

Bits & Atoms II

Bits & Atoms II (Webtechnologies)

Hoi

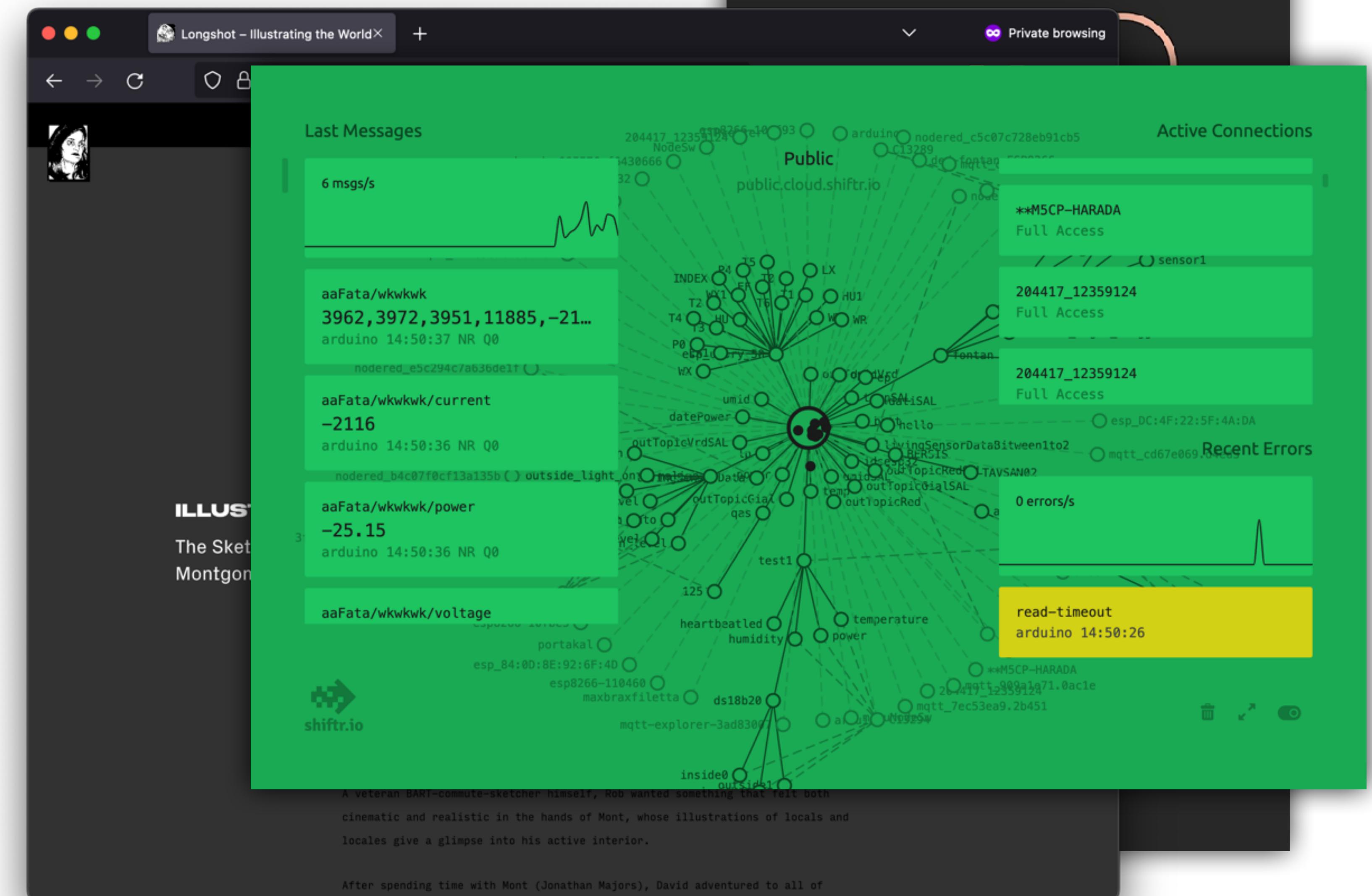


Admin

- 80% Attendance
- Grading
 - Exercises (*details will follow*)
 - Participation in class

Webtechnologies – Why?

- Interfaces/Controls
 - Storytelling & Information
 - (Functional) Prototypes
 - Easy Access (Smartphone)



Sources:
<https://www.wearelucid.ch/projekte/5x14>
<https://longshotfeatures.com/illustrating-the-world/>
<https://www.shiftr.io/trv/>

Goal of this course

- Understanding of possibilities
- Knowledge of tools and terms
- First experiences with web technologies
- Foundation for other modules

What do you already know?

What do you expect?

What do you already know?

What do you expect?

- Networks (Use for quick prototypes)
- HTML/CSS (+ something more please)
- Sustainable Websites
- Scalability/Maintainability (how to work big)
- Frameworks (react or alike)
- Workflow (How to go from figma to a “real” website)
- “How to start”?

What to expect?

- Be patient! It takes time!

«Why do I need this?»

« ... I mean there is: ...»

- Chat GPT
- Website-Builders (Webflow, Squarespace, WIX etc.)

The screenshot shows a web browser window with the URL <https://chat.openai.com>. The chat interface is displayed, with a message from the user asking how to display an image with HTML and CSS and make it fullscreen. The AI response provides step-by-step instructions and code snippets for both HTML and CSS.

How can I display an image with HTML and CSS and make it fullscreen?

To display an image using HTML and CSS and make it fullscreen, you can follow these steps:

1. First, add the image to your HTML document using the `` tag. For example:

```
php

```

1. Next, create a CSS class for the image and set its width and height to 100% to make it fill the entire screen. For example:

```
php
<style>
.fullscreen {
  width: 100%;
  height: 100%;
}
</style>
```

1. Apply the CSS class to the `` tag by adding the `class` attribute. For example:

```
arduino

```

This will make the image fullscreen, but keep in mind that the image might appear stretched or distorted if it doesn't have the same aspect ratio as the screen. To avoid this, you can use additional CSS rules to center the image and maintain its aspect ratio.

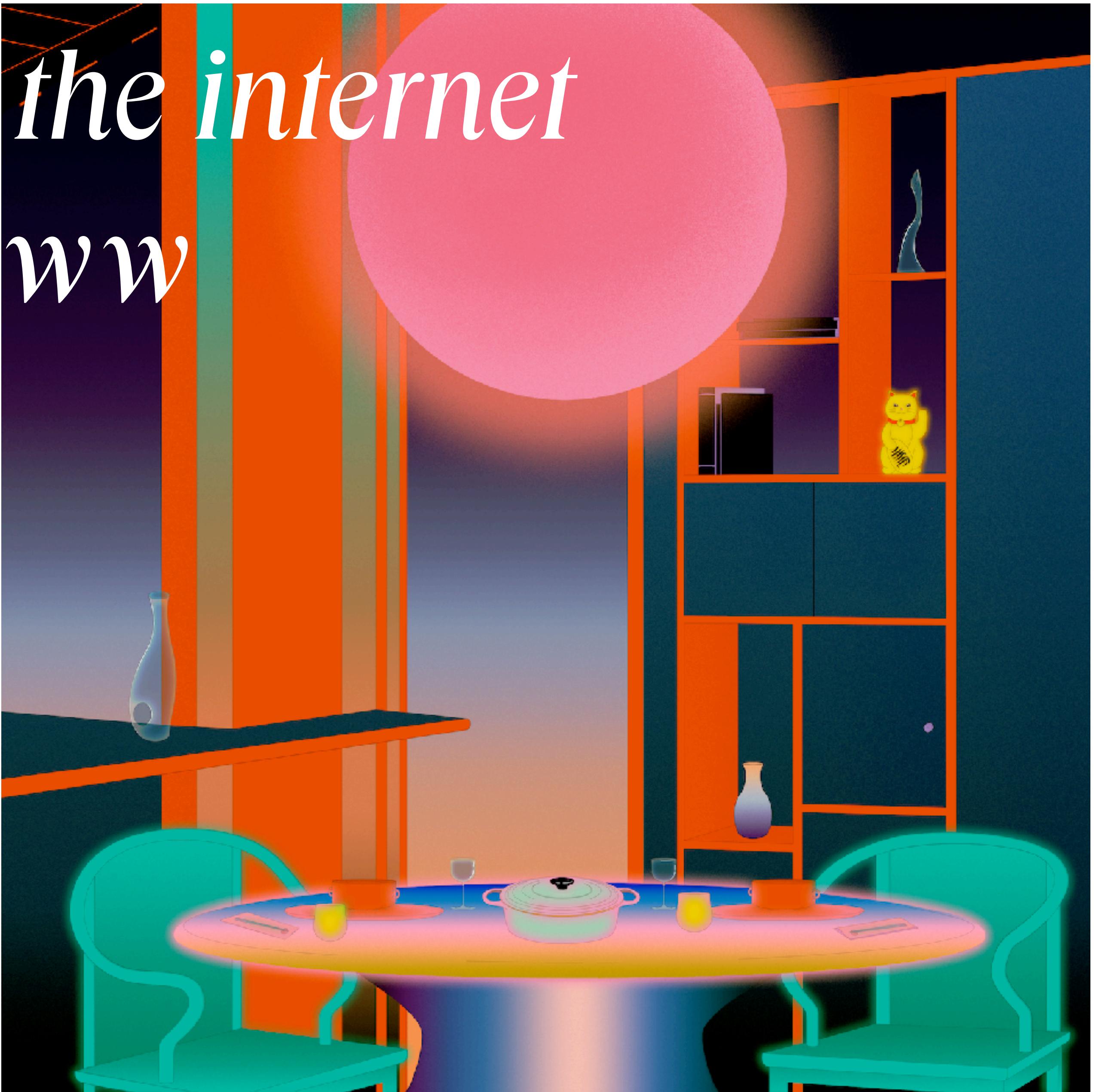
«Why do I need this?»

- Language Models hallucinate!
(Use them, but wisely!)
- You should be able to distinguish between
rubbish and helpful answers.
- You will reach the limits of these tools, as
soon as you want to create something
more custom.
- You'll gain the necessary vocabulary to
talk to designers, developers etc.

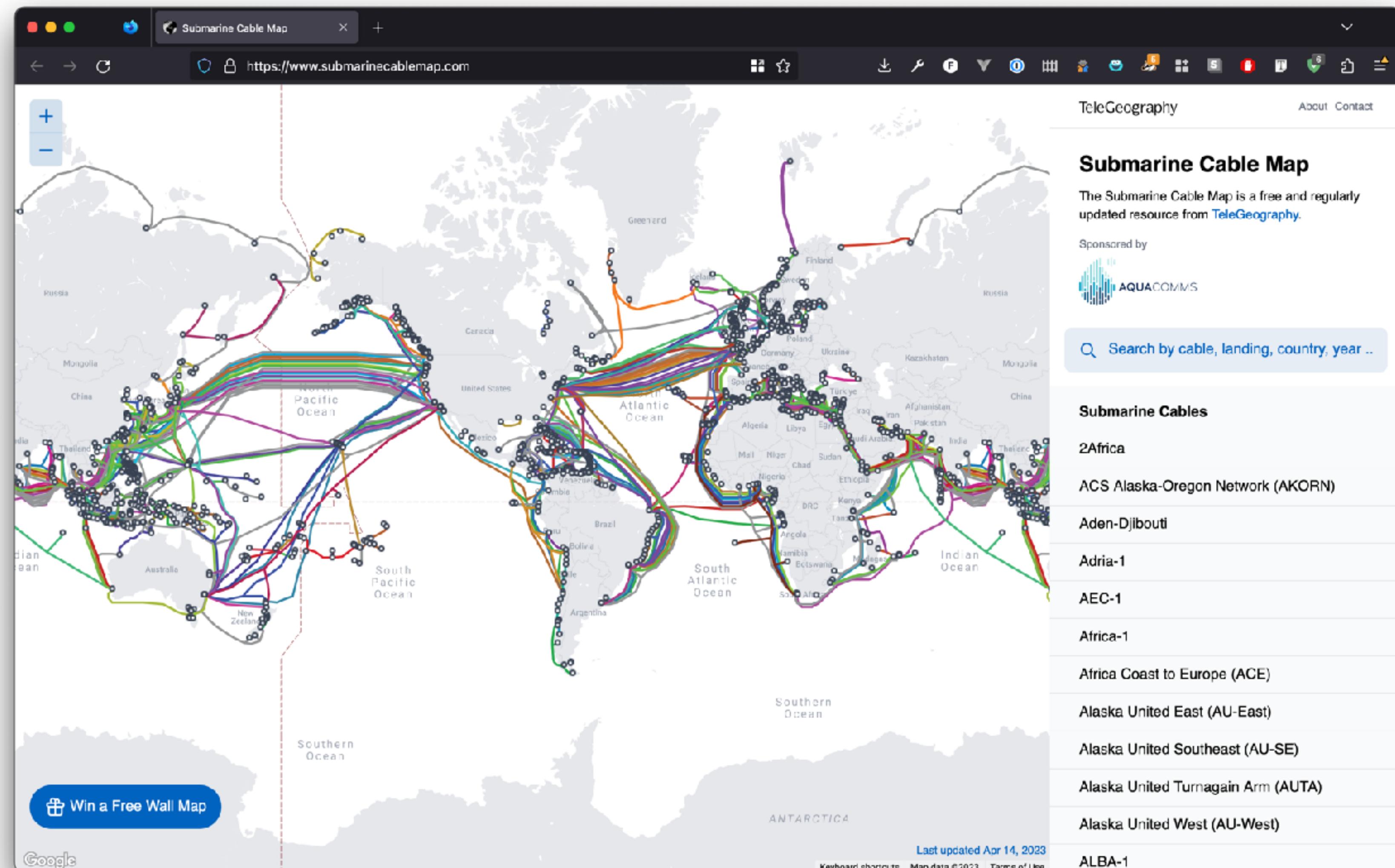
Resources

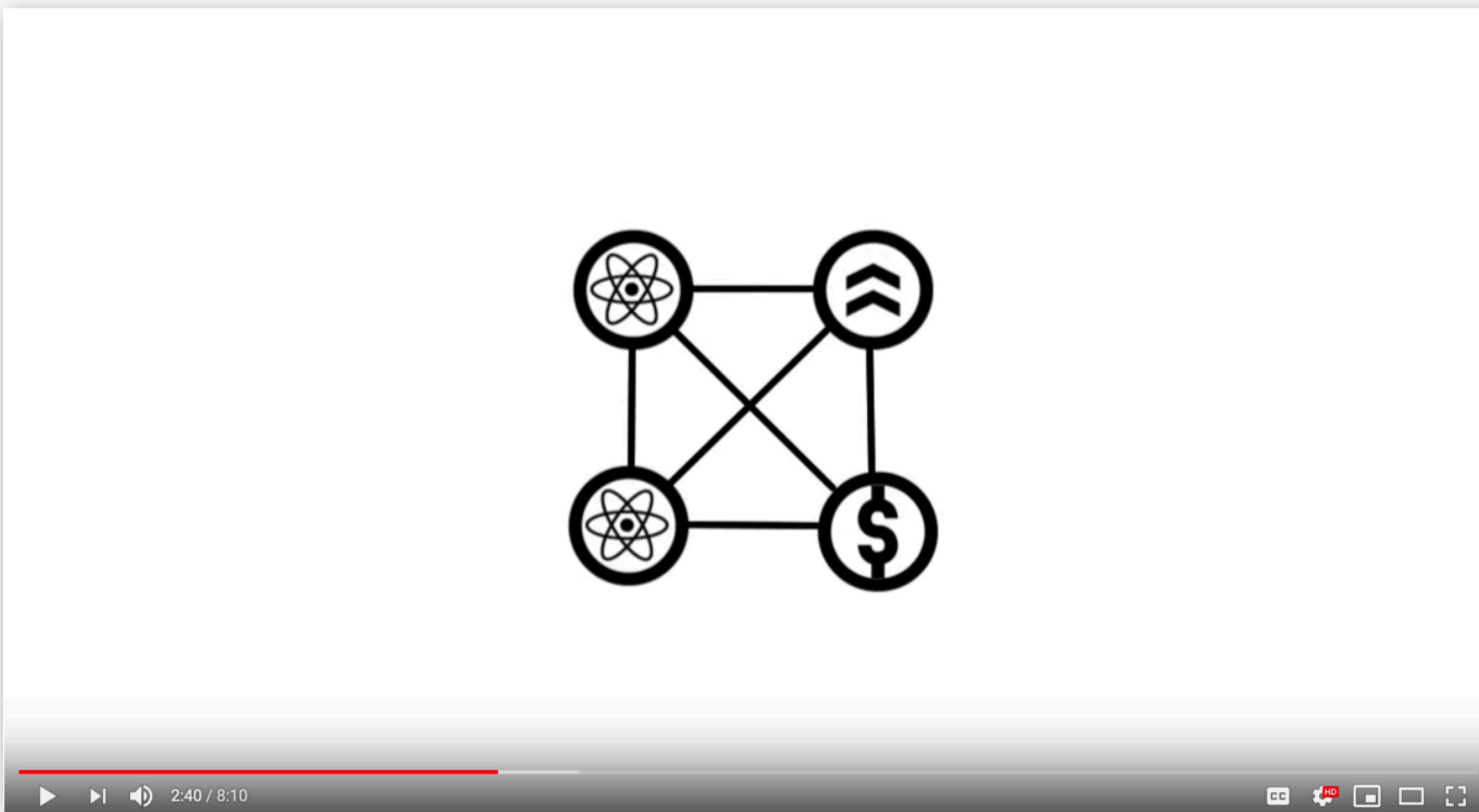
- IAD Calendar (times and room numbers)
- Paul:
<https://paul.zhdk.ch/course/view.php?id=2506>
(... probably only interesting for the slides)
- Github (Link will follow)

History of the internet And the www

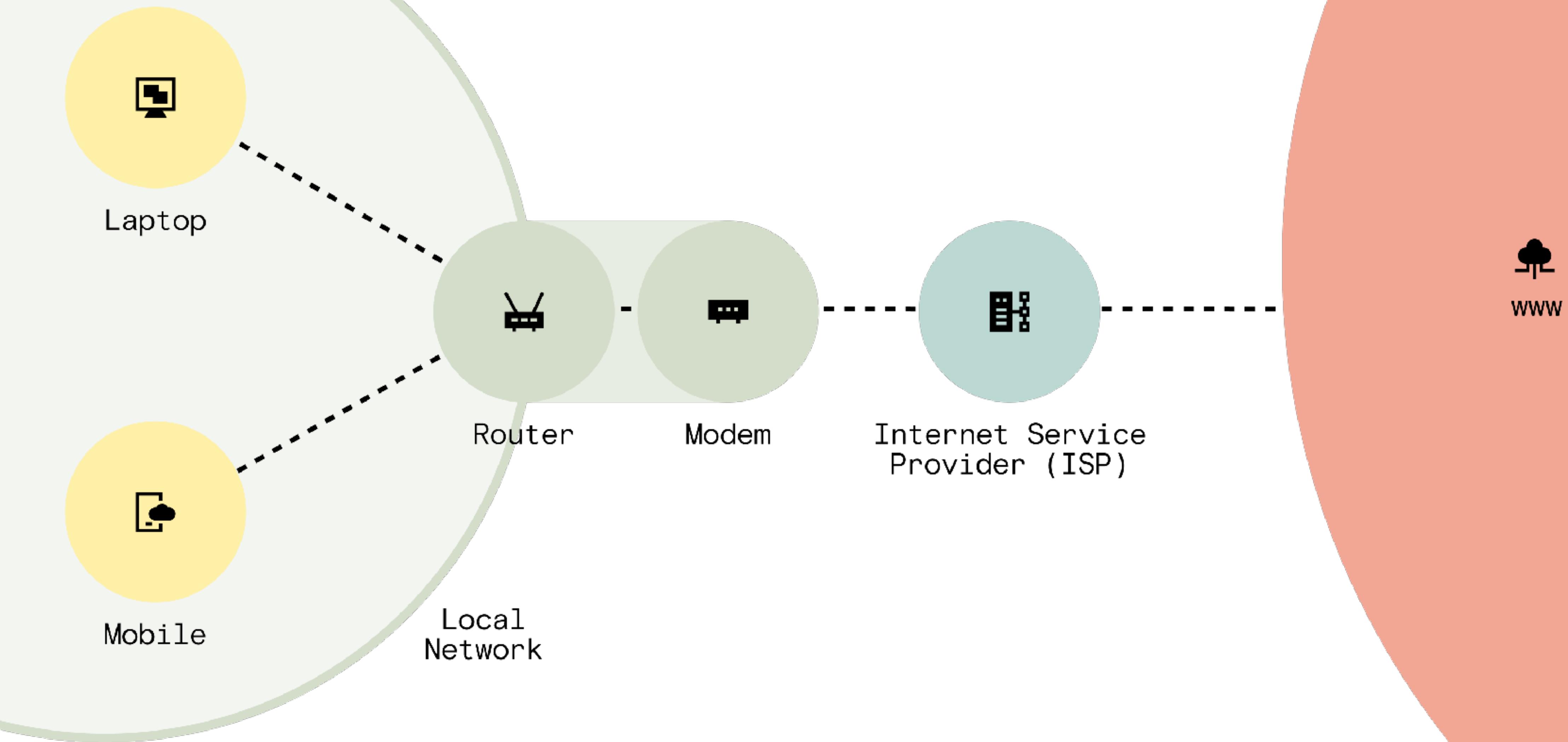


Submarine Cables → Internet





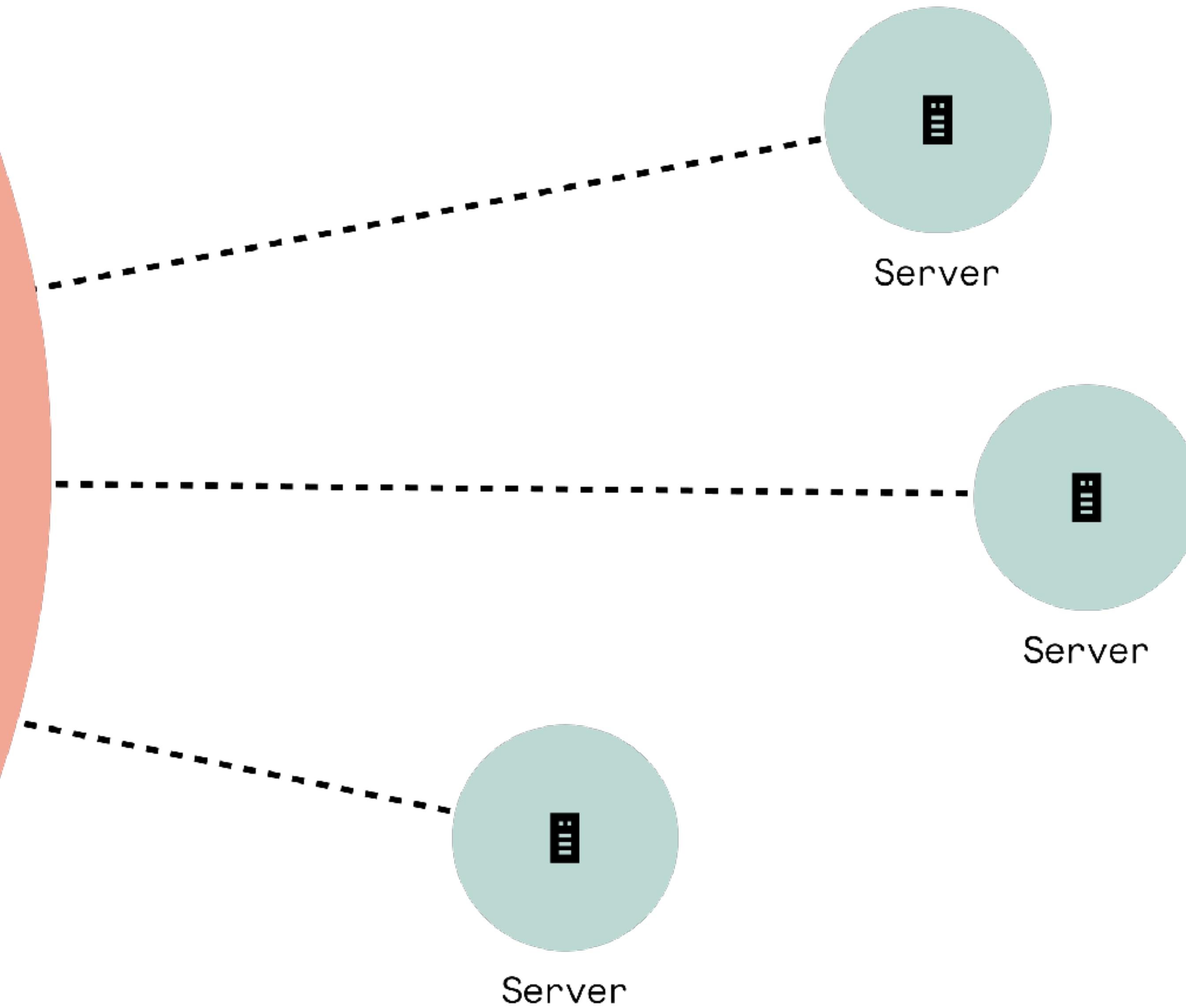
Connection



Connection



WWW

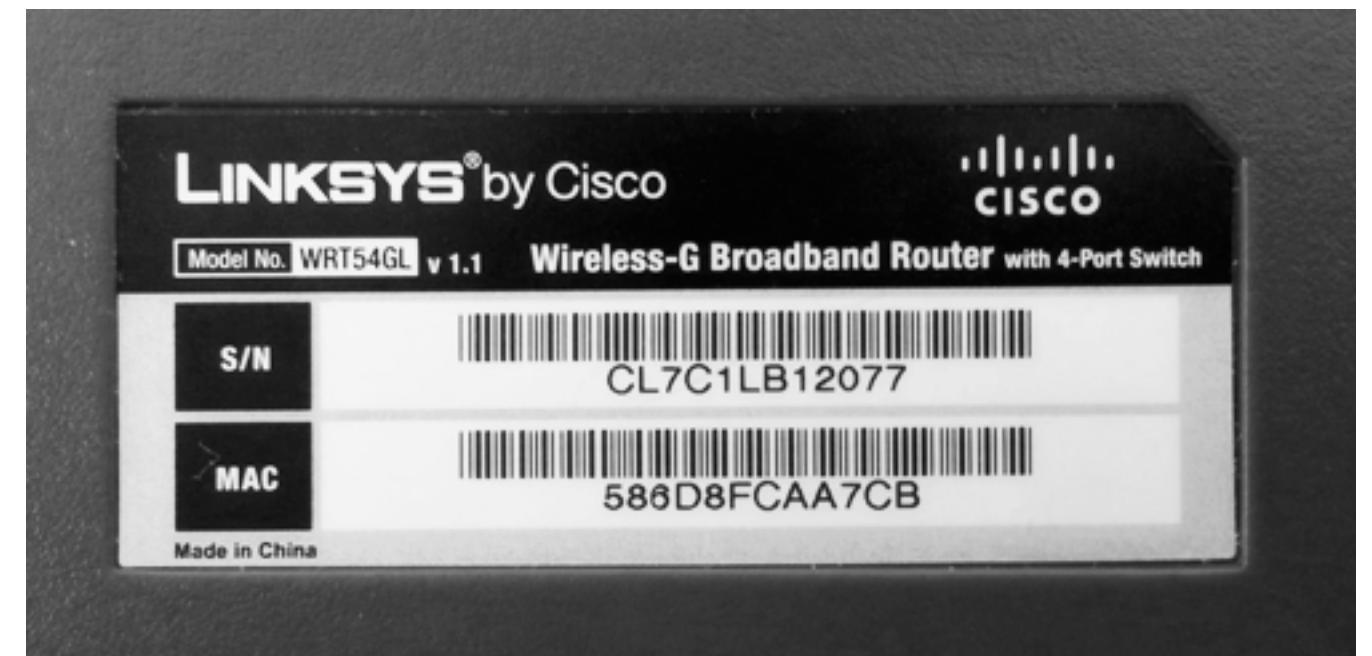


MAC addresses

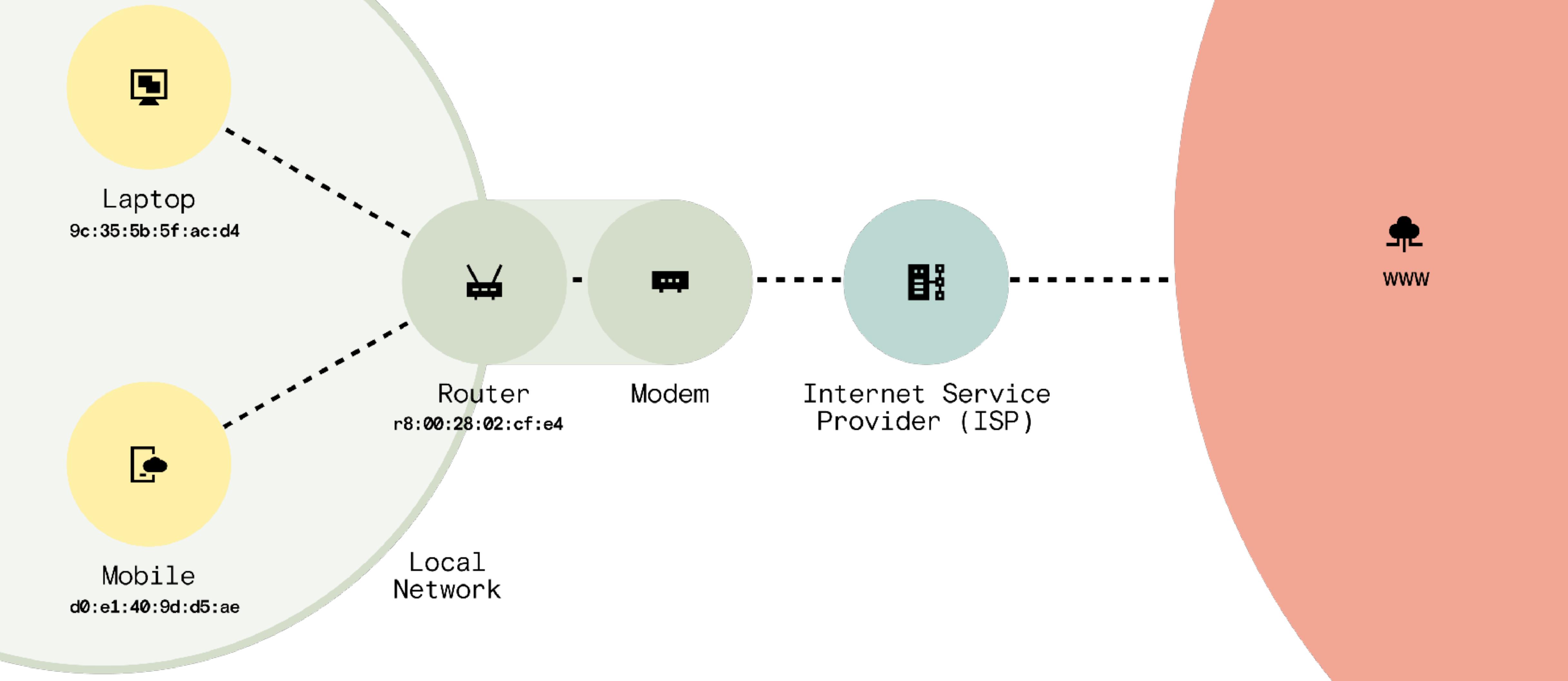
- Every device that connects to a network has a MAC-address.

Example: **d0:e1:40:9d:d5:ac**

- Used to identify a device in a local network.
- $2^{48} = 281,474,976,710,656$ possible MAC addresses
- Device manufacturers are given certain number ranges to assign to their devices.



MAC addresses



Protocols

- Set of rules that governs communication between two computers in a network.
- Different layers:
 - Data-Link – Protocols: e.g. Ethernet Protocol
 - Internet Protocols: e.g. IP4, IP6
 - Transport Protocols: e.g. TCP
 - **Application Protocols**: e.g. Email, FTP, HTTP

Layer architecture [edit]

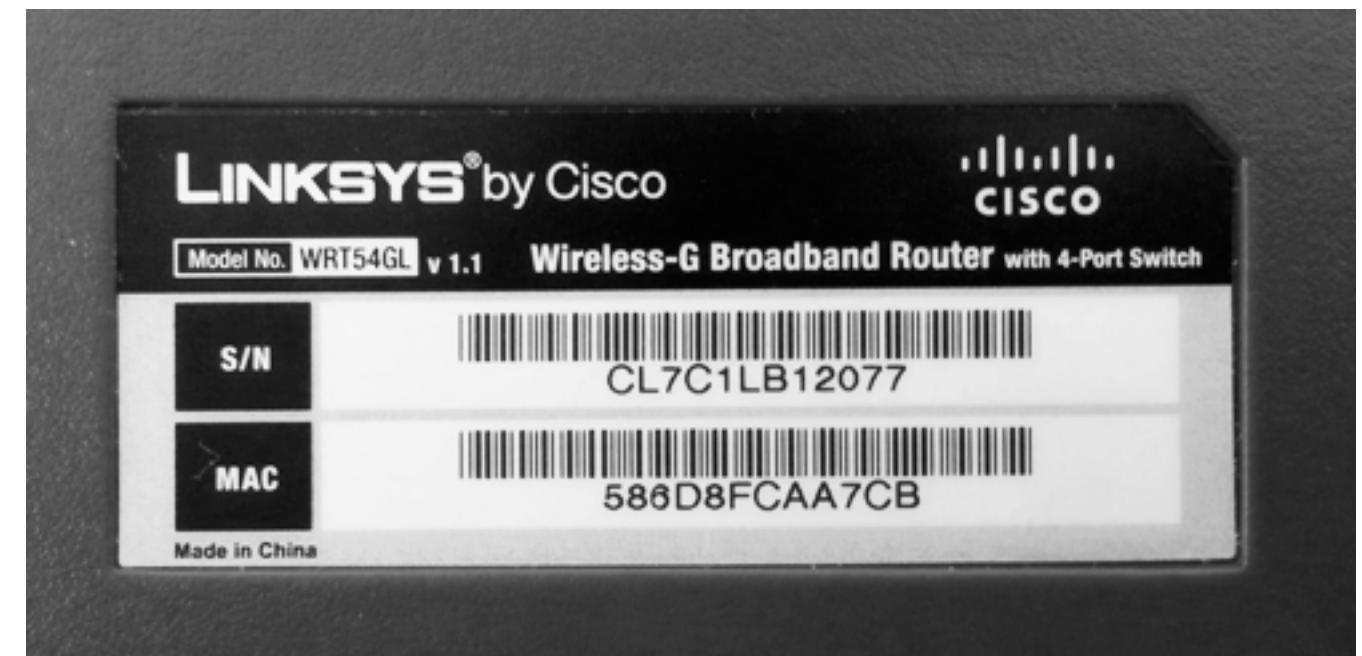
The recommendation X.200 describes seven layers, labelled 1 to 7. Layer 1 is the lowest layer in this model.

OSI model			
	Layer	Protocol data unit (PDU)	Function [28]
Host layers	7 Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP .
	6 Presentation		Translation of data between a networking service and an application; including character encoding , data compression and encryption/decryption
	5 Session		Managing communication sessions , i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4 Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation , acknowledgement and multiplexing
Media layers	3 Network	Packet	Structuring and managing a multi-node network, including addressing , routing and traffic control
	2 Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1 Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

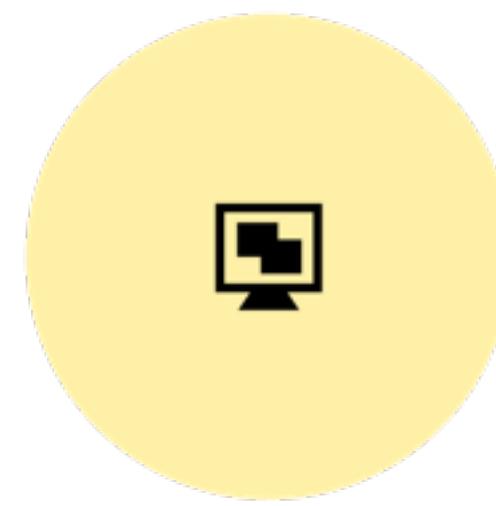
Further reading about layer architecture: https://en.wikipedia.org/wiki/OSI_model

IP (Internet Protocol) addresses

- Every computer has an IPv4 address. Example:
173.194.40.40
- Only 4'294'967'296 addresses world wide!
- Soon (?) devices will have IPv6 addresses:
2001:0db8:0000:0042:0000:8a2e:0370:7334
- About 3.403×10^{38} addresses world wide.
- An IP address is used to identify a device on the internet.

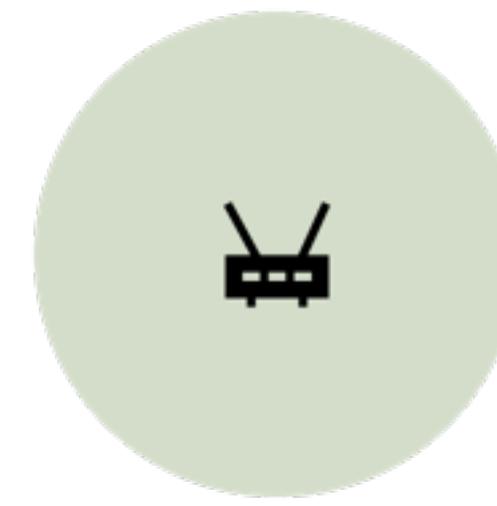


IP (Internet Protocol) addresses



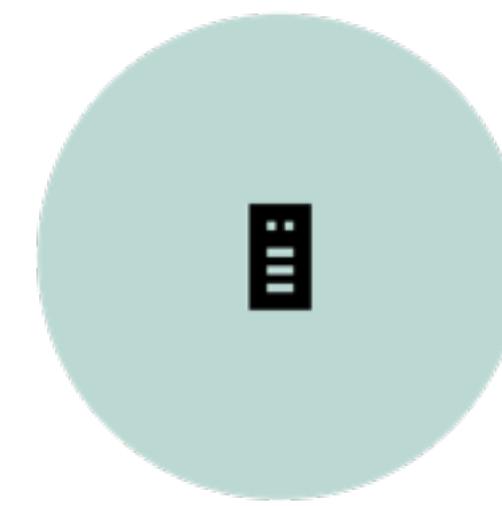
Laptop

IP Address ???



Router/Modem

Public IP: **194.139.248.111**



Server (e.g. Netflix)

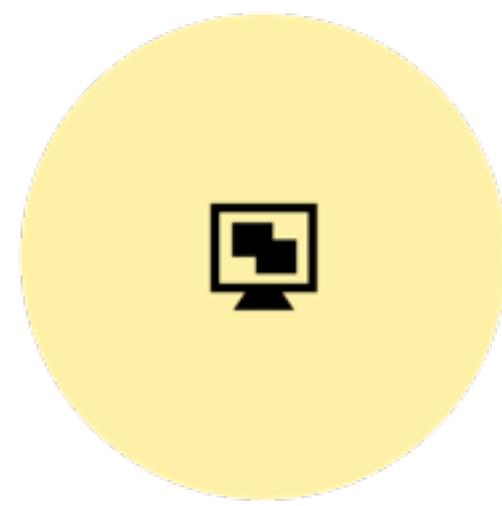
54.57.125.166

Reserved IP-addresses

- Certain ranges are reserved for private networks.
(e.g. Local Area Networks (LAN))

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

IP (Internet Protocol) addresses



Laptop

Public IP: **194.139.248.111**
Local IP: **192.168.1.32**



Router/Modem

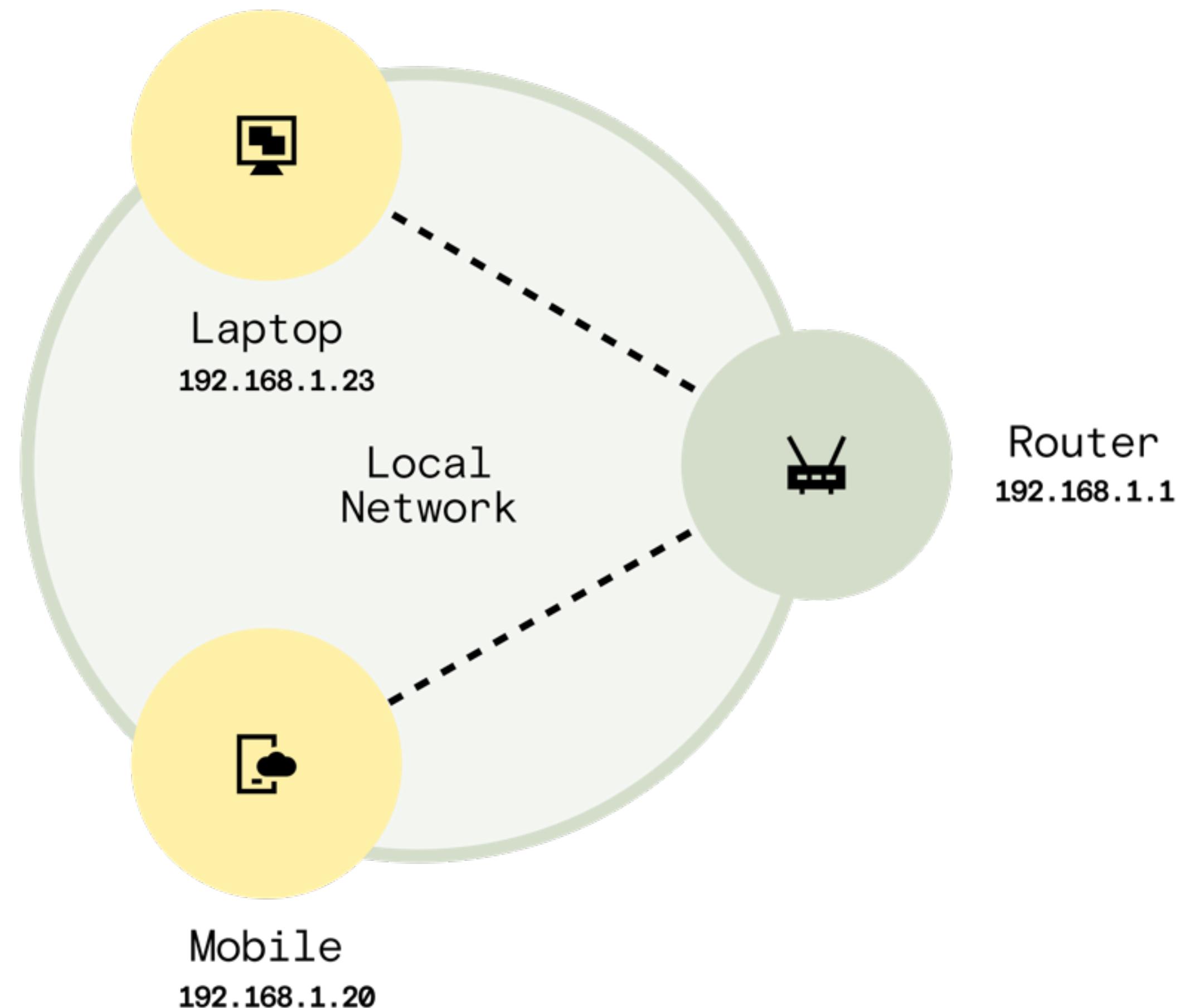
Public IP: **194.139.248.111**
Local IP: **192.168.1.1**



Server (e.g. Netflix)

54.57.125.166

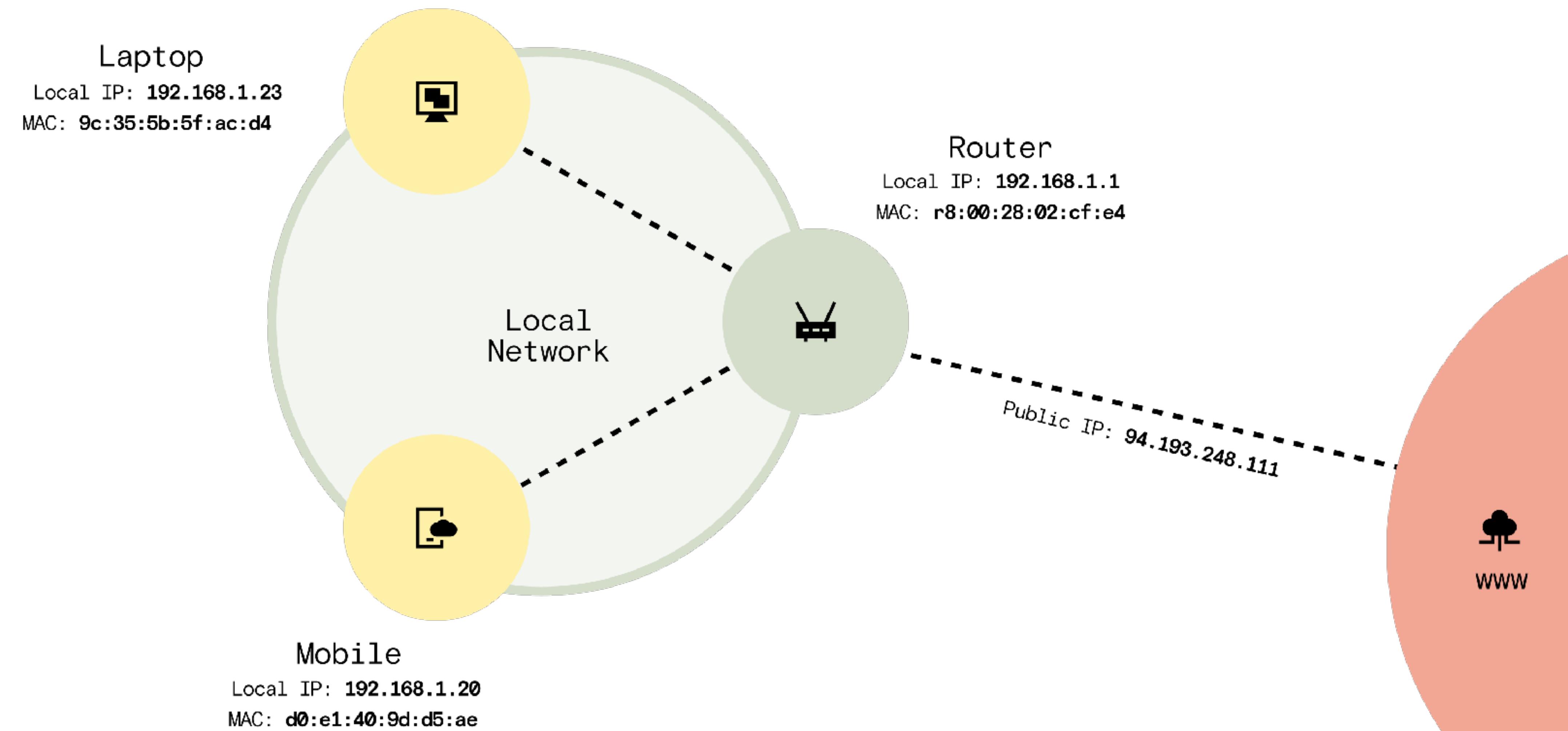
Local Network



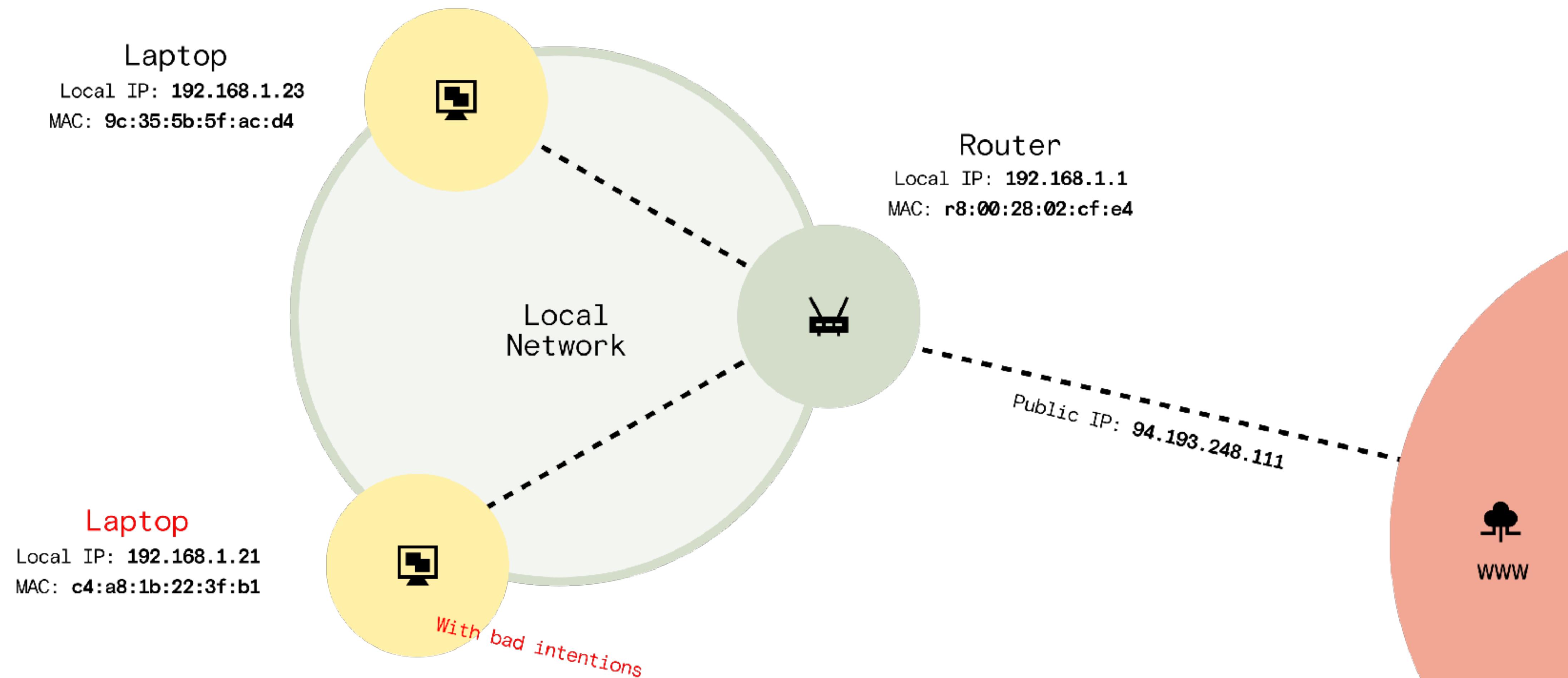
BUT WHEN SHE TRACED THE
KILLER'S IP ADDRESS... IT WAS
IN THE 192.168/16 BLOCK!



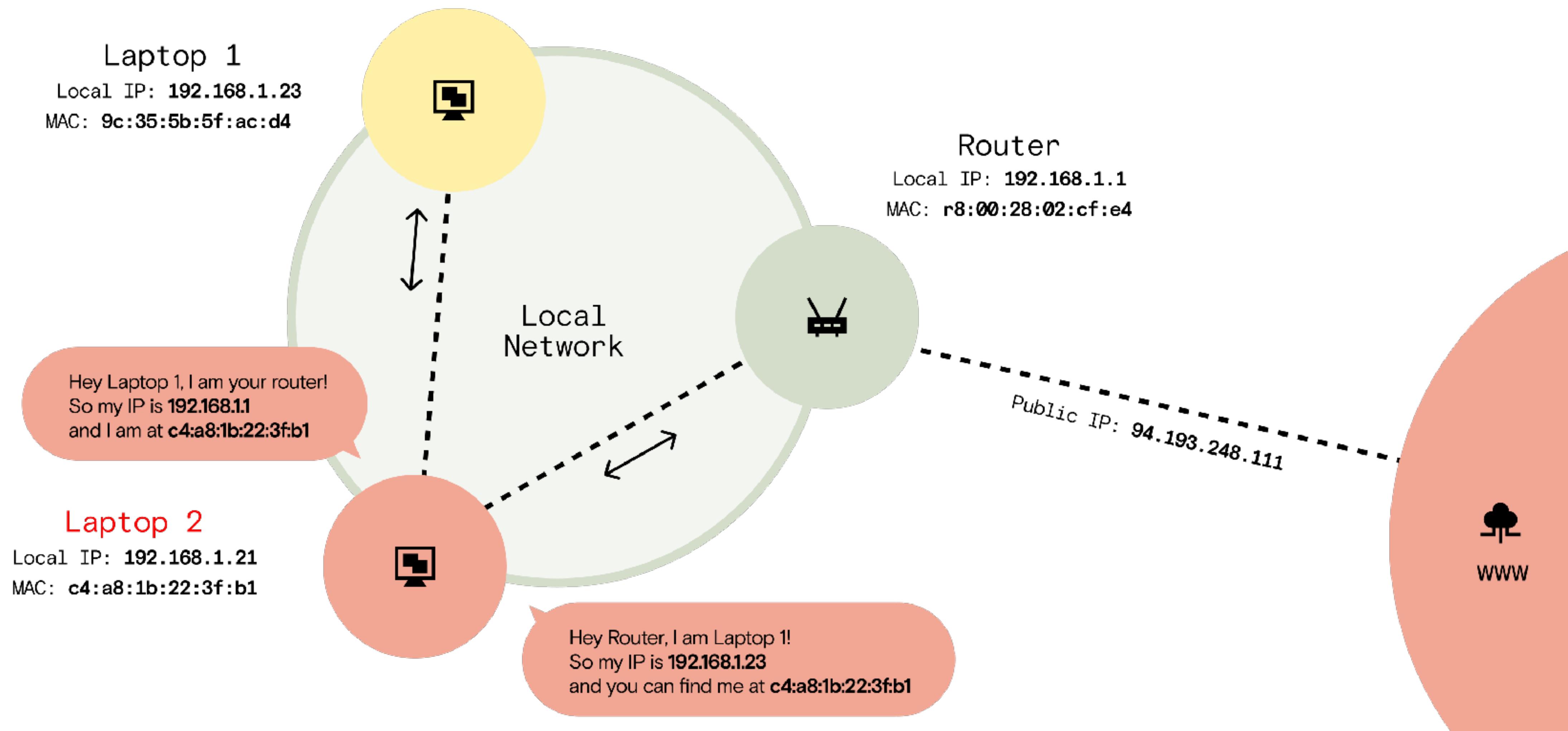
Network



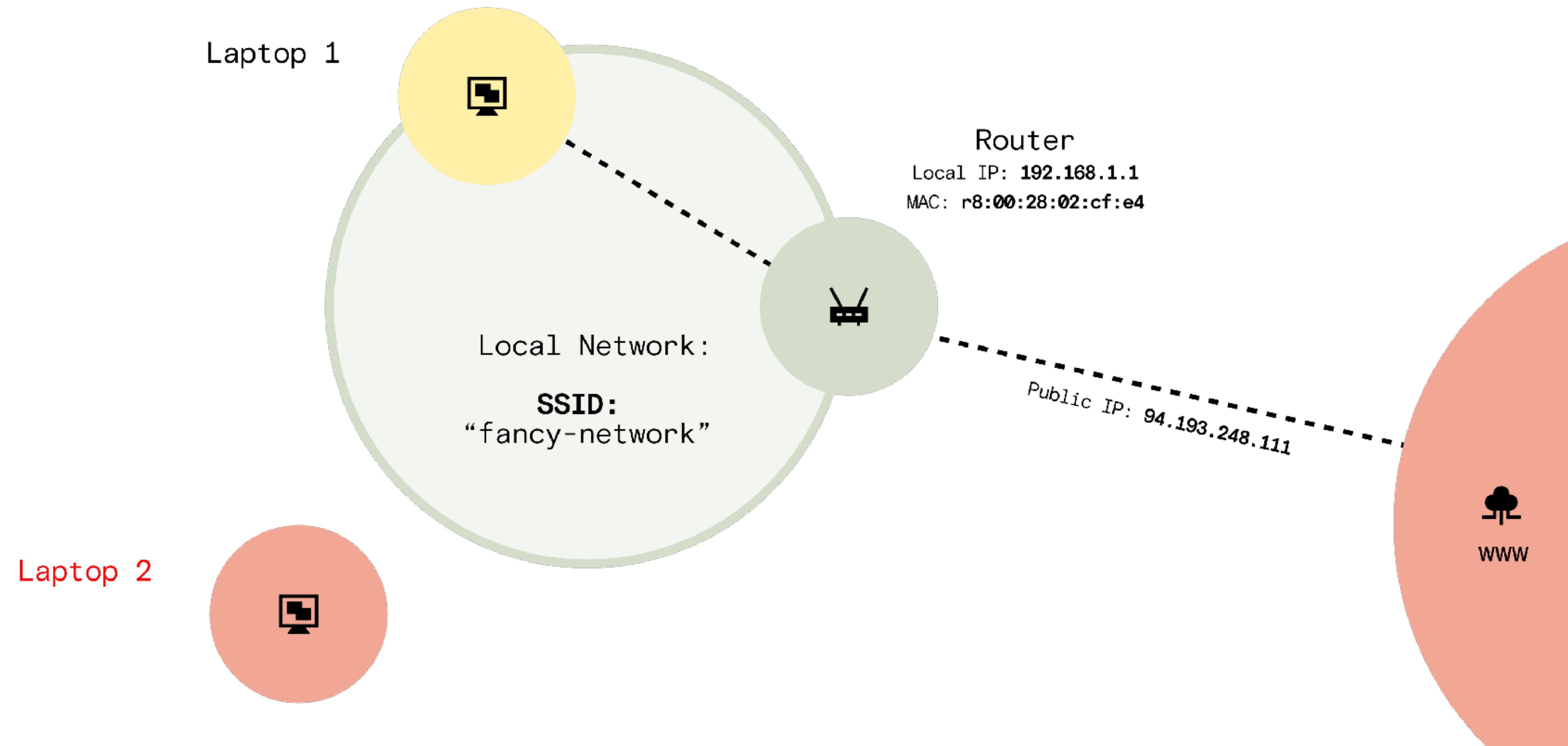
(+) «Man In The Middle Attack»/ «ARP Spoofing» or «ARP Poisoning»



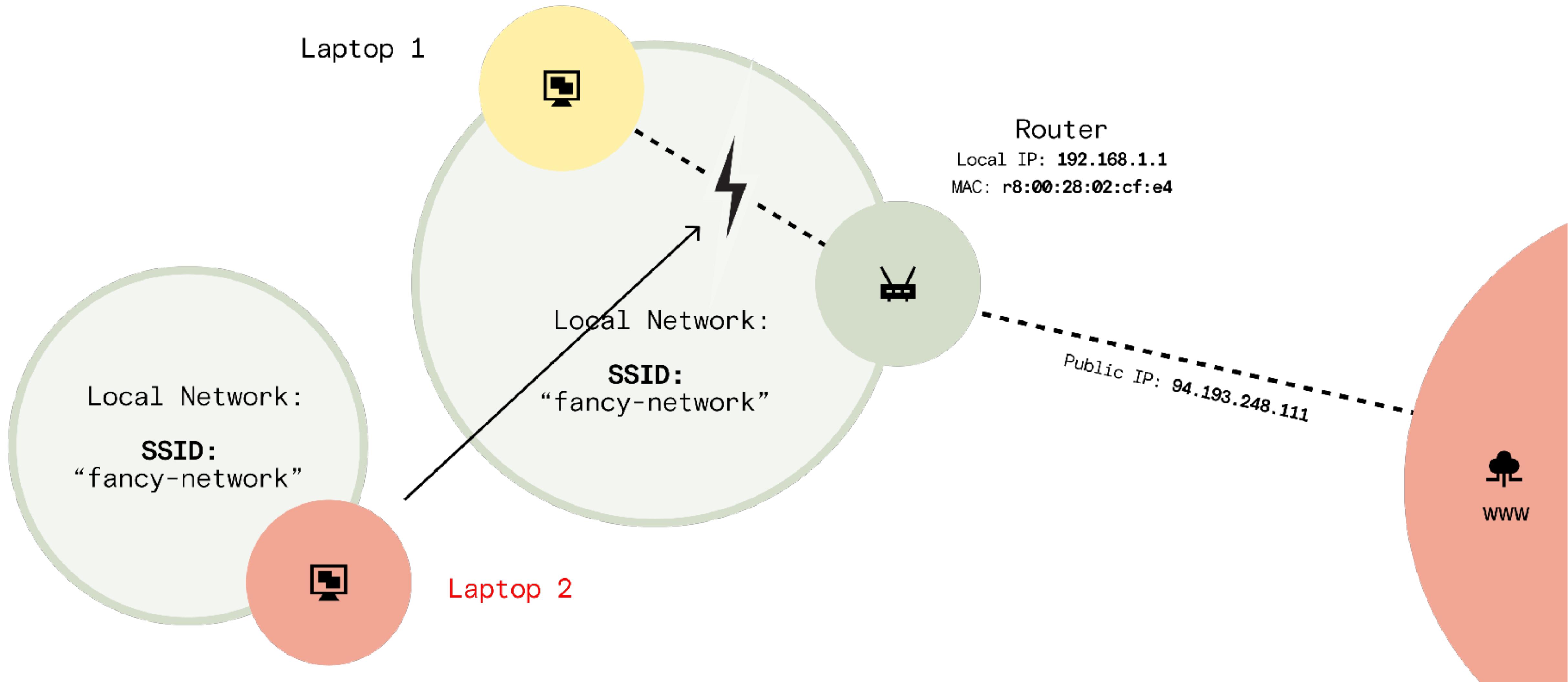
(+) «Man In The Middle Attack»/ «ARP Spoofing» or «ARP Poisoning»



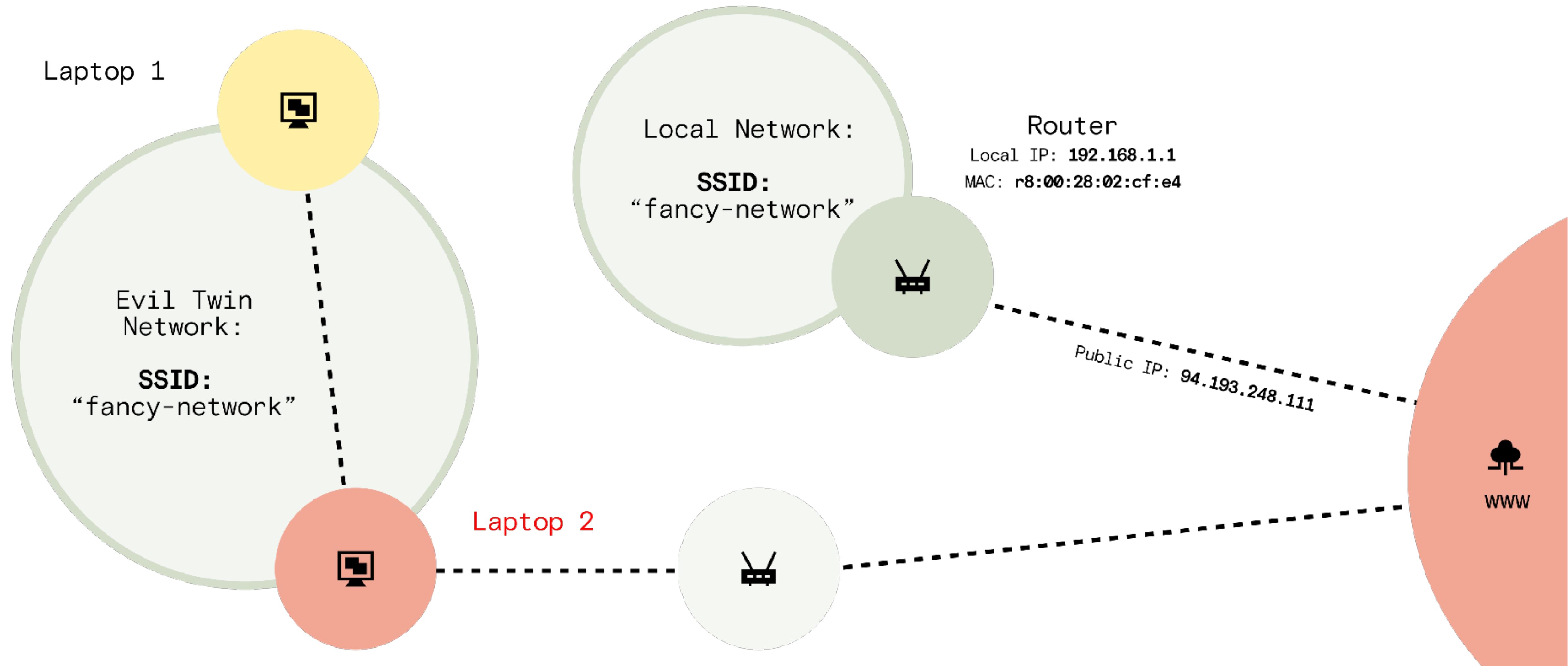
(+) Evil Twin Attack (Duplication of WiFi-Network)



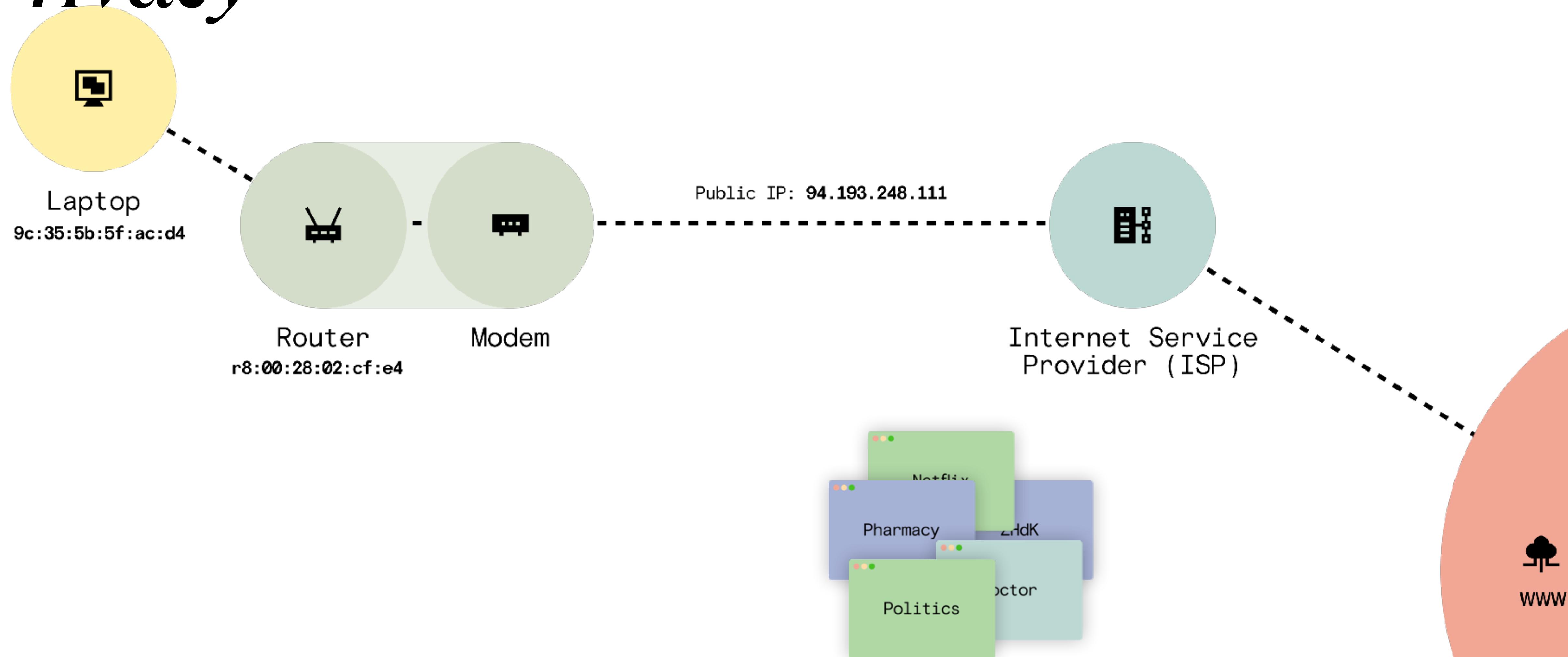
(+) Evil Twin Attack (Duplication of WiFi-Network)



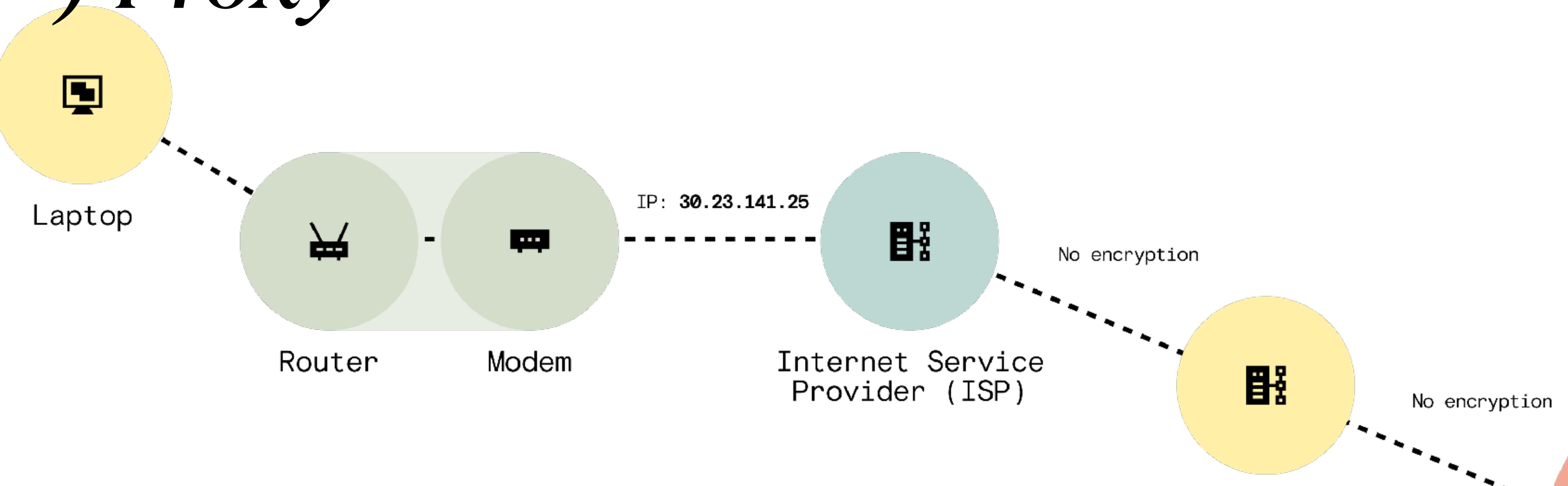
(+) Evil Twin Attack (Duplication of WiFi-Network)



Privacy



(+) Proxy

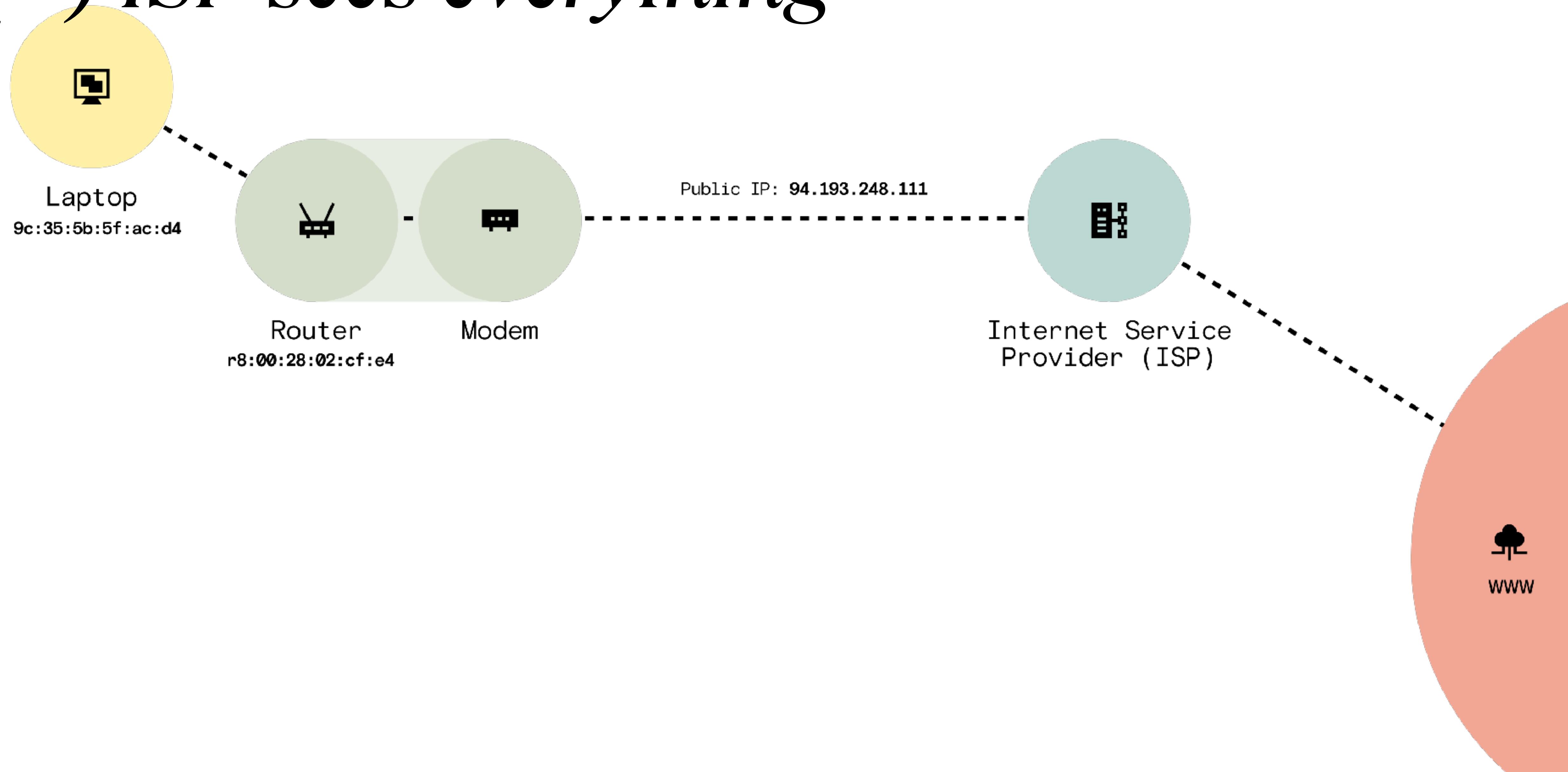


- Website sees **50.123.15.45**
- If proxy does not use encryption, ISP sees which sites you visit.
- Proxy knows your true IP **30.23.141.25**

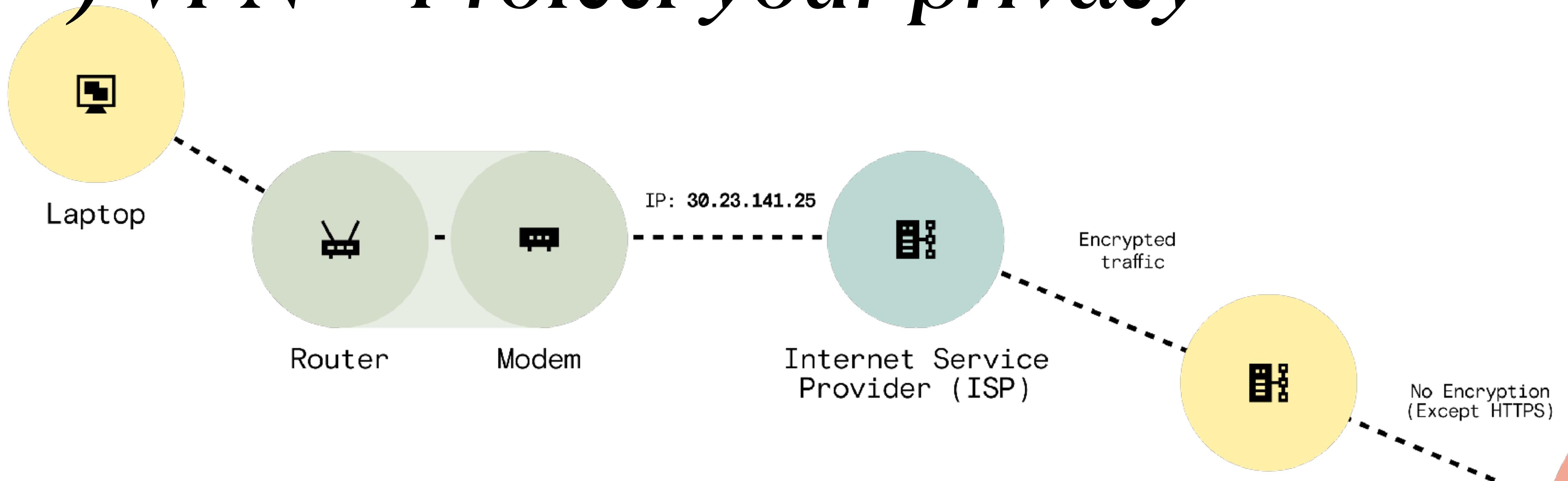


www

(+) ISP sees everything



(+) VPN – Protect your privacy



- Website sees **150.23.145.25**
- All traffic is encrypted → ISP does not know which sites you visit
- VPN knows your true IP **30.23.141.25**
- VPN could theoretically log all the sites you visit. Some VPNs have a no-log policy.



www

Localhost

- Your computer has a local address
127.0.0.1/localhost
- When building a webpage,
you often run a local server →
http://localhost:3000

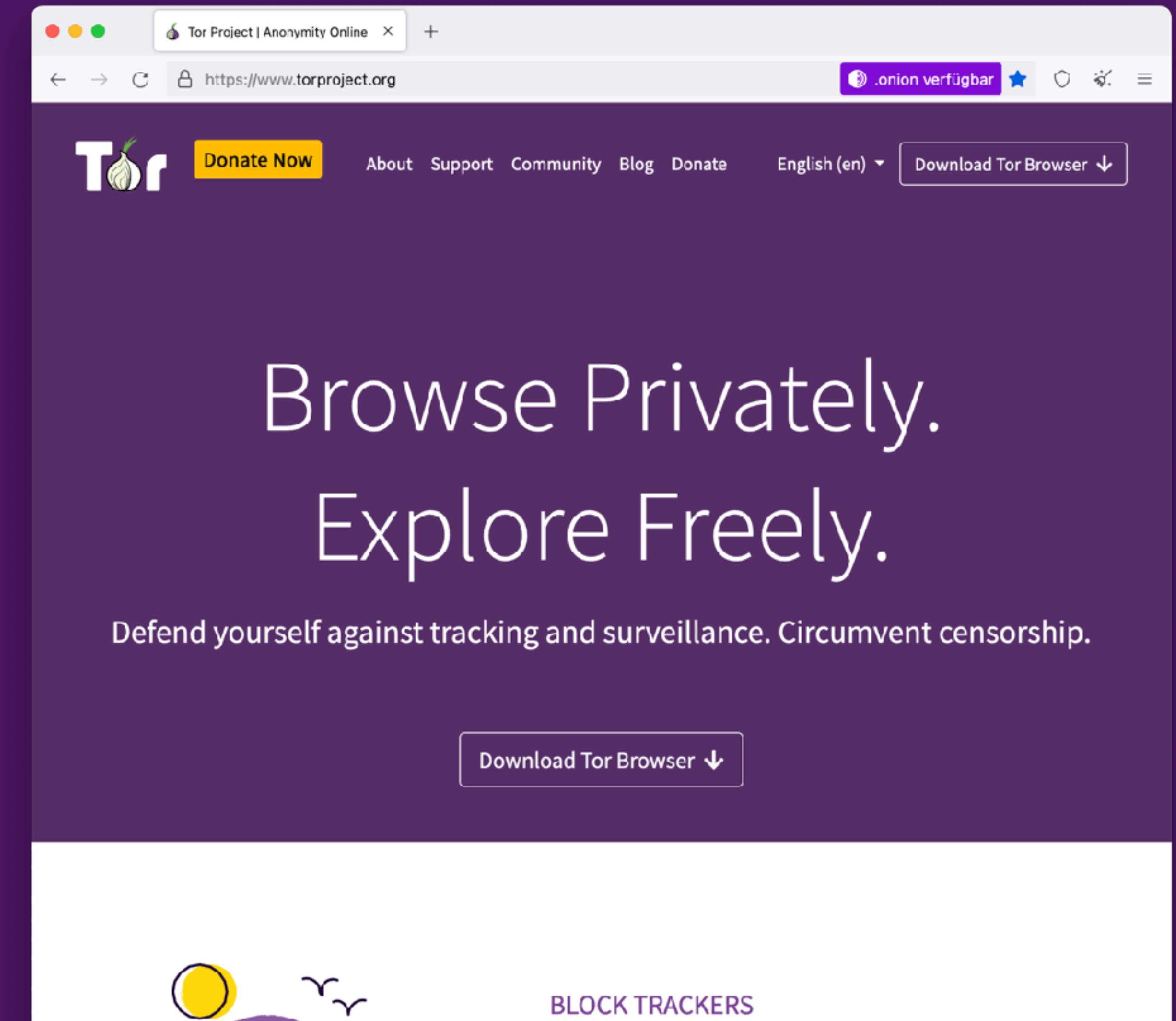


World Wide Web



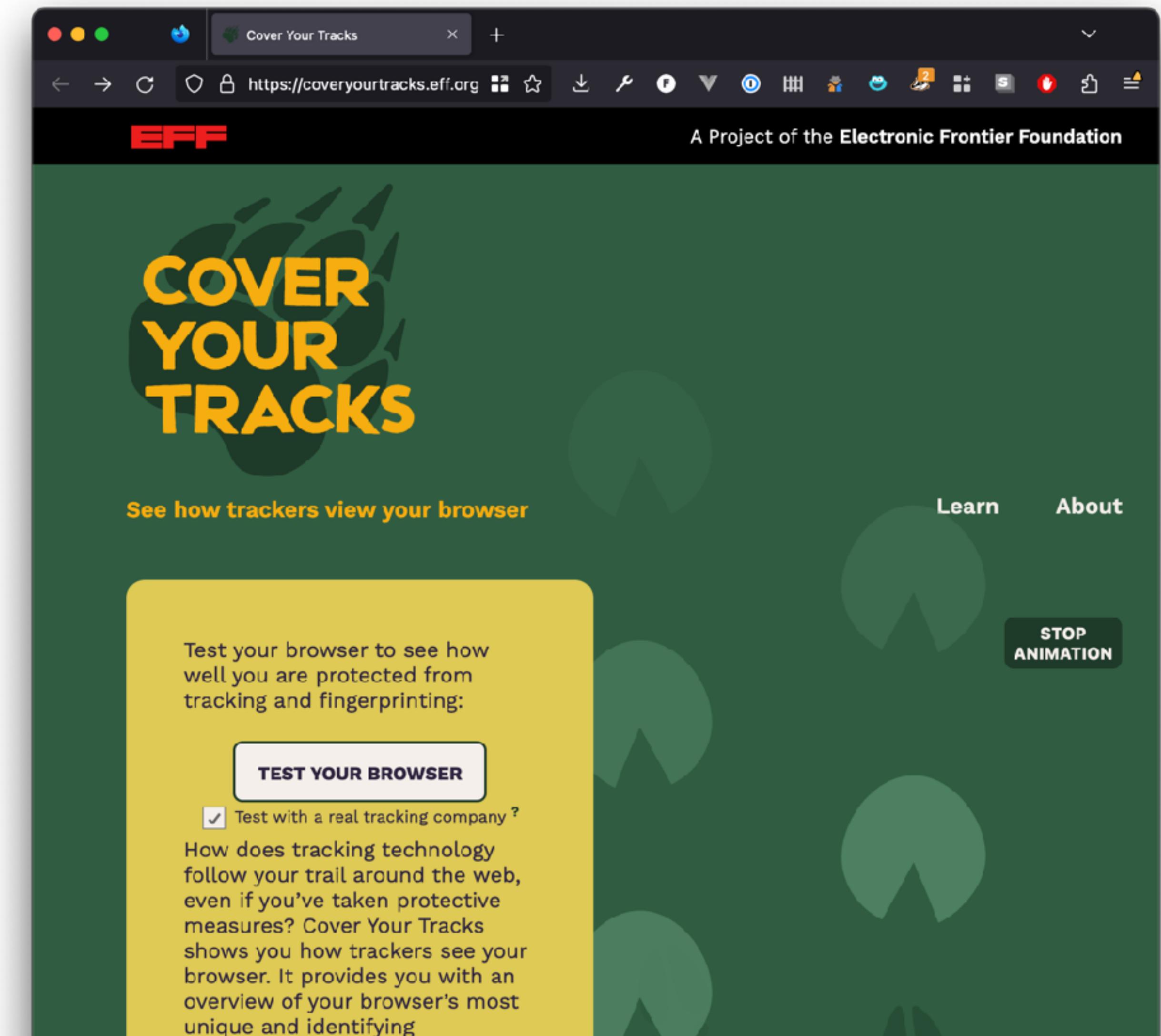
Tor Browser (*The Onion Router*)

- Routes traffic through anonymous Tor network
- Allows access to *.onion* websites
- Resist *fingerprinting*



What is fingerprinting?

- A website can test a lot of your browser's features and its settings to create an almost unique id for you.
- This allows to track your “fingerprint” across multiple sites.
- Especially with “free services” like Google fonts, Facebook Like-buttons, Image-CDNs etc.



What is fingerprinting?

- A website can test a lot of your browser's feature and its settings to create an almost unique id for you.
- This allows to track your “fingerprint” across multiple sites.
- Especially with “free services” like google fonts, Facebook Like-buttons, Image-CDNs etc.

Your Results

Your browser fingerprint **appears to be unique** among the 230,057 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.81 bits of identifying information**.

WEBGL VENDOR & RENDERER

Apple~Apple M1

Bits of identifying information: 6.79

One in x browsers have this value: 110.45

USER AGENT

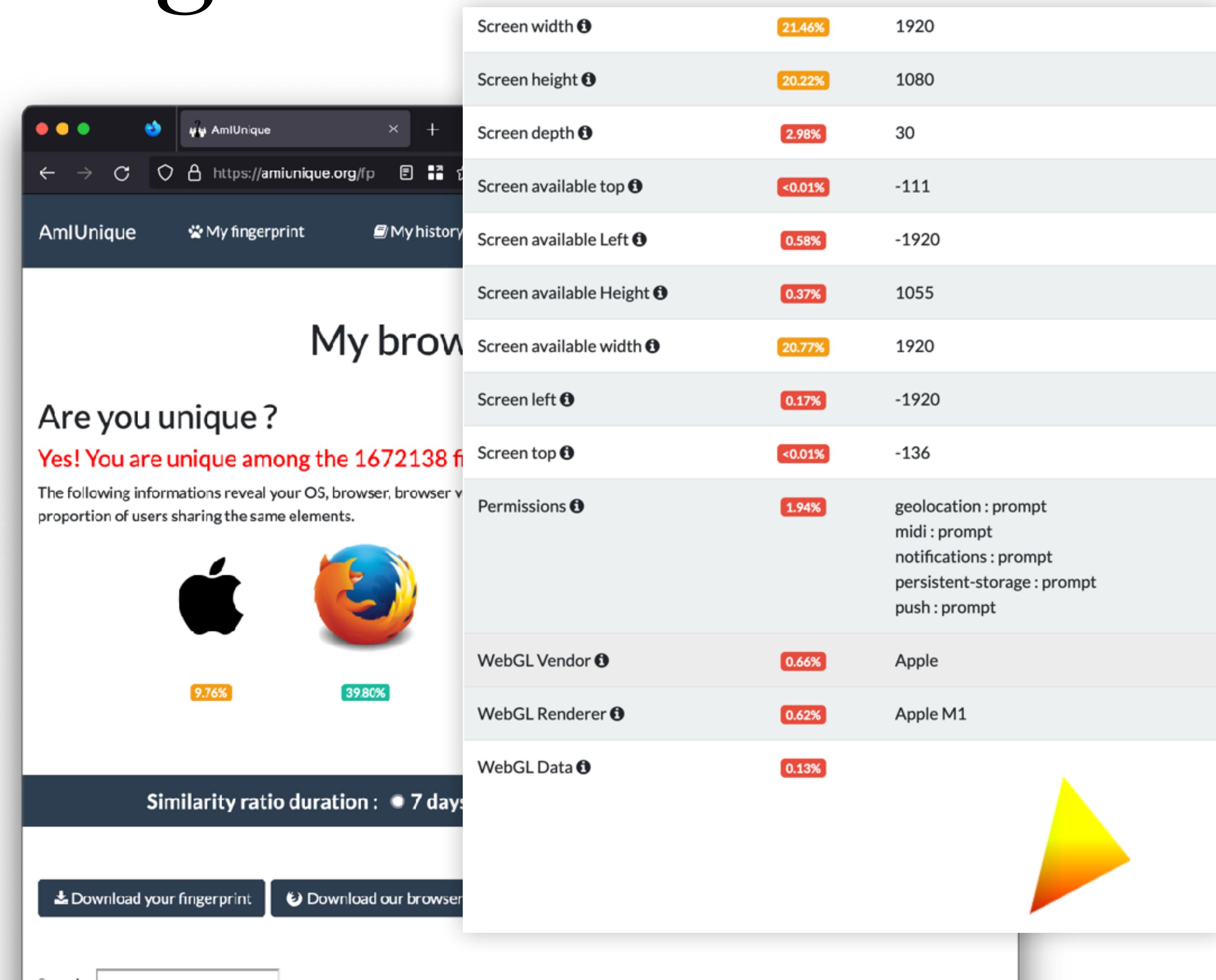
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/112.0

Bits of identifying information: 9.28

One in x browsers have this value: 623.46

What is fingerprinting?

- Screen width and height can give away much information
- Tor has a default sized window.
($x * 200\text{px}$, $y * 100\text{px}$)
→ in my case $1000\text{px} * 800\text{px}$
- Not recommended to resize because of unique fingerprint.



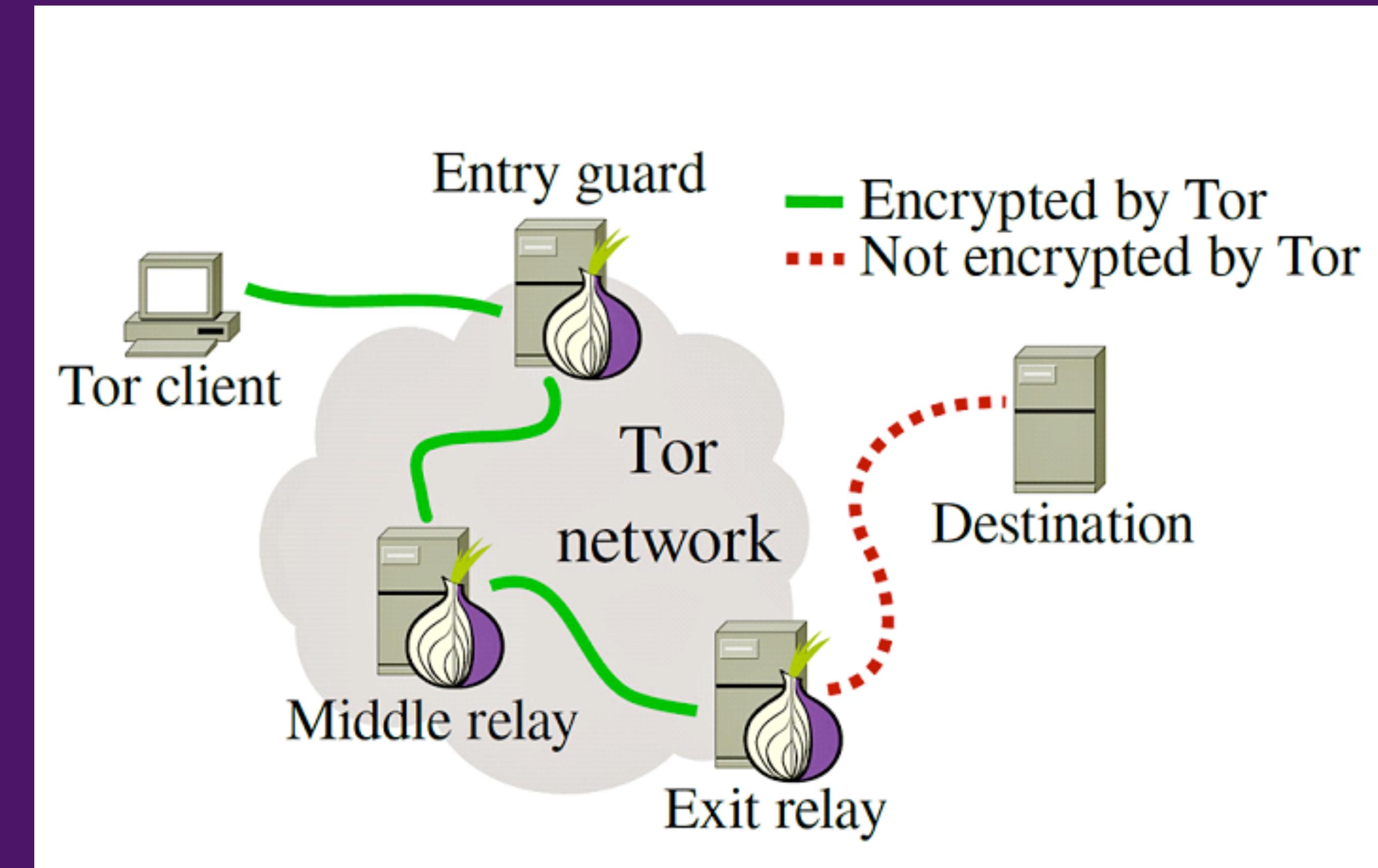
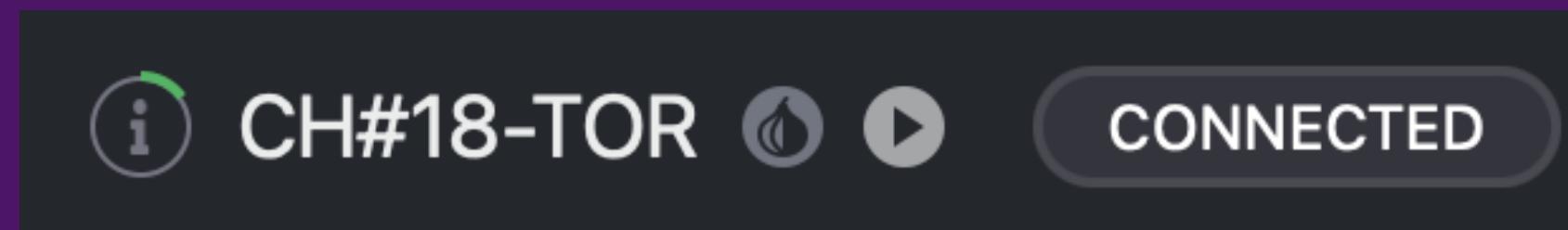
The screenshot shows a web browser window displaying the AmIUnique website (<https://amiunique.org/fp>). The page title is "AmIUnique" and the sub-page is "My fingerprint". The main content asks "Are you unique?" and displays the text "Yes! You are unique among the 1672138 fingerprinted users". Below this, it states "The following informations reveal your OS, browser, browser version, screen resolution, and more. These informations are gathered from your browser and represent the proportion of users sharing the same elements." It shows two icons: an Apple logo and a Firefox logo, with percentages 9.76% and 39.80% respectively. A heatmap titled "Similarity ratio duration : ● 7 days" is shown below, with a color gradient from blue to red. To the right, a detailed table lists various browser fingerprint characteristics with their values and proportions:

Screen width ⓘ	21.46%	1920
Screen height ⓘ	20.22%	1080
Screen depth ⓘ	2.98%	30
Screen available top ⓘ	<0.01%	-111
Screen available Left ⓘ	0.58%	-1920
Screen available Height ⓘ	0.37%	1055
Screen available width ⓘ	20.77%	1920
Screen left ⓘ	0.17%	-1920
Screen top ⓘ	<0.01%	-136
Permissions ⓘ	1.94%	geolocation : prompt midi : prompt notifications : prompt persistent-storage : prompt push : prompt
WebGL Vendor ⓘ	0.66%	Apple
WebGL Renderer ⓘ	0.62%	Apple M1
WebGL Data ⓘ	0.13%	

At the bottom, there are buttons for "Download your fingerprint" and "Download our browser". A search bar is also present at the very bottom.

Tor Browser (The Onion Router)

- Each relay (= Tor node) decrypts the next “onion layer” to reveal only the next relay
- Some VPN Services offer to reroute traffic through Tor



.onion

- 56 mostly random letters and numbers characters
- e.g. DuckDuckGo hidden service:
<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswczad.onion/>
- On server in Tor network (only accessible with Tor-browser)
- No spying possible on Tor exit node,
because it is inside the Tor network