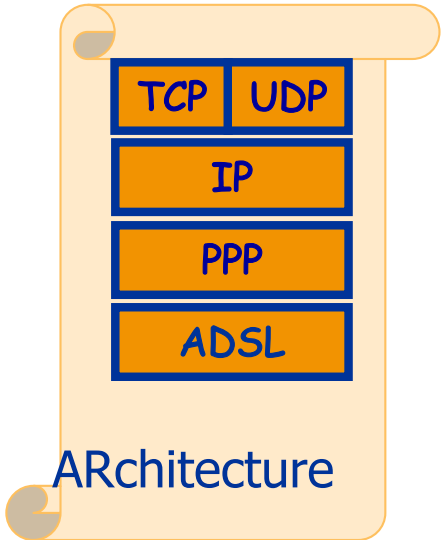
GRENOBLE INP UGA Ensimag

Chapitre AR3

Protocoles de recherche d'adresses
ARP, DHCP
DNS
whois



Avancement du chapitre AR3

- Protocoles de recherche d'adresses: ARP, DHCP

- DNS: l'annuaire de l'internet
  - Fonctionnement du protocole DNS

- Whois
  - Informations sur les utilisateurs des réseaux, les propriétaires de domaines…

Protocoles de recherche d'adresse

- DNS: IP <-> Symbolique
  - permet de trouver l'adresse IP connaissant le nom DNS ou vice-versa
- ARP: IP -> MAC
  - Trouver sur un réseau Ethernet l'adresse MAC connaissant l'adresse IP
- DHCP: MAC -> IP
  - Autoconfiguration, service de découverte
  - Une machine arrivant sur un réseau obtient une adresse IP + autres infos sur le réseau local
- Google: contenu -> URL
  - Peut-être vu comme un service de recherche d'adresse (pas un protocole)

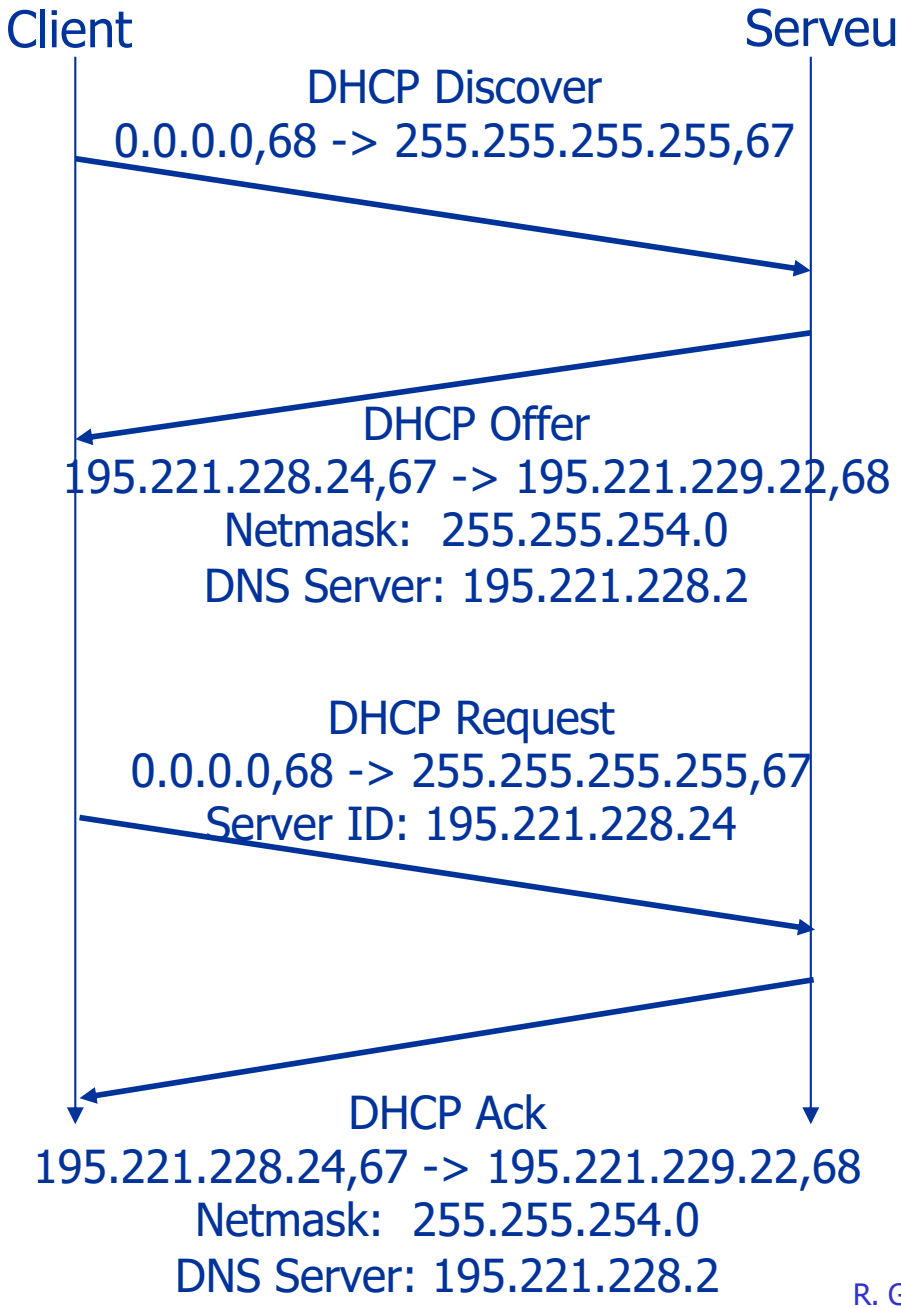
ARP: Address Resolution Protocol

- ARP: `IP->MAC`
  - A l'intérieur d'un sous-réseau, pour trouver l'adresse de liaison afin de communiquer avec la cible.
  - Pas de serveur: c' est la machine cible qui fournit son adresse MAC
  - L' émetteur utilise la diffusion (broadcast niv2) sur le bus Ethernet, seule la machine ayant la bonne IP lui répond en fournissant son adresse MAC
  - Ainsi, les messages suivants se feront en mode unicast
- Quand ?
  - Par le routeur quand un paquet arrive de l'extérieur
  - Par une machine qui n'a pas encore découvert tous ses voisins
    - En fait interrogations régulières
  - « Gratuitous » ARP request: à l'initiative d'une nouvelle machine, pour faire connaître son adresse IP

DHCP: configuration « automatique »

- Sans DHCP: il faut écrire « à la main » l'adresse IP, le masque, l'adresse du routeur et le serveur DNS
  - Dans les fichiers de configuration réseau, ou par les commandes `ifconfig, route`…
- DHCP (Dynamic Host Configuration Protocol): configuration automatique lorsque la machine arrive sur le sous-réseau
  - `myMAC (Ethernet) -> IP` (+ info DNS, sous réseau...)
  - Serveur DHCP, port 67 (client 68)
  - Client envoie IP src:0 dst:255.255.255.255 (broadcast)
  - Serveur fournit: No IP/masque, IP_routeur, IP_DNS
- 2 tables: statiques (IP fixe), dynamiques
  - Statique: adresse réservée à cette machine (ex ensigroz), autoconfigurée lorsqu'elle rejoint ce réseau
  - Dynamique (ex eduroam): alloue une adresse libre

DHCP: déroulement



- Chaque serveur atteint peut faire une offre.
- Le client indique quel serveur il a choisi dans sa Request (qui est diffusée donc tous les serveurs sont au courant)
- Outre addr IP, masque et DNS, le serveur fournit:
  - Adresse routeur
  - Durée du bail
  - Nom du sous-réseau (imag.fr)
  - ...

Quel protocole pour trouver les adresses de niveau 4 ?

Avancement du chapitre AR3

- Protocoles de recherche d'adresses: ARP, DHCP
- DNS: l'annuaire de l'internet
  - Fonctionnement du protocole DNS
- Whois
  - Informations sur les utilisateurs des réseaux, les propriétaires de domaines…

Noms internet: les problèmes

- Qui affecte les adresses IP ? Qui les gère ? Et les noms DNS associés ?
  - Unicité des adresses, unicité des noms
  - Géré par l'ICANN (Internet Corporation for Assigned Names and Numbers)
- Mise à jour permanente ($\sim 10^9$ nœuds)
- Accès « en ligne » à l'annuaire
  - Les utilisateurs ne connaissent que les noms
  - Le réseau n'utilise que les adresses IP
- Taille de l'annuaire -> trafic monstrueux

DNS: les solutions

- Organisationnelles (administratives)
  - Espaces hiérarchiques (arbres) appelés « zones » pour noms et adresses
  - Délégation d'autorité (ICANN -> AFNIC…)

- Techniques (informatiques)
  - Base de données répartie (serveurs de noms)
  - Base à plusieurs niveaux
    - serveurs primaires, secondaires, cache
    - sources autorisées / « non garanties »

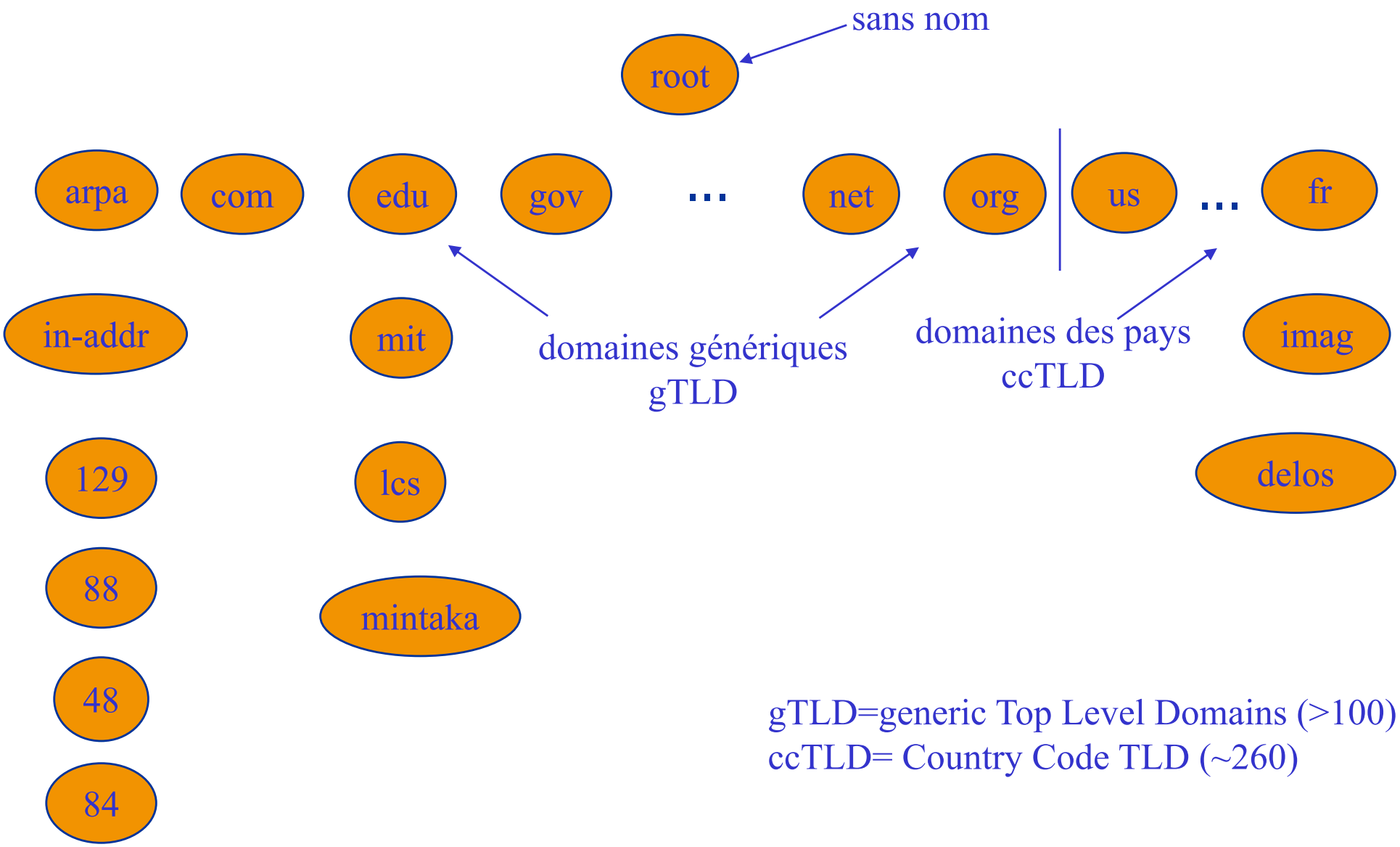
NB: DNS est dans la couche application (le réseau ne connaît que les numéros, comme en téléphonie)

Noms DNS

- Nœud
  - étiquette <= 63 caractères ASCII
    MAJ/min indifférent : IMAG.FR=imag.fr=ImAG.fR
  - Transcodage ASCII des noms internationaux (IDN)
    - xn-- préfixe, suivi du transcodage Punycode
    - www.bücher.de -> www.xn--bcher-kva.de
- Nom
  - liste d'étiquettes séparées par des points
    - `drakkar.imag.fr` *(fully qualified domain name: FQDN)*
    - `delos` *(évalué dans le domaine local)*

  NB: Sens inverse des fichiers Unix, et . pour /
- Autorité hiérarchique
  - crée des sous-domaines et délègue l'autorité

Structure hiérarchique des noms DNS



gTLD=generic Top Level Domains (>100)
ccTLD= Country Code TLD (~260)

Administration de noms

- Zones (ex: `mit.edu, lcs.mit.edu`)
  - sous-arbres gérés séparément (délégation)
  - au moins un serveur de nom par zone (port 53)
    - *primaire, secondaire (=copie du primaire)*
    - redondance
    - cache (=copie locale: les données restent ~ 1 jour)
- Serveurs racine
  - 13 serveurs logiques (répartis sur près de 300 machines)
  - chaque serveur primaire connaît leurs adresses
    - *(pourquoi pas leurs noms ?)*
- Configuration DNS d'un hôte
  - Chaque machine doit connaître sa zone (domain) et au moins un serveur: fichier `/etc/resolv.conf` sur Unix
  - Fichier mis à jour par la configuration réseau (ex: DHCP)

```
/etc/resolv.conf :nameserver 129.88.48.2
                  domain imag.fr
```

Exemples

- Serveur racine (Europe):
  `K.ROOT-SERVERS.NET`
  `Réseaux IP Européens,`
  `Network Coordination Centre (RIPE NCC)`
- Délégation pour `.fr`: AFNIC (`ns1.nic.fr`)
- Délégation pour `imag.fr`: IMAG
  - Serveur primaire: `imag.imag.fr`
  - Serveur secondaire: `isis.imag.fr`
- Chaque responsable de zone peut créer ou détruire des noms ou des sous-zones (et déléguer)

Base de données DNS

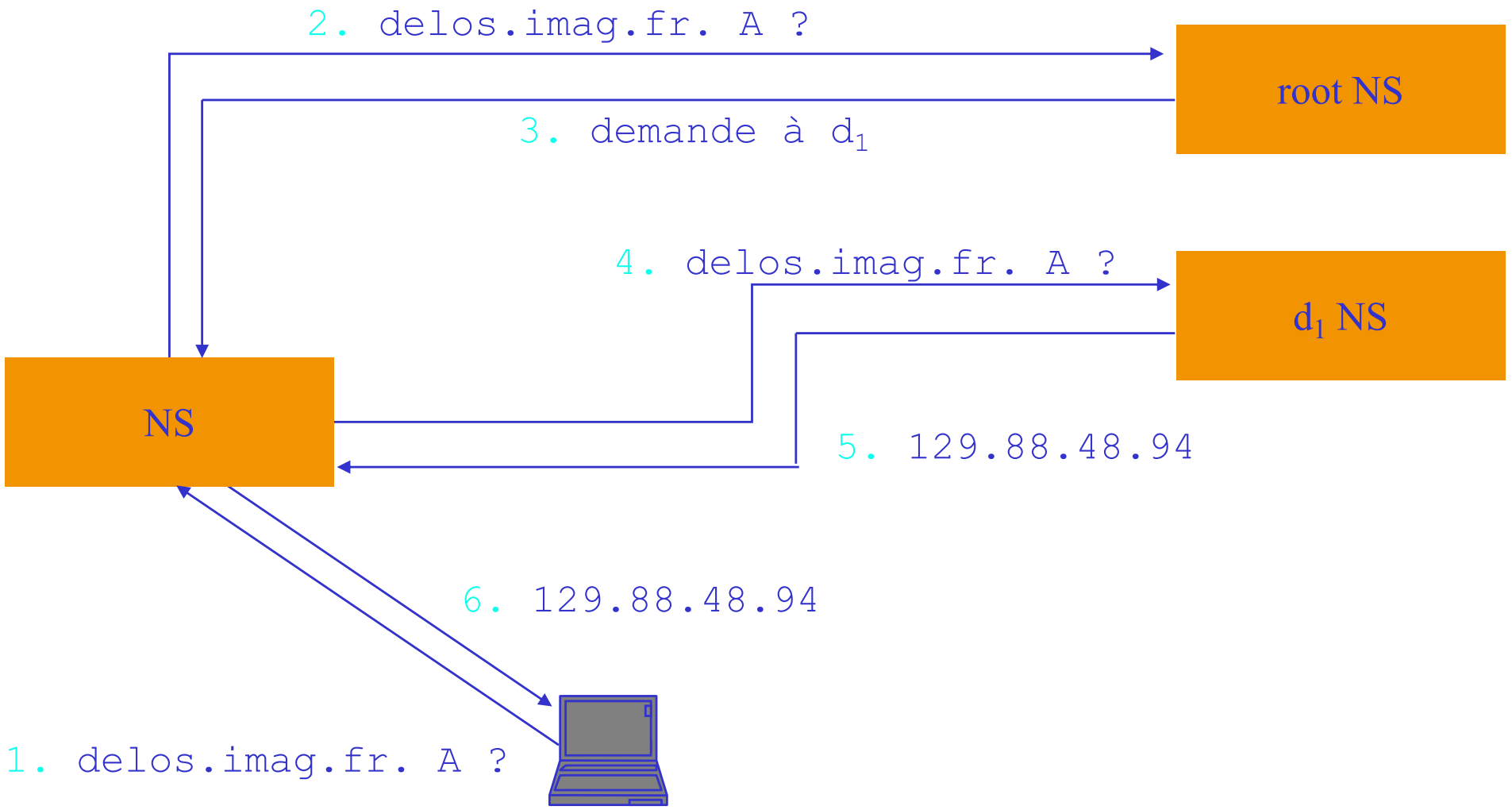
- Une immense BdD répartie sur le monde
  - La répartition suit la découpe en zones
  - Sur chaque zone: un fichier maître
  - Administrateur: met à jour fichier + relance NS (primaire, secondaire)
- Le fichier maître de zone contient:
  - Noms dans la zone (« authoritative » -> réponse « d'autorité », i.e. officielle)
  - Pointeurs vers les serveurs des sous-zones
  - SERIAL: compteur de MAJ (version)
  - Lu par le serveur NS au démarrage
- Les serveurs de noms (primaire/second.) ont une double fonction
  1. Gérer la BdD des noms de leur zone, répondre aux requêtes
  2. Répondre aux consultations du DNS des machines de leur zone (guichet vers le reste du DNS)
  - Au passage, *enregistrer en cache les réponses des autres serveurs*: réponse gardée 24h, évitera de re-solliciter autre serveur

Enregistrements DNS
(au sens des Bases de Données)

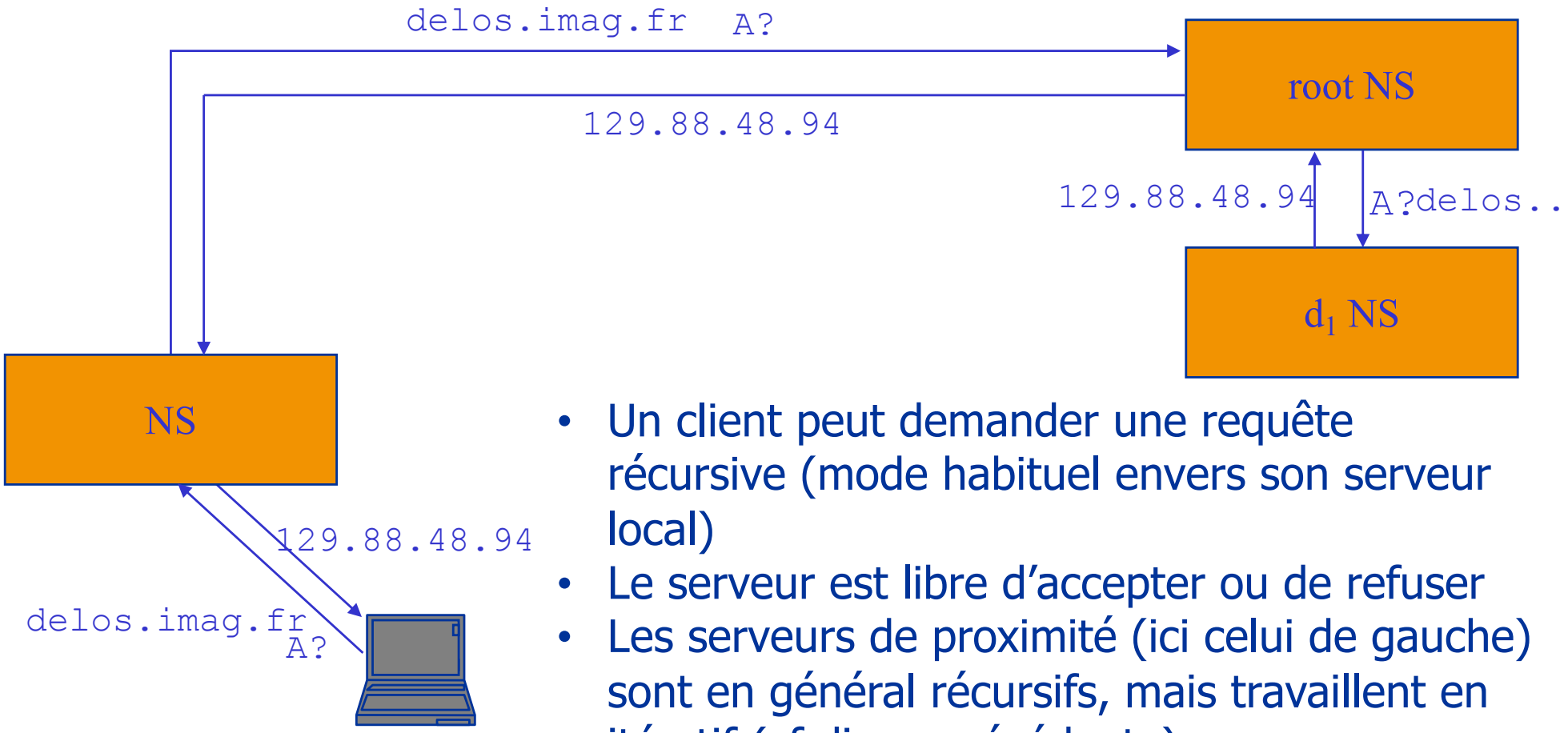
- RR *(Resource Record)* : plusieurs types coexistent
  - A : couple nom - adresse IP (v4: 4 mots de 8 bits)
  - AAAA: couple nom – adresse IPv6 (128 bits, 8 mots de 16 bits)
  - PTR : couple adresse IP - nom
  - CNAME : nom canonique pour un alias
  - NS : serveur de noms du domaine
  - HINFO : info sur l'hôte
  - MX : serveur du courrier pour le domaine
  - SOA: serveur ayant autorité pour le domaine
- PDU DNS:
  - requête
  - réponse

```
+---------------------+
|        Header       |
+---------------------+
|       Question      | the question for the name server
+---------------------+
|        Answer       | RRs answering the question
+---------------------+
|      Authority      | RRs pointing towards an authority
+---------------------+
|      Additional     | RRs holding additional information
+---------------------+
```

Requête itérative (par défaut entre serveurs) de type A (demande IP pour nom DNS)

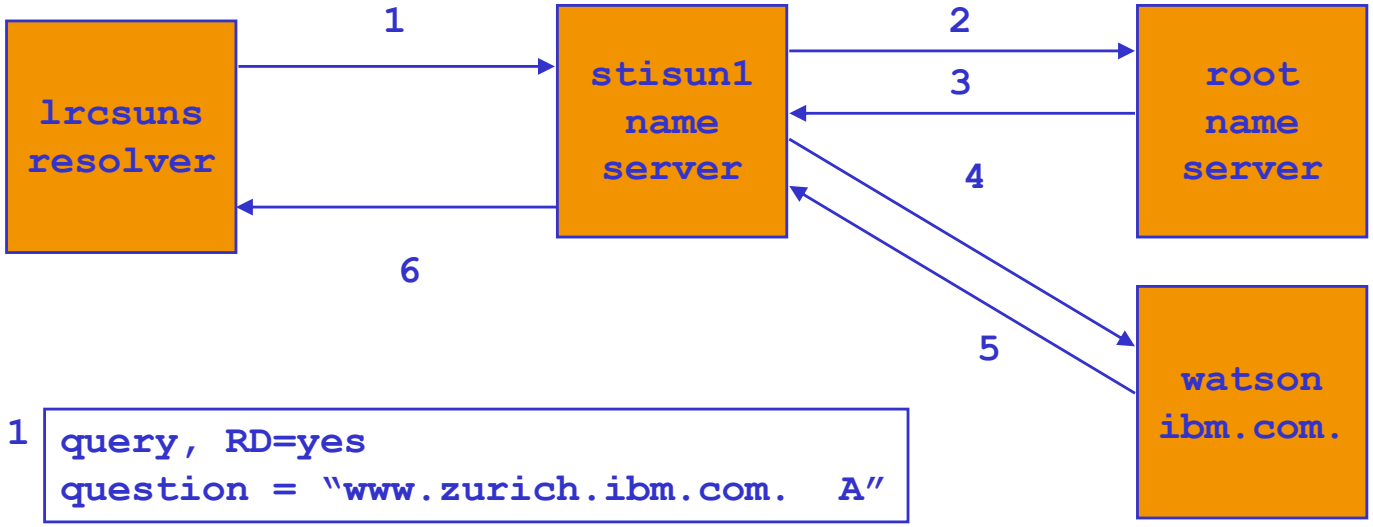


Requête récursive



- Un client peut demander une requête récursive (mode habituel envers son serveur local)
- Le serveur est libre d'accepter ou de refuser
- Les serveurs de proximité (ici celui de gauche) sont en général récursifs, mais travaillent en itératif (cf diapo précédente)
- Chaque serveur utilisera d'abord la réponse en cache si elle est présente

Exemple:



bit RD: recursive
Le serveur est libre de refuser

1
```
query, RD=yes
question = "www.zurich.ibm.com.   A"
```

2,4
```
query, RD=no
question = "www.zurich.ibm.com.   A"
```

3
```
answer
question = "www.zurich.ibm.com.       A"
answer = ""
authority= "ibm.com.    NS   watson.ibm.com.
                        NS   ns.austin.ibm.com.
                        NS   ns.almaden.ibm.com."
additional="watson.ibm.com.     A 192.35.232.34
            ns.austin.ibm.com.  A 129.34.139.4
            ns.almaden.ibm.com A 198.4.83.134"
```

5,6
```
answer
question = "www.zurich.ibm.com.     A"
answer = "www.zurich.ibm.com.     A  193.5.61.131"
```

Commandes pour consulter le DNS (cf TP)

dig, host, nslookup

```
dig www.grenoble-inp.fr
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6
;; QUESTION SECTION:
;www.grenoble-inp.fr.                IN      A

;; ANSWER SECTION:
www.grenoble-inp.fr.        86379   IN      CNAME   webksup4.grenet.fr.
webksup4.grenet.fr.         12473   IN      A       130.190.227.184

;; AUTHORITY SECTION:
grenet.fr.                  114919  IN      NS      ns-1.grenet.fr.
grenet.fr.                  114919  IN      NS      dns.univ-lyon1.fr.
grenet.fr.                  114919  IN      NS      ns-2.grenet.fr.

;; ADDITIONAL SECTION:
ns-2.grenet.fr.             114919  IN      A       130.190.225.99
ns-2.grenet.fr.             114919  IN      AAAA    2001:660:5303:225::99
dns.univ-lyon1.fr.          114919  IN      A       134.214.100.6
ns-1.grenet.fr.             12583   IN      A       130.190.226.99
ns-1.grenet.fr.             12583   IN      AAAA    2001:660:5303:226::99
```

DNS

- Fonctionnement mondial
- Est facilement « passé à l'échelle », grâce à une architecture bien conçue:
  - répartition et délégation d'autorité
  - cache
  - tolérance aux fautes (par réplication)
- Un point clé de l'Internet

Sécurité du DNS

- DNS conçu en 1983, sans sécurité. DNSSEC: 2000-2010
- Attaques MitM (interception) vers le client
  - Oscar observe la requête, et répond avant le serveur en fournissant une fausse adresse (site pirate)

  Failles: UDP, numéro requête non chiffré

- Attaques du serveur sans interception
  - Empoisonnement du cache: Oscar envoie en même temps des requêtes (comme client) pour `banque.com` et des réponses (comme pseudo-serveur) pour `banque.com` renvoyant sur IP pirate.

  Avec grand nombre de réponses, il peut tomber sur bon N° de port et de requête
- Fast-flux: création d'associations IP-FQDN à courte durée de vie pour masquer l'adresse réelle d'un pirate

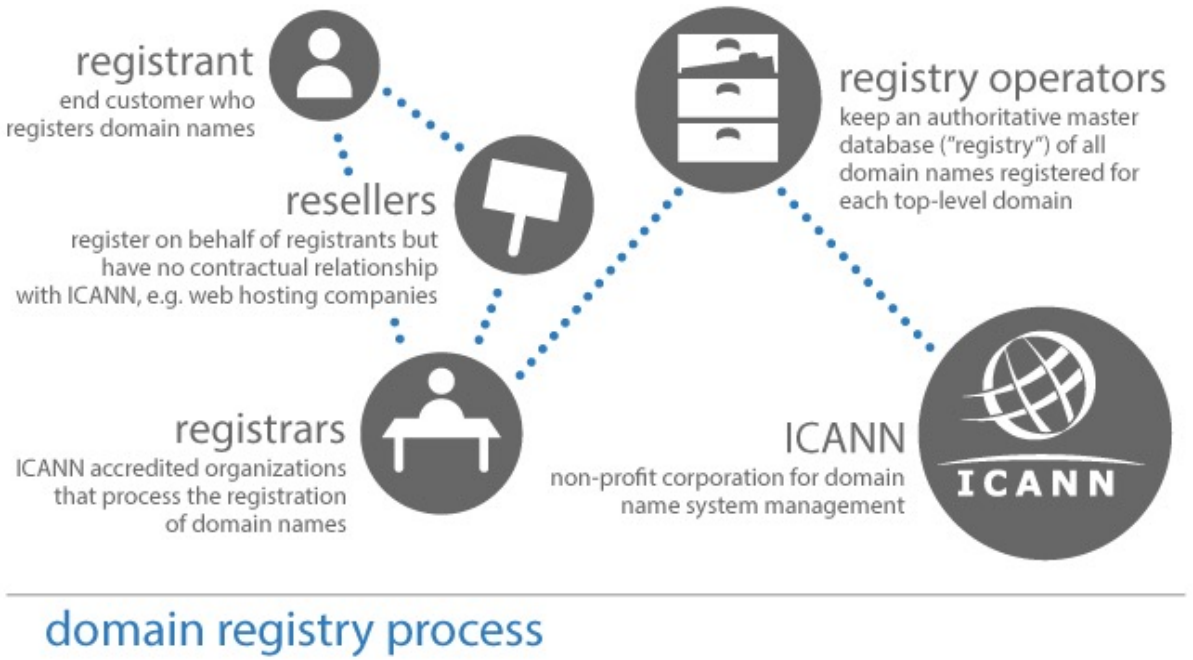
Avancement du chapitre AR3

- Protocoles de recherche d'adresses: ARP, DHCP
- DNS: l'annuaire de l'internet
  - Fonctionnement du protocole DNS
- Whois
  - Informations sur les utilisateurs des réseaux, les propriétaires de domaines…

whois

- Consultation d'une base de données (port 43)
  - Base de données administrative (juridique) du DNS
  - Permet de savoir quelle personne (physique ou morale) a enregistré quel domaine, auprès de quelle autorité
- Interrogation de serveurs d'enregistrements
  - `rs.internic.net`
  - `whois.ripe.net` http://www.ripe.net (Europe)
    `whois.arin.net` http://www.arin.net (Amérique du Nord)
    `whois.apnic.net` http://www.apnic.net (Asie Pacifique)
  - `whois.nic.fr` `http://www.nic.fr`

Enregistrement de noms de domaines



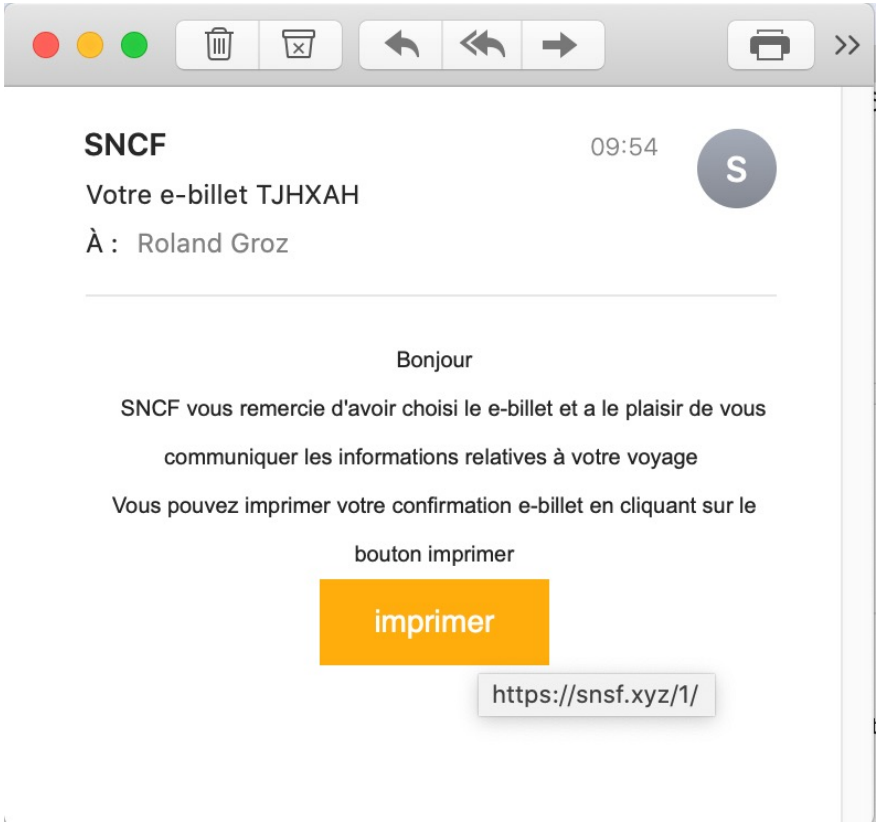
- ICANN: définit les règles et accrédite les organisations
- Gestionnaire TLD (*ex: AFNIC pour .fr*)
- Registrar (bureau d'enregistrement) (*ex. GoDaddy, NameCheap, OVHcloud*)
- Revendeur: intermédiaire de commercialisation
- Registrant: propriétaire du domaine

whois -h whois.nic.fr ensimag.fr (2020)

domain: **ensimag.fr**
holder-c: E2883-FRNIC
admin-c: JLR994-FRNIC
tech-c: PK4031-FRNIC
zone-c: NFC1-FRNIC
registrar: **GIP RENATER**
Expiry Date: 2021-06-26
created: 2000-06-26
nserver: ns0.ensimag.fr [195.221.228.93]
nserver: iroko.infra.grenoble-inp.fr
registrar: **GIP RENATER**
type: Isp Option 1
address: 23-25 Rue Daviel
address: 75013 PARIS
Phone: +33 1 53 94 20 30
Website:http://www.renater.fr

nic-hdl: E2883-FRNIC
type: ORGANIZATION
contact:INSTITUT POLYTECHNIQUE DE GRENOBLE
address:Informatique ENSIMAG
address:681, r. Passerelle
address:38400 St Martin Hères
e-mail: infra@ensimag.fr
registrar: GIP RENATER
changed: 2018-01-08 nic@nic.fr
nic-hdl: JLR994-FRNIC
type: PERSON
contact: Jean-Louis ROCH
e-mail: direction@ensimag.fr
nic-hdl: PK4031-FRNIC
type: PERSON
contact: Patrick KOCELNIAK
phone: +33 4 76 82 72 59

Exemple de mél frauduleux (hameçonnage)
mél reçu le 28/9/2020 à 9h54 (GMT+2)



- Domain Name: SNSF.XYZ
- Updated Date: 2020-09-28T03:54:49.0Z
- Creation Date: 2020-09-28T01:38:40.0Z
- Registry Expiry Date: 2021-09-28T23:59:59.0Z
- Registrar: Namecheap
- Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
- Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
- Registrant Organization: WhoisGuard, Inc.
- Registrant State/Province: Panama
- Registrant Country: PA
- Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Bilan AR3: notions essentielles

- Organisation du DNS (serveurs, niveaux)
- Types des requêtes DNS: A, NS, MX
- En TP: DHCP et configuration d'interface réseau

Références utiles

- Une mine de liens utiles sur les adresses (IP surtout), le DNS etc:

  www-public.it-sudparis.eu/~maigron/Internet

  Le tour du Net en questions: « Questions-réponses sur le réseau Internet », associé au cours de Patrick Maigron (Institut Télécom)

- Sites de l'ICANN www.icann.org, de l'IANA www.iana.org de l'AFNIC www.afnic.fr et du RIPE www.ripe.net
- Les RFC: 1035, ,1123, 1591 etc pour DNS… 826 et 2390 pour ARP; 2131 pour DHCP…