



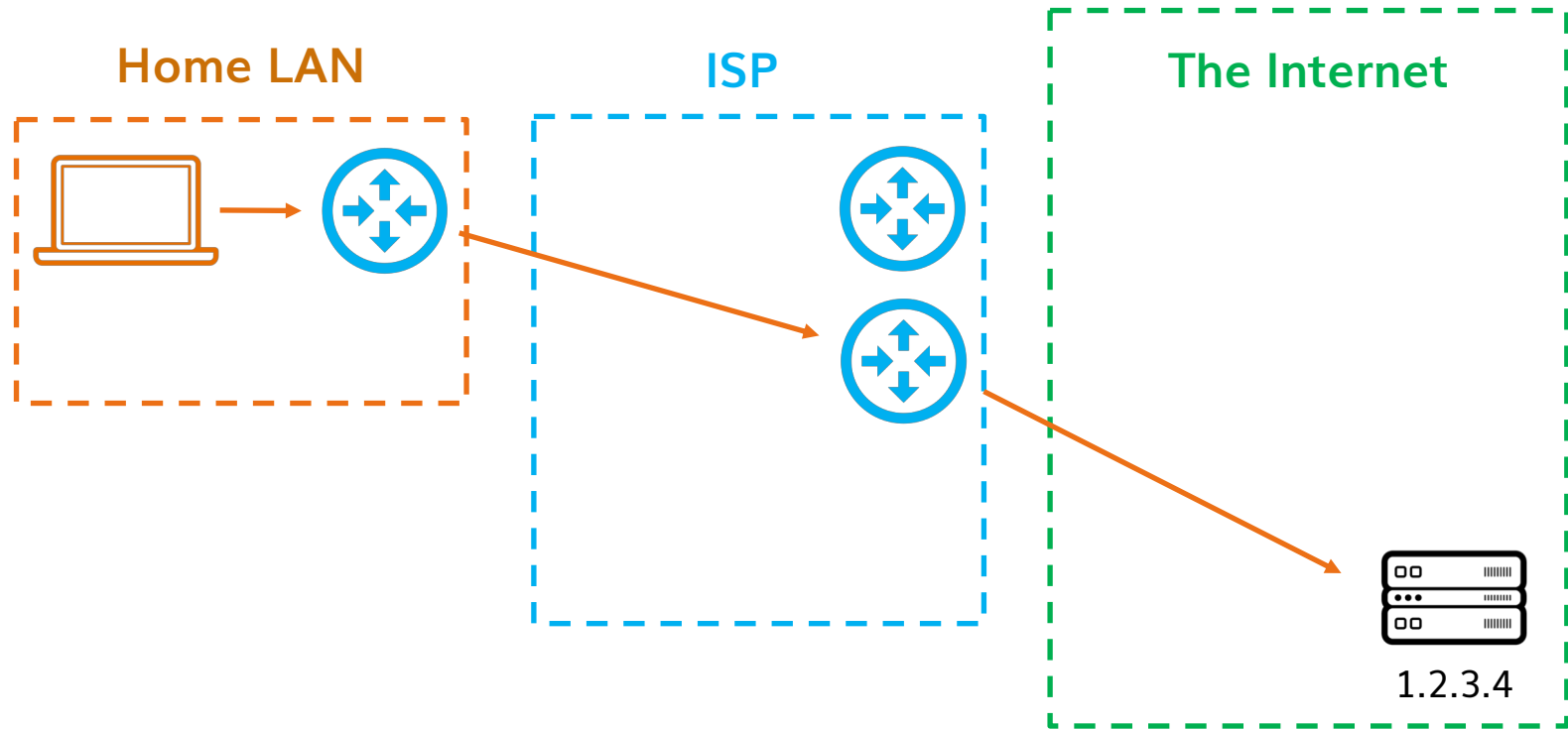
# The DoH dilemma

Impacts of DNS-over-HTTPS on  
how the Internet works

*Vittorio Bertola, FOSDEM 2019*

# 1.

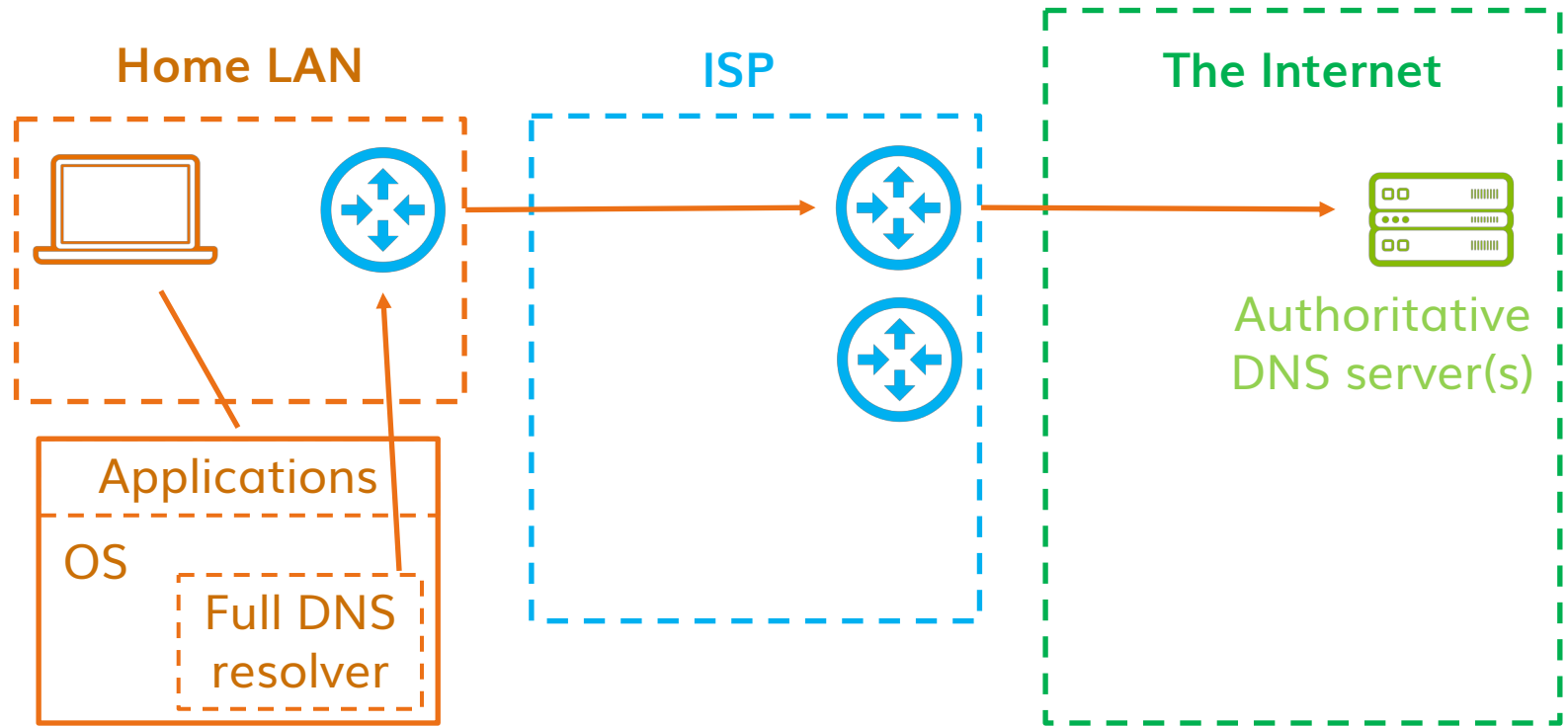
Where is my  
DNS?



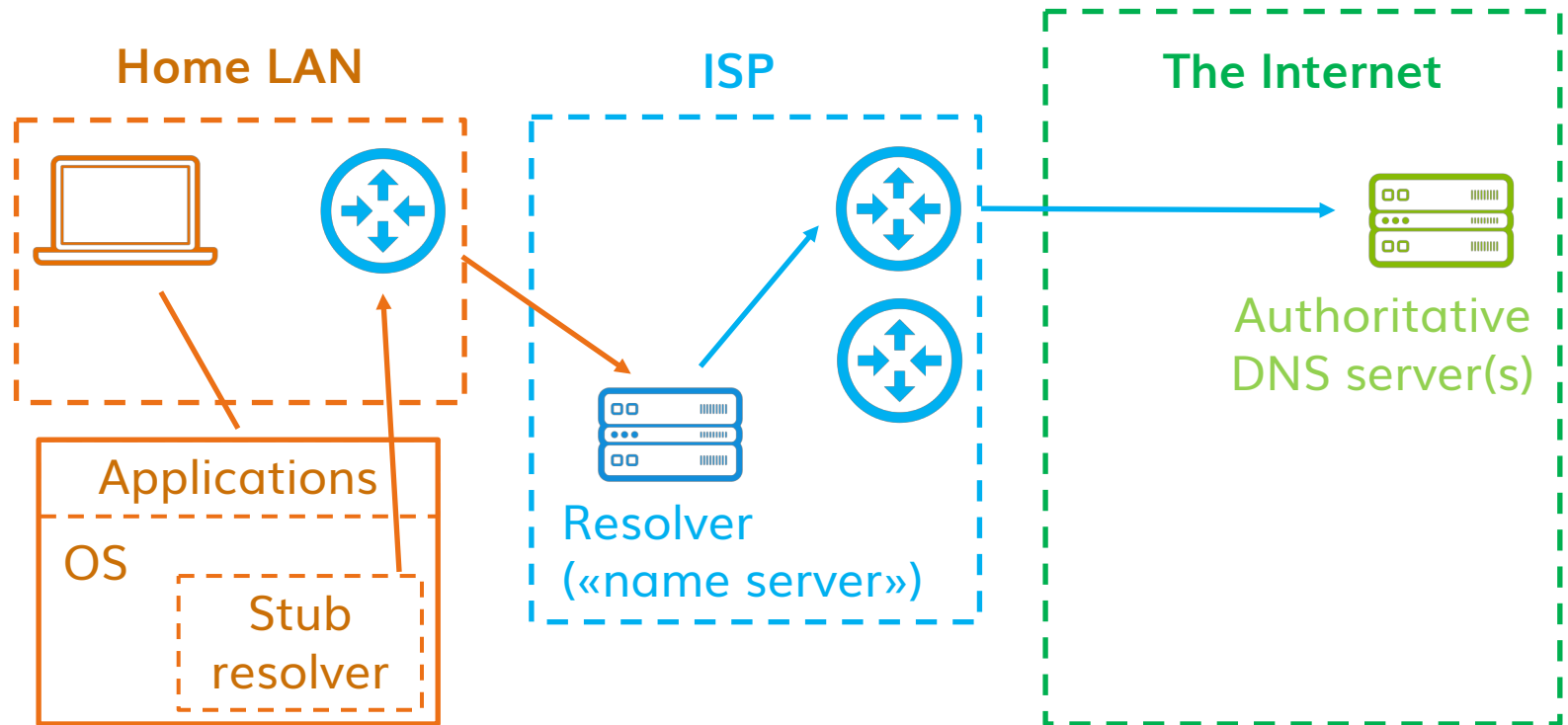
*Connection by IP address*

“

*Hey! I don't like addresses,  
I want to use names!*



*On-device DNS resolution*



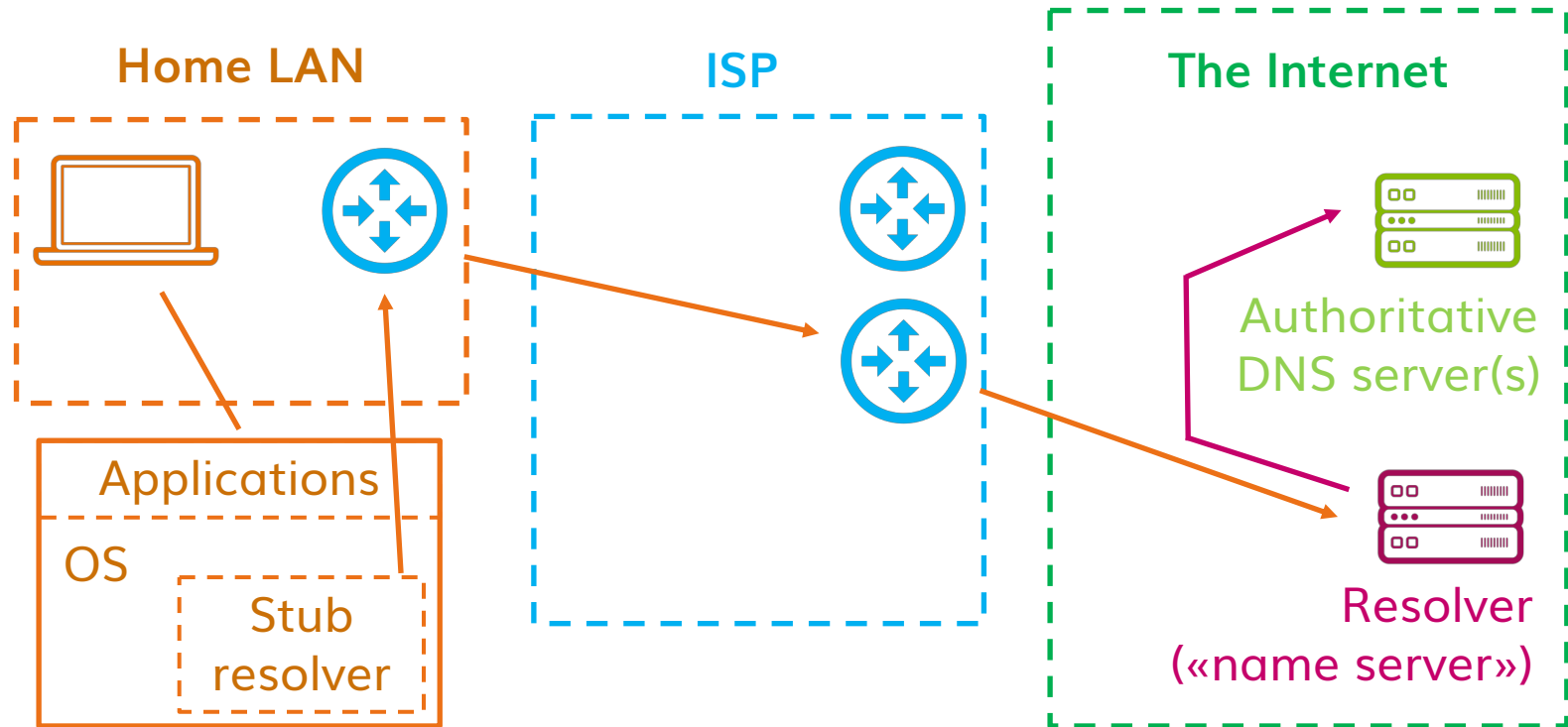
*Local DNS resolution*

# Why «local»?

The ISP's network is the first that you traverse to get to the Internet, no matter where you go

The ISP is normally in the same country, usually in the same city

- ❑ Same jurisdiction
- ❑ Same language
- ❑ Maybe they suck, but you know how to reach them



*Remote DNS resolution*



# Why «remote»?

It is topologically distant from you

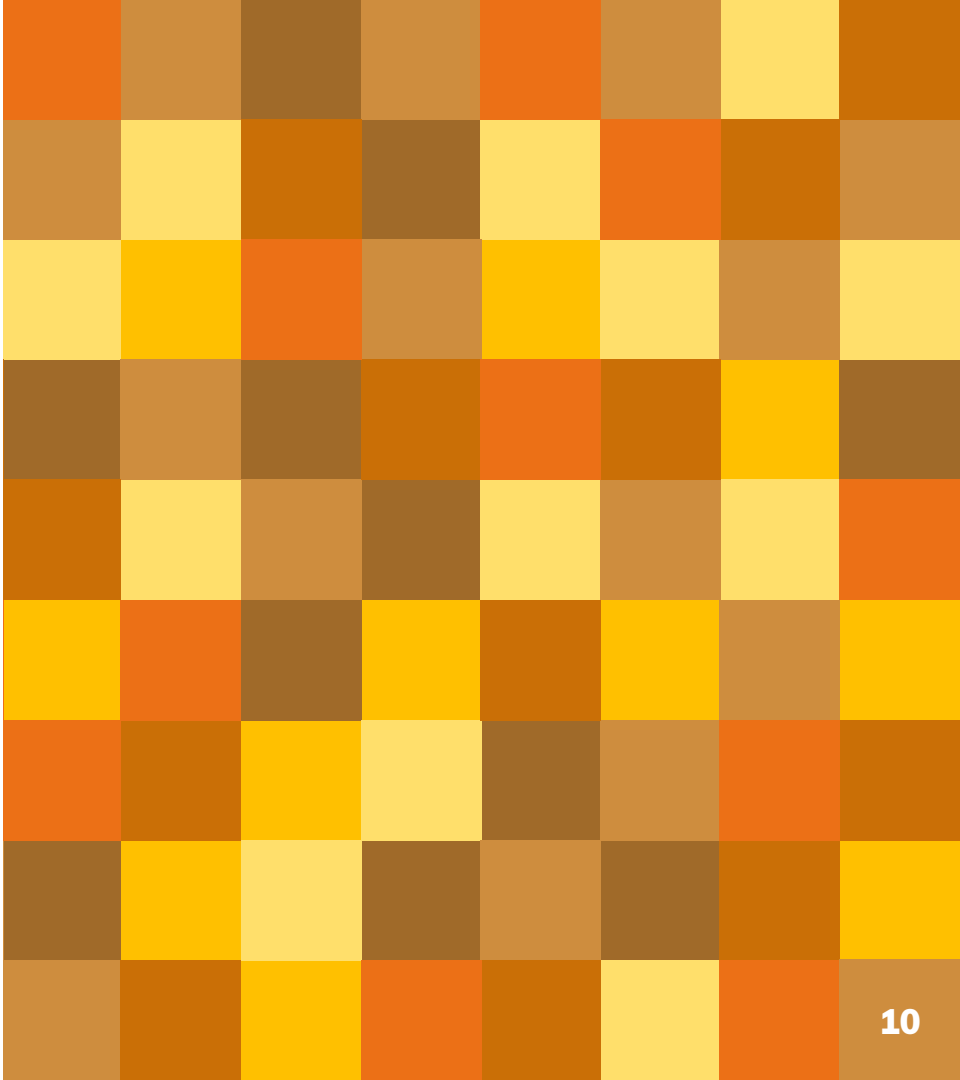
- Often in another country

It is run by a third party

- For free («public resolver»)  
E.g. 8.8.8.8, 9.9.9.9, 1.1.1.1
- Or as a paid premium service  
E.g. Cisco Umbrella/OpenDNS

# 2.

What does  
DoH do?



# What is DoH?

DNS-over-HTTPS (RFC 8484)

New IETF standard by Web people (that also operate public resolvers)

Transmits DNS queries to the resolver over an HTTPS connection (encrypted)

Can be used by any HTTPS-speaking app, bypassing the OS and its settings

Requires upgraded DNS servers

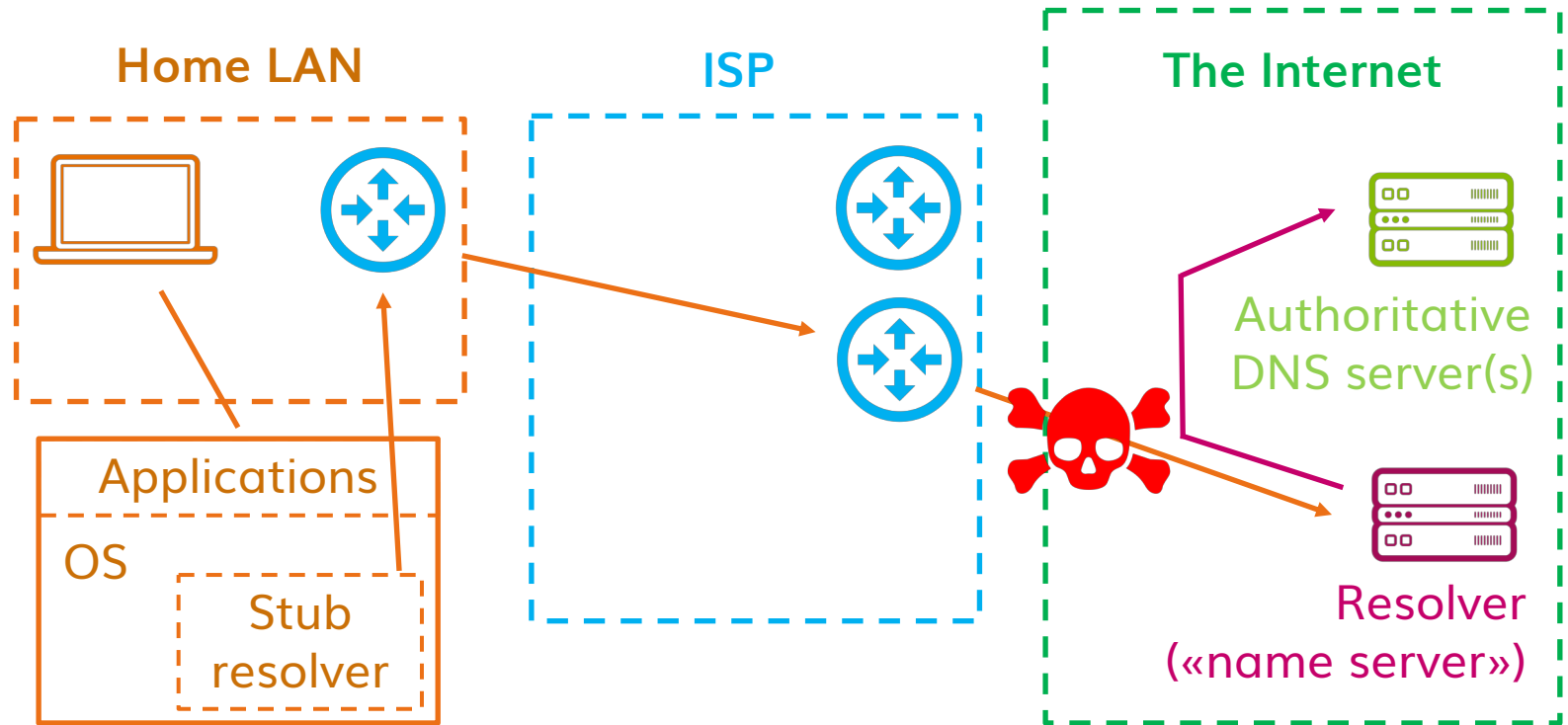
# Three main changes to resolution

1. The device-to-resolver connection is encrypted and hidden inside Web traffic
2. Each application can use a different resolver (DNS becomes an application level service, not a network one)
3. Each application maker can hardwire their own remote resolver, at least as a default

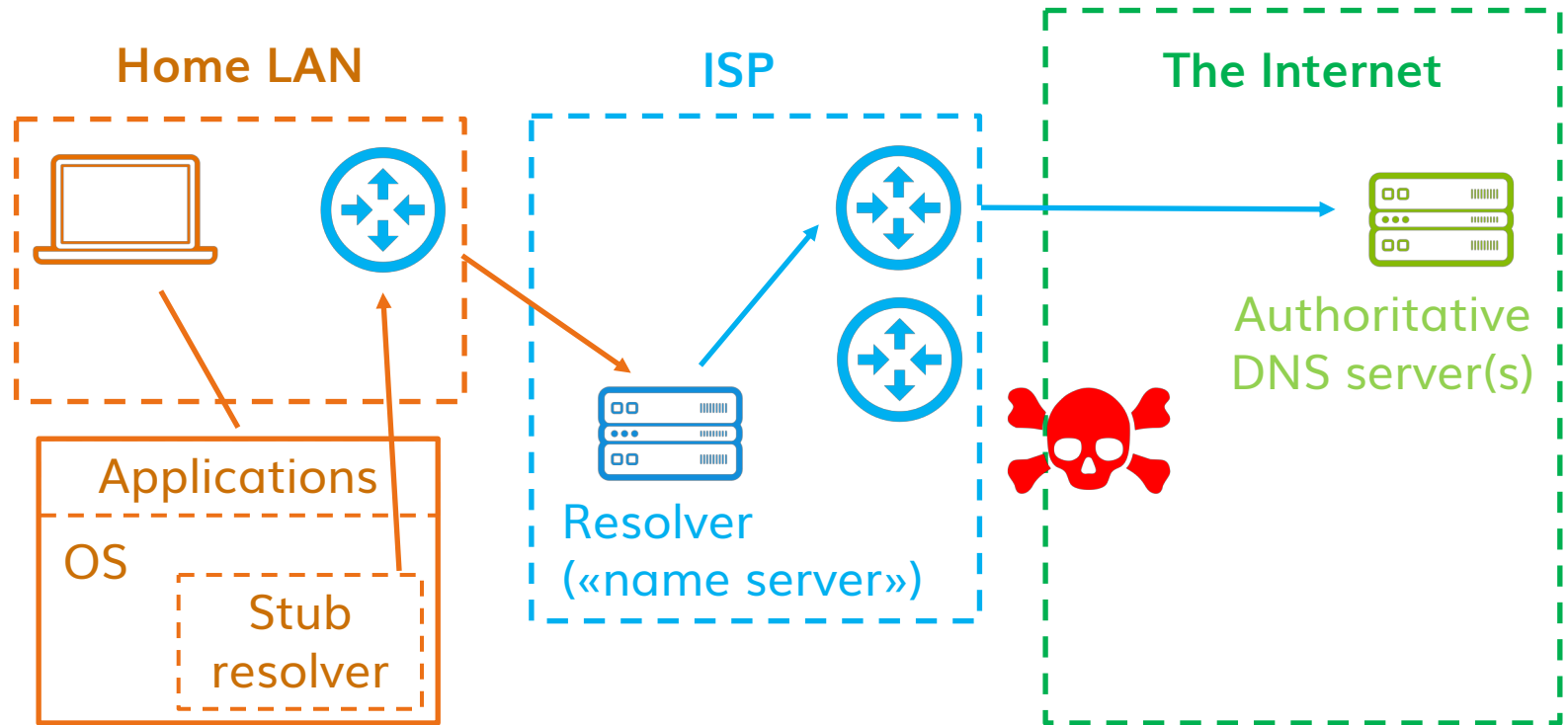


*#1*

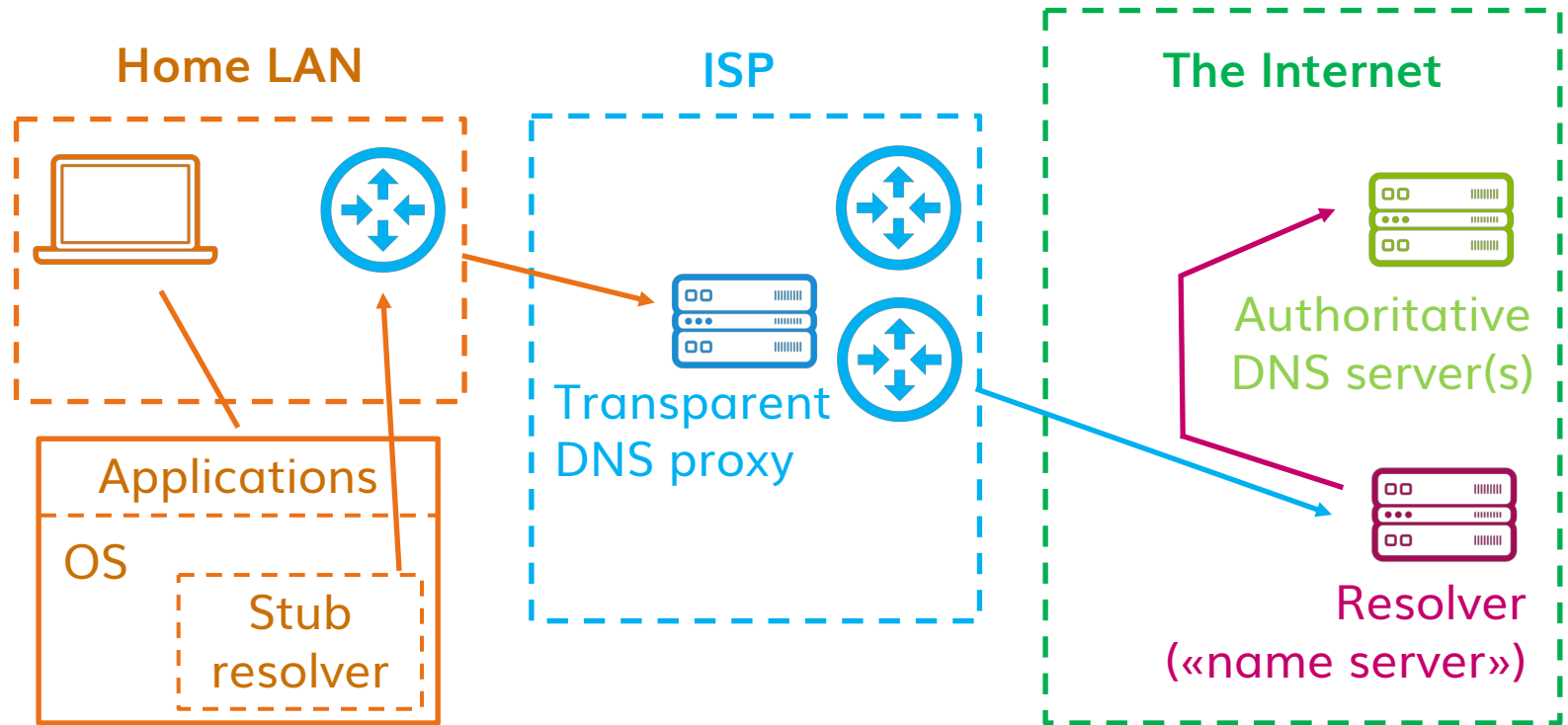
The device-to-resolver connection  
is encrypted and hidden  
inside Web traffic



*Remote DNS resolution, intercepted*



*Local DNS resolution, not intercepted unless the ISP is hacked*



*Remote DNS resolution, proxied by the ISP*



# Is this good or bad?

## Good

If you use remote resolution and are attacked or tracked

If you don't trust your ISP / it does bad things to you

## Indifferent

If you use local resolution and are attacked or tracked, unless the attacker is on the ISP's network

## Bad

If you trust your ISP / it does good things for you

**It depends.**

***But mostly good.***

## #2

Each application can use a different resolver (DNS becomes an application level service, not a network one)

# Is this good or bad?

## Good

If the application maker is smarter than the user, and is honest

If you don't trust your OS

## Indifferent

If all DoH applications used the OS settings (but you can't really force them to)

## Bad

If the application maker is smarter than the user, and is dishonest

If the user is smarter than the application maker

# Is this good or bad?

## Bad

If the application doesn't let you configure the DoH server

If the remote DoH server provided by the application maker fails

## Bad

If the application maker's interests and the user's interests are opposite

## Bad

If each application starts giving you different IPs for the same name

If each application starts using its own (augmented) namespace

# Bad.

*«Crossing the streams» bad!*



# #3

Each application maker can  
hardwire their own remote resolver,  
at least as a default

## What is the status?

You can enable DNS over HTTPS in Firefox today, and we [encourage you to](#).

We'd like to turn this on as the default for all of our users. We believe that every one of our users deserves this privacy and security, no matter if they understand DNS leaks or not.



# The real change

## **Now (and for the last 20 years)**

Local resolution is the default

You get the nearest resolver when you connect

You can change your resolver once for all in your OS

## **In the DoH future**

Remote resolution with multiple servers is the default

You get the application maker's resolver when you install the app

You have to change your resolver for every new application



*Is this good or bad?*

# 3.

What would  
«remote  
resolution as a  
default» do?

# Concentration

## Now

DNS traffic is spread  
across hundreds of  
thousands of server  
And they are everywhere  
across the world  
And you can easily pick  
the server you want

## In the DoH future

Four browser makers  
that have 90% of the  
market control 90% of  
the world's Web traffic  
resolutions  
And they are all in the  
same country and  
jurisdiction  
How easily can you  
choose?

# Privacy ?

## Now

Your queries can be sniffed

You are covered by your own country's privacy, law enforcement and neutrality rules

Your DNS is normally supplied by a company that does not live off targeted advertising

## In the DoH future

Your queries cannot be sniffed

Your DNS data will be subject to the U.S. privacy, law enforcement and neutrality rules

Many of the likely DNS providers live off data monetization (and use cookies / fingerprinting)

# Freedom from censorship ?

## Now

You get the DNS-based content filters mandated by the law of your country

## In the DoH future

You get the DNS-based content filters mandated by the law of the remote resolver's country

And your country may start mandating IP address filters as a response

# Network neutrality ?

## Now

Your ISP may break network neutrality, unless there are laws to prevent this

## In the DoH future

Your application maker or resolver operator may break network neutrality, unless there are laws to prevent this

# Performance ?

## Now

The application has to wait for the OS

Your local resolver is near, though it can be slow and unreliable

Your local resolver gets the topologically better result from CDNs

## In the DoH future

The application doesn't have to wait for the OS

Your remote resolver is far, but it could still perform better

Your remote resolver cannot get the topologically better result from CDNs unless it violates your privacy



# Security ?

## Now

Your ISP can block botnets and malware with localized DNS filters

Your ISP can detect network problems and infections via the DNS

Your ISP can use split horizon, local names...

## In the DoH future

Will your remote resolver get real-time threat feeds for your country?

Your ISP will be blind

Local names won't work any more

DoH can be used for data exfiltration

# User empowerment ?

## Now

- You can easily pick a different server
- You can get DNS-based services (parental control...) from whomever you want
- You can easily know where all your queries go
- Smarter users expect things to work this way

## In the DoH future

- You have to change the server in each app, and not all apps may let you
- All other DNS-based services stop working
- Your queries go wherever the app wants
- No one expects or understands the change

**Privacy in transport != Privacy**

**Concentration + Less user control  
= Surveillance machine**



*Is this good or bad?*

# Is this good or bad?

## Good

If you are a Turkish dissident without a clue

If you trust Google/Apple/Mozilla/Cloudflare more than your ISP

If you trust the U.S. government and laws more than yours

If you don't care about centralization

## Bad

If you are ok with your current resolver

If you like to control DNS

If you trust your ISP more than Google etc.

If you trust your own government and laws more than the U.S. ones

If you are worried about the centralization of the net

**It depends.**

***But mostly bad.***

*Especially without appropriate policies.*

# 4.

The DoH  
dilemma:  
who chooses  
your resolver?

**The user?**      **The ISP?**      **The browser?**

**The ISP, on behalf of the user?**

**The browser, on behalf of the user?**



...and there's more: who should be  
entitled to apply policies to your DNS?

The government?

The resolver?

The network administrator?

# Thanks!

Any questions?

You can find me at

@vittoriobertola  
vb@bertola.eu



*Credits: Original presentation template by [SlidesCarnival](#) modified by myself*

*License: This presentation is distributed under a Creative Commons Attribution (CC-BY) license*