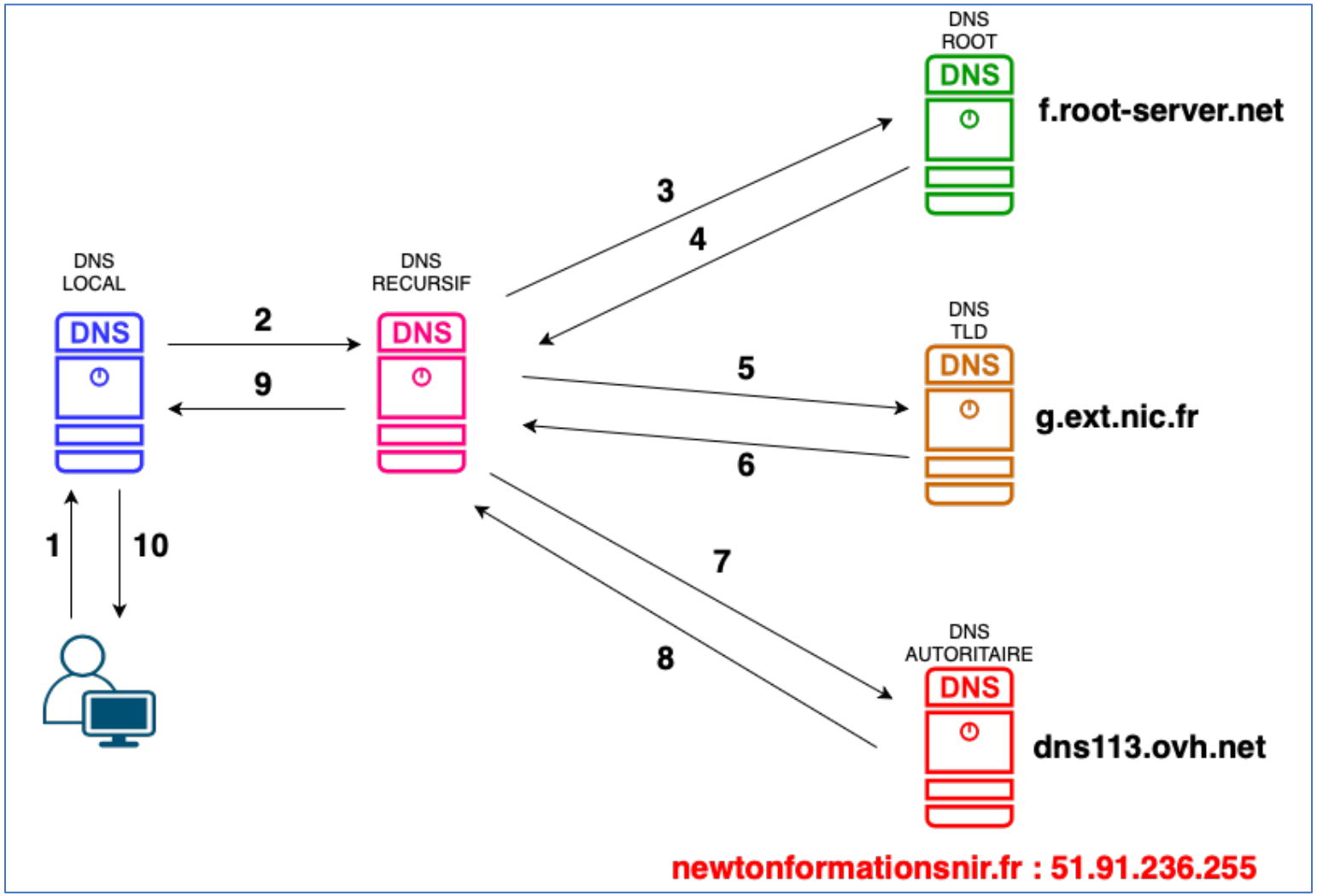
# DNS : Domain Name System



# SERVEUR RACINE (ROOT)

Il existe 13 groupes de serveurs racine DNS, souvent désignés par les lettres A à M. Chacun de ces groupes peut être composé de plusieurs serveurs physiques répartis dans le monde entier grâce à la technologie anycast. Anycast permet à plusieurs serveurs physiques situés à différents endroits de partager la même adresse IP, ce qui améliore la redondance, la disponibilité et la vitesse de réponse du système DNS.

Les serveurs racine sont une composante cruciale de l'infrastructure du DNS. Ils servent de point de départ pour la résolution des noms de domaine en adresses IP, orientant les requêtes vers les serveurs de noms appropriés pour les domaines de premier niveau (TLD) comme .com, .net, .org, .fr, etc.

Il est important de noter que, bien qu'il y ait techniquement 13 adresses IP différentes pour les serveurs racine DNS (une pour chaque groupe de A à M), il y a en réalité beaucoup plus de 13 serveurs racine physiques. La technologie anycast permet à de nombreux serveurs situés dans différents centres de données et régions géographiques de répondre aux requêtes destinées à ces 13 adresses, ce qui renforce la stabilité et la résilience du système DNS global.

# TLD (TOP LEVEL DOMAIN)

Les domaines de premier niveau (TLDs) sont classés en plusieurs groupes en fonction de leur nature et de leur utilisation. Voici les principaux types de TLDs :

**1.gTLDs (generic Top-Level Domains) :**

1. Ce sont les TLDs génériques et les plus connus, incluant des extensions comme .com, .org, .net, .info, .biz, et .name.
2. Les gTLDs peuvent être utilisés pour diverses fins et par des entités dans le monde entier.

**2.ccTLDs (country code Top-Level Domains) :**

1. Ce sont des TLDs spécifiques à un pays ou un territoire, comme .fr pour la France, .uk pour le Royaume-Uni, .de pour l'Allemagne, ou .jp pour le Japon.
2. Les ccTLDs sont généralement gérés par des organisations ou des agences situées dans le pays ou le territoire correspondant.

**3.sTLDs (sponsored Top-Level Domains) :**

1. Les sTLDs sont une sous-catégorie des gTLDs et sont sponsorisés par des organisations spécifiques. Ces TLDs représentent des communautés spécifiques d'intérêt.
2. Des exemples incluent .edu (établissements d'enseignement), .gov (gouvernement des États-Unis), .mil (militaire des États-Unis), et .aero (industrie aéronautique).

# TLD (TOP LEVEL DOMAIN)

**4. nTLDs (new Top-Level Domains) :**

1. Les nTLDs sont des TLDs plus récents, créés dans le cadre d'un programme d'expansion du DNS initié par l'ICANN.
2. Ces TLDs incluent une grande variété de noms génériques et thématiques, comme .app, .blog, .tech, et .music.

**5. IDN ccTLDs (Internationalized Domain Name country code TLDs) :**

1. Les IDN ccTLDs sont des TLDs de code de pays internationalisés, permettant l'utilisation de caractères non latins, comme les caractères arabes, chinois ou cyrilliques.
2. Par exemple, la Russie a .рф (pour "Fédération de Russie" en cyrillique), et la Chine a .中国 (pour "Chine" en chinois)

# SERVEUR DE DOMAINE AUTORITAIRE

Un serveur DNS autoritaire est un serveur qui détient les informations définitives sur un domaine spécifique. En d'autres termes, il est la source de référence pour les informations concernant un domaine donné dans le système de noms de domaine (DNS). Voici quelques points clés sur les serveurs DNS autoritaires :

**1.Source d'Information** : Lorsqu'une requête DNS est faite pour un domaine spécifique, c'est le serveur DNS autoritaire pour ce domaine qui fournit la réponse définitive. Par exemple, si une requête est faite pour obtenir l'adresse IP associée à www.example.com, c'est le serveur DNS autoritaire pour example.com qui répond.

**2.Enregistrements DNS** : Les serveurs DNS autoritaires gèrent les enregistrements DNS pour les domaines dont ils sont responsables. Ces enregistrements incluent, entre autres, les enregistrements de type A (pour les adresses IPv4), AAAA (pour les adresses IPv6), MX (pour les serveurs de messagerie), CNAME (pour les alias de domaine), TXT (pour divers textes et informations de configuration), etc.

**3.Mise à Jour des Données** : Les propriétaires de domaines (ou leurs administrateurs DNS) configurent et mettent à jour les enregistrements DNS sur leurs serveurs DNS autoritaires. Ces mises à jour sont ensuite propagées dans tout le système DNS grâce à la nature distribuée de ce dernier.

**4.Pas de Mise en Cache** : Contrairement aux serveurs DNS récursifs, les serveurs DNS autoritaires ne mettent pas en cache les réponses provenant d'autres serveurs. Ils fournissent uniquement des informations qu'ils gèrent directement.

# COMMANDE NSLOOKUP

nslookup est un outil en ligne de commande utilisé pour interroger les serveurs DNS et obtenir des informations sur les enregistrements DNS pour un nom de domaine ou une adresse IP. Il est disponible sur la plupart des systèmes d'exploitation, y compris Windows, Linux et macOS.
Voici quelques exemples d'utilisation de nslookup :

**Requête de Base**
Pour obtenir l'adresse IP d'un nom de domaine : **`nslookup newtonformationsnir.fr`**

**Réponse** :

```
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   newtonformationsnir.fr
Address: 51.91.236.255
```

**Cette commande retournera les enregistrements de type A (adresse IPv4) pour newtonformationsnir.fr**

# COMMANDE DIG

**dig** (Domain Information Groper) est un outil de ligne de commande pour interroger les serveurs DNS. Il est utilisé pour diagnostiquer et analyser les problèmes de DNS en récupérant les informations DNS telles que les adresses IP (enregistrements A et AAAA), les enregistrements de serveurs de messagerie (MX) et d'autres types d'enregistrements DNS. dig offre une sortie détaillée qui est utile pour comprendre le fonctionnement du DNS et pour déboguer les configurations DNS.

**Requête de Base**
Pour obtenir l'adresse IP d'un nom de domaine : **`dig newtonformationsnir.fr`**

```
; <<>> DiG 9.10.6 <<>> newtonformationsnir.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8060
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;newtonformationsnir.fr.                IN      A

;; ANSWER SECTION:
newtonformationsnir.fr. 3600    IN      A       51.91.236.255

;; Query time: 52 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Dec 11 18:02:35 CET 2023
;; MSG SIZE  rcvd: 67
```

flags: qr rd ra : Drapeaux DNS.

- qr (query response) indique qu'il s'agit d'une réponse.
- rd (recursion desired) indique que la récursivité était demandée.
- ra (recursion available) indique que la récursivité est disponible sur le serveur.

La commande **dig +trace** est utilisée pour effectuer un suivi détaillé du processus de résolution DNS d'un nom de domaine, en affichant chaque étape du chemin de la requête à travers la hiérarchie DNS. Elle commence par interroger les serveurs racine DNS, puis passe aux serveurs de noms de domaine de premier niveau (TLD), et finalement aux serveurs DNS autoritaires, montrant comment un nom de domaine est résolu en adresse IP.

```
(base) MacBook-Pro-380:~ samuelbouhenic$ dig +trace newtonformationsnir.fr

; <<>> DiG 9.10.6 <<>> +trace newtonformationsnir.fr
;; global options: +cmd
.                       63046   IN      NS      j.root-servers.net.
.                       63046   IN      NS      m.root-servers.net.
.                       63046   IN      NS      i.root-servers.net.
.                       63046   IN      NS      e.root-servers.net.
.                       63046   IN      NS      g.root-servers.net.
.                       63046   IN      NS      c.root-servers.net.
.                       63046   IN      NS      b.root-servers.net.
.                       63046   IN      NS      d.root-servers.net.
.                       63046   IN      NS      a.root-servers.net.
.                       63046   IN      NS      h.root-servers.net.
.                       63046   IN      NS      f.root-servers.net.
.                       63046   IN      NS      k.root-servers.net.
.                       63046   IN      NS      l.root-servers.net.
.                       63046   IN      RRSIG   NS 8 0 518400 20231223050000 20231210040000 46780 . Ey70ZEwlcFERvXOQxYIc3vEc3u1S02DDtWQzO1YyptdxJgwafbOLFrkI 25UgqIrUyijI3Cd2qBBmvnc1FNiidgLR/FTTpR5rwjUEUr
1zhAiepUF wNtGHLcQotfBOkW7jPvAK19ZOQAxNrCsnVXAtT4ftRjUdCVcbrCSRGMd 1ZUKdJ1V3V/vyA9L+vIlDayxYcmw+gP4hXP4SxhO/AbLwnsZhbOjr0ok rA5mOlB0qewq0MtJhjstaDAsu55HDl5Qa4l3AZYQ3VJxqhVtWFCgaCBg LU7LXrVMJLEwUsGd87ZzE6
f4jEqjU2jLyL3ElfSWt8yPkrtaHDAvs5a gUospA==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 57 ms

fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
fr.                     86400   IN      DS      29133 13 2 1303E8DA8FB60DB500D5BEA1EE5DC9A2BCC93DFE2FC43D346576658F ECCF5749
fr.                     86400   IN      RRSIG   DS 8 1 86400 20231223050000 20231210040000 46780 . kxTY/BIOUMdHoVzkl4c0UPkXJ8HdaKXvJMscnw2EQVSitFt9BI1G2oci m/L4ZMU5qr42qiqc51nCxfeeThN/Nbhjh8zQr9YRZo1hFBV
xJLBKfJ/ u0Zl9Y5vWig+KOtWiBR3Qo1WPqiBuye/qBEiP7XhQx7Xpq5qz6Csnl2K gdDqCNb/CDrmdSWBniVXA0GB8I3X0vt5+DBbe5IUaz+NACmtU1gLSmd4 RF59P/qrBcM7XUNNe5L556p9CfCfjfwA12ewzZYj7ZJY0optkOWUwiCu Ed5kovuqL1VRiG5VFg+YGtZ
zKW0f3R0n7hArRBYGJDSbnCvPArDC4fr fKMUtA==
;; Received 634 bytes from 192.5.5.241#53(f.root-servers.net) in 5 ms

newtonformationsnir.fr. 3600    IN      NS      ns113.ovh.net.
newtonformationsnir.fr. 3600    IN      NS      dns113.ovh.net.
SFBLG7NFATQ81CQJGT5Q91BQS3H9V6ND.fr. 600 IN NSEC3 1 1 0 - SFBN9RJNNUEVSB0GNER878N1GN41D23I  NS SOA TXT RRSIG DNSKEY NSEC3PARAM
SFBLG7NFATQ81CQJGT5Q91BQS3H9V6ND.fr. 600 IN RRSIG NSEC3 13 2 600 20240206000912 20231210120235 60747 fr. mjE/rSojW2+5kOaORFxDbbkzqhjG3akxE47D3pY95Py4y18I72GlmpqM QoC5cfsMRhiHSMDAosMJYzIZuAU4Ug==
6R5RC8JL3E02V0E7S55UJC5EK7QDQVSJ.fr. 600 IN NSEC3 1 1 0 - 6R5S40AKUHUH0OPEQE6VJ3P75DC2LQ4L  NS DS RRSIG
6R5RC8JL3E02V0E7S55UJC5EK7QDQVSJ.fr. 600 IN RRSIG NSEC3 13 2 600 20240118081449 20231119073228 60747 fr. lnN/NfO8SPv3nhUV0gPFC9bBON53h7iz00PJ6BaXVckLi2LudOpjxNOq yHiMX4p06NItWjsKSXV4CX1pojbkiA==
;; Received 454 bytes from 2001:678:4c::1#53(g.ext.nic.fr) in 2 ms

newtonformationsnir.fr. 3600    IN      A       51.91.236.255
;; Received 67 bytes from 2001:41d0:1:4a9e::1#53(dns113.ovh.net) in 6 ms
```

Signatures à chaque niveau dns pour intégrité et authentification des données transmises

**8.8.8.8 est le serveur DNS récursif**

**Serveur root : f.root-servers.net**

**Serveur TLD : g.ext.nic.fr**

**IP de newtonformationsnir.fr : 51.91.236.255**

**Serveur autoritaire : dns113.ovh.net**

# LE PROTOCOLE

| | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 583 | 6… | 192.168.1.39 | 8.8.8.8 | DNS | Standard query 0xdee5 A newtonformationsnir.fr |
| 586 | 6… | 8.8.8.8 | 192.168.1.39 | DNS | Standard query response 0xdee5 A newtonformationsnir.fr A 51.91.236.255 |

Le protocole est très simple. C’est une question et une réponse. Dans l’exemple suivant, c’est une requête de type A sur le nom de domaine newtonformationsnir.fr, suivi de sa réponse.

Le protocole utilise UDP comme protocole de transport. Les serveurs DNS sont accessibles sur le port 53.