

# DNS: Domain Name System

*an overview*

Xavier Belanger  
January 24, 2015

# 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.

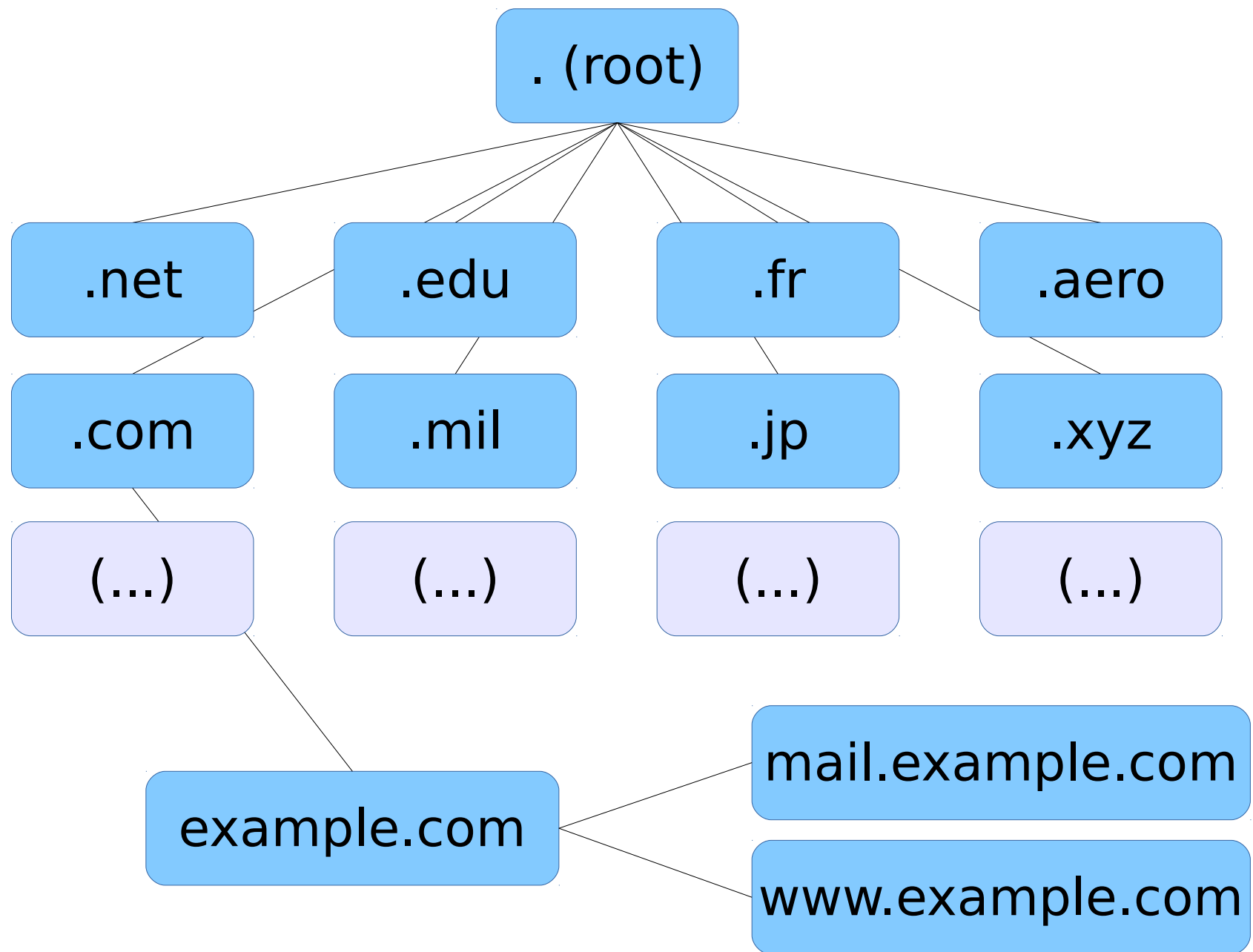
The licensor cannot revoke these freedoms as long as you follow the license terms.

## 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.

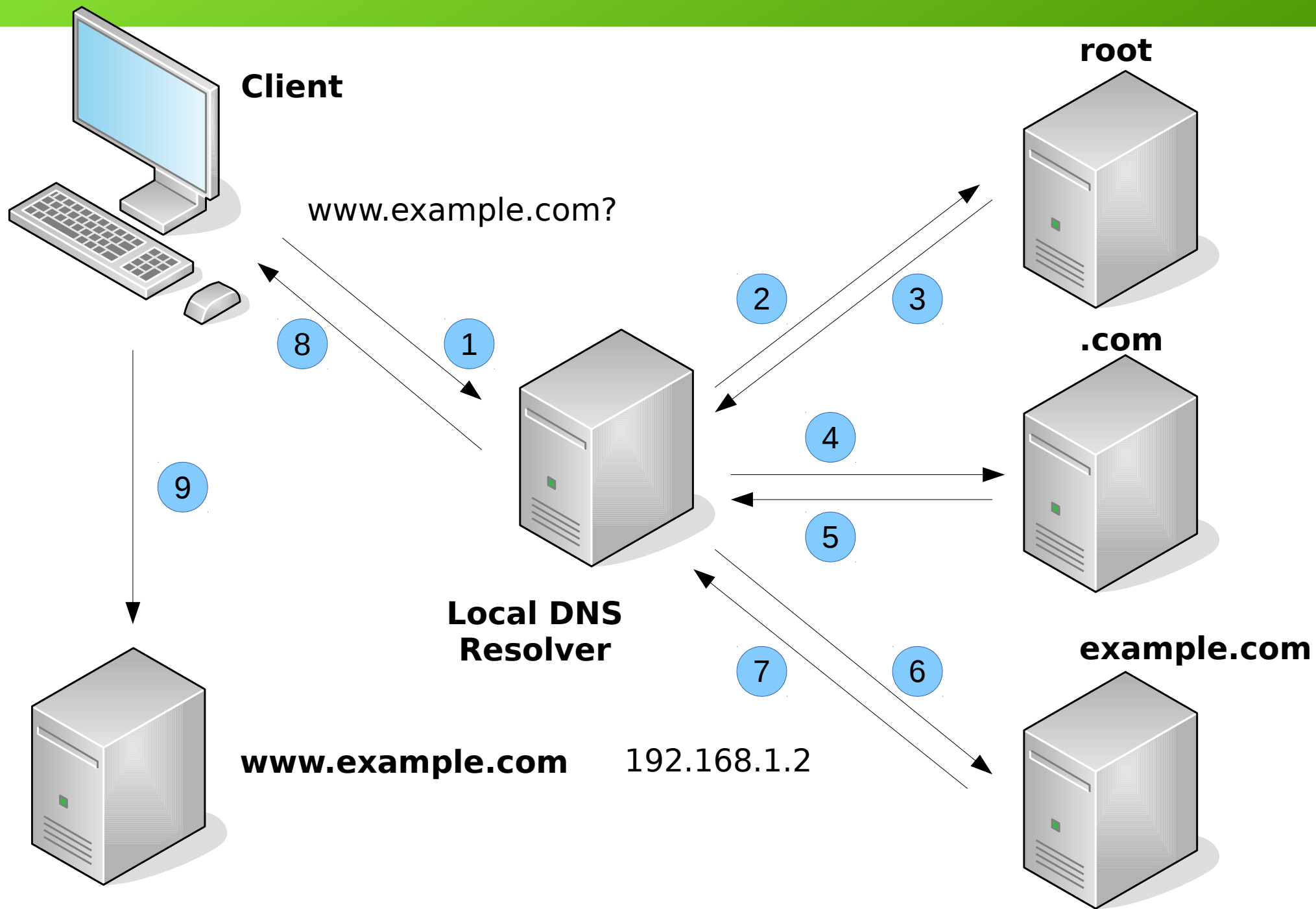
# Why do we need DNS?

- Computers can talk to each other by using the Internet Protocol (IP), relying on IP addresses.
- Humans beings are not very good at working with IP addresses:
  - IPv4 address example: 192.168.44.237
  - IPv6 address example: 2001:0db8::ca45:56b6:20fa
- 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.



# How does DNS work?

- Your computer (the client) asks the local DNS resolver: *“I need to reach example.com do you know his IP address?”*
- If the local resolver doesn't know, then it will ask the root. From the response the resolver will ask other servers, and get a response.
- Then your computer knows where to go.
- All of this in few milli-seconds on average.



# DNS is more than that...

- Other services rely on DNS:
  - Email (including various antispam tools)
  - Server authentication
  - Services localization
  - ...
- And there is DNSSEC: cryptography is used to check on data authenticity: a local resolver can check a signature to verify that is the real thing. This require DNSSEC-aware systems.

# What are the limits?

- It is possible to attack 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.
- **Breaking news: NSA MoreCowBell**



# Some solutions

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

# And if I want to have my own domain name?

- Contact a Domain Name Registrar, and you should be able to register a domain name for a fee, and for a specific time period.
- A domain name doesn't give you any service by itself: you will still need to contact a hosting provider to run a mail server, a web server, etc. (many companies provide a registration service with hosting services).

# Resources

- **DNS for Rocket Scientists**  
<http://www.zytrax.com/books/dns>
- **Google Public DNS Servers**  
<https://developers.google.com/speed/public-dns>
- **Google Apps Toolbox**  
<https://toolbox.googleapps.com/apps/dig>
- **Unbound**  
<http://www.unbound.net/>

# Resources

- Extensions for Mozilla Firefox:
  - **Domain Details**
  - **DNSSEC/TLSA Validator**
- <https://addons.mozilla.org/>

- This presentation has been created with LibreOffice 4.3.5.
- Fonts:
  - *Source Sans Pro Semibold* for the titles
  - *DejaVu Sans* for the text
- Icons from *VRT Systems*:

<http://www.vrt.com.au/downloads/vrt-network-equipment>