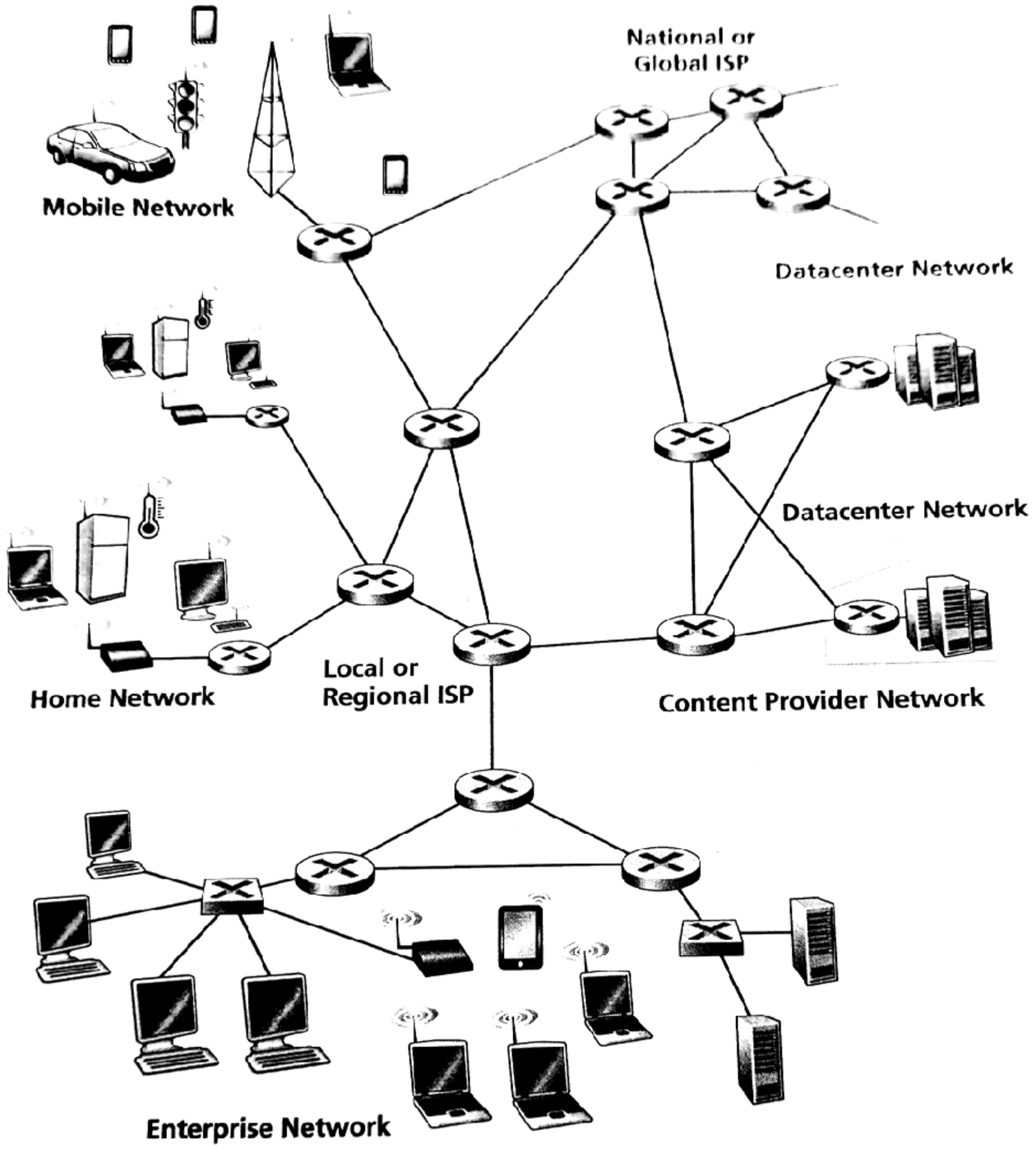


INF105 - 15
DNS

David Grellscheid

Internet er et nettverk av nettverk



Kurose/Ross,
"Computer Networking,
a top-down approach",
Pearson 2022

5-layer model

- **Application**: **HTTP**, SMTP, FTP, SSH, DNS
  lett å lage nye protokoller her
  end system <-> end system
- Transport
- Network
- Link
- Physical

DNS

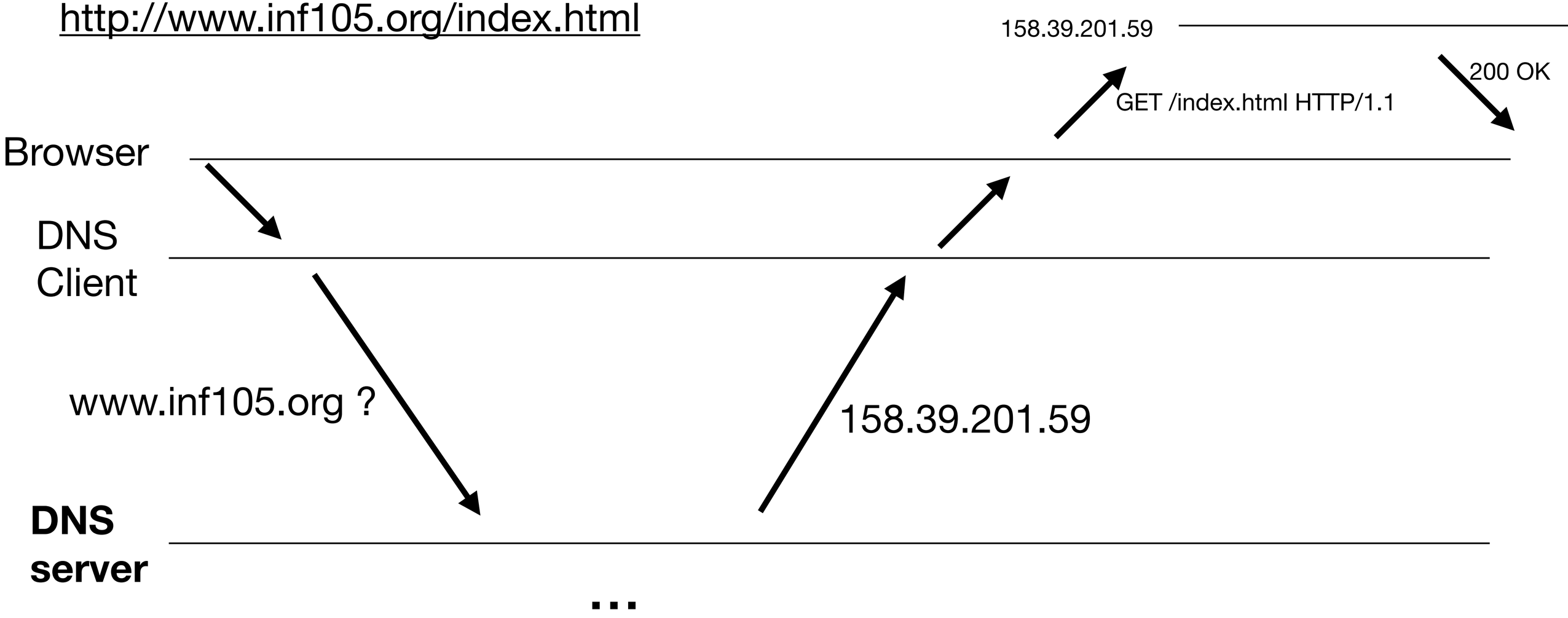
- Domain Name System
- oversetter lesbare navn til IP-adresser
- Uten DNS: kan editere /etc/hosts for å legge inn navn:

  172.66.147.243 foobar.example.com
  0.0.0.0 spamalot.advertising.example.com

- Tidlig i arpanet, mulig å dele hosts-filer / oppdatere manuelt
  skalerer ikke til milliarder av hosts
- må ha en ekstern tjeneste som holder oversikten

DNS

http://www.inf105.org/index.html



DNS - kan ikke sentraliseres

- sentralisert database? **ikke** en god løsning
  - single point of failure - ingen IP lookups når serveren er nede
  - flaskehals - all trafikk må snakke med denne serveren
  - latency - tar lang tid å sende pakke frem og tilbake
  - DB må oppdateres veldig ofte

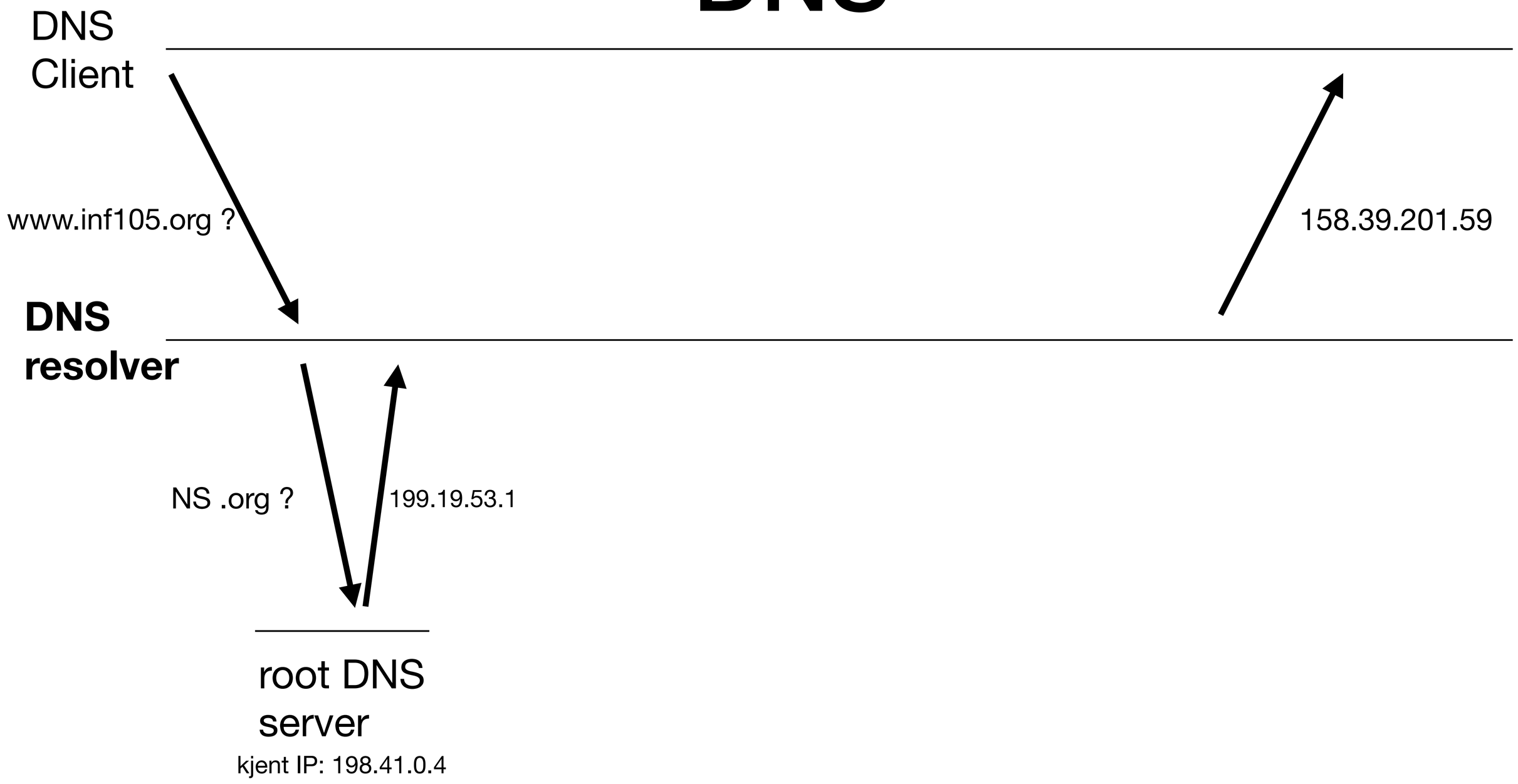
DNS - distribuert database

- distribuert, hierarkisk database
- få titalls Root DNS servers (med kjent IP) som inneholder info om
  - .com DNS server / .org DNS server / .no DNS server / ...
    - hver av disse har info om **sitt** neste nivå:
      DNS server til inf105.org, til uib.no, ...
      - DNS server til inf105.org vet om IP til www.inf105.org

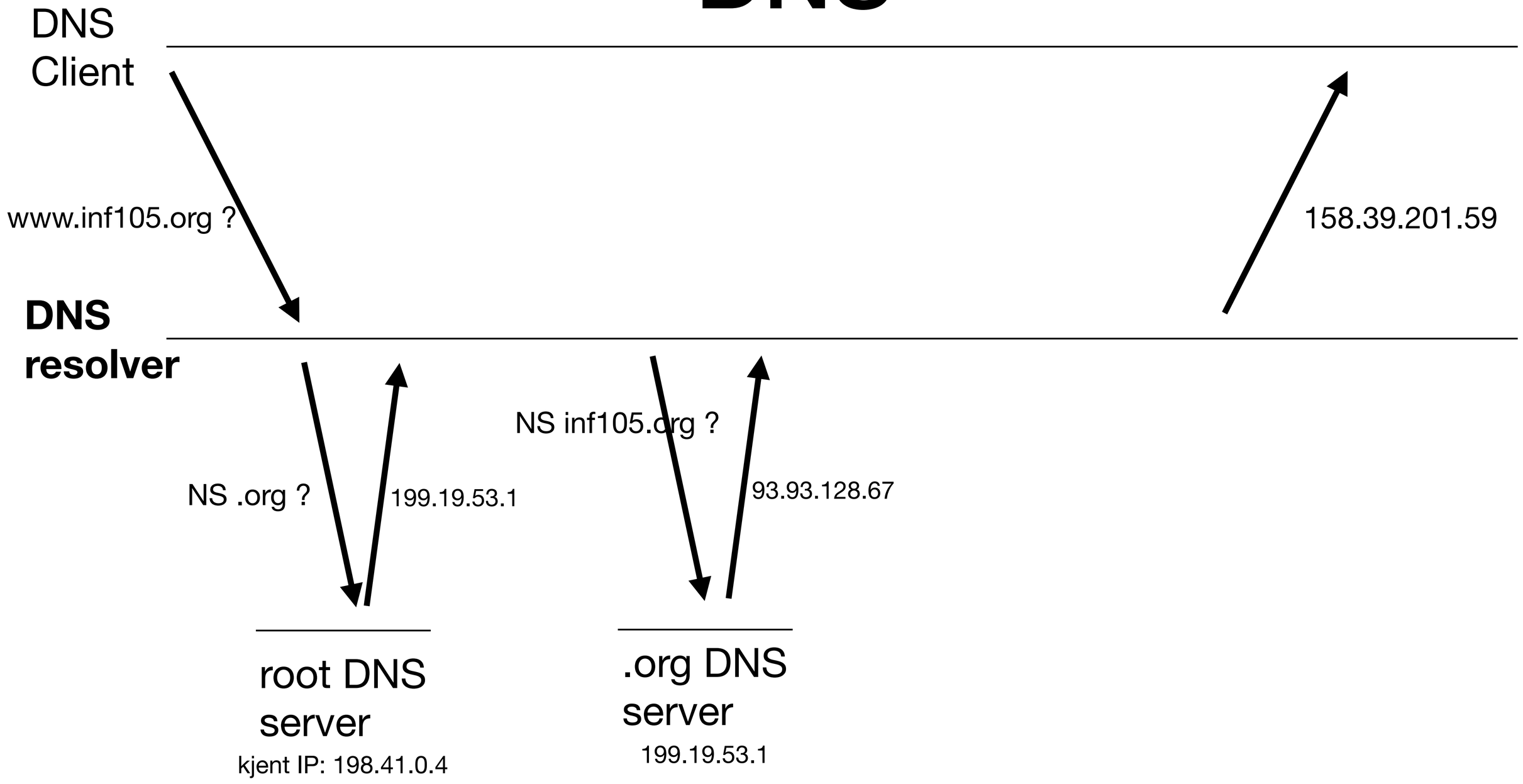
DNS



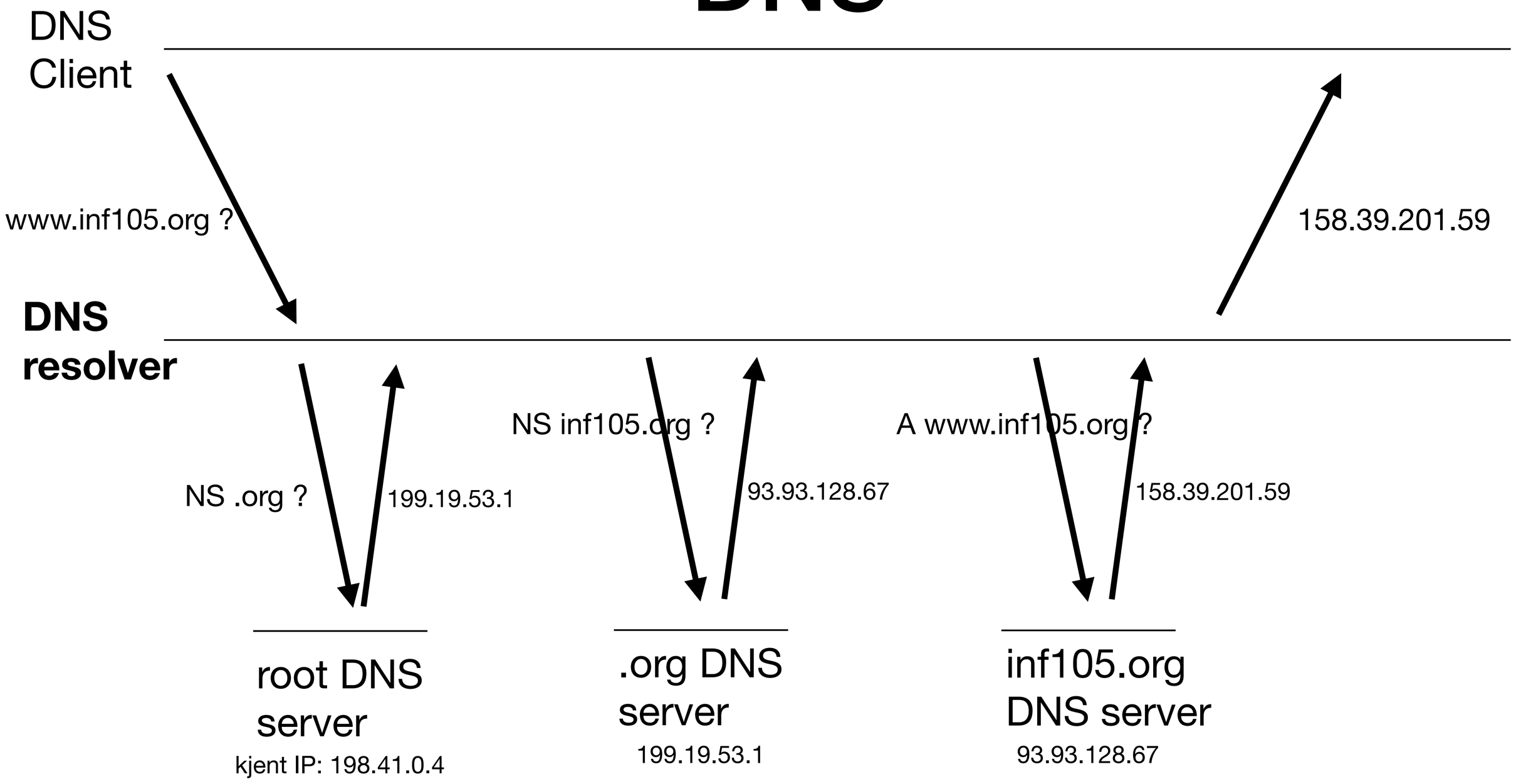
DNS


DNS
Client
www.inf105.org ?
158.39.201.59
DNS
resolver
NS .org ?
199.19.53.1
root DNS
server
kjent IP: 198.41.0.4

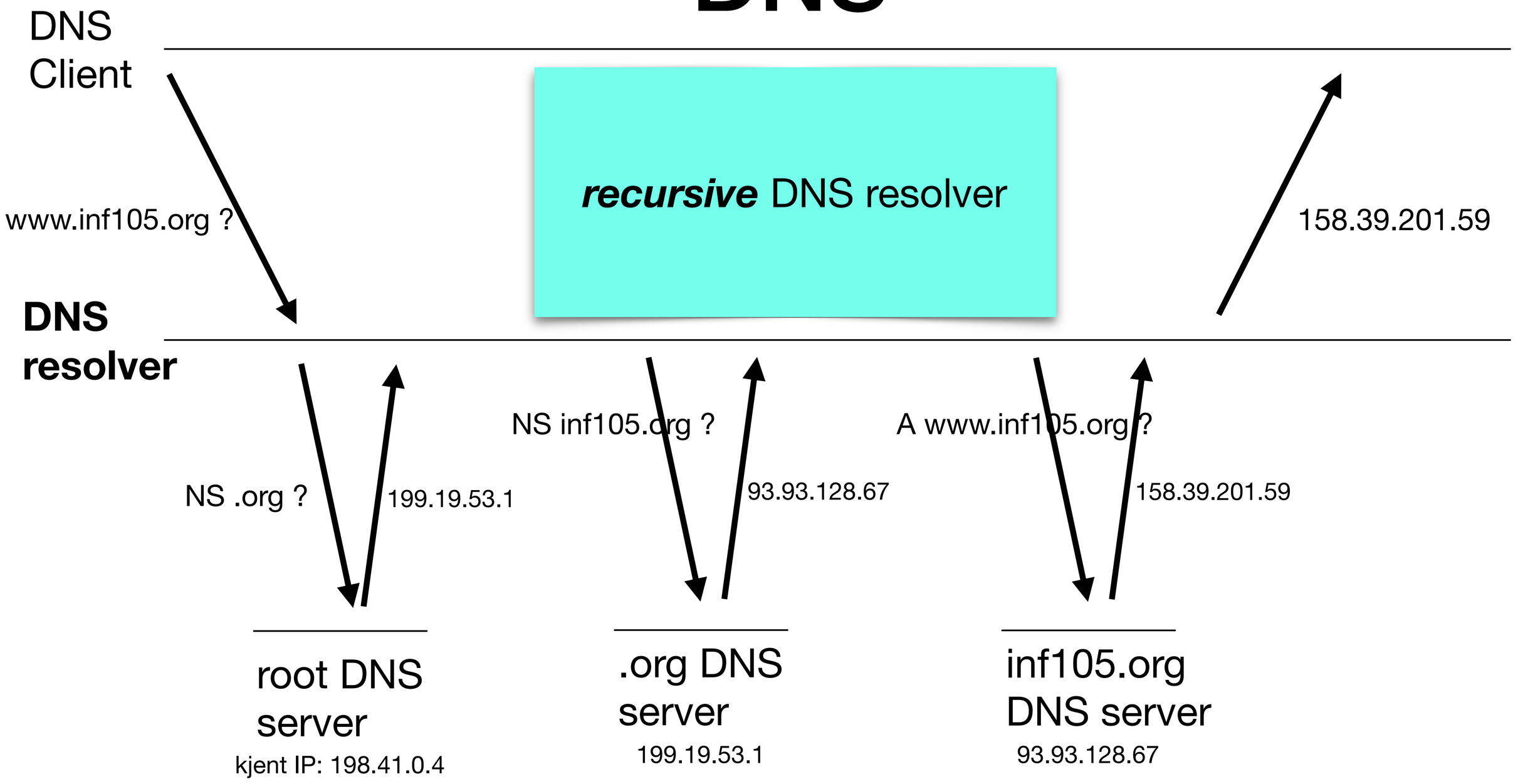
DNS


DNS
Client
www.inf105.org ?
158.39.201.59
DNS
resolver
NS .org ?
199.19.53.1
NS inf105.org ?
93.93.128.67
root DNS
server
kjent IP: 198.41.0.4
.org DNS
server
199.19.53.1

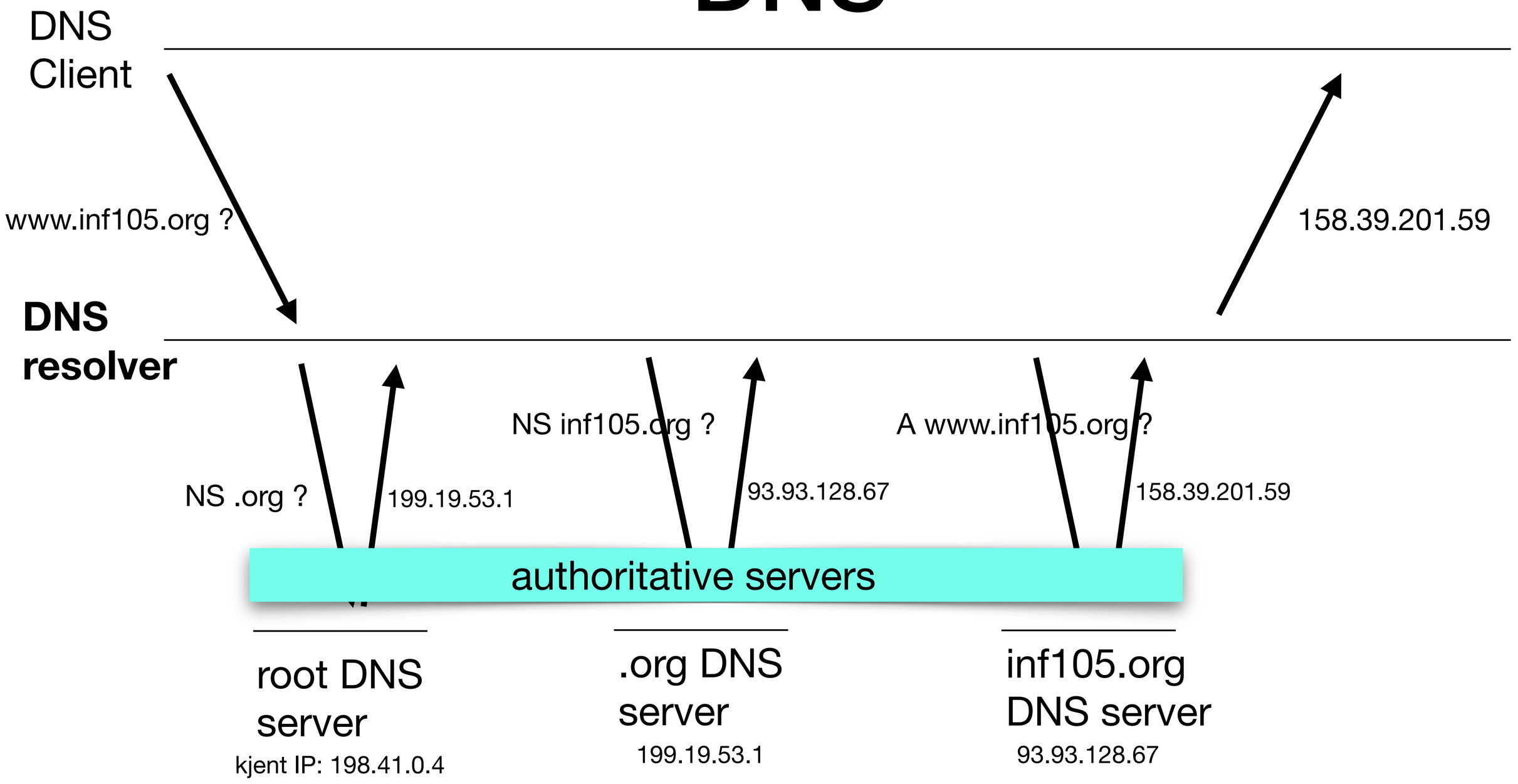
DNS


DNS
Client
www.inf105.org ?
158.39.201.59
DNS
resolver
NS .org ?
199.19.53.1
NS inf105.org ?
93.93.128.67
A www.inf105.org ?
158.39.201.59
root DNS
server
kjent IP: 198.41.0.4
.org DNS
server
199.19.53.1
inf105.org
DNS server
93.93.128.67

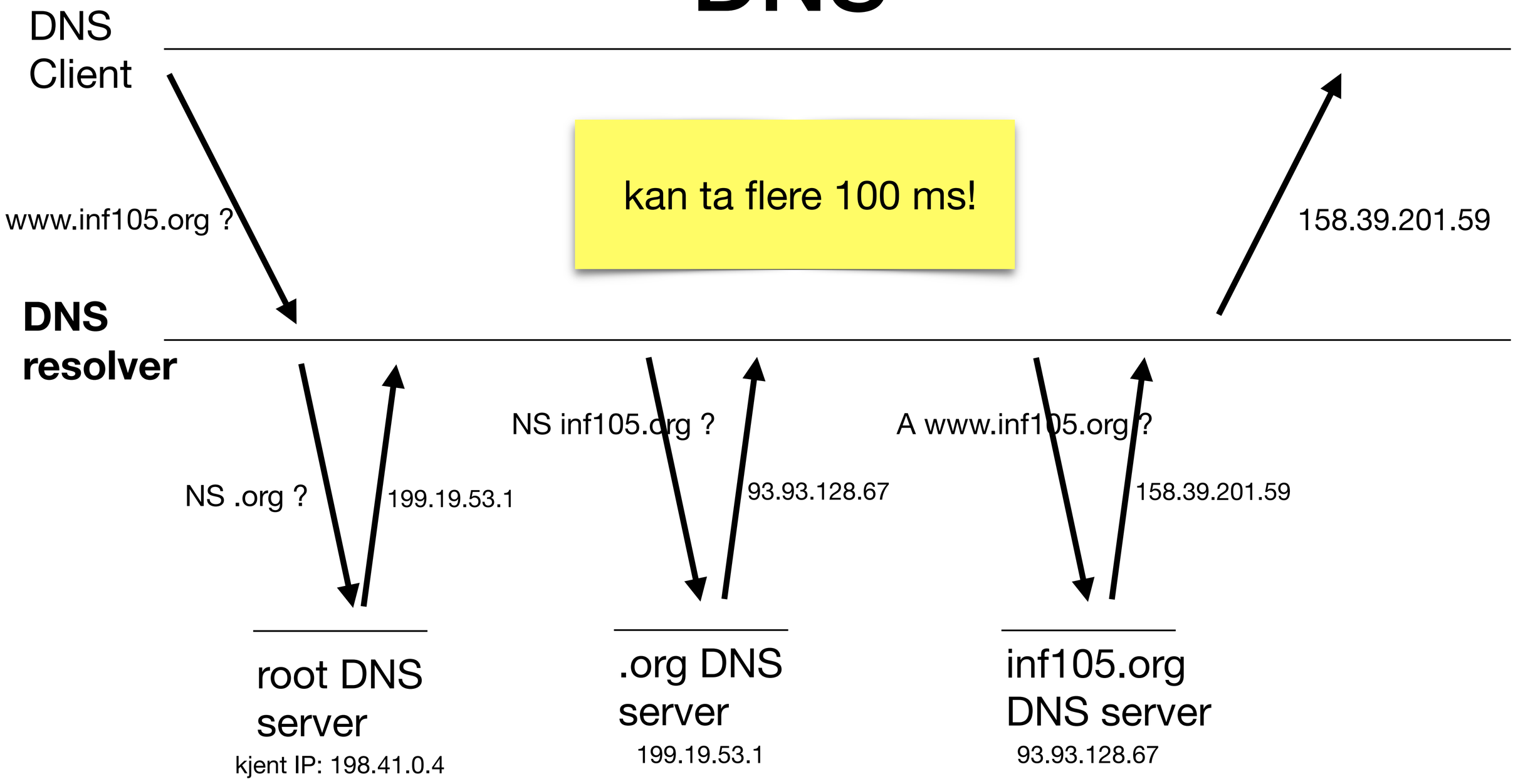
DNS


DNS Client
www.inf105.org ?
recursive DNS resolver
158.39.201.59
DNS resolver
NS .org ?
199.19.53.1
NS inf105.org ?
93.93.128.67
A www.inf105.org ?
158.39.201.59
root DNS server
kjent IP: 198.41.0.4
.org DNS server
199.19.53.1
inf105.org DNS server
93.93.128.67

DNS


DNS Client
www.inf105.org ?
158.39.201.59
DNS resolver
NS .org ?
199.19.53.1
NS inf105.org ?
93.93.128.67
A www.inf105.org ?
158.39.201.59
authoritative servers
root DNS server
kjent IP: 198.41.0.4
.org DNS server
199.19.53.1
inf105.org DNS server
93.93.128.67

DNS


DNS Client
www.inf105.org ?
kan ta flere 100 ms!
158.39.201.59
DNS resolver
NS .org ?
199.19.53.1
NS inf105.org ?
93.93.128.67
A www.inf105.org ?
158.39.201.59
root DNS server
kjent IP: 198.41.0.4
.org DNS server
199.19.53.1
inf105.org DNS server
93.93.128.67

DNS Client

www.inf105.org ?

DNS resolver

NS .org ?

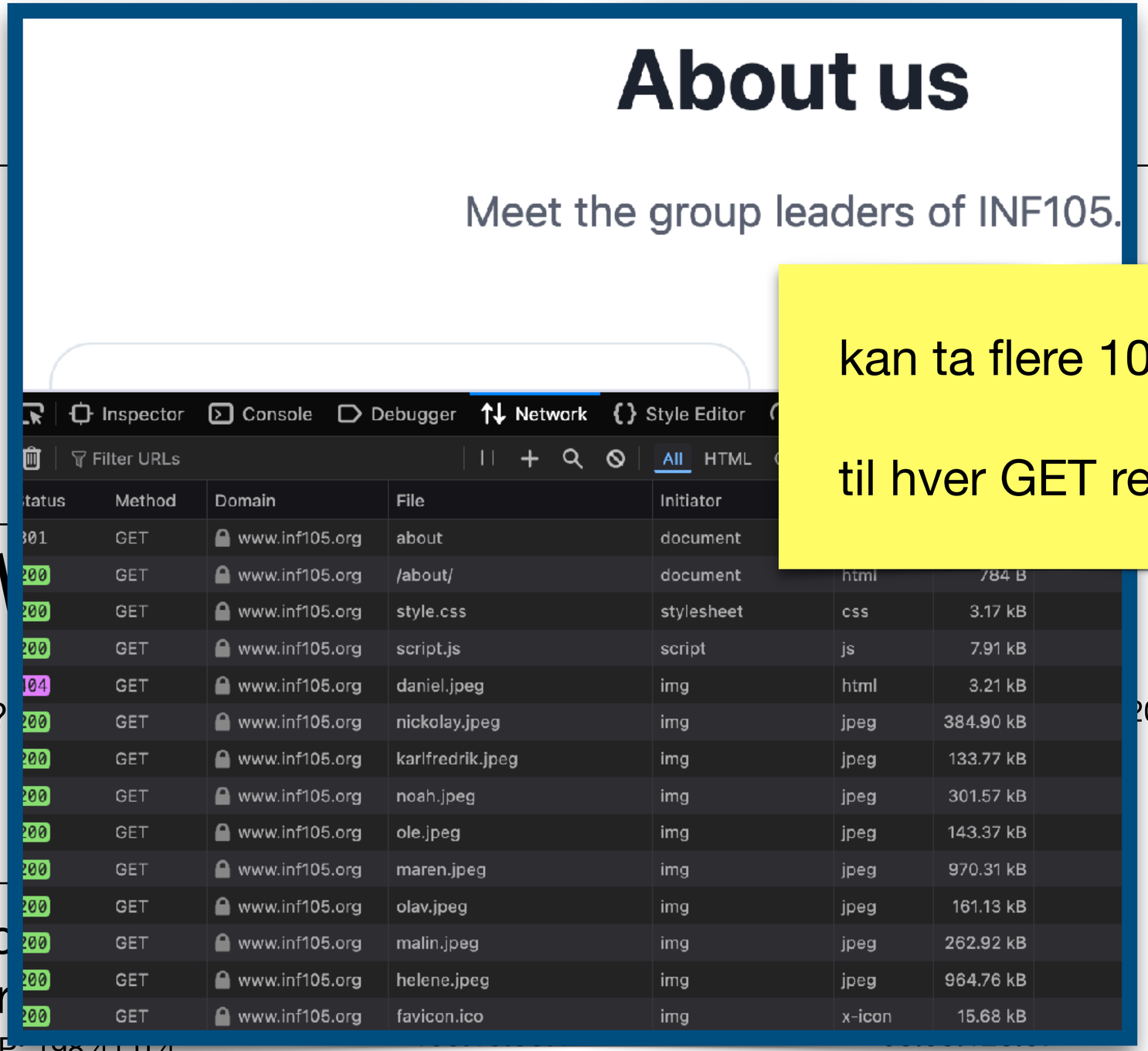
roo

ser

kjent IP: 198.41.0.4

.201.59

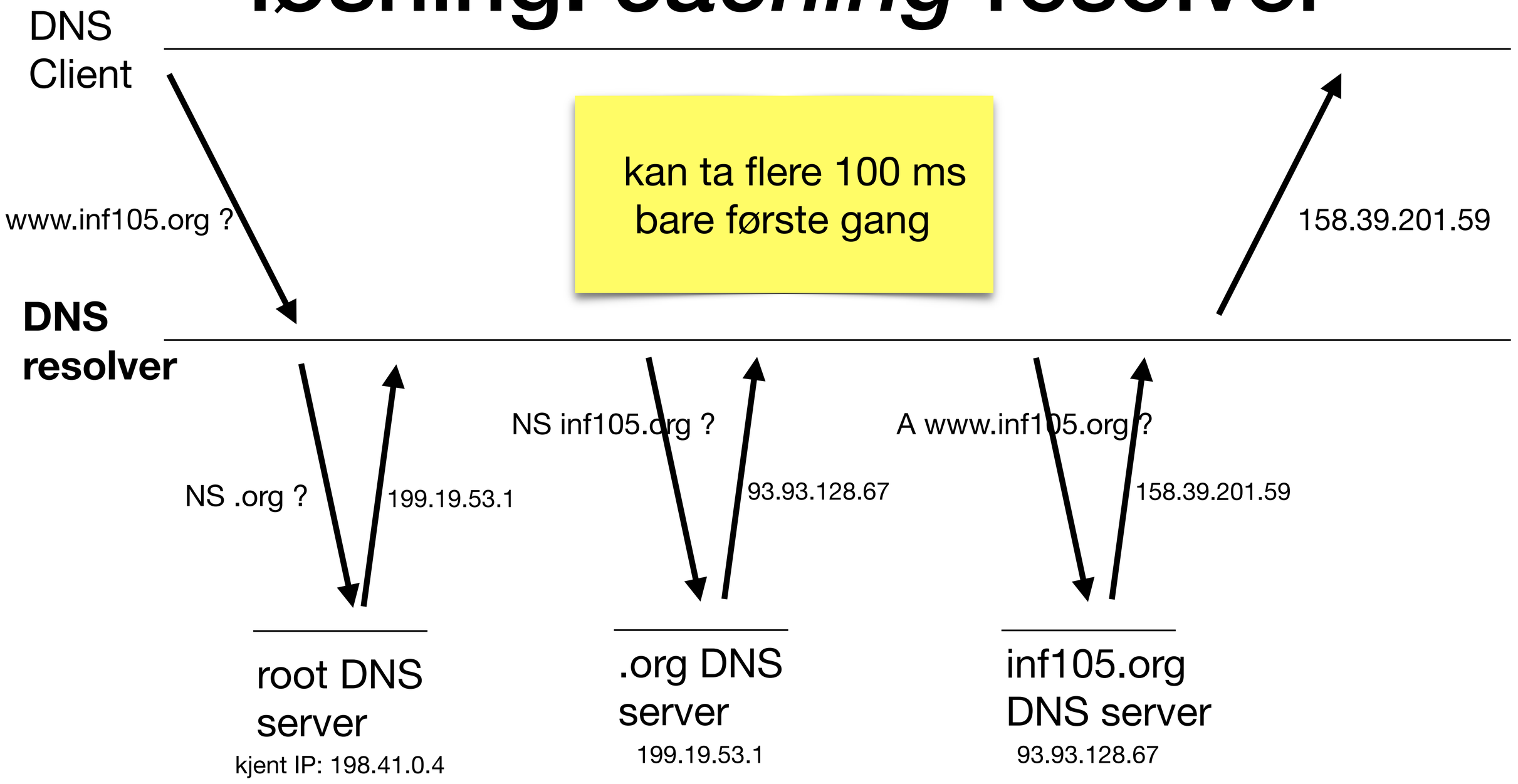
201.59



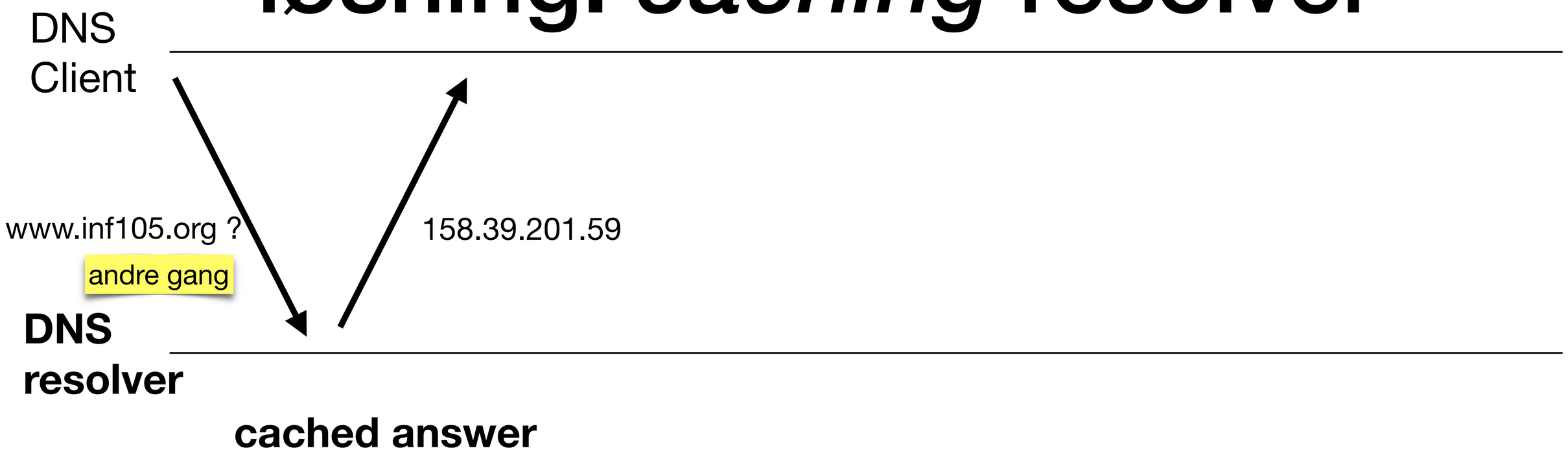
kan ta flere 100 ms!

til hver GET request?

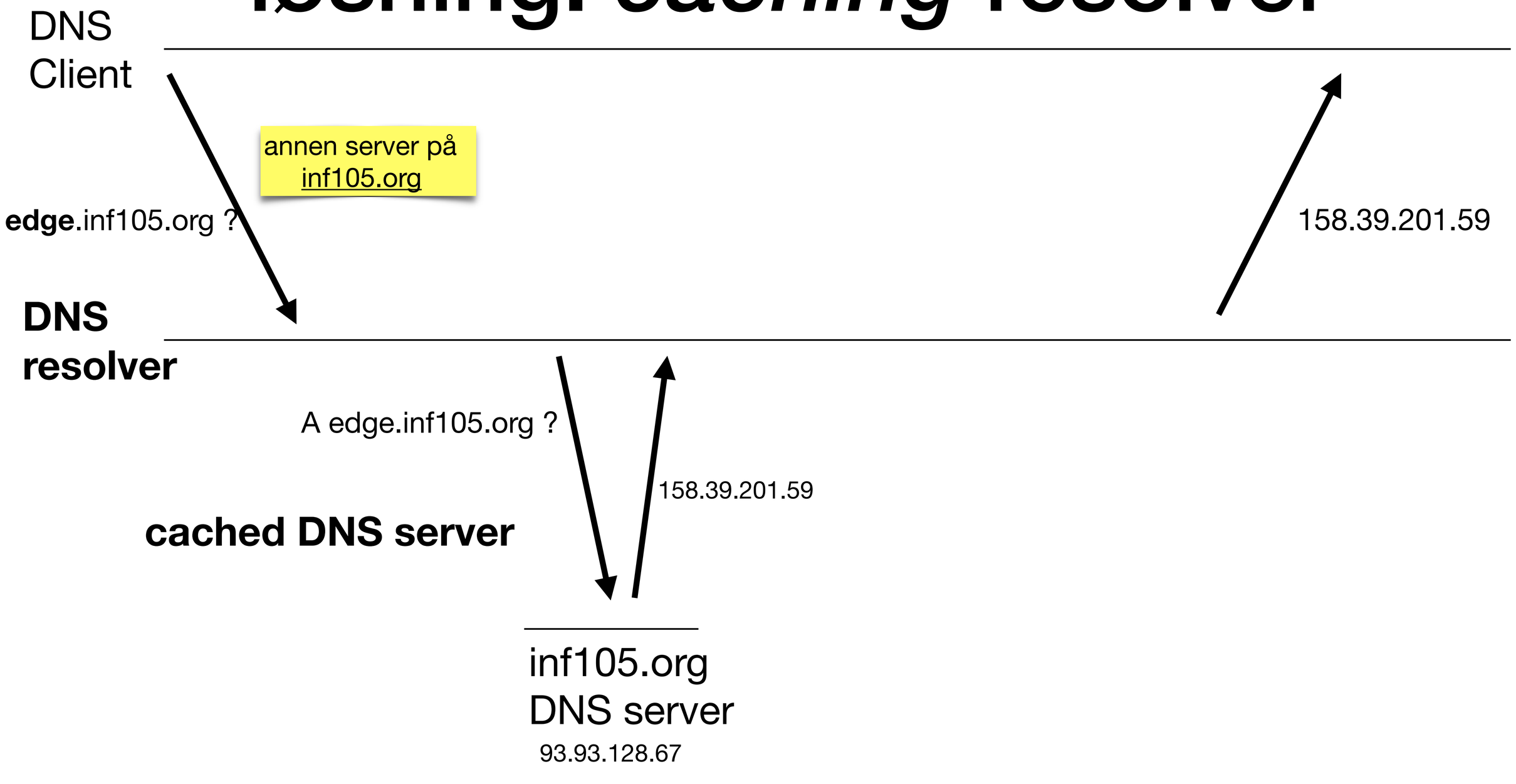
løsning: *caching* resolver



løsning: *caching* resolver



løsning: *caching* resolver



DNS TTL

- Time To Live - hvor mange sekund skal svaret caches?

edge	300	A	158.39.201.59	•••
edge	300	AAAA	2001:700:2:8300::24b8	•••



egen resolver?

- vanlig å bruke ISP sin resolver, forhåndsinstilt i hjemmesentralen / ruter
- mulig å bruke egen til f.eks:
  - reklameblokker - Adguard / PiHole
  - navn til maskiner på hjemmenettverk
  - ...

triks med DNS

- load sharing

  flere IP svar til en domene

- interne nettsider / eksterne nettsider

  ulike svar avhengig av hvilken DNS server er brukt

få info inn i DNS

- hierarkisk organisert i linje med server-strukturen, en **Registrar** deler ut adresser
- ICANN har ansvar for øverste nivået siden 1998:
  - TLD (top-level domain): com, org, net, info
  - restricted TLD: edu, gov, mil
  - mange flere generiske TLD (siden ~2000): aero, kiwi, paris, online, top, ...
- country-code TLD: no, uk, de, fr, tv, me, ly, ... (ISO 3166) med lokale regler:
  - .no - må ha personnummer / bronnøysund-nr.
  - .ac.uk / .co.uk / .me.uk

få info inn i DNS

- ikke vanlig å kjøpe direkte fra ansvarlig registrar
- kan kjøpe et domenenavn fra ulike resellers, konkurrerer på pris, komfort ved oppdateringer, antallet subdomener (burde ikke være begrenset) ...
- Vanlig at reseller kjører authoritative DNS server til din domene, men det burde ikke være begrenset til bare det, kan også gjøre det selv
- Web GUI til reseller (eller egen config fil) har linjer som:

edge	300	A	158.39.201.59	•••
edge	300	AAAA	2001:700:2:8300::24b8	•••

5-layer model

- **Application**: **HTTP**, SMTP, FTP, SSH, DNS
  lett å lage nye protokoller her
  end system <-> end system
- Transport
- Network
- Link
- Physical

DNS-protokoll

- Hvordan ser DNS-pakker ut?
- De fleste protokoll er definert i RFC
  "Request for comments" - de facto standard
- https://www.rfc-editor.org/
- https://www.rfc-editor.org/info/rfc1035/ første DNS-RFC (1987)

eksempler fra RFC1035

2.3.3. Character Case

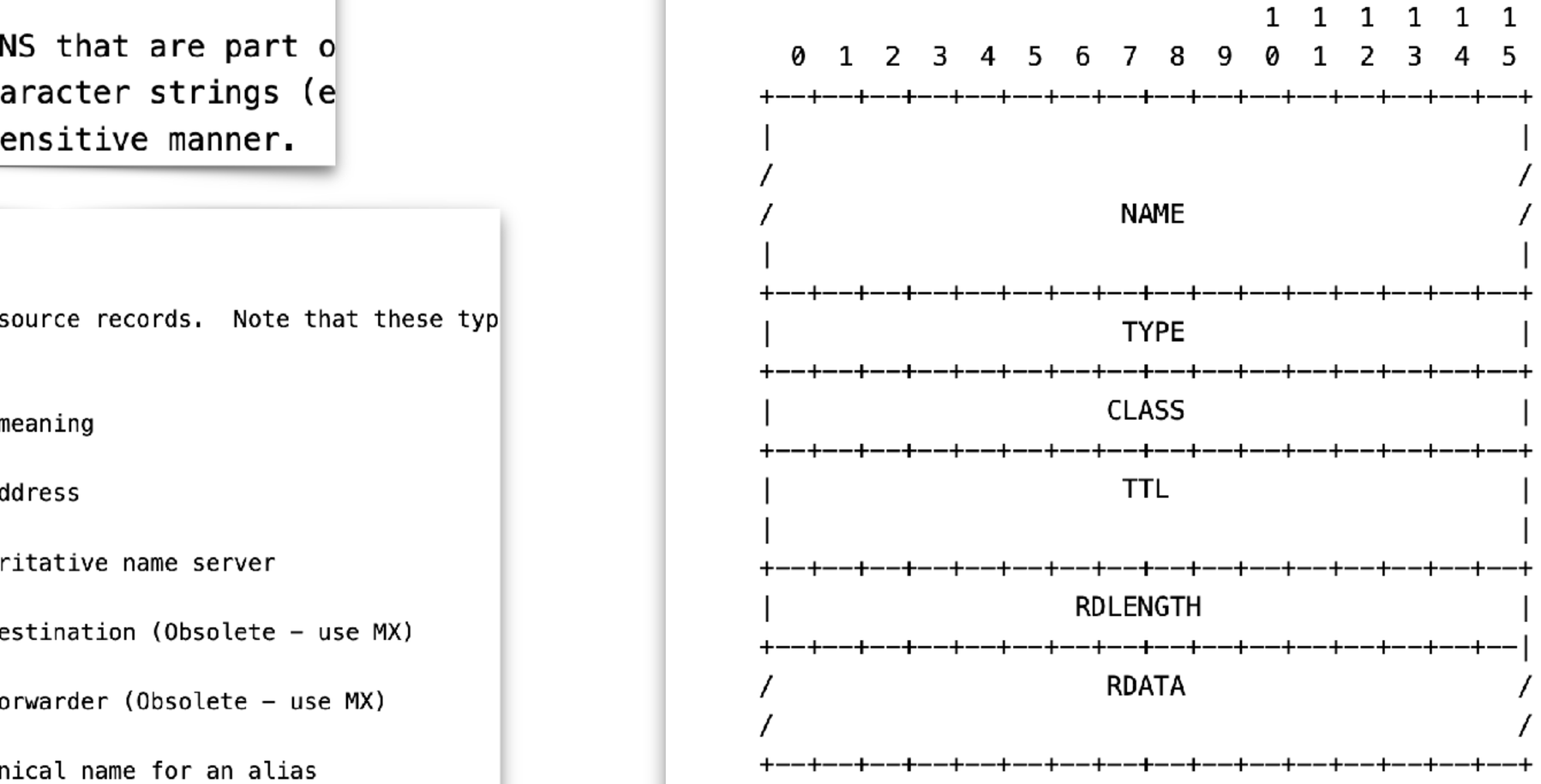
For all parts of the DNS that are part o
comparisons between character strings (e
are done in a case-insensitive manner.

3.2.2. TYPE values

TYPE fields are used in resource records. Note that these typ
subset of QTYPEs.

TYPE	value and meaning
A	1 a host address
NS	2 an authoritative name server
MD	3 a mail destination (Obsolete - use MX)
MF	4 a mail forwarder (Obsolete - use MX)
CNAME	5 the canonical name for an alias

All RRs have the same top level format shown below:



DNS-protokoll

- DNS databasen holder RRs (resource records) knyttet til domenenavn
  - A - IP adresse
  - AAAA - IPv6 adresse
  - CNAME - alias fra en domene til en annen
  - NS - name server til domenen
  - TXT - hva som helst text
  - ...

DNS-protokoll

- En DNS pakke:
  - Header
  - Questions
  - Answers
  - ...

DNS-protokoll

- demo: wireshark with local VM

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- **Transport**: **TCP** (connection) eller **UDP** (connectionless)
  sender "segments" fra end system <-> end system
- Network
- Link
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- **Network**: **IP** (ingen andre valg på Internet)
  sender "datagrams / packets"
  mellom end systems fra en router til den neste
- Link
- Physical

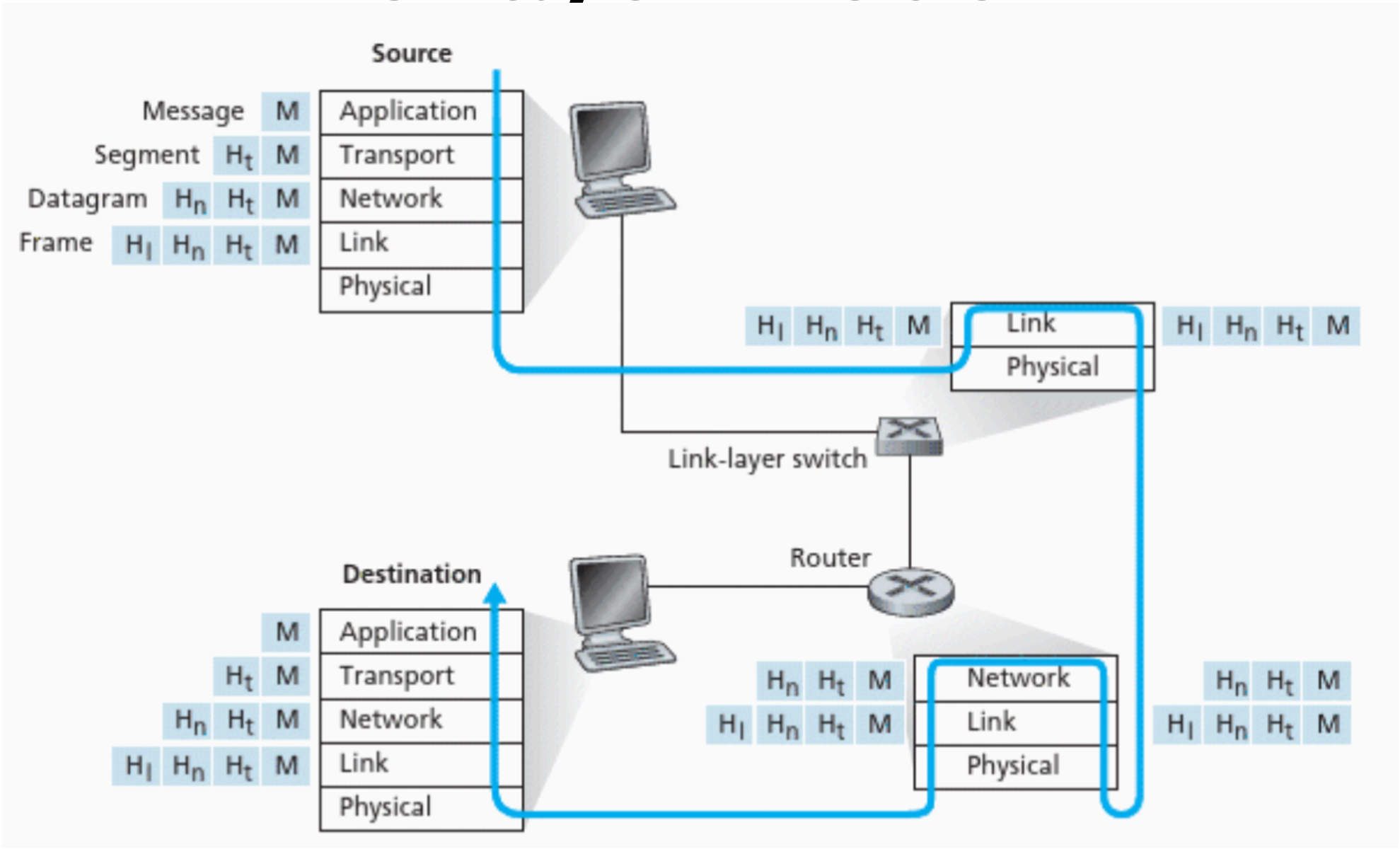
5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: IP
- **Link**: Ethernet, WiFi, PPP
  sender "frames" fra en enhet til den neste
- Physical

5-layer model

- Application: HTTP, SMTP, FTP, SSH, DNS
- Transport: TCP / UDP
- Network: IP
- Link: Ethernet, WiFi, PPP
- **Physical**: elektriske signaler, radiosignaler, ...
  sende bits fra en enhet til den neste

5-layer model



Application layer

- HTTP
- SMTP
- FTP
- SSH
- DNS
- ...
- alle har sin liste med RFC som definerer protokollen