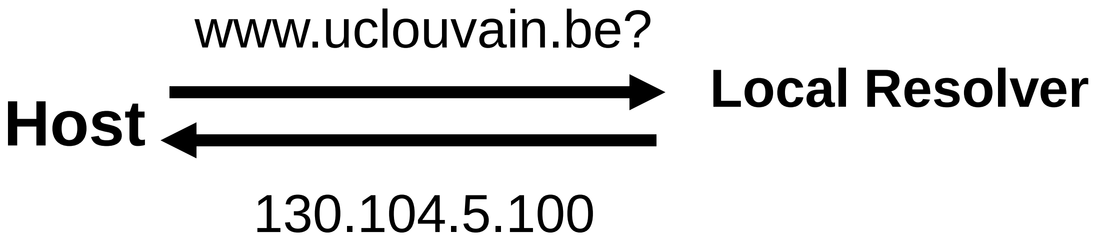
How does DNS work?

Resolving a name: Simple case



www.uclouvain.be?

Host

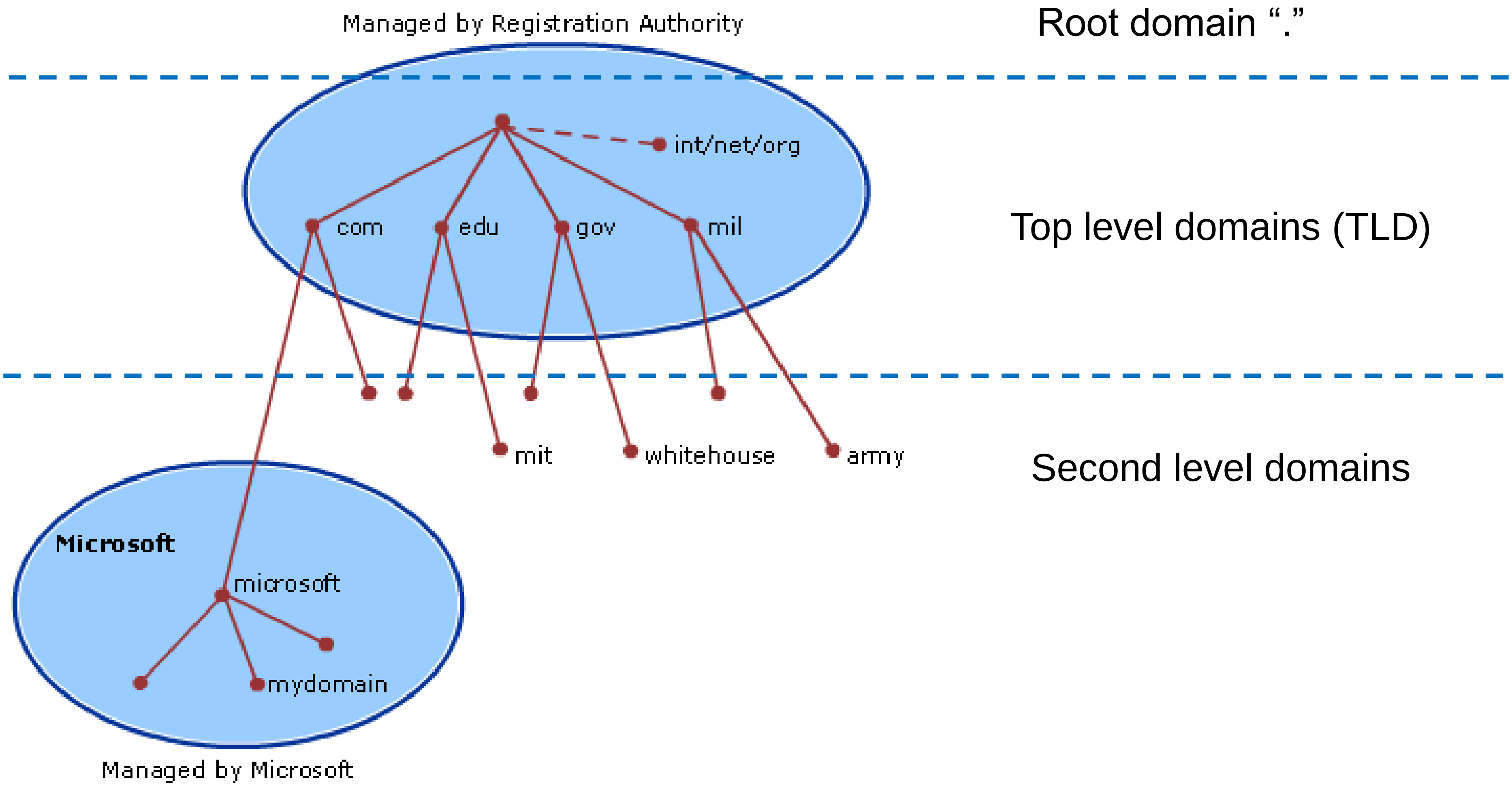
Local Resolver

130.104.5.100

- The client queries the *A Resource Record* (IPv4 address) or the *AAAA Resource Record* (IPv6 address) of the name
- This only works if the Local Resolver knows the answer

DNS

- DNS is a hierarchical distributed database



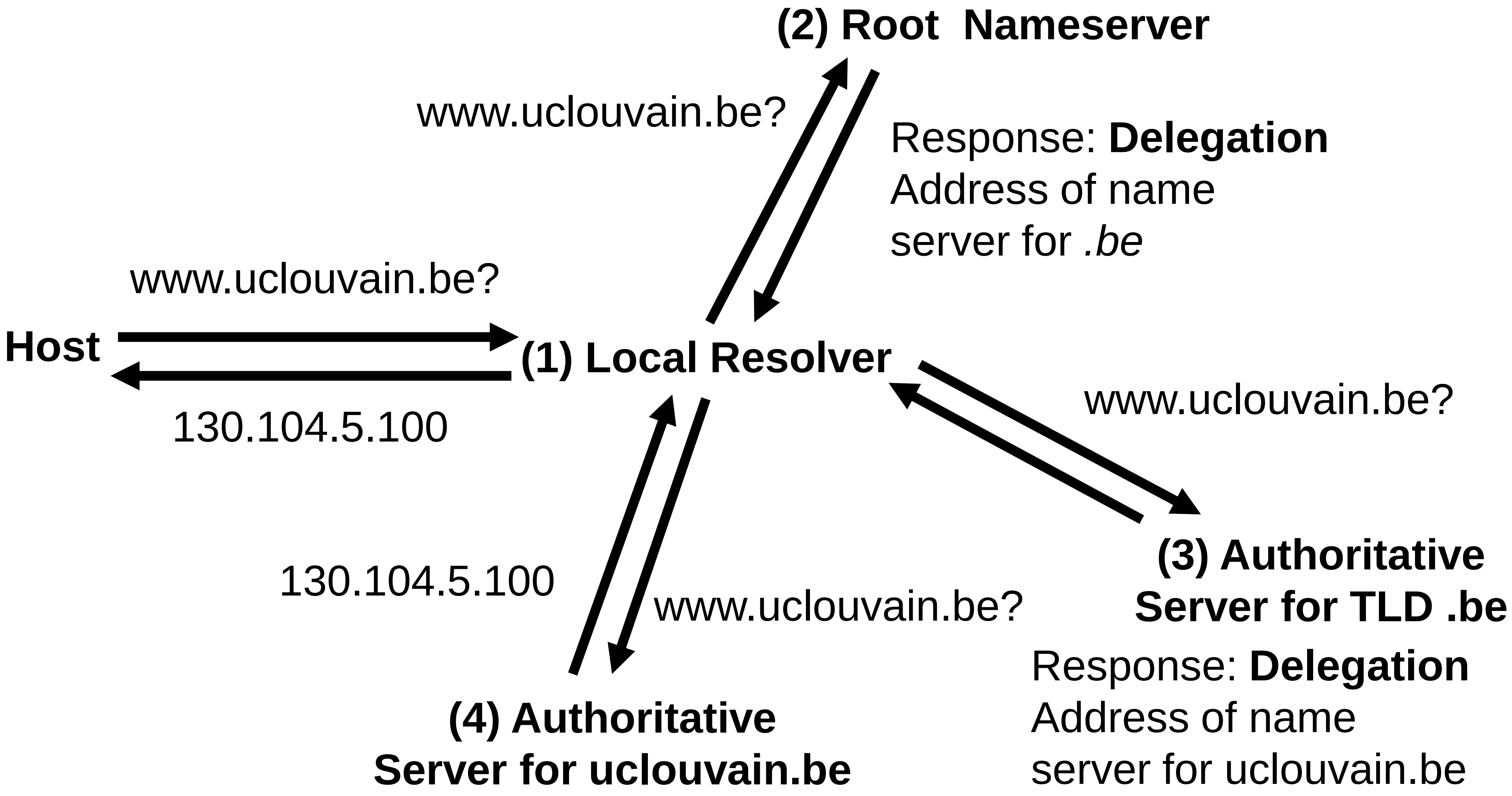
Root domain "."

Top level domains (TLD)

Second level domains

Source: Microsoft

Recursive DNS Query



(2) Root Nameserver

www.uclouvain.be?

Response: **Delegation**
Address of name
server for *.be*

www.uclouvain.be?

Host

(1) Local Resolver

130.104.5.100

www.uclouvain.be?

(3) Authoritative
Server for TLD .be

130.104.5.100

www.uclouvain.be?

Response: **Delegation**
Address of name
server for uclouvain.be

(4) Authoritative
Server for uclouvain.be

Root Nameservers

- There a 13 root nameservers: A – M
- See https://en.wikipedia.org/wiki/Root_name_server for the complete list
- The root nameservers have a database (*root zone file*) with the IP addresses of the authoritative DNS servers for all TLDs

https://www.iana.org/domains/root/db

https://www.iana.org/domains/root/files

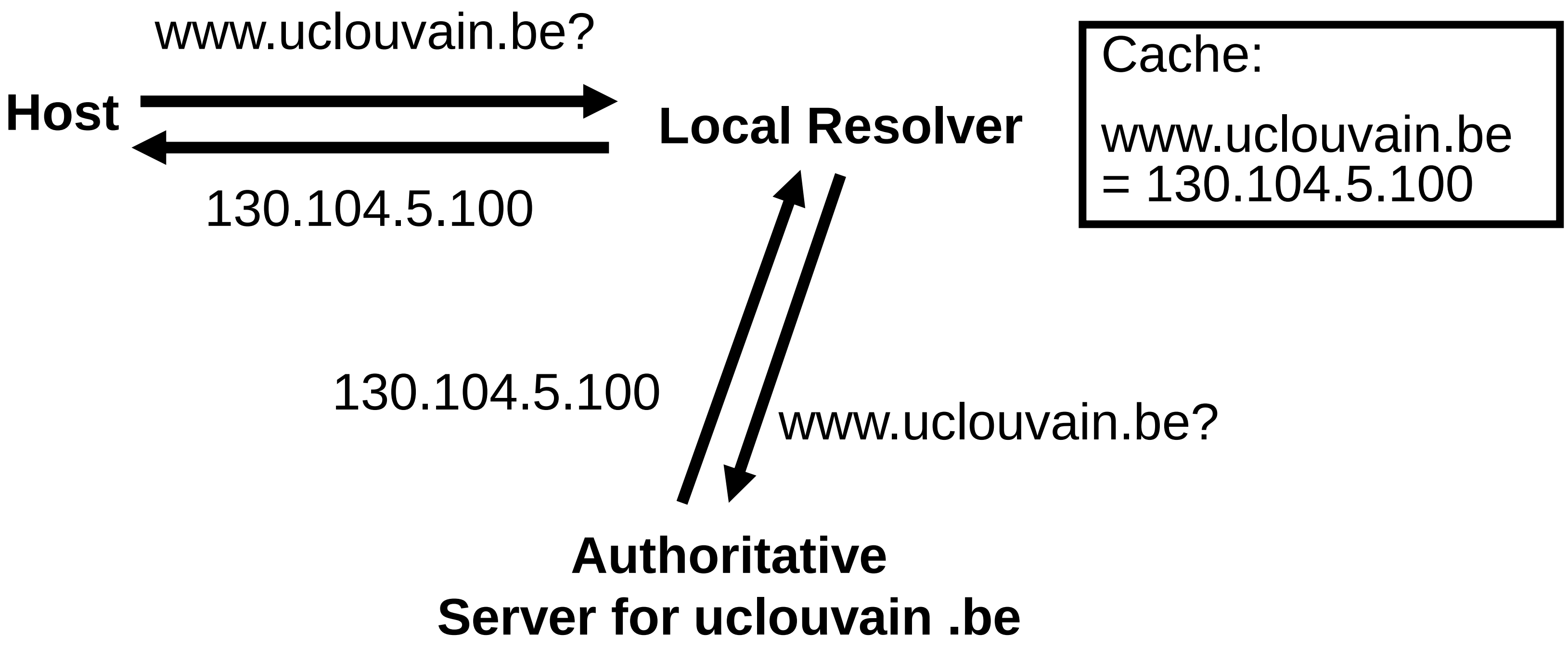
Root Nameservers (2)

- Of course, there are more than 13 physical root servers
  - The servers are locally replicated in the datacenter
- In addition, *Anycast* is used to *geographically* replicate
  - (Started around 2003)
  - There are several servers with the *same* IP address distributed over the world
  - Routers typically forward traffic to the closest copy

- Example: the K-root server (managed by RIPE NCC in Amsterdam)
  https://www.ripe.net/analyse/dns/k-root/

Caching in DNS

- To improve performance, the results of recursive DNS queries are cached in local resolvers
- DNS records have a Time-To-Live (TTL) defined by the authoritative name server. After that time, they are removed from the cache.



Caching in DNS (2)

- Your computer gets the address of the local resolver(s) manually or through DHCP
- Show address of local resolver:
  - Windows ipconfig /all
  - Linux (Ubuntu) nmcli device show eth0
- In addition, your computer can also have a local DNS cache
  - Applications like Firefox and Chrome have their own DNS cache
  - Windows also has one ipconfig /displaydns
    ipconfig /flushdns
  - Linux: no default DNS cache

dig tool

- “dig” is a command-line tool (Linux) to send queries to DNS servers
- Or use
  https://toolbox.googleapps.com/apps/dig/
- Try it
  - Example: use Google’s public DNS server 8.8.8.8

DNS and security

- DNS is essential for the Internet → interesting target for attacks. Possible attacks:

1. Make DNS unusable. Example: DoS attacks
   - Very difficult. The DNS infrastructure is quite robust.
   - On November 30, a DDoS attack was performed on the Root DNS. 5 million queries/s Peak: >35 Gb/s. Impact was moderate.
2. Try to modify the information in the DNS database. Example: Cache Poisoning

- As we have seen DNS can be also used to attack other hosts (DDoS+amplification)