein du service informatique de l'ARCEP.

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Nom de domaine (suite...)

★ Exemple 2

ftp.aecnam.asso.fr

fr = ccTLD pour la France ; géré par l'AFNIC

aecnam.asso = Domaine composé d'une association enregistré et validé par l'AFNIC

ftp = Nom d'une machine (ou d'un service) de l'association.

★ Dans l'exemple 2 ci-dessus, **aecnam** est un élément de nom de domaine ou *label*.

★ Un élément d'un nom de domaine a au maximum 63 caractères.

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Nom de domaine (suite...)

★ Exemple 3 - La hiérarchie du domaine « ru.wikipedia.org. »

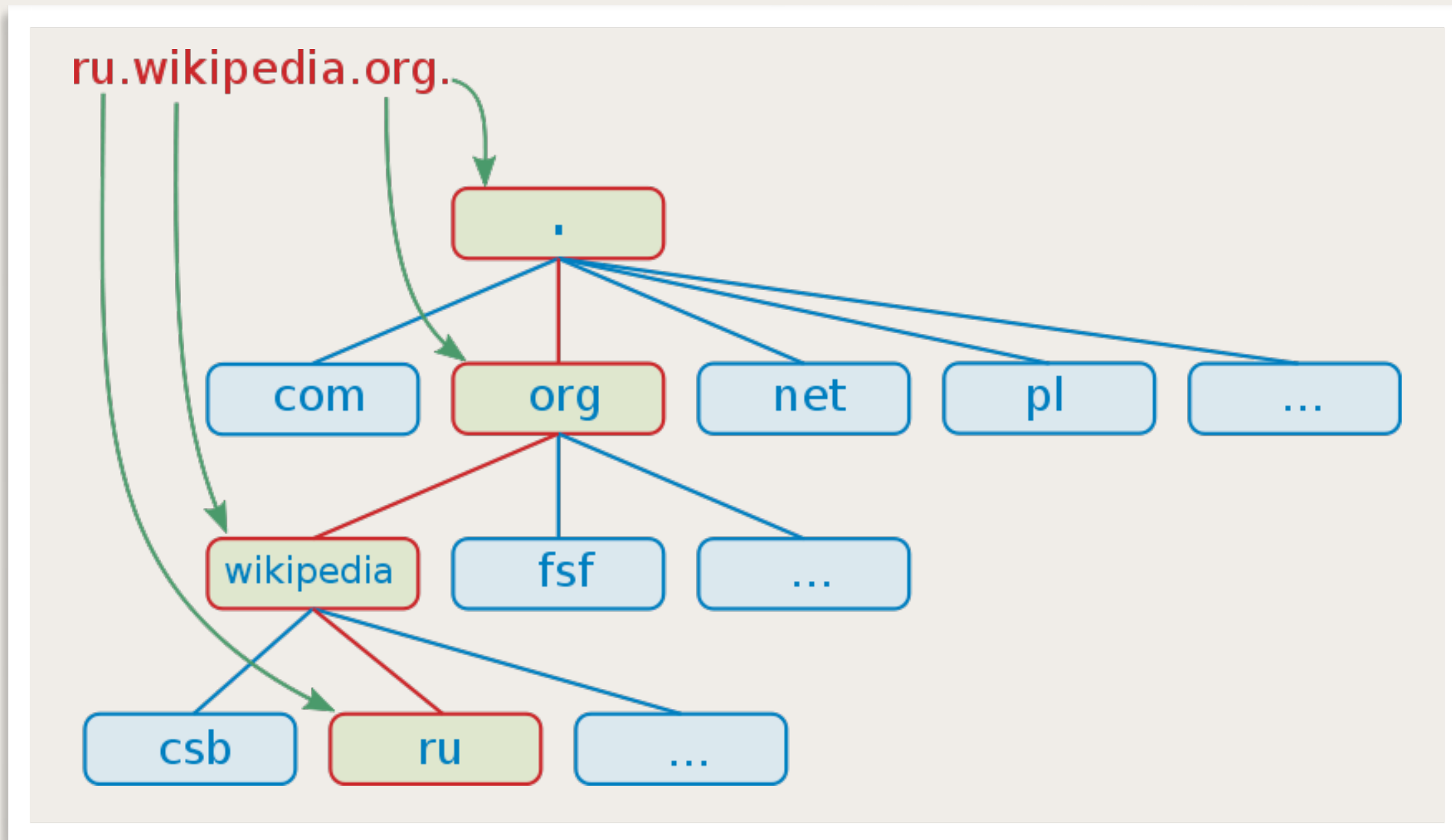


Fig 2.1 - Hiérarchie de domaine

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ FQDN : Fully Qualified Domain Name

- ★ Un nom de domaine pleinement qualifié (FQDN) est un nom de domaine écrit de façon absolue.

Il comporte donc :

- tous les sous-domaines (ou labels),
- le domaine de premier niveau (TLD),
- et il est ponctué par un point final qui représente la racine.

- ★ Exemple : **ru.wikipedia.org.**

Avec un point final !

❖ Enregistrer un nom de domaine

- ★ On utilise un **bureau d'enregistrement** de noms de domaine, *registrar* en anglais, qui gère la réservation de nom de domaine, conformément aux règles imposées par les registres de haut-niveau (*registry*).

- ★ Voir :

- www.gandi.net, www.ovh.com/fr/domaines/, etc.
- ou l'annuaire des bureaux d'enregistrement de l'AFNIC : www.afnic.fr/fr/votre-nom-de-domaine/comment-choisir-et-cree-mon-nom-de-domaine/

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Enregistrement de ressources

- ★ Un enregistrement de ressources, *resource record*, se compose de **cinq éléments** :

Nom de domaine ; Durée de vie ; Classe ; Type ; Valeur

- ★ **Nom de domaine** : un **FQDN**, qui se termine donc par un point (.), symbole de la racine des domaines. Ex. : **simon.info.arcep.fr.**
- ★ **Durée de vie** en secondes
- ★ **Classe** : IN pour Internet
- ★ **Type** : type d'enregistrement
 - A = Address Record : la valeur est l'adresse IP v4 du nom de domaine
 - AAAA = Address Record : la valeur est l'adresse IP v6 du nom de domaine
 - MX = Relai de messagerie
 - SOA = Start of Authority : serveur principal d'une zone
 - NS = Serveur de noms
 - CNAME = nom canonique : Alias de nom de domaine
 - PTR = Pointeur
 - HINFO = description de l'hôte
 - TXT = Texte de commentaire
- ★ **Valeur** : en fonction du type

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Enregistrement de ressources

★ Exemple :

<i>Nom de domaine</i>	<i>Durée de vie</i>	<i>Classe</i>	<i>Type</i>	<i>Valeur</i>
fr.wikipedia.org.	575	IN	CNAME	text.wikimedia.org.
text.wikimedia.org.	1522	IN	CNAME	text.esams.wikimedia.org.
text.esams.wikimedia.org.	2193	IN	A	91.198.174.232

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Exemple avec l'utilisation de dig :

- ★ *dig* est une commande du package *dnsutils* sous Linux pour **interroger** des serveurs DNS. Les réponses sont des **enregistrements de ressources**.

```
iMac-F:~ francois$ dig fr.wikipedia.org

; <<>> DiG 9.6.0-APPLE-P2 <<>> fr.wikipedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 28507
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fr.wikipedia.org.      IN      A

;; ANSWER SECTION:
fr.wikipedia.org.      575      IN      CNAME    text.wikimedia.org.
text.wikimedia.org.    1522     IN      CNAME    text.esams.wikimedia.org.
text.esams.wikimedia.org. 2193    IN      A        91.198.174.232

;; Query time: 42 msec
;; SERVER: 212.27.40.241#53(212.27.40.241)
;; WHEN: Sat Aug 27 20:15:20 2011
;; MSG SIZE  rcvd: 104
```

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Résolution de noms

- ★ L'espace des noms DNS est divisé en zones distinctes. Cet espace forme un arbre et chaque zone contient :
 - ★ une partie de l'arbre
 - ★ des serveurs de noms :
 - ★ un serveur primaire
 - ★ des serveurs secondaires
- ★ Un programme demandeur transmet une requête pour un nom de domaine à un solveur (*resolver*) local.
 - ★ Si la destination est locale, le solveur local donne la réponse, en retournant un enregistrement officiel.
 - ★ si la destination est distante, le solveur local peut répondre si l'information est disponible dans son cache.
 - ★ sinon, le solveur interroge le serveur primaire, qui résout la requête directement ou par requêtes **itératives** ou **récurives** jusqu'à l'obtention de l'enregistrement officiel.

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Résolveurs DNS

- ★ **BIND 9** est un logiciel client-serveur (C-S) répandu pour fournir un service de noms. Il utilise un démon (*daemon*) : **named**, pour sa partie serveur.
- ★ Voir aussi Knot Resolver et Unbound.

❖ Commandes et outils

- ★ **dig** est une commande du package `dnsutils` sous Linux pour interroger des serveurs DNS.
 - ★ `dig fr.wiktionary.org`
 - ★ `dig any fr.wiktionary.org`
 - ★ `dig mx gmail.com`
- ★ **host** affiche plus simplement les redirections DNS.
 - ★ `host fr.wiktionary.org`
- ★ **nslookup** sera utilisable sous Windows au lieu de `dig`.
- ★ **whois** permet d'effectuer des recherches sur les bases de données de bureau d'enregistrement.
- ★ RDAP, *Registration Data Access Protocol* est une alternative à Whois ; voir rdap.org

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ DoH ; DNS over HTTPS

- ★ DNS via HTTPS, *DNS over HTTPS* (**DoH**) est un protocole pour la résolution DNS à distance via le protocole HTTPS.
- ★ Les requêtes DNS habituelles sont réalisées en clair (non chiffrés) vers le port 53 du serveur DNS par défaut, ce qui pose des problèmes de sécurité et de confidentialité.
- ★ **DoH** permet de sécuriser les requêtes en faisant passer le trafic DNS sur le protocole sécurisé HTTPS, vers un serveur tel que Cloudflare (<https://mozilla.cloudflare-dns.com/dns-query>) ou NextDNS (<https://trr.dns.nextdns.io/>).
- ★ Mozilla Firefox est le premier navigateur web à proposer ce protocole DoH
 - ★ Voir : <https://support.mozilla.org/fr/kb/dns-via-https-firefox>

❖ À voir :

- ★ [RFC 9499: DNS Terminology](#) - Stéphane Bortzmeyer
- ★ [Guide pratique du titulaire d'un nom de domaine en .fr](#) - AFNIC

2 - Applications client-serveur dans internet

2.1 - DNS - Domain Name System

❖ Exercices

Vos réponses avec le document [Exercices-RSX102-DNS.docx](#)

Interrogation de serveurs DNS :

- ★ a/ Quelle est l'adresse IP de [amio-millau.fr](#) ?
- ★ b/ Quel est l'enregistrement de type MX lié à [amio-millau.fr](#) ?

Enregistrement de nom de domaine :

- ★ c/ Comment procéder pour enregistrer un nom de domaine :
 - ★ en .fr ;
 - ★ en .com ?
- ★ d/ Combien coûte l'enregistrement de nom de domaine :
 - ★ en .fr ;
 - ★ en .com ;
 - ★ en .security ?
- ★ e/ Quel est le rôle de l'AFNIC ?
- ★ f/ Qui est le propriétaire du domaine [aliceandbob.io](#) ?
 - ★ Et comment avez-vous fait pour le savoir ?

DoH :

- ★ g et h/ Activez DNS-over-HTTPS (DoH) dans Firefox et dans Windows 11.
 - ★ Quels pages web vous a aidé.