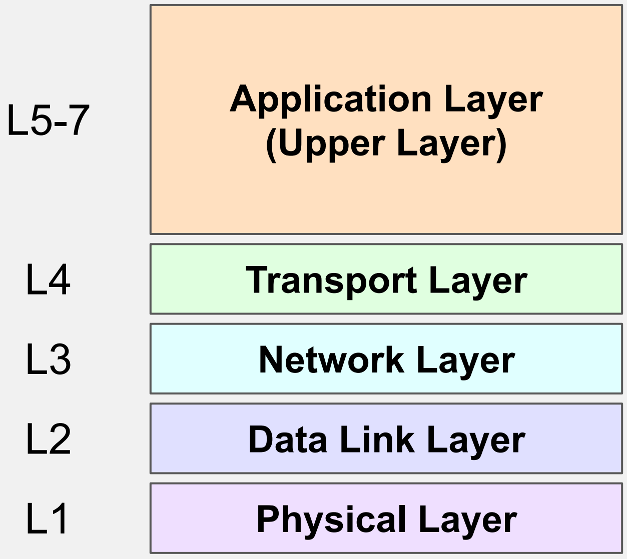
Network Security

Cache me if you Can: DNS resolution

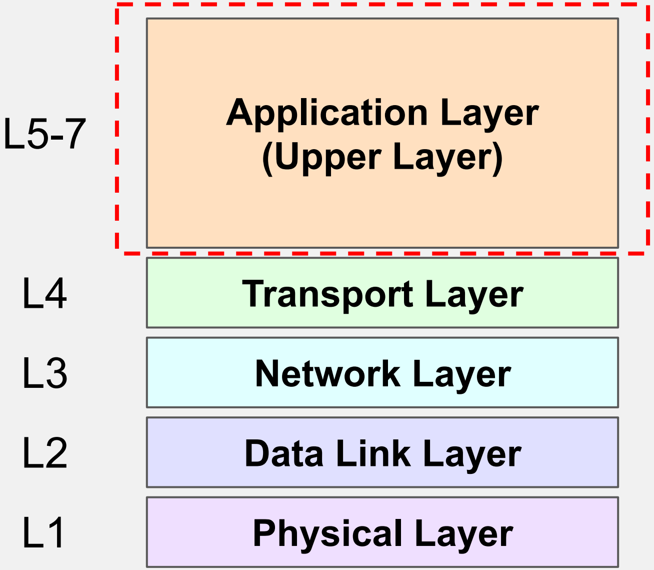
Gwendal Patat
Univ Rennes, CNRS, IRISA
2025/2026

Recall TCP/IP Model



TCP/IP Model

Today's Topic: Application Layer



L5-7 Application Layer (Upper Layer)

L4 Transport Layer

L3 Network Layer

L2 Data Link Layer

L1 Physical Layer

TCP/IP Model

How can we find each other?

- Pretty easy for the network:
  - Just use IP addresses.
- For humain:
  - Who want to remember IP addresses by heart?
  - Names are easier and don't change that often.

The solution: **DNS**.

Domain Name System (DNS)

Domain Name System (DNS)

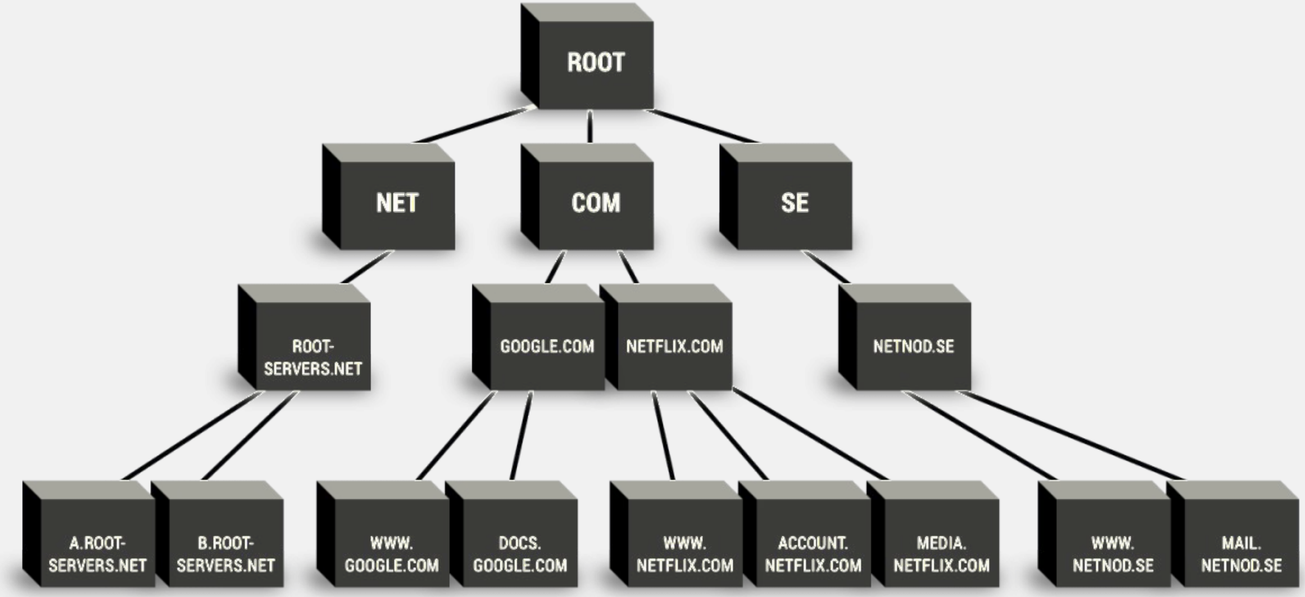
- Application Layer.
- First proposed in 1982 with the RFC819.
- Here to convert Names to IP addresses (Ipv4 and IPv6).
  - Can also be used to convert IP to names.
- A pillar stone of a working Internet.
  - If DNS is down, most people will believe the internet is down.

DNS Domain Hierarchy 1/4

etudiant.univ-rennes.fr

DNS Domain Hierarchy 2/4

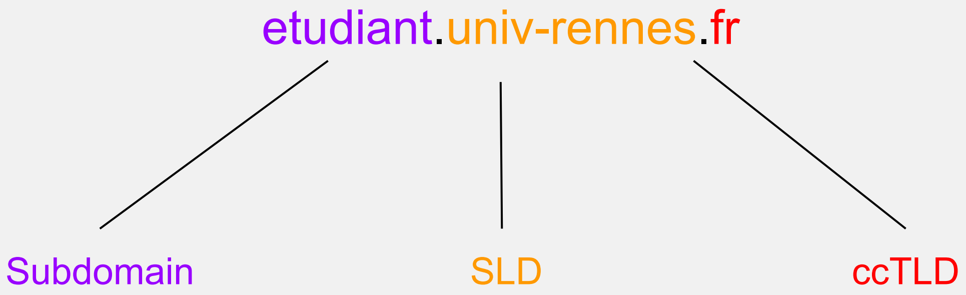
etudiant.univ-rennes.fr



DNS Domain Hierarchy 3/4

- **Root**: .
- **Top-level Domain (TLD)**
  - ***Generic TLD (gTLD)***: com, net, gov…
  - ***Country code TLD (ccTLD)***: us, fr, uk, cn, in…
  - ***Sponsored TLD (sTLD):*** .sncf, .total, .paris, .bzh…
  - ***Technical TLD:*** .arpa, .local, .onion…
- **Second-level Domain (SLD)**: google, amazon, univ-rennes…
- **Subdomains:** www., ent., etc…

DNS Domain Hierarchy 4/4



etudiant.univ-rennes.fr

Subdomain

SLD

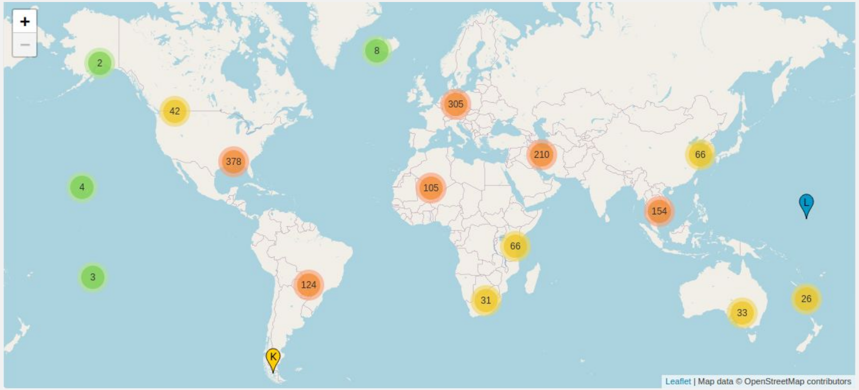
ccTLD

DNS Subdomains & Zones

- Subdomains allow servers to dispatch ressources.
  - For example, different instances based on:
    - **Geo localisation**: uk.example.com, fr.example.com…
    - **Services**: ent.univ-rennes.fr, planning.univ-rennes1.fr…
    - **Personal pages**: avalonswanderer.github.io…
    - Etc…
- Subdomains are not to be confused with DNS Zones:
  - **Domain:** name in the hierarchy.
  - **Zone:** contains the records for the managed domains (can be seen as an area).

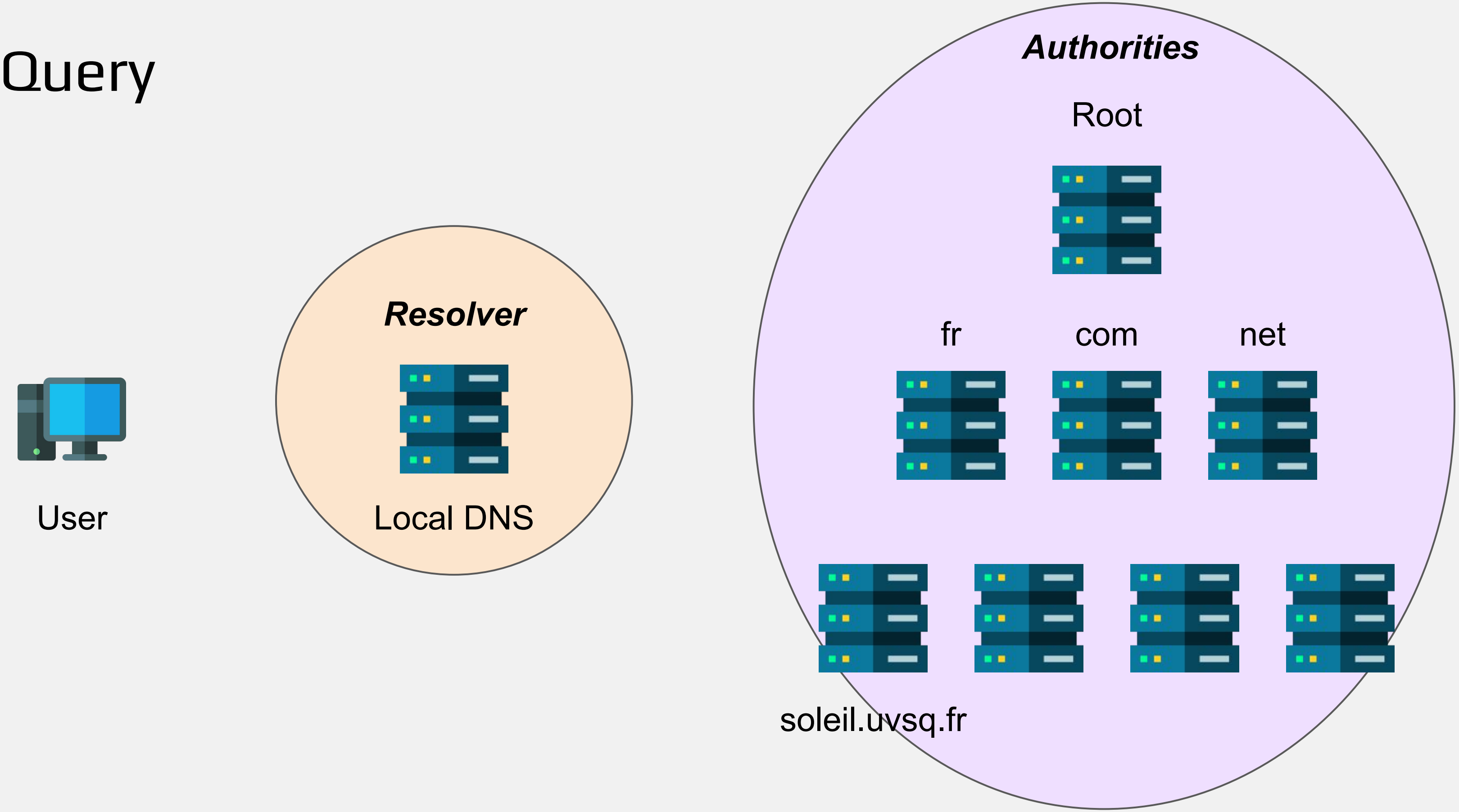
Root Servers

- Root DNS "." is managed by the Internet Corporation for Assigned Names and Numbers (ICANN), and is operated by 13 Root servers.
    - 13 names, 13 IPs (+ 13 IPv6) in the worlds: but hundreds of servers in the world!
- This redundancy allows scalability, reliability, and efficiency.

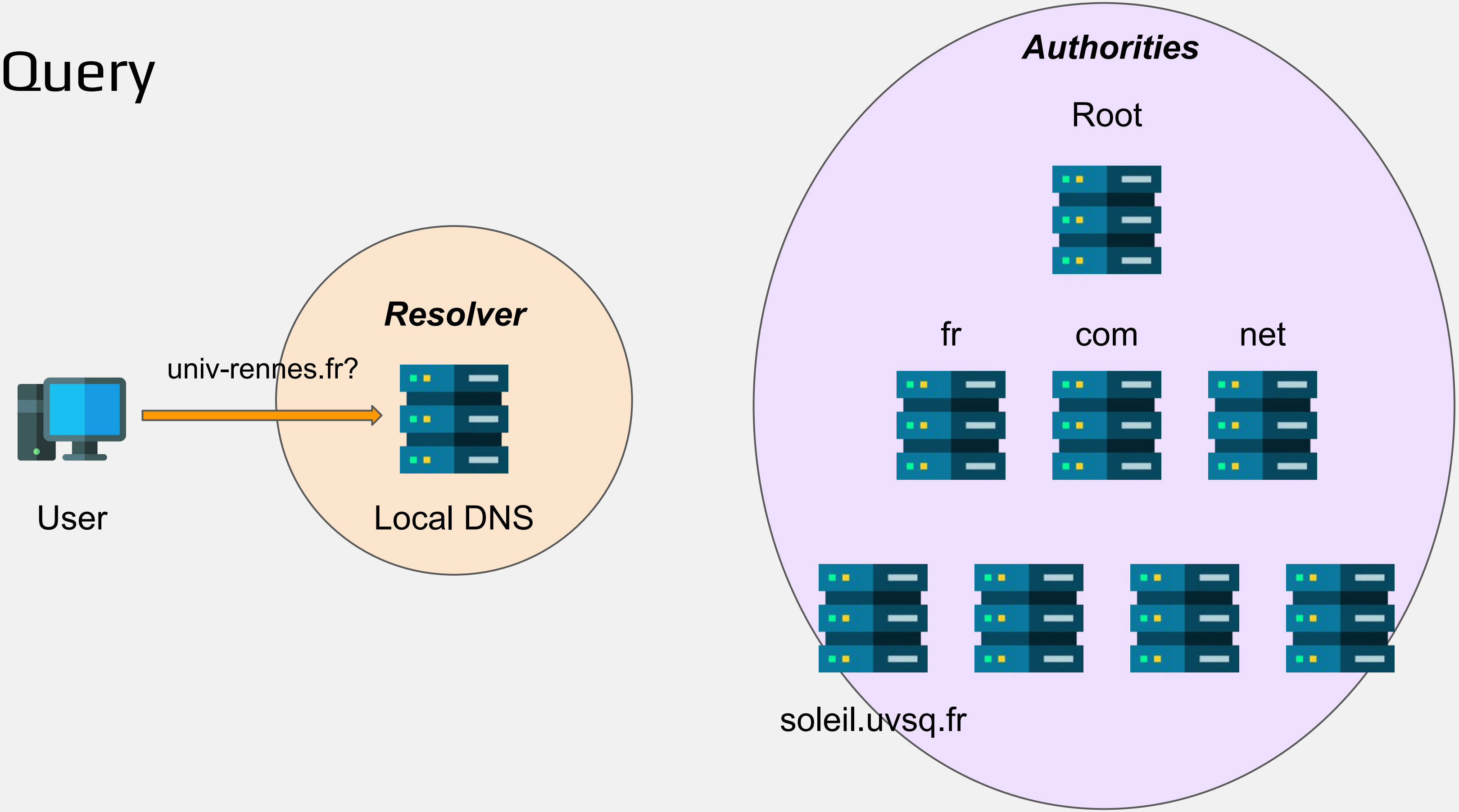


https://root-servers.org/

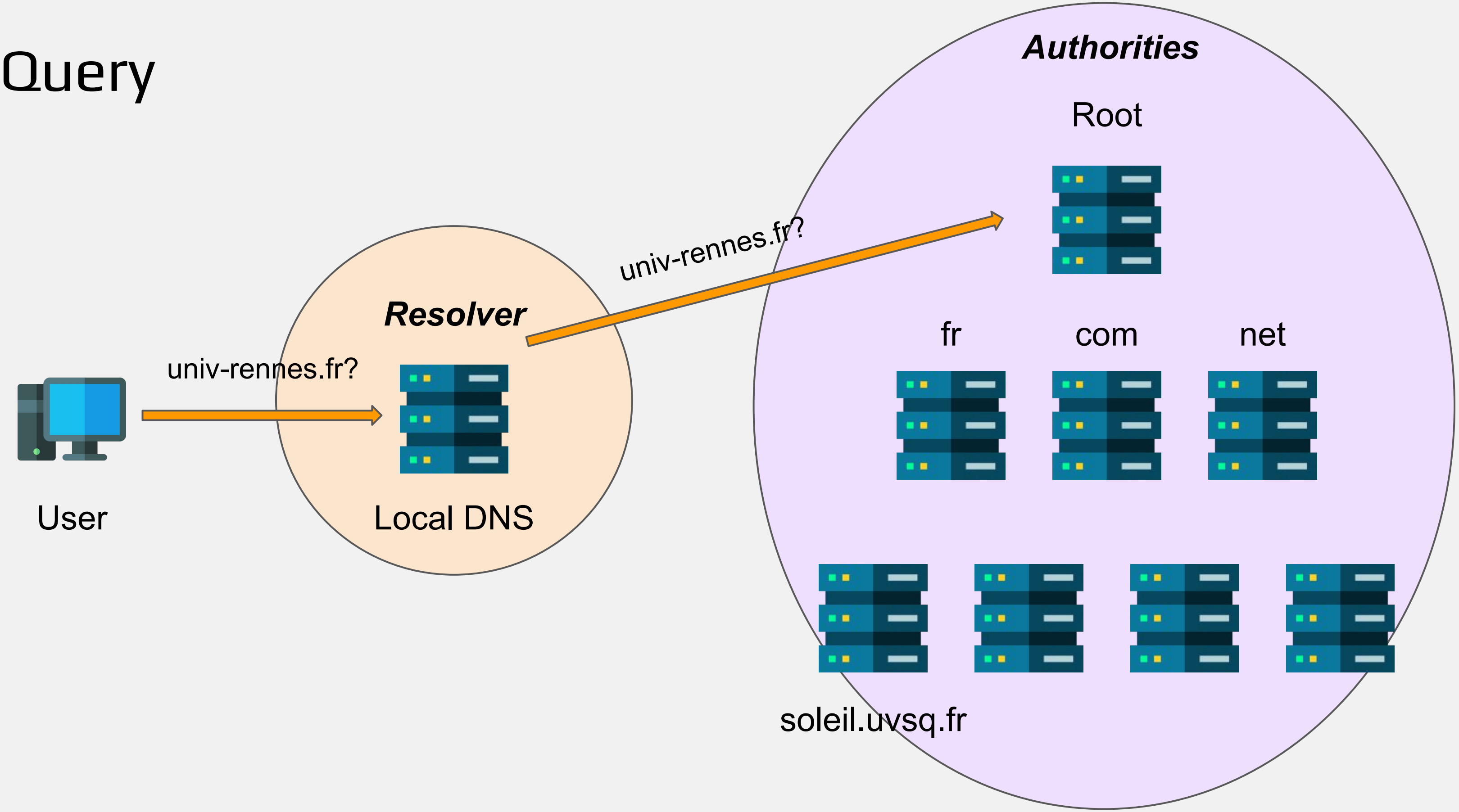
DNS Query


Authorities
Root
fr
com
net
soleil.uvsq.fr
Resolver
Local DNS
User

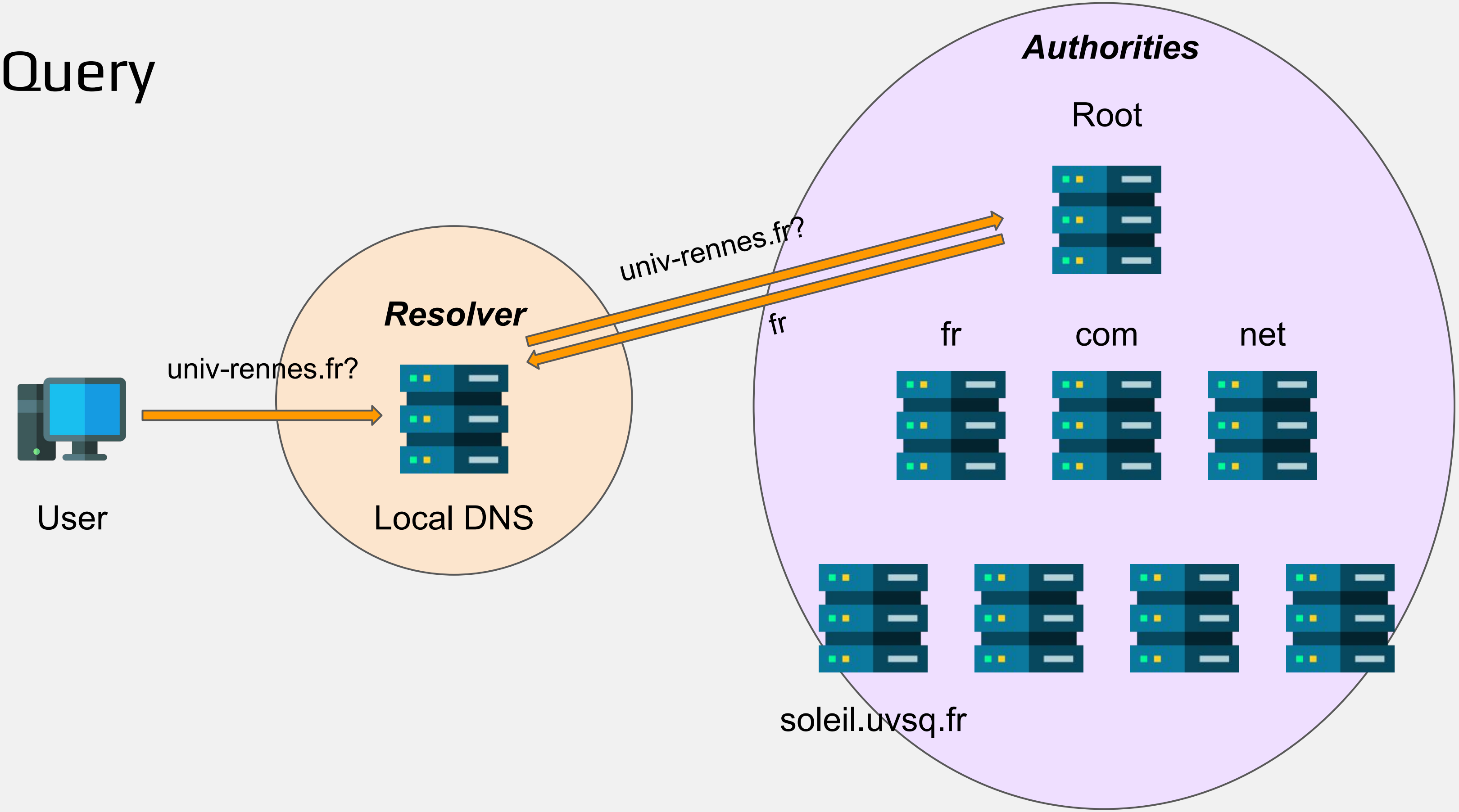
DNS Query


Authorities
Root
fr
com
net
soleil.uvsq.fr
Resolver
univ-rennes.fr?
User
Local DNS

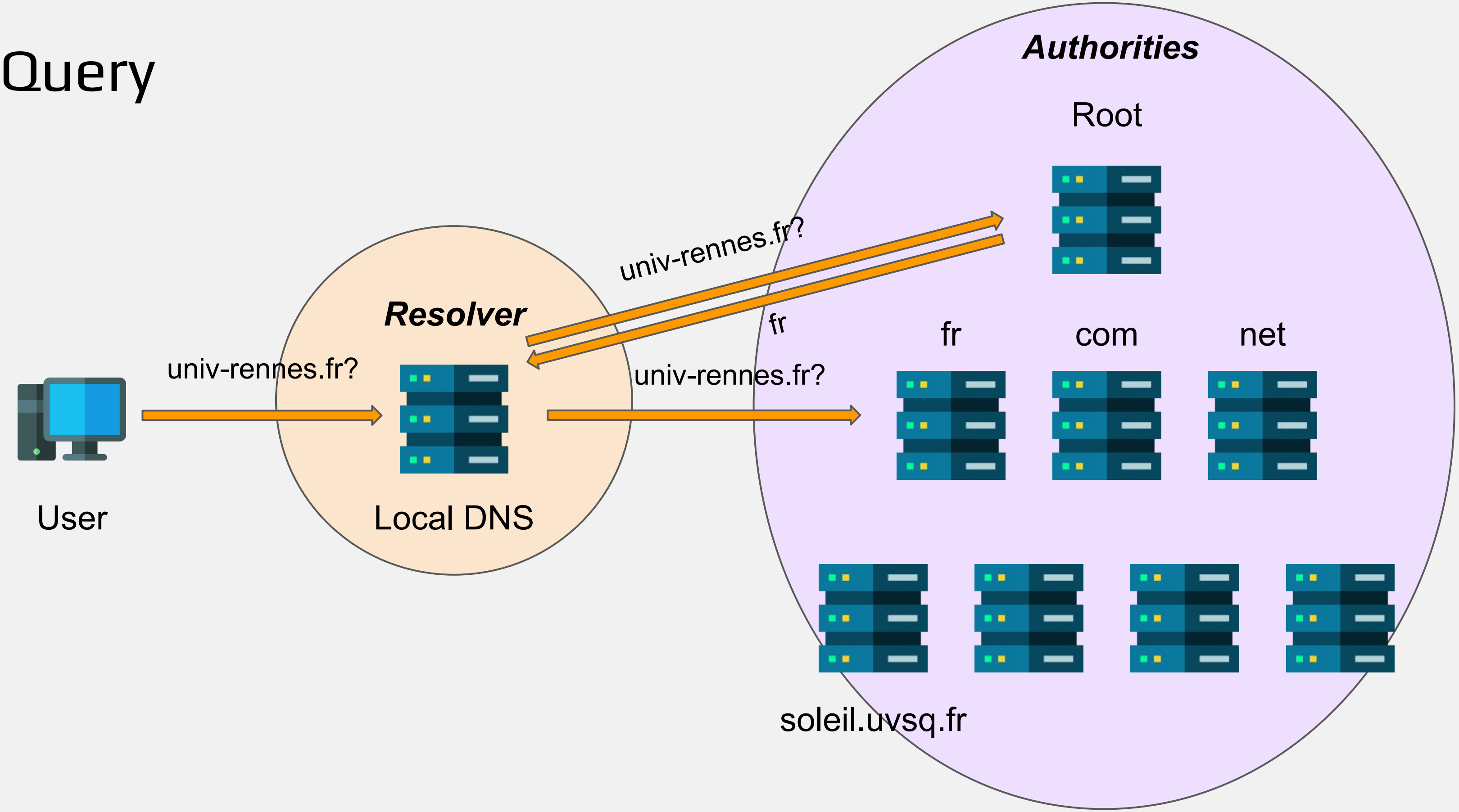
DNS Query


Authorities
Root
univ-rennes.fr?
Resolver
fr
com
net
univ-rennes.fr?
User
Local DNS
soleil.uvsq.fr

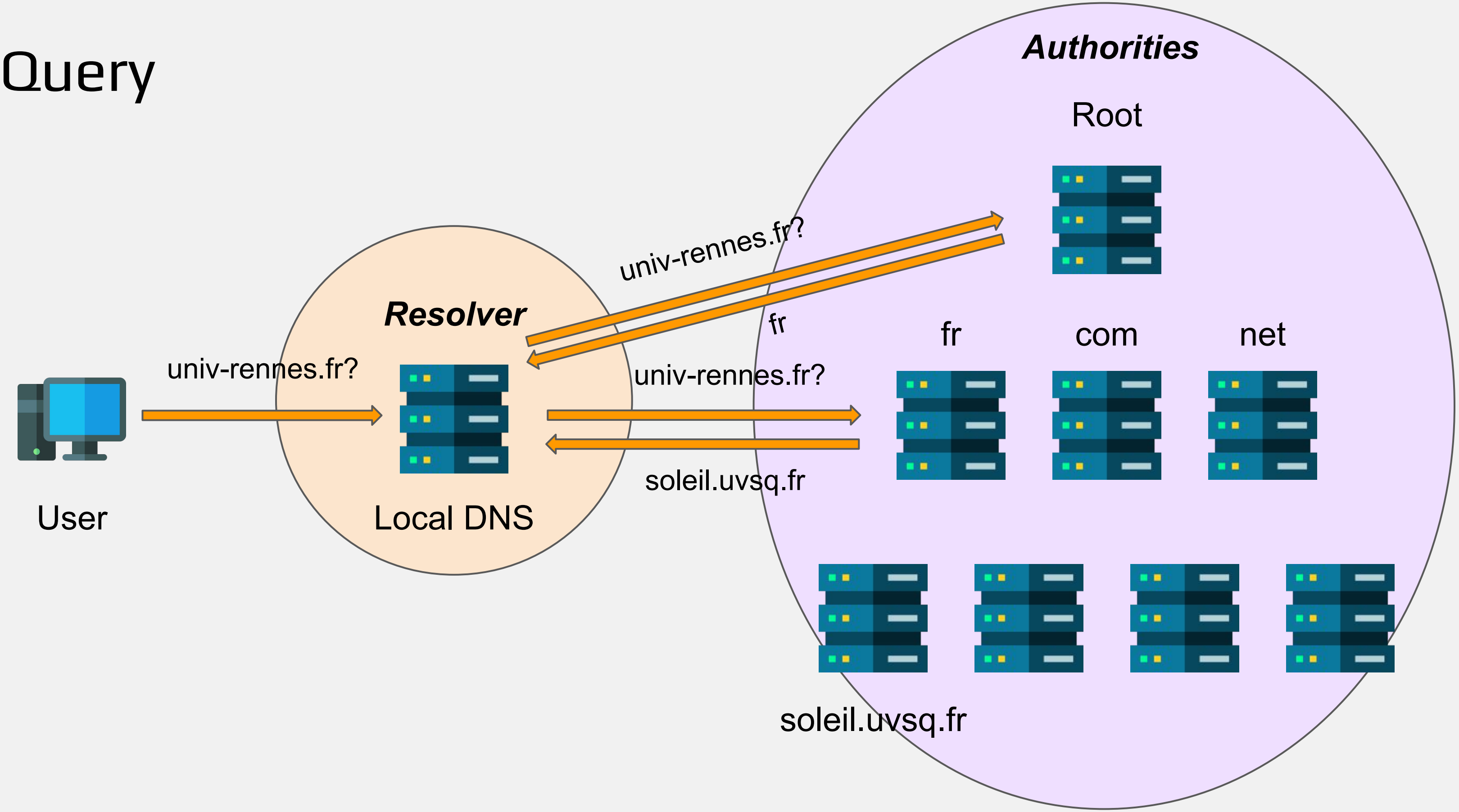
DNS Query


Authorities
Root
univ-rennes.fr?
fr
Resolver
fr
com
net
univ-rennes.fr?
User
Local DNS
soleil.uvsq.fr

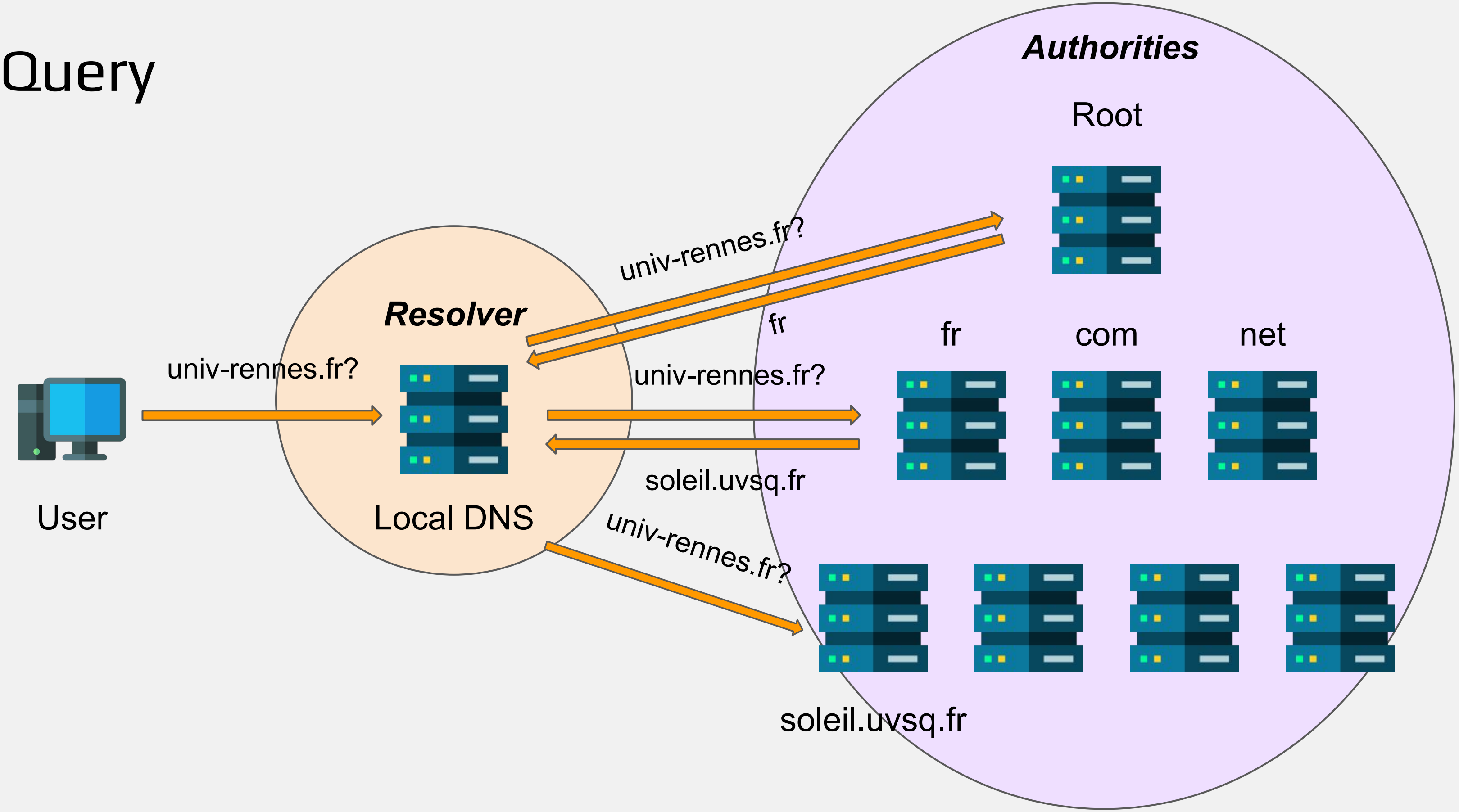
DNS Query


Authorities
Root
univ-rennes.fr?
fr
Resolver
fr
com
net
univ-rennes.fr?
univ-rennes.fr?
User
Local DNS
soleil.uvsq.fr

DNS Query

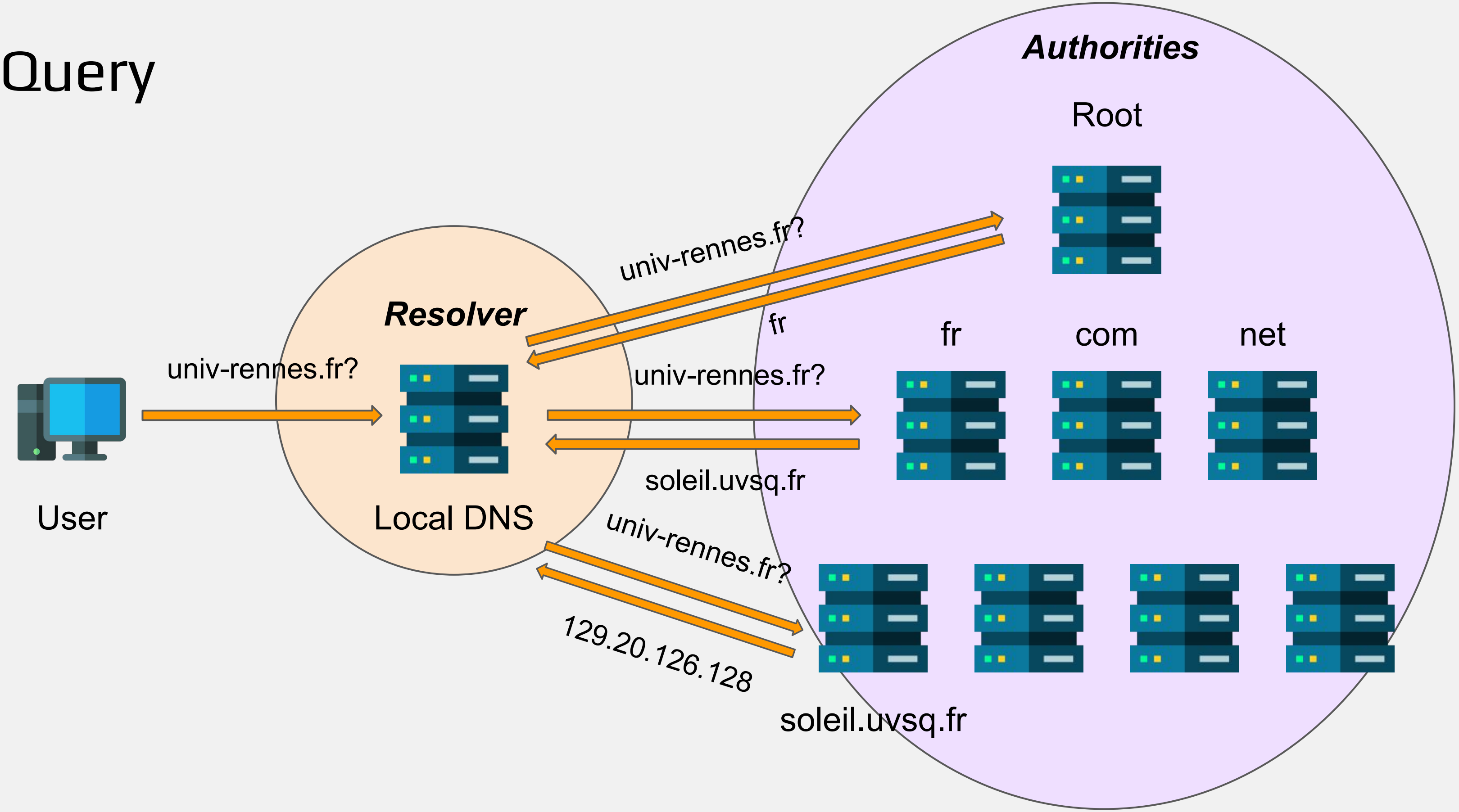

Authorities
Root
univ-rennes.fr?
fr
Resolver
univ-rennes.fr?
fr
com
net
univ-rennes.fr?
User
Local DNS
soleil.uvsq.fr
soleil.uvsq.fr

DNS Query

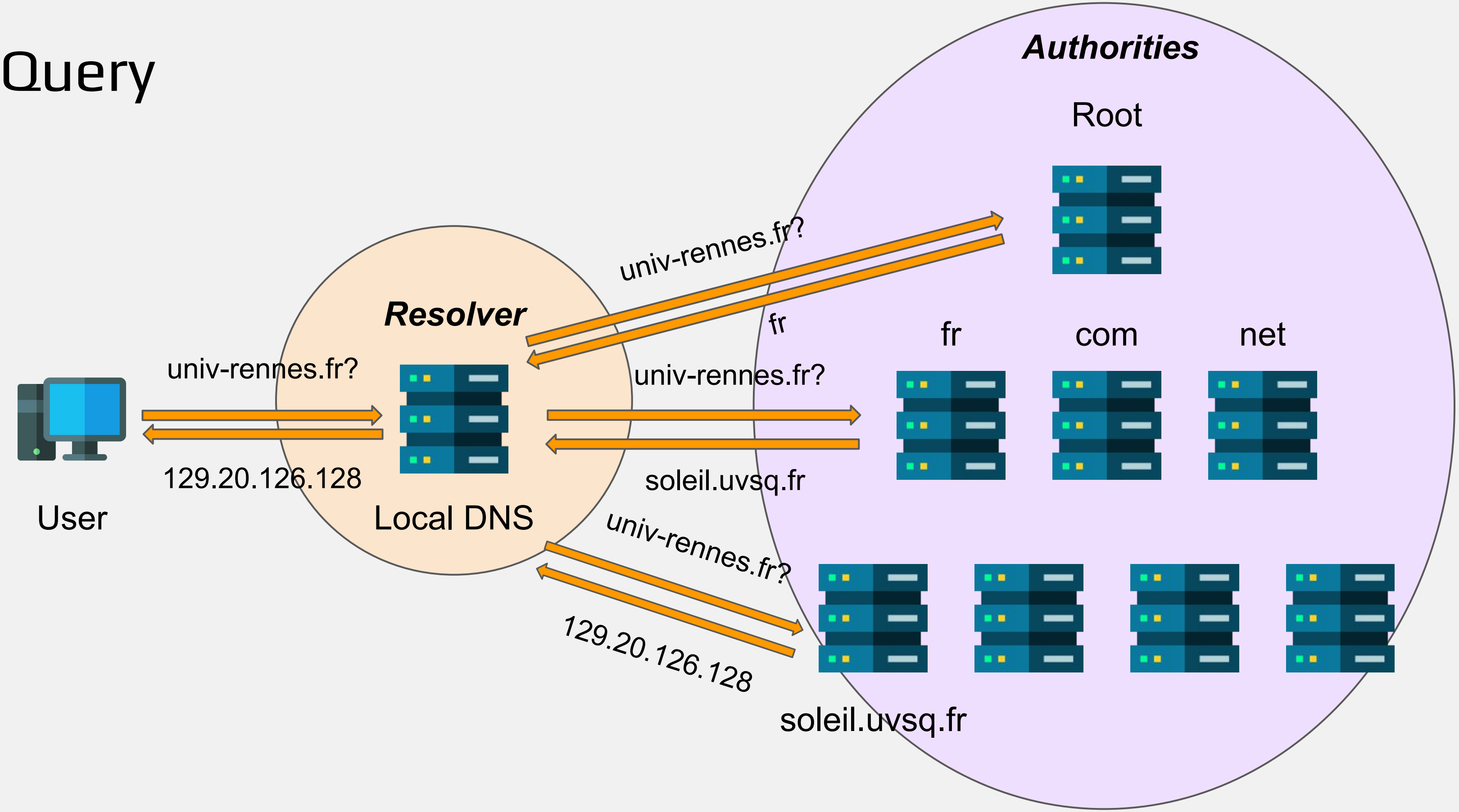


Authorities
Root
Resolver
univ-rennes.fr?
fr
univ-rennes.fr?
fr
com
net
univ-rennes.fr?
soleil.uvsq.fr
User
Local DNS
univ-rennes.fr?
soleil.uvsq.fr

DNS Query


Authorities
Root
univ-rennes.fr?
fr
Resolver
fr
com
net
univ-rennes.fr?
univ-rennes.fr?
User
Local DNS
soleil.uvsq.fr
univ-rennes.fr?
129.20.126.128
soleil.uvsq.fr

DNS Query

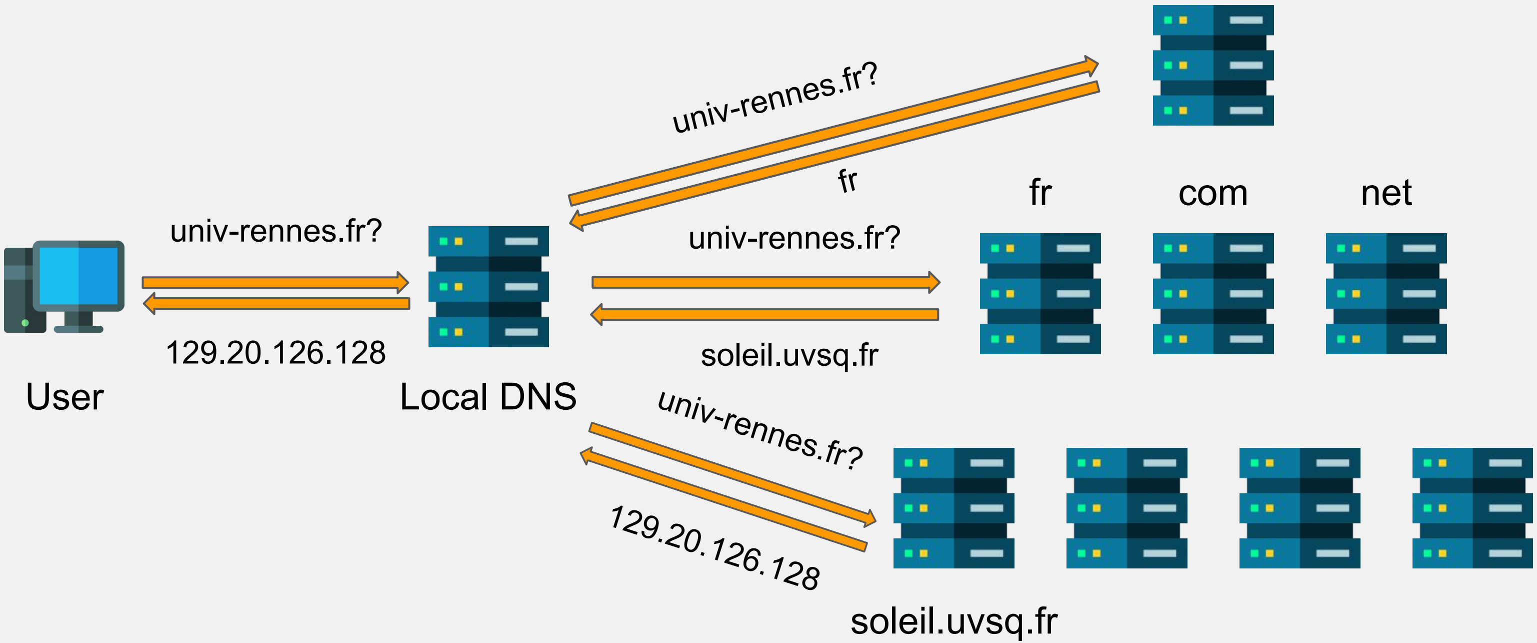

Authorities
Root
fr
com
net
Resolver
univ-rennes.fr?
fr
univ-rennes.fr?
univ-rennes.fr?
User
129.20.126.128
Local DNS
soleil.uvsq.fr
univ-rennes.fr?
129.20.126.128
soleil.uvsq.fr

DNS Recursive vs Iterative Queries

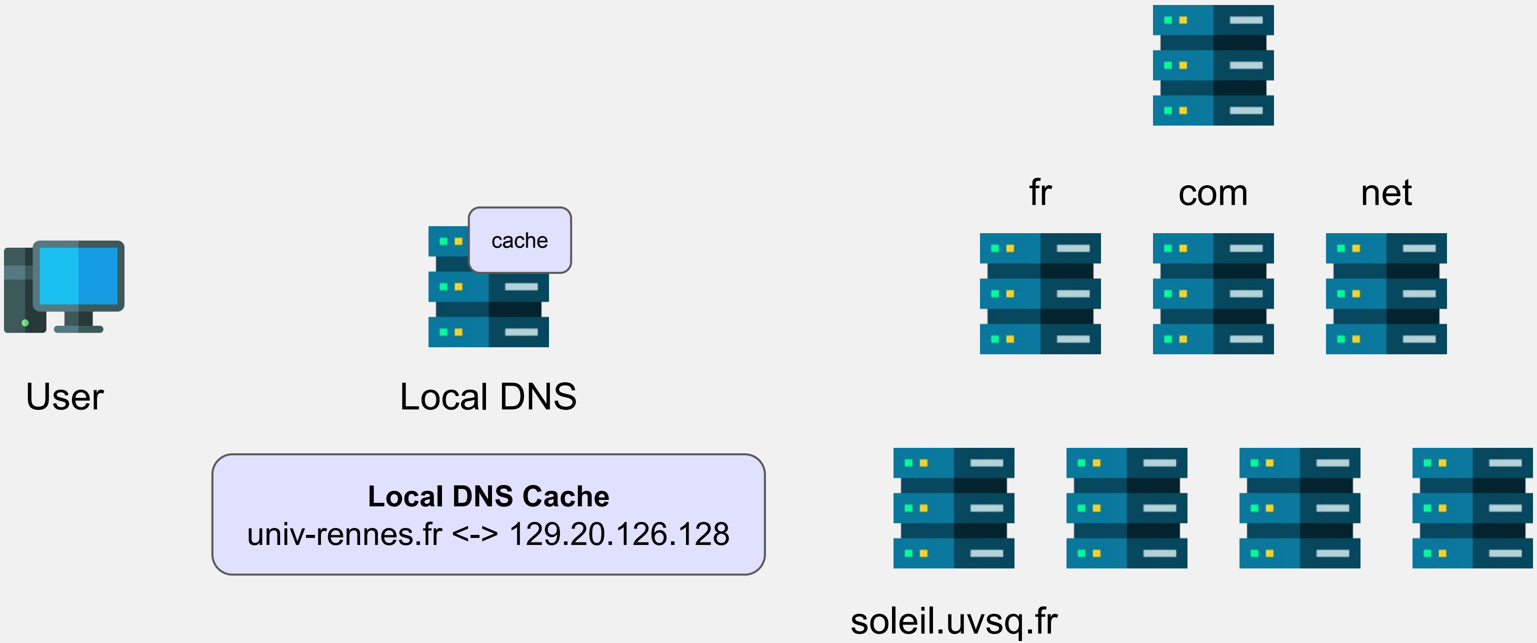
In our previous example, we can distinguish two types of queries:

- **Recursives**:
  - In recursive queries, the resolver takes full responsibility for the answers resolution.
  - The resolver will perform iterative queries to solve the name - IP association.
- **Iteratives**:
  - Here the server will answer with the next referral for our request or the final answer.
  - A referral does not include the answer but the next **Authority Name Server** to contact.

DNS Cache 1/2

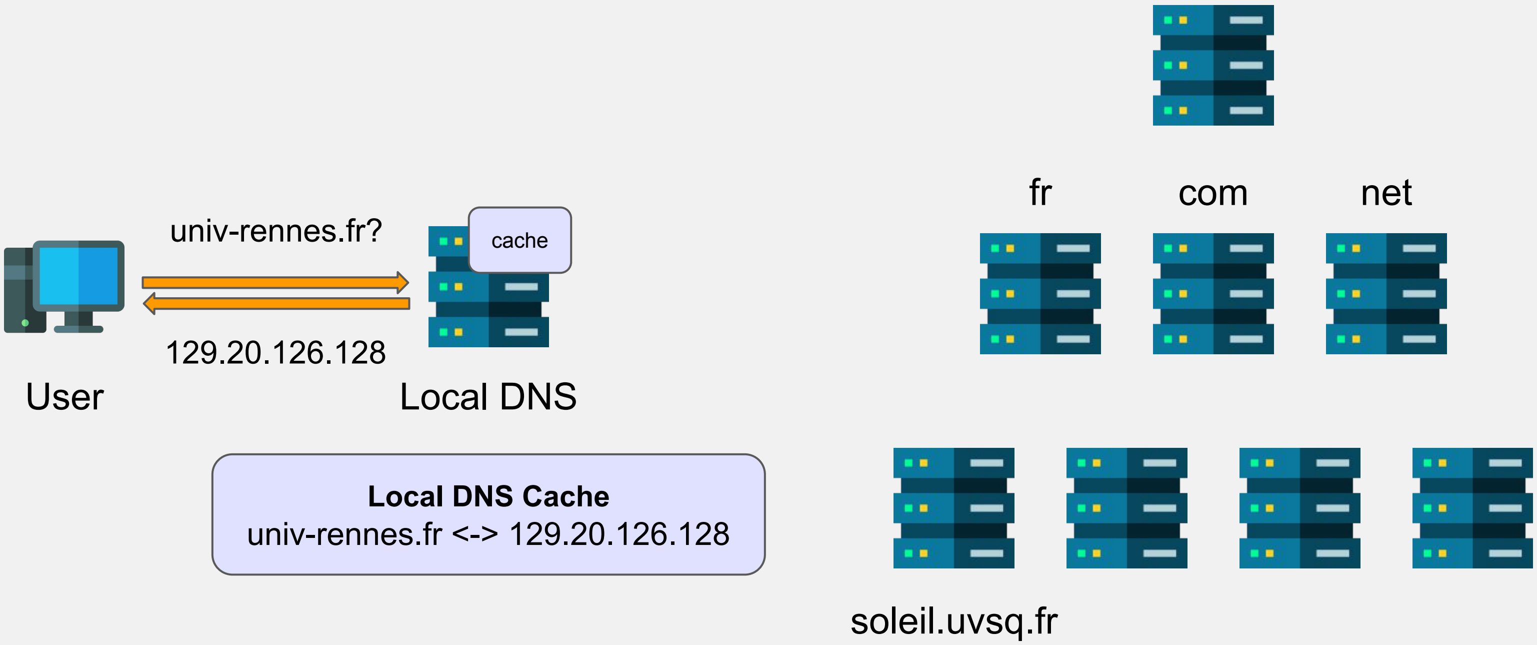

univ-rennes.fr?
fr
fr
com
net
univ-rennes.fr?
univ-rennes.fr?
User
129.20.126.128
Local DNS
soleil.uvsq.fr
univ-rennes.fr?
129.20.126.128
soleil.uvsq.fr

DNS Cache 1/2



Local DNS Cache
univ-rennes.fr <-> 129.20.126.128

DNS Cache 1/2



Local DNS Cache
univ-rennes.fr <-> 129.20.126.128

DNS Cache 2/2

Performance matters: DNS interactions need to be fast, msec counts.

Caching allows devices to resolve DNS queries faster based on previous lookups.

For instance:

1. Records for *.fr* authorities are valid for 172800 seconds (2 days).
2. Records for *univ-rennes.fr* authorities are valid for 3600 seconds.
3. And the IP of *etudiant.univ-rennes.fr* is valid for 300 seconds.

When a TTL is reached the previous step is done again on the next lookup.

Note: There is no way for an authority to force a resolver to expire an entry before TTLs.

DNS Redundancy

As foreshadowed by root servers ".", DNS allows server redundancy.

- On linux, you can check them directly with `dig +short NS . | sort`

If one takes time to answer a query, the resolver will fallback to the others. The same is true for all authorities.

- This mechanisms can also be used to distribute traffic with authority's responses containing multiple referrals in a randomized order. This technique is called **Round Robin DNS**.
- Answers can also be influence by geo localisation of the client, this is called **GeoDNS**.

DNS Synchronization

The problem with redundancy is to make sure that every servers is synchronized.

The DNS protocol includes way for server to push, pull, and fetch versions between servers and zones.

The versioning is handled by looking at the info from the **Start of Authority (SOA)** of a domain (this includes serial number, interval between version check in sec, time for retry, expiration, and negative response TTL).

E.g., `dig SOA . +short`

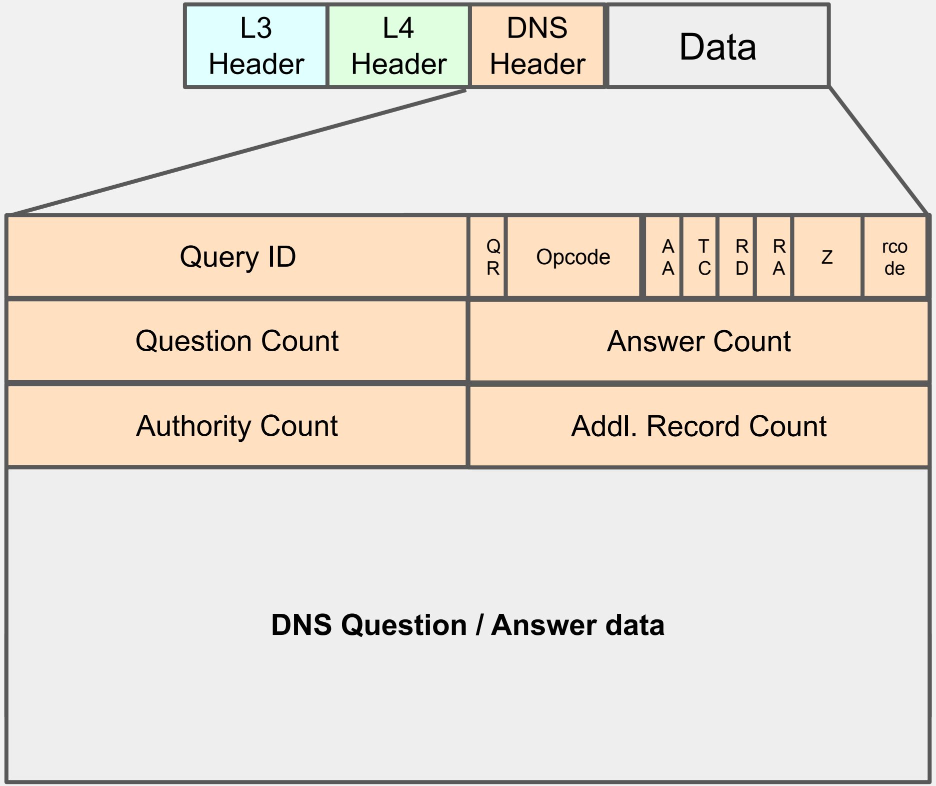
DNS Record Types

DNS records have types, here are some of the most important ones:

- **SOA** for the Start of Authority (control info) of a domain
- **A** for IPv4 address(es) of a domain.
- **AAAA** for the IPv6 address(es) of a domain.
- **NS** for the NameServer(s) of a domain.
- **MX** for the Mailserver(s) of a domain.
- **CNAME** for aliases.
- **TXT** free text field. (e.g., `dig -t txt univ-rennes.fr`)

DNS Packets 1/3

- By default on port 53.
    - **Q:** UDP or TCP?
- An exchange between a client/server is always linked to a **Query ID**.
- Question or answer are found in the data section of the DNS packet.



L3 Header

L4 Header

DNS Header

Data

Query ID

QR

Opcode

AA

TC

RD

RA

Z

rcode

Question Count

Answer Count

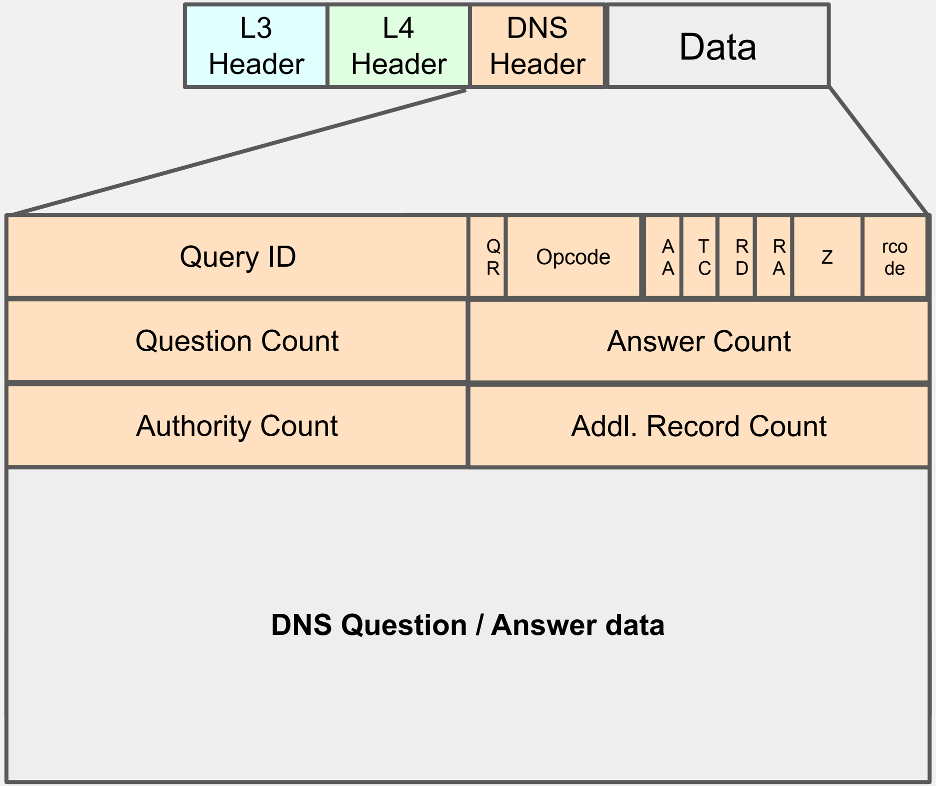
Authority Count

Addl. Record Count

DNS Question / Answer data

DNS Packets 1/3

- By default on port 53.
  - **BOTH**
  - ***UDP*** for fast comm. but fragmentation can cause issue, therefore packets should avoid being larger than 512 bytes.
  - ***TCP*** for bigger packers (for instance with crypto materials or IPv6 addresses), more reliable.



L3 Header

L4 Header

DNS Header

Data

Query ID

QR

Opcode

AA

TC

RD

RA

Z

rcode

Question Count

Answer Count

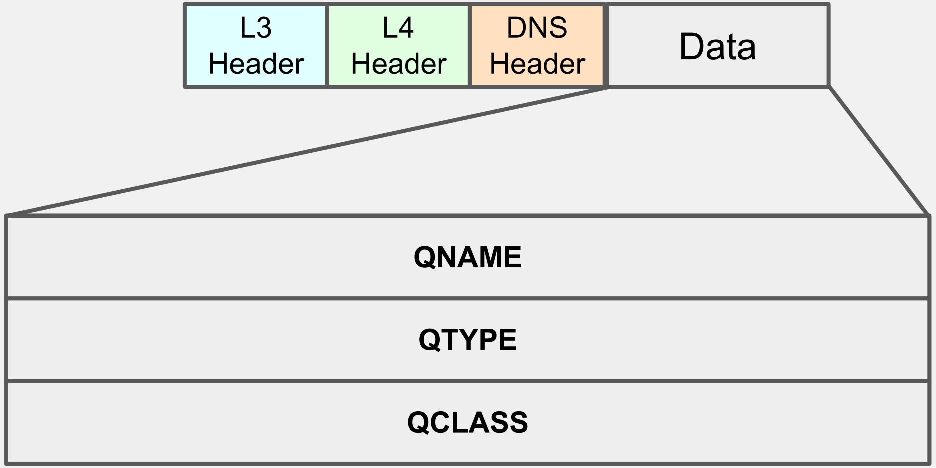
Authority Count

Addl. Record Count

DNS Question / Answer data

DNS Packets 2/3: Query

- QNAME: domain name
- QTYPE: Type of query, e.g.:
  - A: for IPv4 addresses.
  - MX: Mail servers.
- QCLASS: Class of the query:
  - IN: Internet



L3 Header

L4 Header

DNS Header

Data

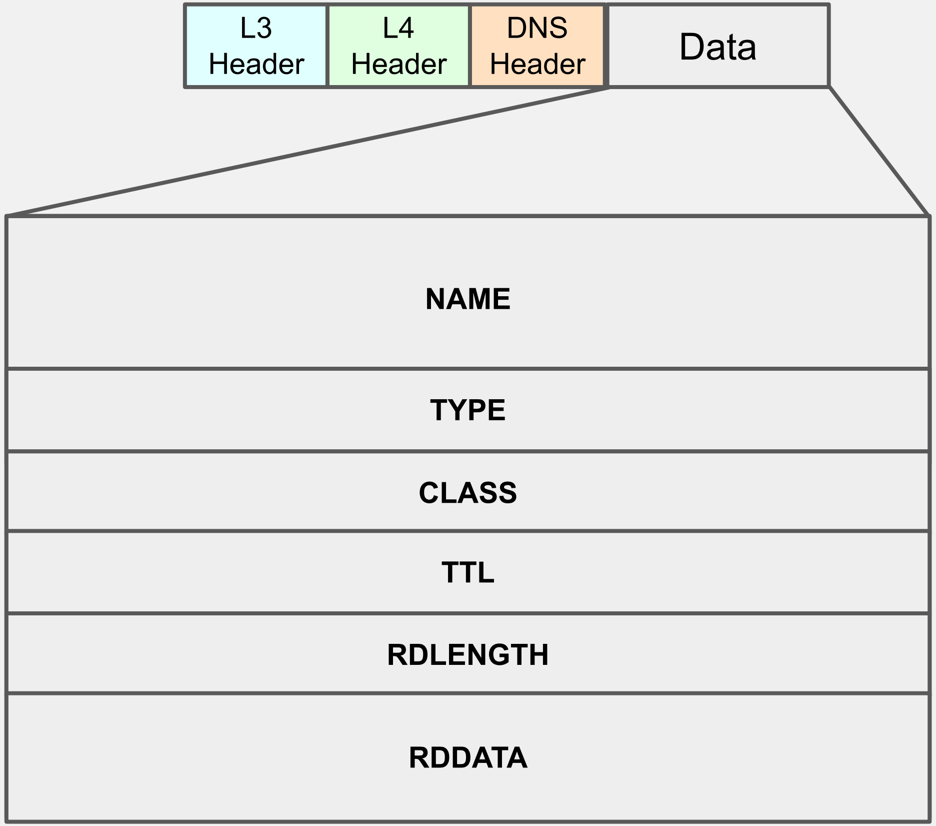
QNAME

QTYPE

QCLASS

DNS Packets 3/3: Answer

- NAME: domain name
- TYPE: Type of the records.
- CLASS: Class of the records.
- TTL of answers.
- RDLENGTH: size of records.
- RDDATA: records.



L3 Header | L4 Header | DNS Header | Data

NAME

TYPE

CLASS

TTL

RDLENGTH

RDDATA

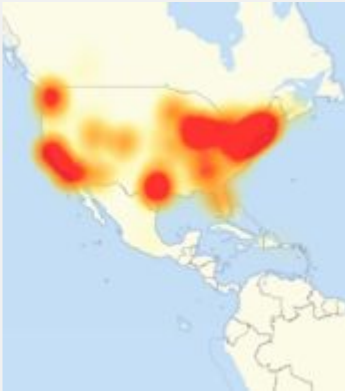
International Domain Names (IDN)

- DNS was originally limited to ASCII characters. But not everybody use ASCII.
  - International Domain Names solve the problem using Punycode.
  - All non ASCII characters are transformed in DNS records.
  - For instance: https://仕手株.コム is translated to https://xn--7mq578b3ie.xn--tckwe/
- **Q:** what about lookalike characters now?

DNS Attacks

DoS Attacks on DNS

As any server exposed to the Internet, the DNS infrastructure can be vulnerable to DoS (and by extension DDoS) attacks.



- An attacker could try to bombard servers to takedown the Internet.
  - Was never achieved on Root servers but on the DNS provider Dyn in 2016.
- Mitigations:
  - For critical servers: better filtering and pipes.
  - For domains owner: redundancy of operators. (**Q:** How?)

DoS Attacks using DNS

DNS is mainly used over UDP.

- Therefore it could be used as a DDoS amplificator.
  - Queries source IP can be spoofed to overload the victim with answers.
  - E.g., `dig +notcp ANY . @a.root-servers.net.` amplifies the request by 10.
- Mitigations:
  - Rate-limiting, or source filtering like BCP38:
    - Filter UDP packets based on src IP from unlikely origin.
    - Hard to deploy since your own network does not benefit directly from it.
    - Nevertheless, it seems to be largely deployed (or at least similar filters are).

DNS MitM

Most DNS exchanges are in plaintext over the Internet.

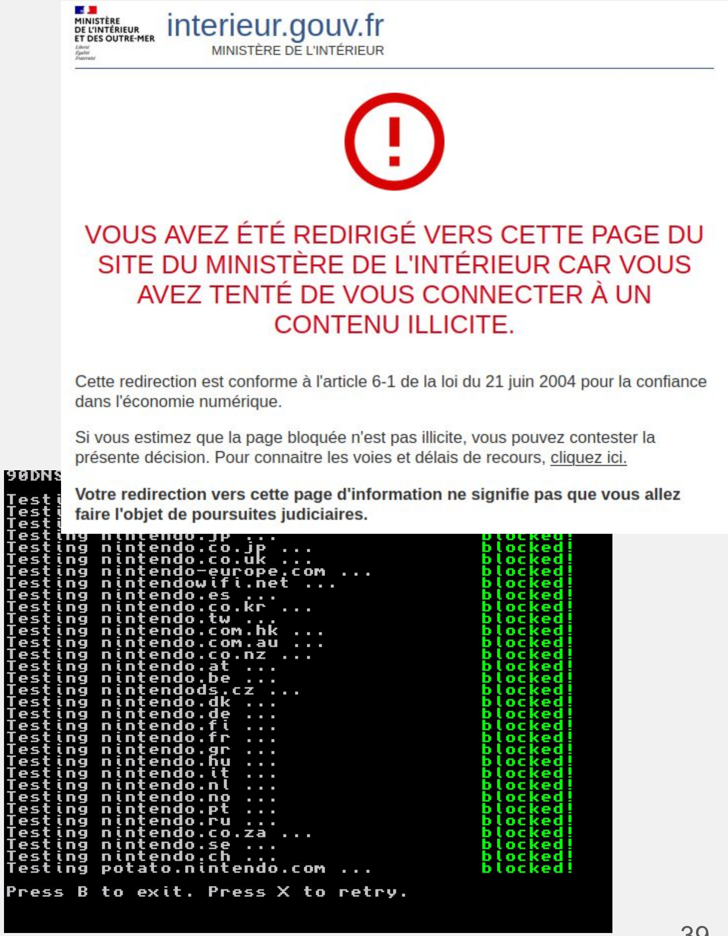
- An adversary could easily modify DNS responses.
- **Q:** How? And Why?

DNS MitM

Most DNS exchanges are in plaintext over the Internet.

- An adversary could easily modify DNS responses.
- **How:** data tampering from the resolver or a router.
- **Why:** Could be used to block access to various websites:
  - For intellectual property enforcement.
  - For censorship.
  - For fun.
  - And more…

Mitigations: Using encrypted channel or signed content (foreshadowing).



interieur.gouv.fr
MINISTÈRE DE L'INTÉRIEUR

VOUS AVEZ ÉTÉ REDIRIGÉ VERS CETTE PAGE DU SITE DU MINISTÈRE DE L'INTÉRIEUR CAR VOUS AVEZ TENTÉ DE VOUS CONNECTER À UN CONTENU ILLICITE.

Cette redirection est conforme à l'article 6-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

Si vous estimez que la page bloquée n'est pas illicite, vous pouvez contester la présente décision. Pour connaitre les voies et délais de recours, cliquez ici.

Votre redirection vers cette page d'information ne signifie pas que vous allez faire l'objet de poursuites judiciaires.

```
90DNS
Testi
Testi
Testi
Testing nintendo.jp ...                    blocked!
Testing nintendo.co.jp ...                 blocked!
Testing nintendo.co.uk ...                 blocked!
Testing nintendo-europe.com ...            blocked!
Testing nintendowifi.net ...               blocked!
Testing nintendo.es ...                    blocked!
Testing nintendo.co.kr ...                 blocked!
Testing nintendo.tw ...                    blocked!
Testing nintendo.com.hk ...                blocked!
Testing nintendo.com.au ...                blocked!
Testing nintendo.co.nz ...                 blocked!
Testing nintendo.at ...                    blocked!
Testing nintendo.be ...                    blocked!
Testing nintendods.cz ...                  blocked!
Testing nintendo.dk ...                    blocked!
Testing nintendo.de ...                    blocked!
Testing nintendo.fi ...                    blocked!
Testing nintendo.fr ...                    blocked!
Testing nintendo.gr ...                    blocked!
Testing nintendo.hu ...                    blocked!
Testing nintendo.it ...                    blocked!
Testing nintendo.nl ...                    blocked!
Testing nintendo.no ...                    blocked!
Testing nintendo.pt ...                    blocked!
Testing nintendo.ru ...                    blocked!
Testing nintendo.co.za ...                 blocked!
Testing nintendo.se ...                    blocked!
Testing nintendo.ch ...                    blocked!
Testing potato.nintendo.com ...            blocked!

Press B to exit. Press X to retry.
```

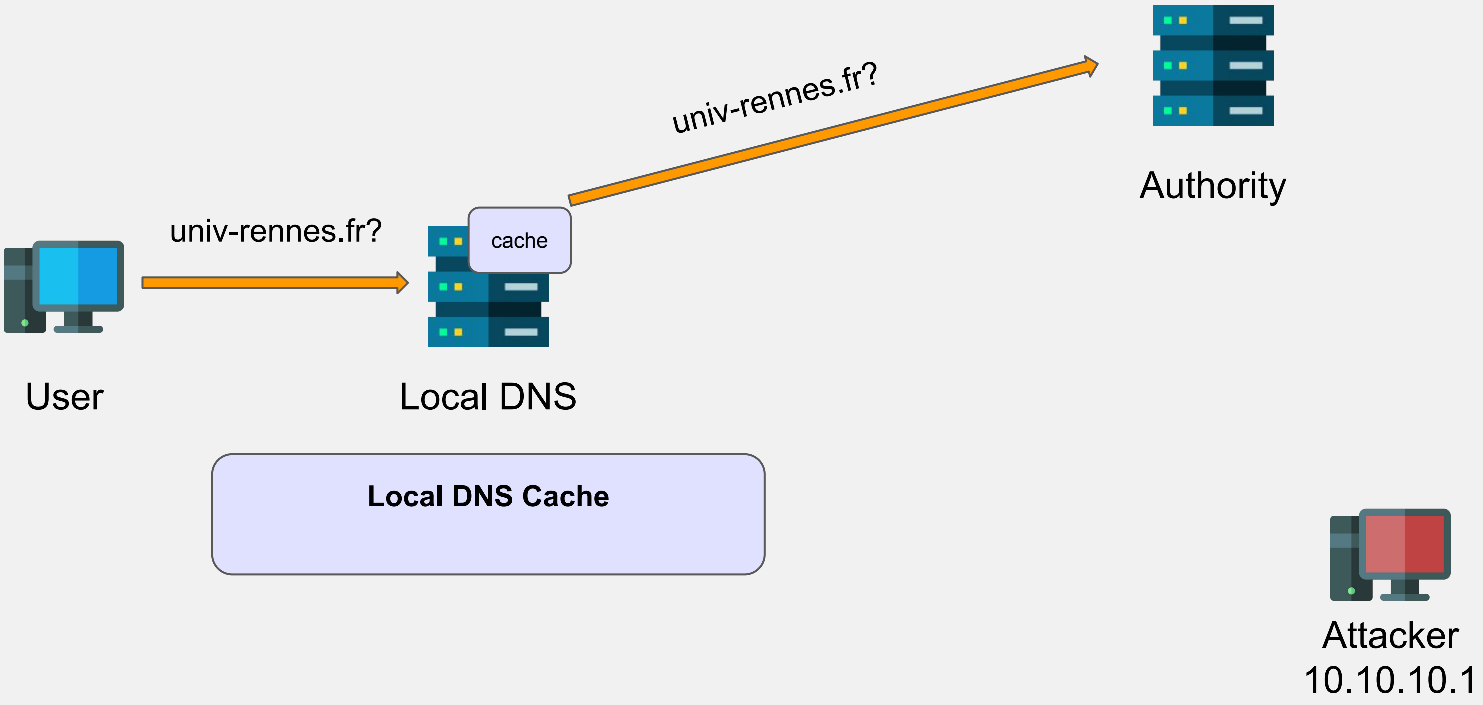
DNS Privacy Issues

In addition to tampering, DNS messages are vulnerable to ***pervasive monitoring***.

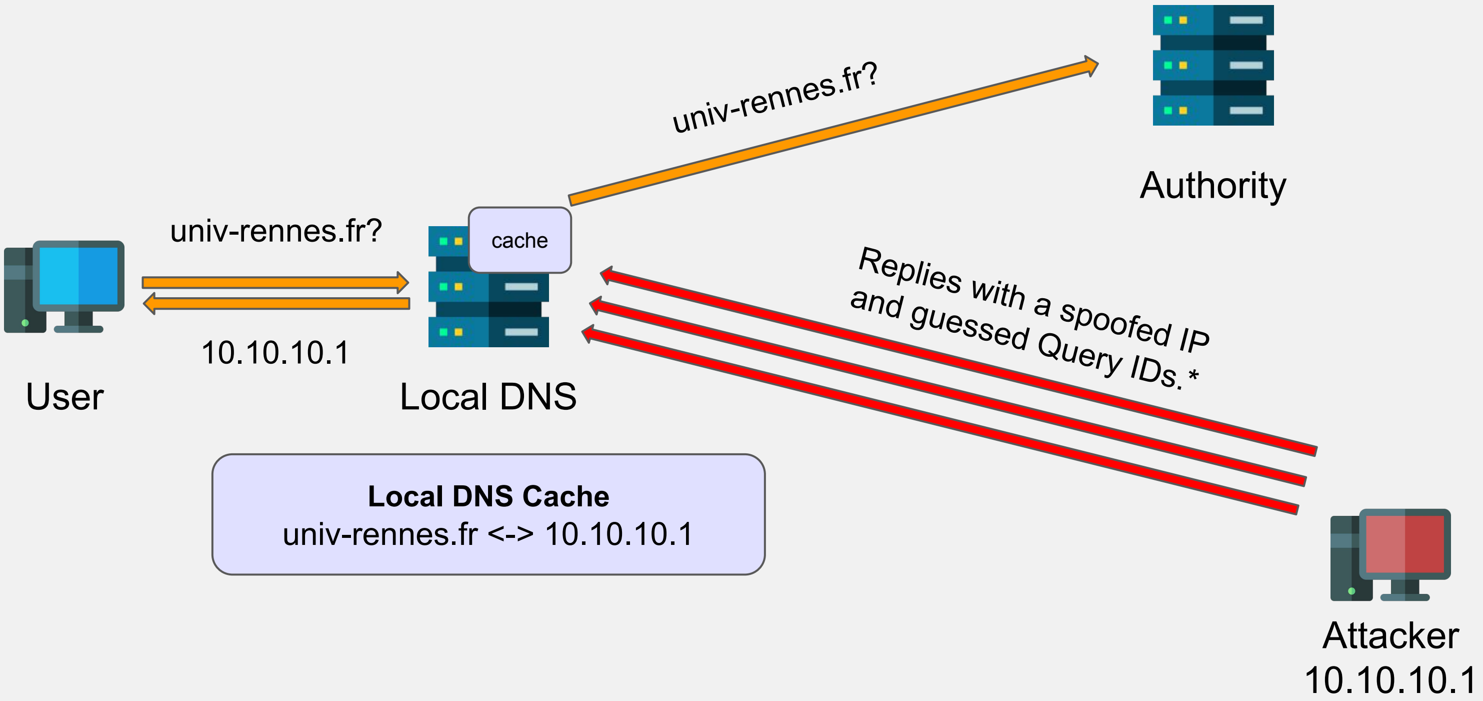
- By collecting DNS messages, surveillance mechanisms can easily be setup.
- To prevent this, and resolve privacy issues **DNS PRIvate exchange (DPRIVE)** was introduced in 2014 by adding ways to transport encrypted DNS messages:
  - For clients:
    - DNS over TLS aka **DoT**, over HTTPS aka **DoH**, or over QUIC* aka **DoQ**.
  - For server synchronization:
    - Zone transfer over TLS (XFR queries).
  - For resolvers:
    - Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS (RFC9539).

** protocol from 2012 intended to be the replacement of TCP.*

DNS Cache Poisoning



DNS Cache Poisoning



Local DNS Cache
univ-rennes.fr <-> 10.10.10.1

* And why not a huge TTL.
Note: Here the User can also be the attacker when the resolver is accessible.

Kaminsky's Cache Poisoning Attack

- Attack on DNS in 2008.
  - 5 min video on the subject dubbed by Kaminsky himself.
- Cache cannot be modified once updated -> if you did not guess the ID you need to wait for the TTL…
  - But what about subdomain? With random value there is a good guarantee of no existing cache entry.
- A forged reply could then be used to tell the resolver that, for instance, random1234.google.com was not known but another name server (NS) for google.com was attacker.com with A records toward the attacker IP.

DNS Cache Poisoning

- The huge problem here is the Query ID.
  - Before IDs were incremental.
  - After it was random (but Kaminsky was bored).
  - Now it is random + random source port number (2^{16} + ~2^{16} bits of entropy)
    - The issue is not solved but harder to do.
- Other mitigations:
  - Case randomization of DNS query (e.g., uNiV-REnNes.fR).
  - DNS Cookies.
  - Encryption between resolvers and authority servers.
  - DNSSEC

DNSSEC

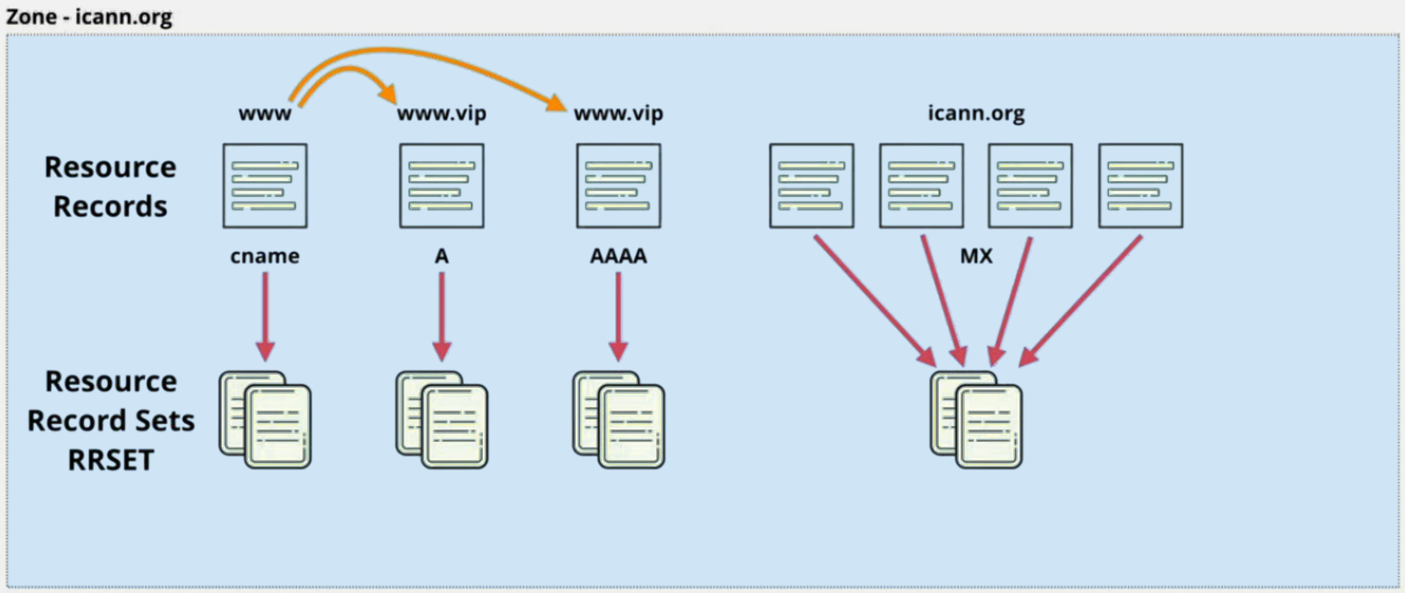
DNSSEC

Domain Name System Security Extensions (DNSSEC)

- Extension to the DNS protocol.
- Provides authentication and integrity for DNS replies.
    - **Warning**: No confidentiality.
- DNSSEC is used by resolver to verify the identity of authority servers.

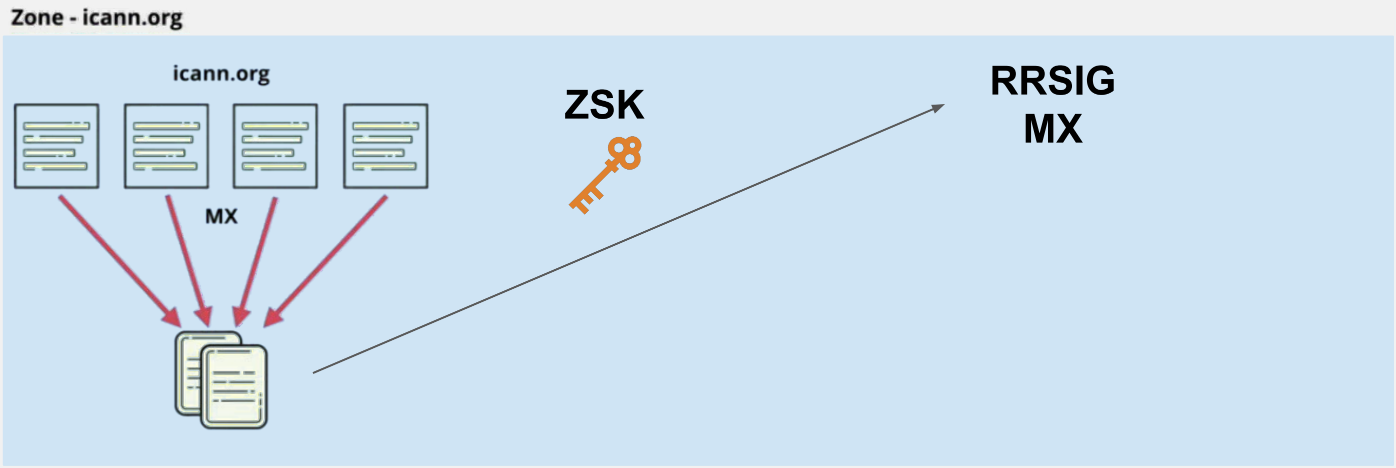
DNSSEC - RRSET

DNSSEC is used to verify Resource Record Sets (**RRSET**) not individual records.



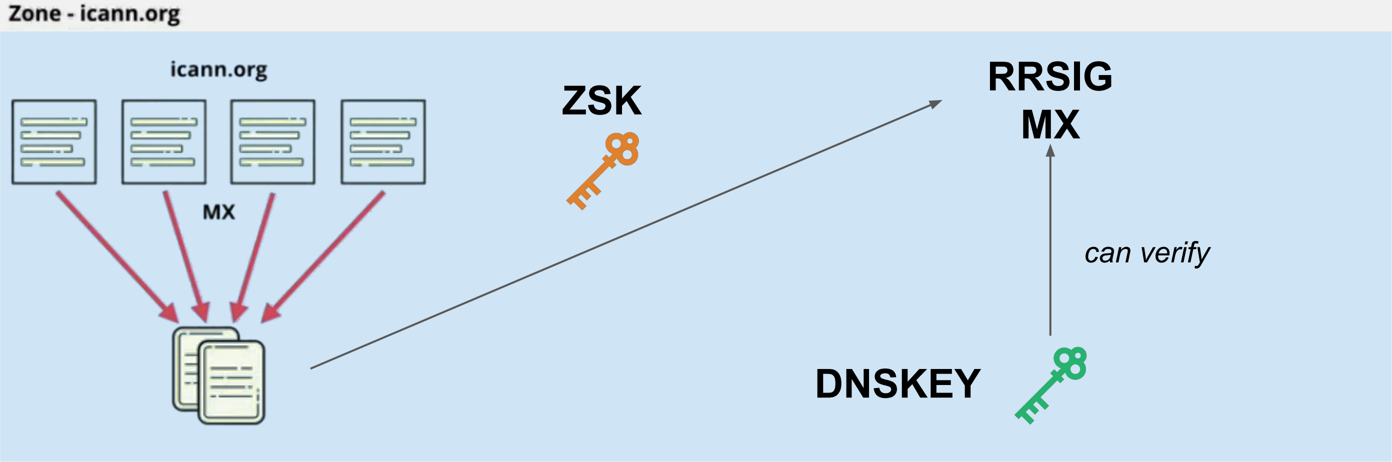
DNSSEC - RRSIG & Zone Signing Key (ZSK)

To be sure that nothing has been modified, RRSET are signed by the **ZSK** to create an **RRSIG**. The ZSK is the private part of the public/private key pairs of the zone, and need to be kept secret.



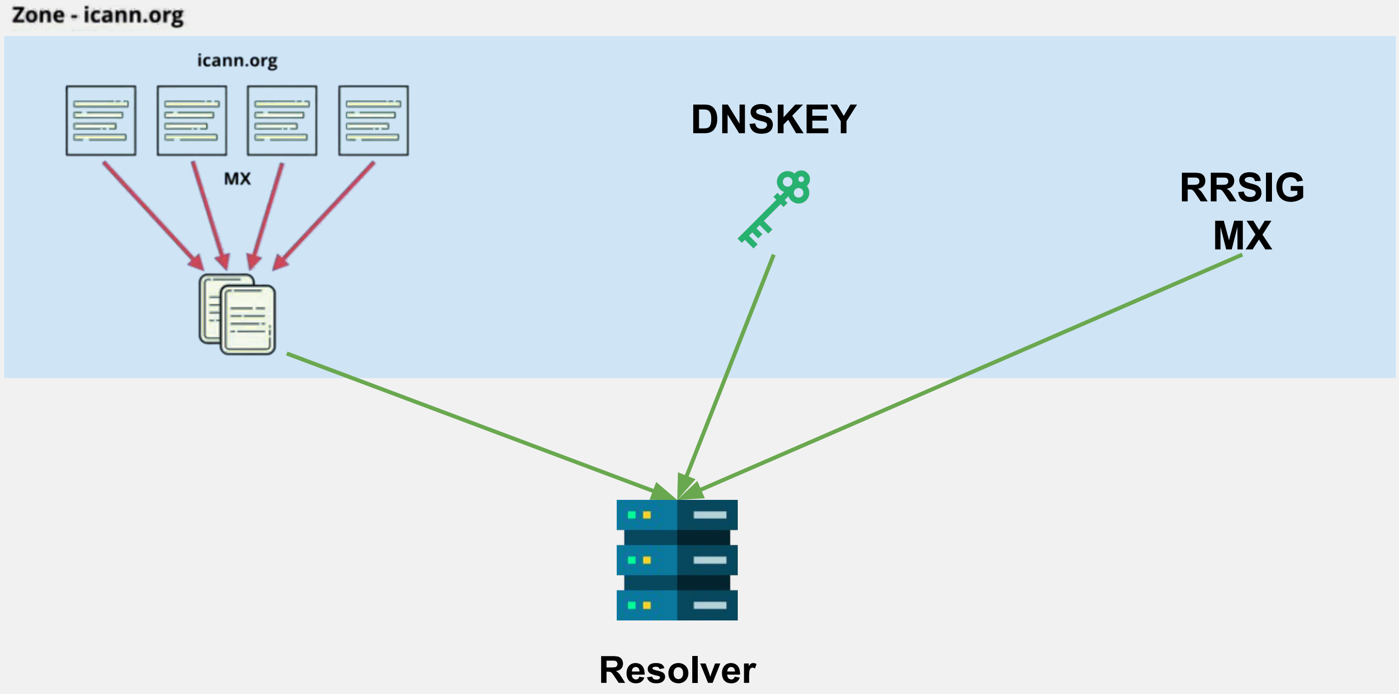
DNSSEC - DNSKEY 1/2

The public part, the **DNSKEY**, is used to verify the RRSIG of the related RRSET.



DNSSEC - DNSKEY 2/2

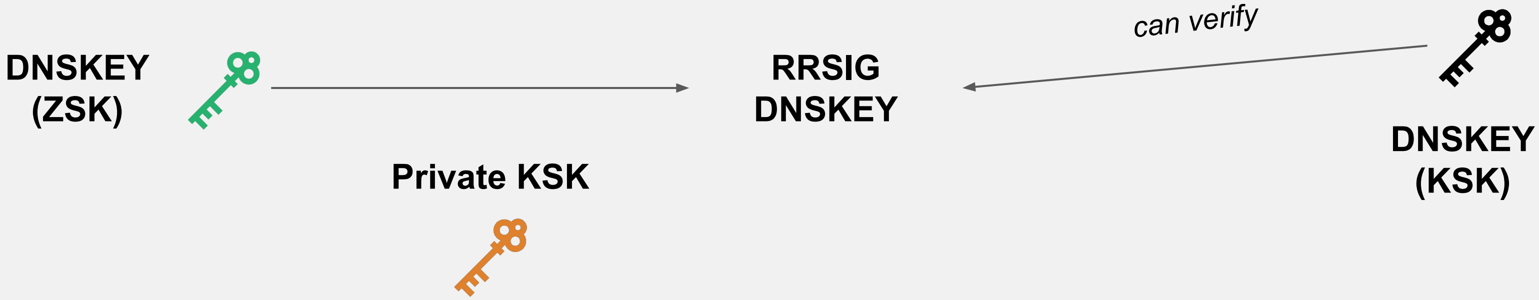
Now a resolver can verify an RRSET **if** it trust the DNSKEY of the zone.



DNSSEC - Key Signing Key (KSK) 1/2

To achieve this, the zone generates another key pairs called the **Key Signing Key (KSK)** to link the DNSKEY ZSK to a parent zone. The DNSKEY is **signed by the private KSK** and can be **verify with the KSK DNSKEY**.

- Why creating another layer of keys? For easier update with rolling ZSK keys.



DNSKEY (ZSK)

RRSIG DNSKEY

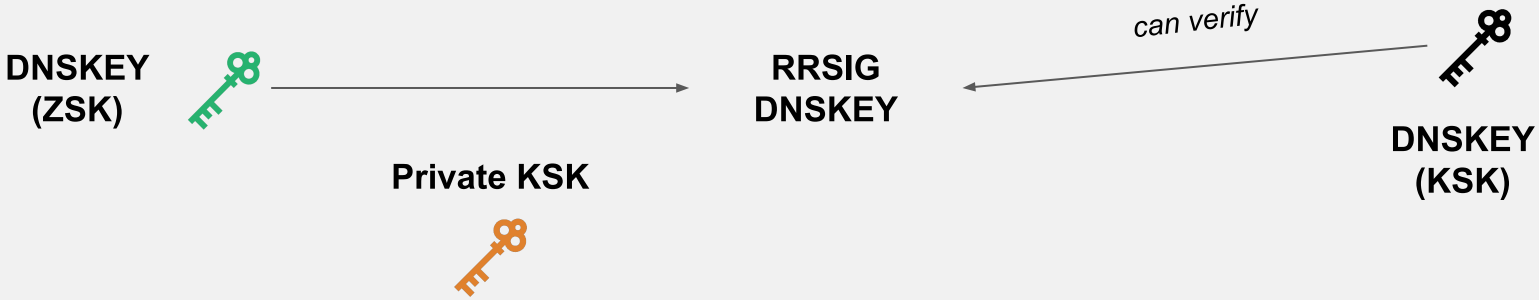
can verify

DNSKEY (KSK)

Private KSK

DNSSEC - Key Signing Key (KSK) 2/2

- Now the public KSK key can be referenced by the parent zone using what we call a **DS Record**.



DNSSEC DS Record

A DS Record contains the ***hash of a child domain public KSK***.

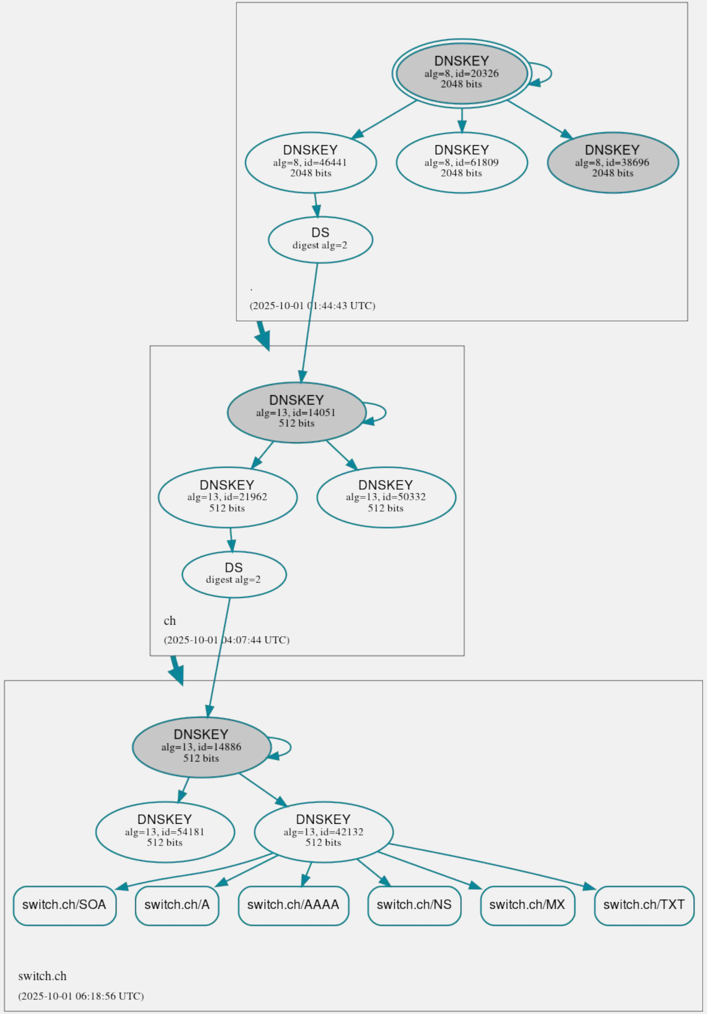
- Hashing being a one-way mechanism: a resolver can hash the public key of a zone and check the DS record of the parent.

DS Records stored in a zone are themselves signed using its private ZSK to generate a **RRSIG DS**.

Here the cycle start again with the KSK of the zone and the public KSK to be trusted.

DNSSEC Chain of Trust

- Root Servers: DNSKEY signed in 2010, and is now the **Root of Trust (RoT)** of the chain.


DNSKEY alg=8, id=20326 2048 bits
DNSKEY alg=8, id=46441 2048 bits
DNSKEY alg=8, id=61809 2048 bits
DNSKEY alg=8, id=38696 2048 bits
DS digest alg=2
.
(2025-10-01 01:44:43 UTC)
DNSKEY alg=13, id=14051 512 bits
DNSKEY alg=13, id=21962 512 bits
DNSKEY alg=13, id=50332 512 bits
DS digest alg=2
ch
(2025-10-01 04:07:44 UTC)
DNSKEY alg=13, id=14886 512 bits
DNSKEY alg=13, id=54181 512 bits
DNSKEY alg=13, id=42132 512 bits
switch.ch/SOA
switch.ch/A
switch.ch/AAAA
switch.ch/NS
switch.ch/MX
switch.ch/TXT
switch.ch
(2025-10-01 06:18:56 UTC)

Resources and Acknowledgements

- *Computer Networking: A Top-down Approach* by James F. Kurose, Keith W. Ross
- Internet Security: A Hands-on Approach, 3rd Edition, Du Wenliang
- Based on previous material from Mathieu Goessens.
- Based on material from Adrian Cantrill.