DNS

Name Resolution and beyond

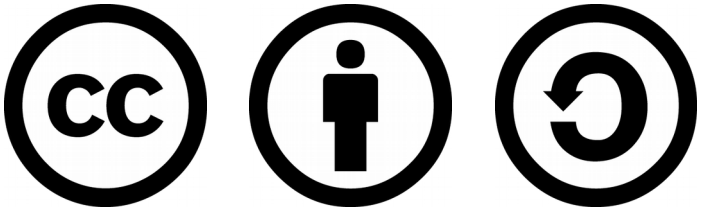
Xavier Belanger

xavier@belanger.fr

June 2017

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

http://creativecommons.org/licenses/by-sa/4.0/



You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

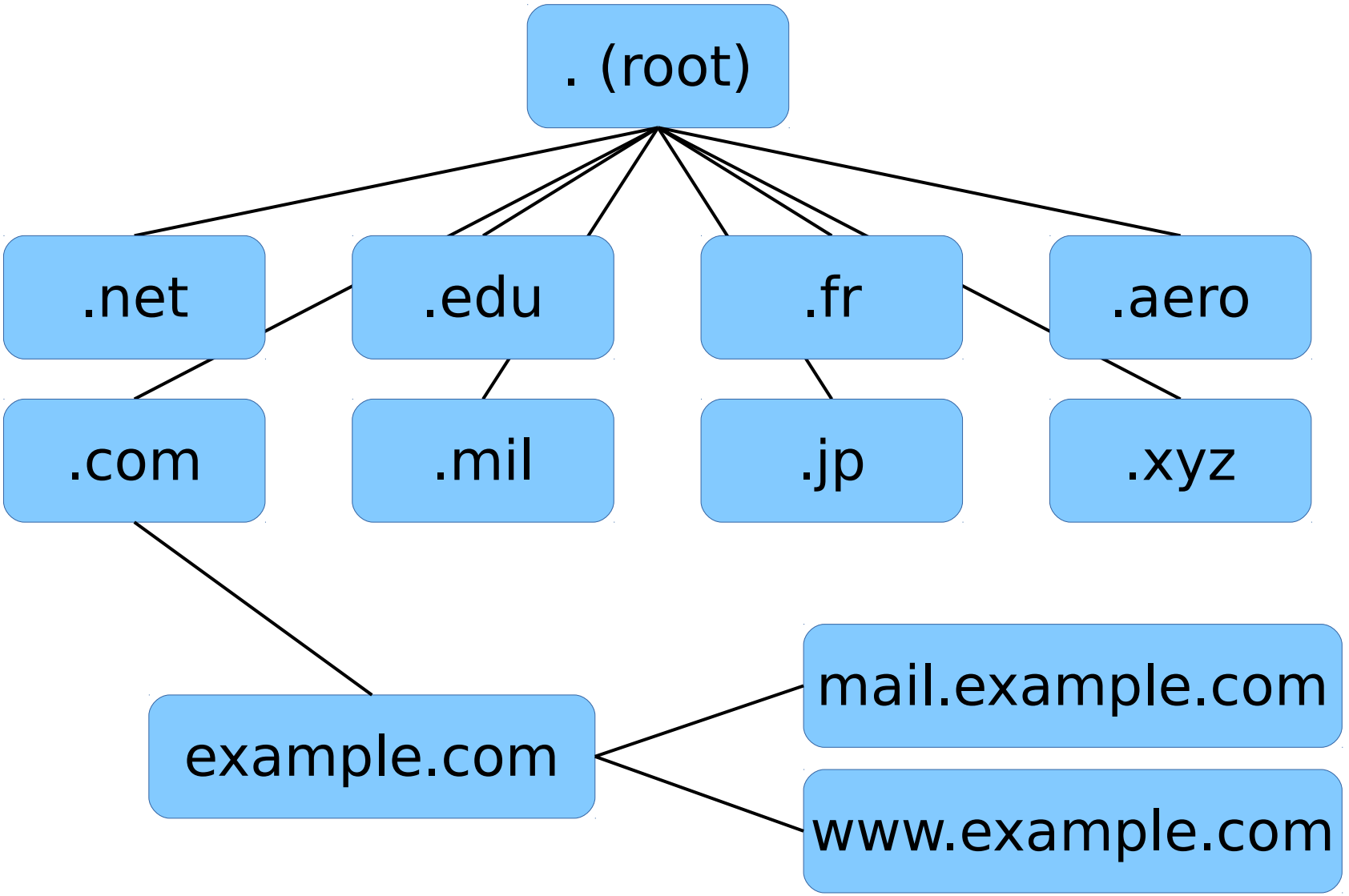
- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
- **No additional restrictions** — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

About the speaker

- French Linux Enthusiast
- Working in IT since 1999
  System and Network Administrator, CISSP
- Managing DNS servers since 2001

Why do we need DNS?

- Computers can talk to each other by using the Internet Protocol (IP), relying on IP addresses.
- Human beings are not very good at working with IP addresses.
- Some servers are used to host many services for different uses, each one needs a different name (the server will still use only one IP address). Also some services are hosted by more than one server.
- Hence, we need a service to resolve names to IP addresses (and vice-versa): the Domain Name System.

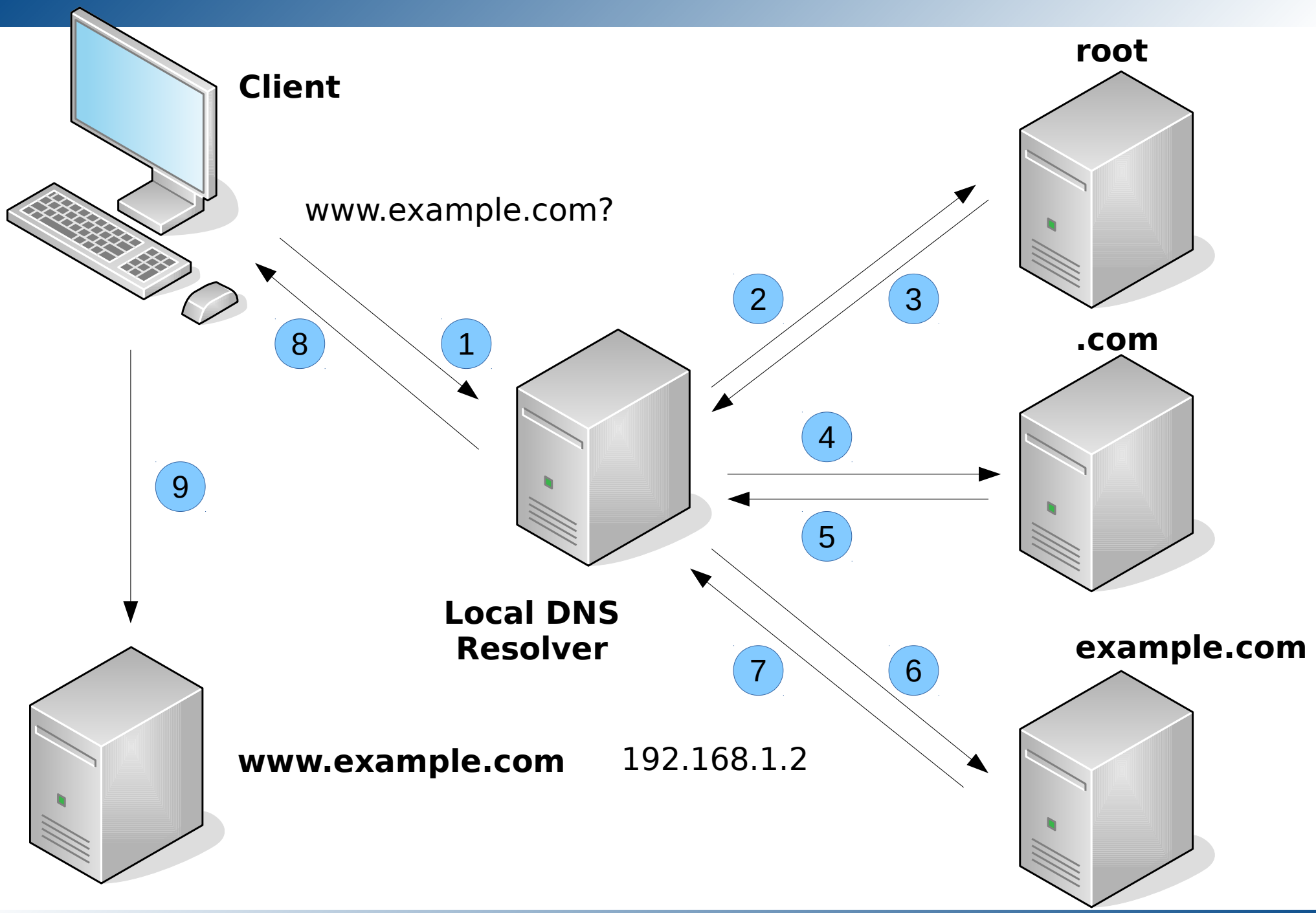

. (root)
.net
.edu
.fr
.aero
.com
.mil
.jp
.xyz
example.com
mail.example.com
www.example.com

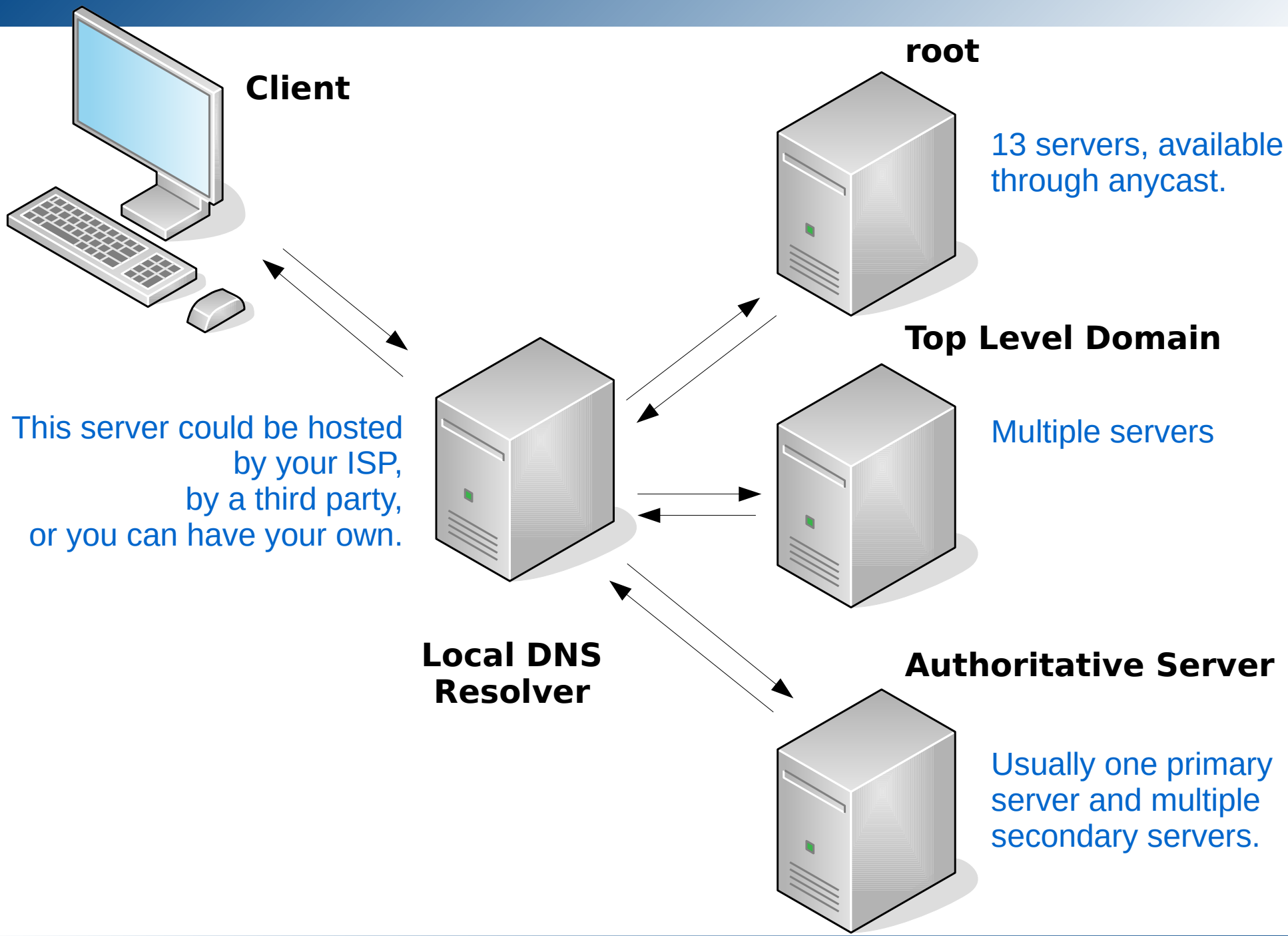
History

- A long time ago, names and addresses were managed manually by Jon Postel.
- With the expansion of Arpanet, a better system was needed. Jon Postel asked Paul Mockapetris to evaluate five different solutions. Mockapetris came with another idea instead, the Domain Name System.
- DNS became official with RFC 882 and 883 in November 1983.

How DNS does work?

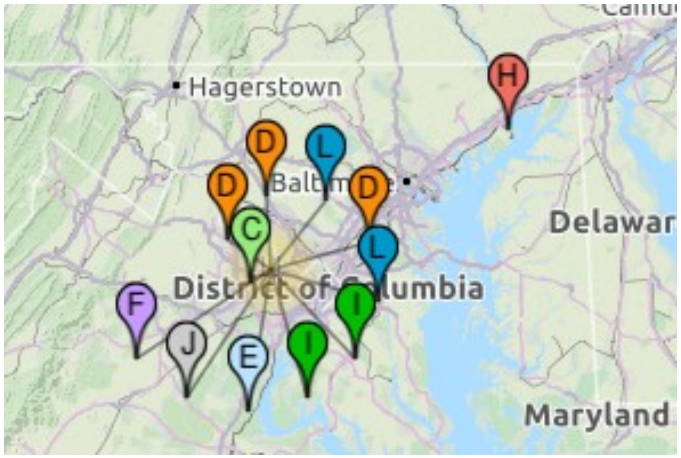
- Your computer (the client) asks the local DNS resolver: “*I need to reach www.example.com do you know its IP address?*”
- If the local resolver doesn’t know, it will ask the root. From the response the resolver will ask other servers, and get a response.
- All of this in few milli-seconds on average.
- DNS traffic uses UDP/53 and in some specific circumstances TCP/53.


Client
root
www.example.com?
2
3
8
1
.com
4
9
5
Local DNS
Resolver
example.com
7
6
www.example.com
192.168.1.2


Client
root
13 servers, available through anycast.
Top Level Domain
This server could be hosted by your ISP, by a third party, or you can have your own.
Multiple servers
Local DNS Resolver
Authoritative Server
Usually one primary server and multiple secondary servers.

The Root Servers

- 13 root name servers are operated by 12 organizations (Verisign, Cogent, NASA, University of Maryland, ICANN, DoD, ISC, …)
- Multiple physical servers, spread across the globe.



Map from
www.root-servers.org

DNS Resource Record Types

- SOA and NS
- A, AAAA, PTR and CNAME
- MX, TXT
- And many, many more

Note: domains and records are not limited to the ASCII character encoding anymore. Arabic, Chinese, Russian and other alphabets can be used. Punycode is used to “translate” those names into ASCII.

SOA and NS Records

- Start of Authority (SOA) is the essential record to define a zone with the primary name server, a contact email address and various time values used by the secondary servers:
  - refresh
  - retry
  - expire
  - negative caching TTL
- Name Server (NS) will list all the DNS servers for a zone.

```
$ dig SOA example.com


example.com. 86400 IN SOA ns1.example.com.
hostmaster.example.com. (
2017051601 ; serial
86400      ; refresh (1 day)
3600       ; retry (1 hour)
3600000    ; expire (5 weeks 6 days 16 hours)
86400      ; minimum (1 day)
)
```

```
$ dig NS example.com

example.com.    86400 IN NS ns1.example.net.
example.com.    86400 IN NS ns2.example.net.
ns1.example.net.      86400 IN A 10.1.0.10
ns2.example.net.      86400 IN A 10.2.0.30
```

A, AAAA, PTR and CNAME Records

- A hostname for an IPv4 address is registered with a ‘A’ record; for an IPv6 address, an ‘AAAA’ record is used.
- A pointer from an IP address to a hostname is handled by a PTR record (`in-addr.arpa` and `ip6.arpa` special domains).
- CNAME records are used to create aliases for a hostname.
- If Dynamic DNS (DDNS) is used, hosts can ask the DNS server to register their hostname (via the DHCP server).

```
$ dig A www.example.com

www.example.com.  86400 IN CNAME web01.example.com.
web01.example.com.       86400 IN A     10.5.4.47

$ dig -x 10.5.4.47

47.4.5.10.in-addr.arpa. 86400 IN PTR web01.example.com.

$ dig AAAA www.example.com

www.example.com.  86400 IN CNAME web01.example.com.
web01.example.com.       86400 IN AAAA
2001:db8:4:6b00:473:186:33:77
```

MX and TXT Records

- Servers accepting e-mails for a domain must be listed as Mail Exchangers in the DNS with MX records.
- Those records also provides a weight for each server; that is the priority for e-mail delivery (low value = high priority).
- TXT records are generic text records; specific text records are used to store SPF, DKIM and DMARC information.
- Anti-spam tools and services heavily rely on DNS (DNSBL / RBL).

```
$ dig MX example.com


example.com.     86400  IN  MX  100
mx01.example.com.

example.com.     86400  IN  MX   50
mx02.example.com.


$ dig TXT example.com


example.com.     86400  IN  TXT
"v=spf1 include:smtp.example.com ~all"
```

SSHFP Record

- A SSHFP record stores the fingerprint of a SSH server; this can be used to check the validity of that fingerprint at the first connection attempt.

```
$ ssh -o "VerifyHostKeyDNS ask" server.example.net
The authenticity of host 'server.example.net (192.168.1.2)'
can't be established.
RSA key fingerprint is
e9:8b:c4:5b:8f:bc:98:07:5f:20:ff:c4:23:7f:cb:aa.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

Tools and Troubleshooting

- nslookup, host, dig, drill
- Server logs, dnstap
- Third party tools:
- dnscheck.iis.se, intodns.com, zonemaster.fr, mxtoolbox.com, ...
- Public DNS servers:
  Google Public DNS, Verisign Public DNS, OpenDNS, ...

Limits and Issues

- One can try to poison a DNS server, and then affect all the clients.
- Clients can be redirected to a rogue DNS server and get wrong answers.
- Servers operators can see all DNS queries and trace network activity; they can also block access to some domain names.
- Open DNS servers can be used for DoS/DDoS attacks.
- NSA MoreCowBell.

Some solutions

- Check the DNS servers that your computer is using: are they trustworthy?
- Use some DNS public servers.
- Run and manage your own DNS local resolver.

Software

- ISC BIND `https://www.isc.org/`
- NSD `https://www.nlnetlabs.nl/`
- Unbound `https://www.nlnetlabs.nl/`
- Knot DNS `https://www.knot-dns.cz/`
- and others...

BIND

- Berkeley Internet Name Domain
- Developed by the Internet Software Consortium (ISC) under the Mozilla Public License.
- Could be set as a cache and recursive server or as an authoritative server.
- named.conf, plus the zone files
- named-checkconf, named-checkzone
- rndc

Unbound

- Developed by NLnet Labs, under the BSD license.
- Could be set as a cache, recursive server.
- unbound.conf
- unbound-checkconf
- Dnssec-Trigger can be used on laptops to reconfigure Unbound as needed (experimental).

DNSSEC

- DNSSEC is an extension of the DNS protocol, providing cryptographic tools to validate the information from a signed zone.
- Records are signed by the server operator with a private key; clients can check the records validity by using a public key.

Keys and Records

- The root provide a special key, the DNS Root trust anchor, that is used to validate other keys.
- Each zone use two sets of keys:
  - the Zone Signing Keys (ZKS), used to sign the data within the zone
  - the Key Signing Keys (KSK), used to sign the ZKS; used as the secure entry point for the zone
- Keys should be rotated on a regular basis (key rollover).

```
$ dig +dnssec SOA example.com

example.com.  86400 IN SOA ns1.example.com. hostmaster.example.com. (
2017051601 ; serial
86400      ; refresh (1 day)
3600       ; retry (1 hour)
3600000    ; expire (5 weeks 6 days 16 hours)
86400      ; minimum (1 day)
)
example.com.  86400 IN RRSIG SOA 7 2 86400 (
20170615141724 20170516141724 4502 example.com.
VCyDbhpxWgF5eRHRQt9o4fFtuN4PEzNvnUs+VRnOr+us
0zl/de9NqFlcbwP7HMuhJhyJrfFBMnFUFJq6ye98Dywc
exaqEmpdc8KL8PlllFQwB/jUe6LPQpHKAx10HUdqyOUT
ci2+qCWlc85oTwGixh4FoBuFe3lIf//Vzx/1OOE= )
```

DANE

- DNS-based Authentication of Named Entities
- Now you can provide security certificates (X.509, used with TLS) with DNS. This could be mostly used to secure websites and email servers.
- Different options are possible, from confirming the information on a Certificate Authority (CA) to providing a full certificate.
- DANE doesn’t have a widespread support yet, and require DNSSEC.

CAA Record

- Certification Authority Authorization, defined by RFC 6844
- That record list the the Certification Authorities authorized to issue security certificates for a domain.
- This doesn’t involve or apply to TLS, it is mostly used to certificate issuing.
- Following a decision of the CA/Browser Forum, all certificate authorities must check CAA records starting September 2017.

Around DNS

- **mDNS**: multicast DNS. RFC 6762, used for stand-alone networks, using TCP/5353. Also known as *Avahi* or *Bonjour*.
- **Alternative roots or systems**: .42, namecoin, emercoin, OpenNIC, .onion, Distributed Hash Tables (DHT), ...

Resources - Official Sources

- **Internet Corporation For Assigned Names and Numbers**
  https://www.icann.org/
- **Internet Assigned Numbers Authority**
  https://www.iana.org/
- **Root Servers**
  http://www.root-servers.org/

Resources - Third Party

- **DNS for Rocket Scientists**
  http://www.zytrax.com/books/dns
- **Calomel**
  https://calomel.org/
- **Team Cymru**
  https://www.team-cymru.org/
- **Google Public DNS Servers**
  https://developers.google.com/speed/public-dns
- **Google Apps Toolbox**
  https://toolbox.googleapps.com/apps/dig

Resources - Books

- **DNS and BIND**, 5th ed.
  Cricket Liu and Paul Albitz - O'Reilly
- **DNS and Bind Cookbook**
  Cricket Liu - O'Reilly
- **Pro DNS and BIND**
  Ron Aitchison - Apress
- **DNS Security**
  Allan Liska and Geoffrey Stowe - Syngress