DNS-over-HTTPS and the Rise of Over-the-top DNS: impact on security, performance, autonomy

Madrid.es
DNS server

IP www.madrid.es

Resolver

IP www.madrid.es?

CPE/Router/
Modem/Wifi

IP www.madrid.es?

Computer

Madrid.es
DNS server

88.221.24.7
2

Resolver

88.221.24.7
2

CPE/Router/
Modem/Wifi

88.221.24.7
2

Computer

Madrid.es
DNS server

88.221.24.72

Resolver

https://www.madrid.es/

CPE/Router/
Modem/Wifi

88.221.24.7
2

Computer

“Internet performance is never better than DNS performance”

“Slow DNS: Slow internet.
No DNS: No internet”

“The brave new world of Cloud DNS over HTTPS, where DNS moves to a third party, frequently foreign, by default”

Madrid.es
DNS server

LOGS

~~Resolver~~

IP www.madrid.es

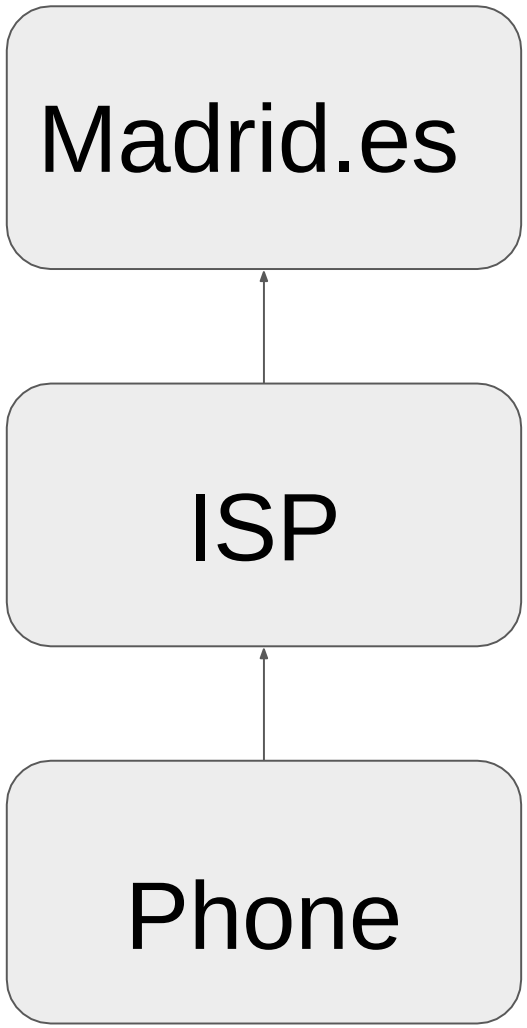
~~CPE/Router/~~
~~Modem/Wifi~~

Cloudflare DNS
over HTTPS

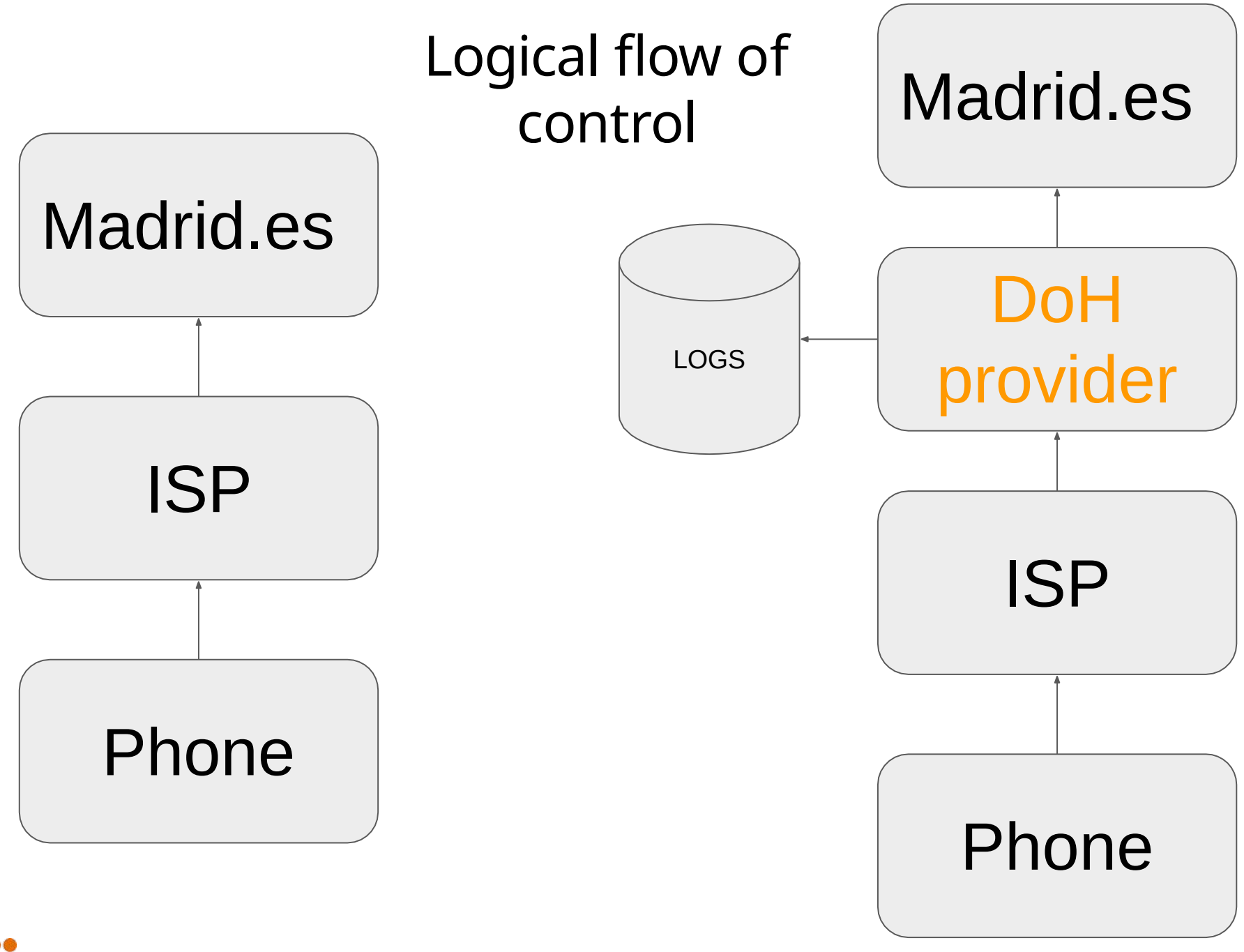
IP www.madrid.es.?

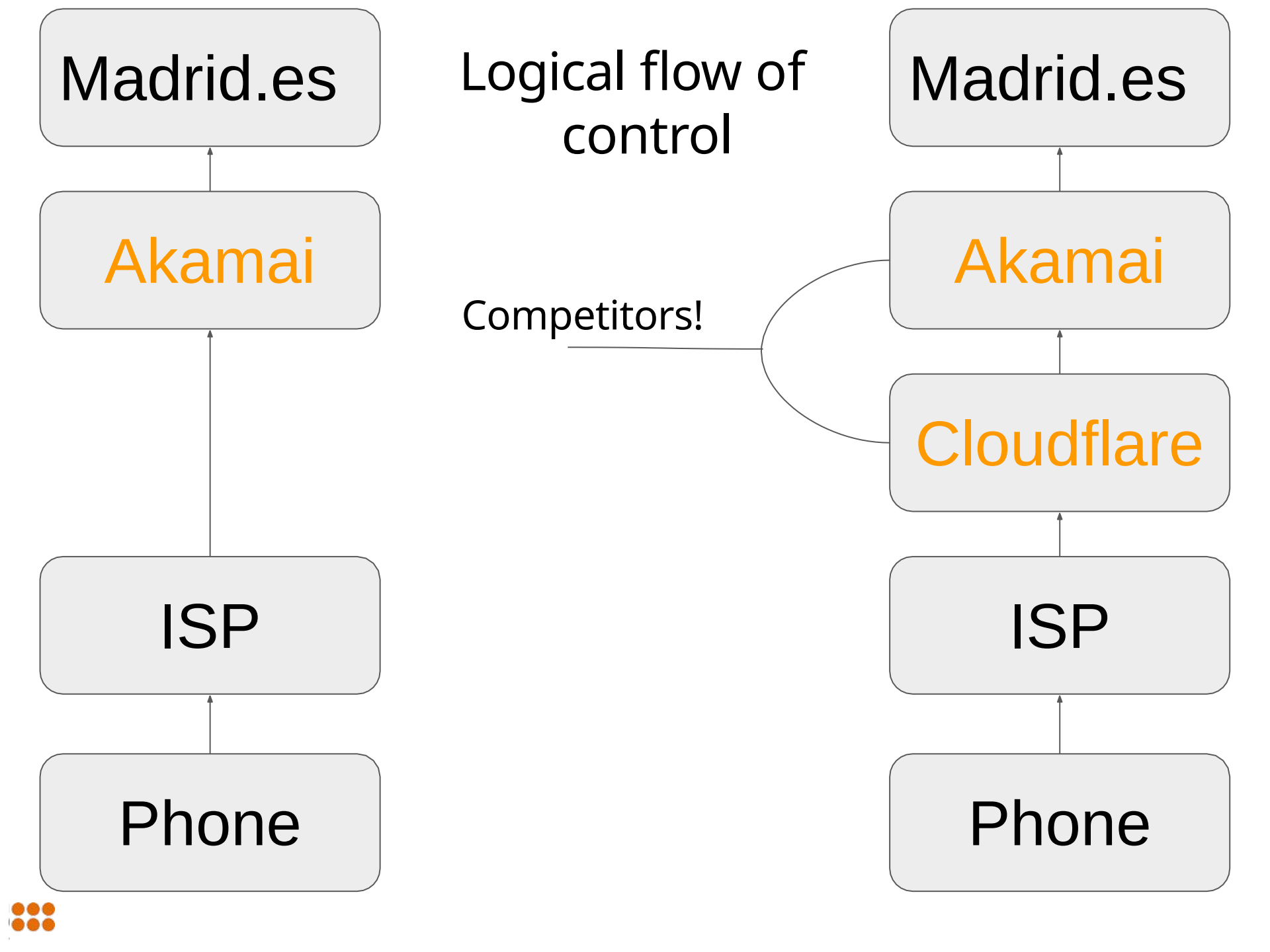
Computer

Logical flow of control



Logical flow of control




Madrid.es
Logical flow of control
Madrid.es
Akamai
Akamai
Competitors!
Cloudflare
ISP
ISP
Phone
Phone

Mozilla / Firefox: Rolling this out by default in the US. No opt-in, **only notification**, all DNS going to Cloudflare. Stated goal: Third party DoH for everyone.

Google / Chrome / Android: Ready for DoT/DoH, will currently only **upgrade** if configured DNS provider offers DoT/DoH. Some mixed messages.

Microsoft /Edge: Will only upgrade if existing nameservers does encryption. Careful approach.

Apple / iPhone / Safari: Unclear. Are working on a sort of ‘TOR for DNS’ standard, but may not be a commercial effort (but research).

WHY?

- Providers supposedly selling traffic data
- NXDOMAIN redirection
- Government blocking
  - Including by oppressive governments like Turkey, Russia, China, Indonesia, Iran
  - But also “governments in general”
- Google fighting for our privacy!

WILL BREAK:

- Local security **monitoring** (botnet outbreaks, spam)
- Local security **filtering** (stopping phishing, malware)
- Local parental control **(*)**
- VPN / Intranets
- CDN performance
- **Your privacy**

Does it help for privacy?

- DNS information is highly privacy sensitive
  - Where you live, work, go to school, medical conditions, sexual preferences etc etc
- Currently in plaintext as: DNS, SNI header, OCSP check, IP address
- After DoH, plaintext in: SNI header, OCSP check, IP address
- **New: Cloudflare, US government**
- Actually makes it *numerically* worse!

"The decision of who to include in (or remove from) Mozilla's Trusted Recursive Resolver (TRR) program is at Mozilla's sole discretion"

https://wiki.mozilla.org/Security/DOH-resolver-policy#Enforcement

Encryption: Good!

Stopping NXDOMAIN redirection: Good!

Centralising all DNS: Bad!

DNS-over-HTTPS and the Rise of Over-the-top DNS