I don’t do title slides

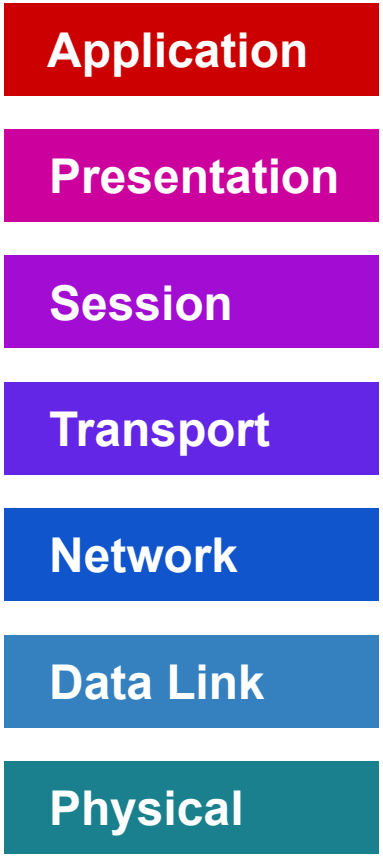
I don’t do title slides

or matching socks

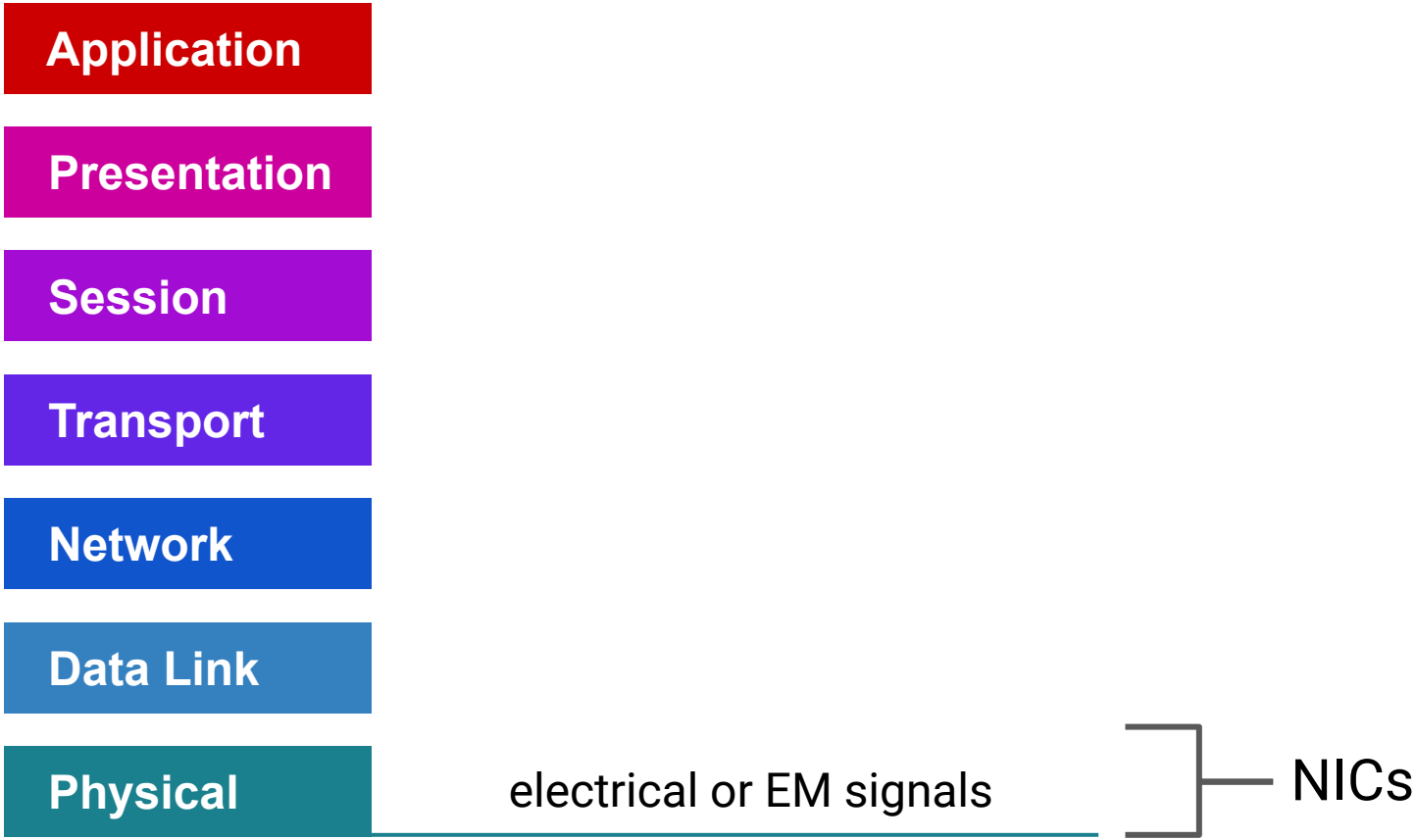
TRUST

& how the net works

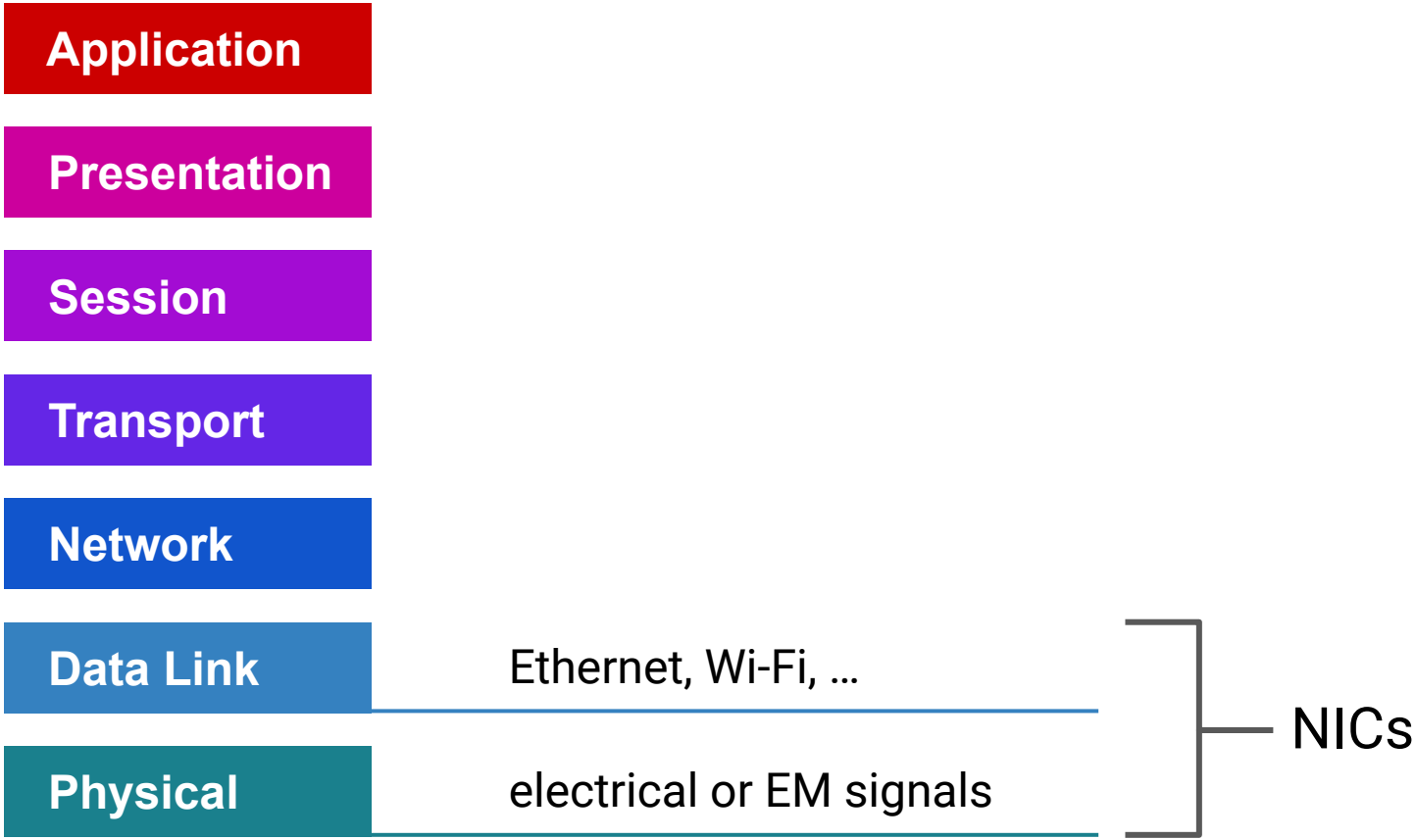
The OSI layers



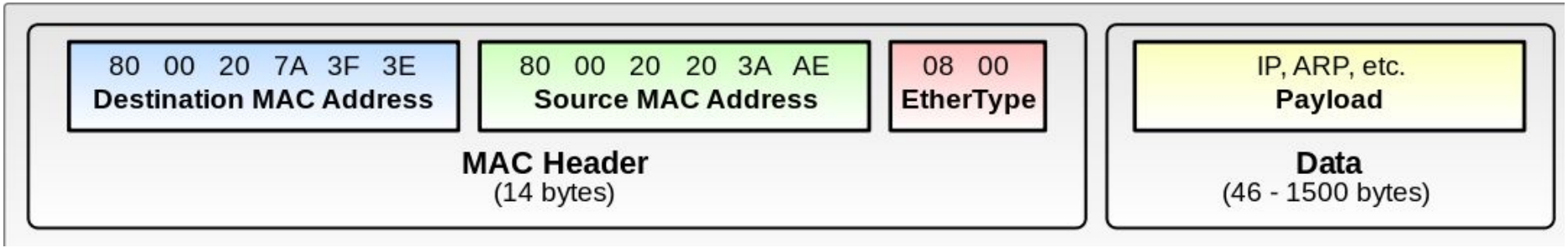
The OSI layers



The OSI layers

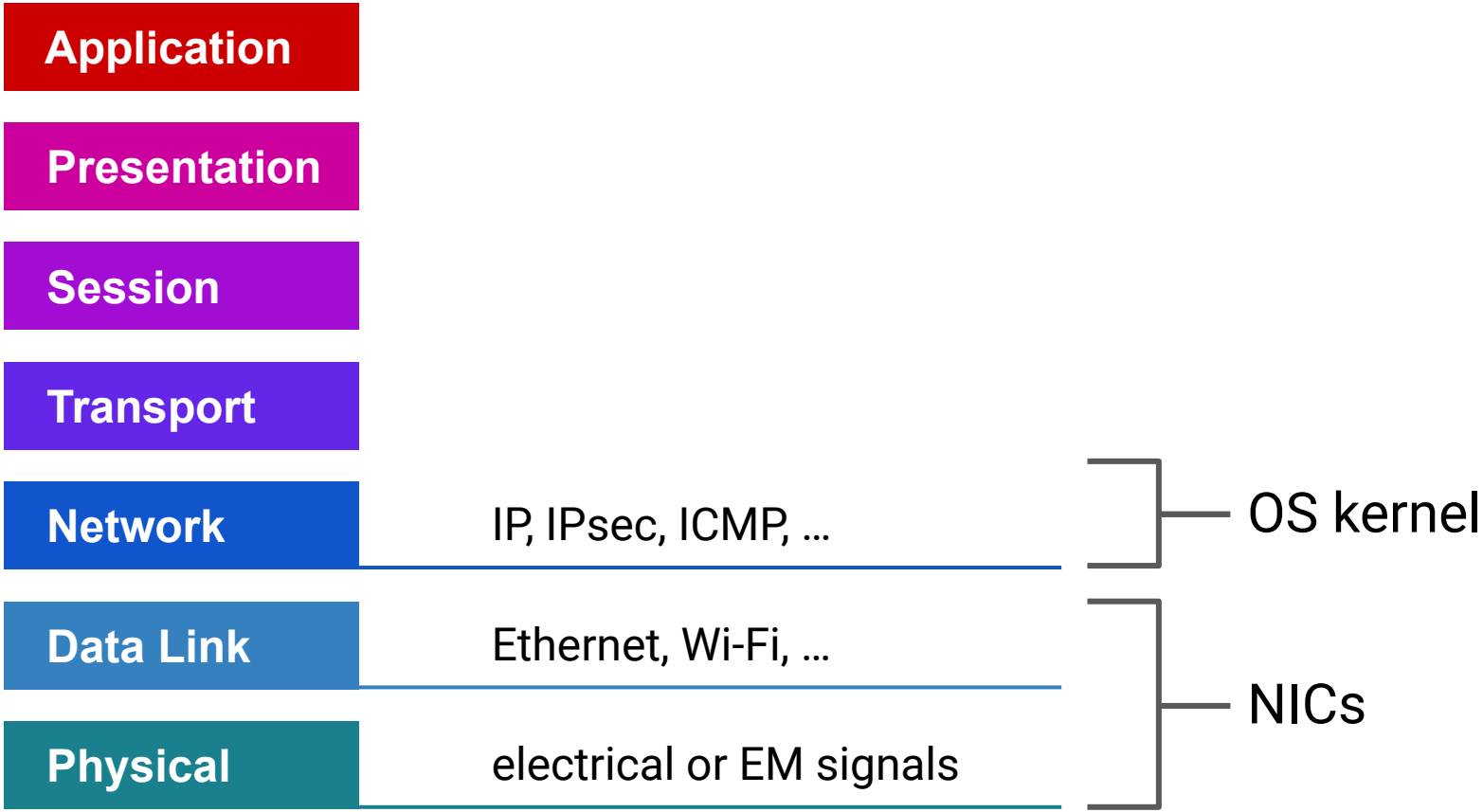


Ethernet (IEEE 802.3) frame

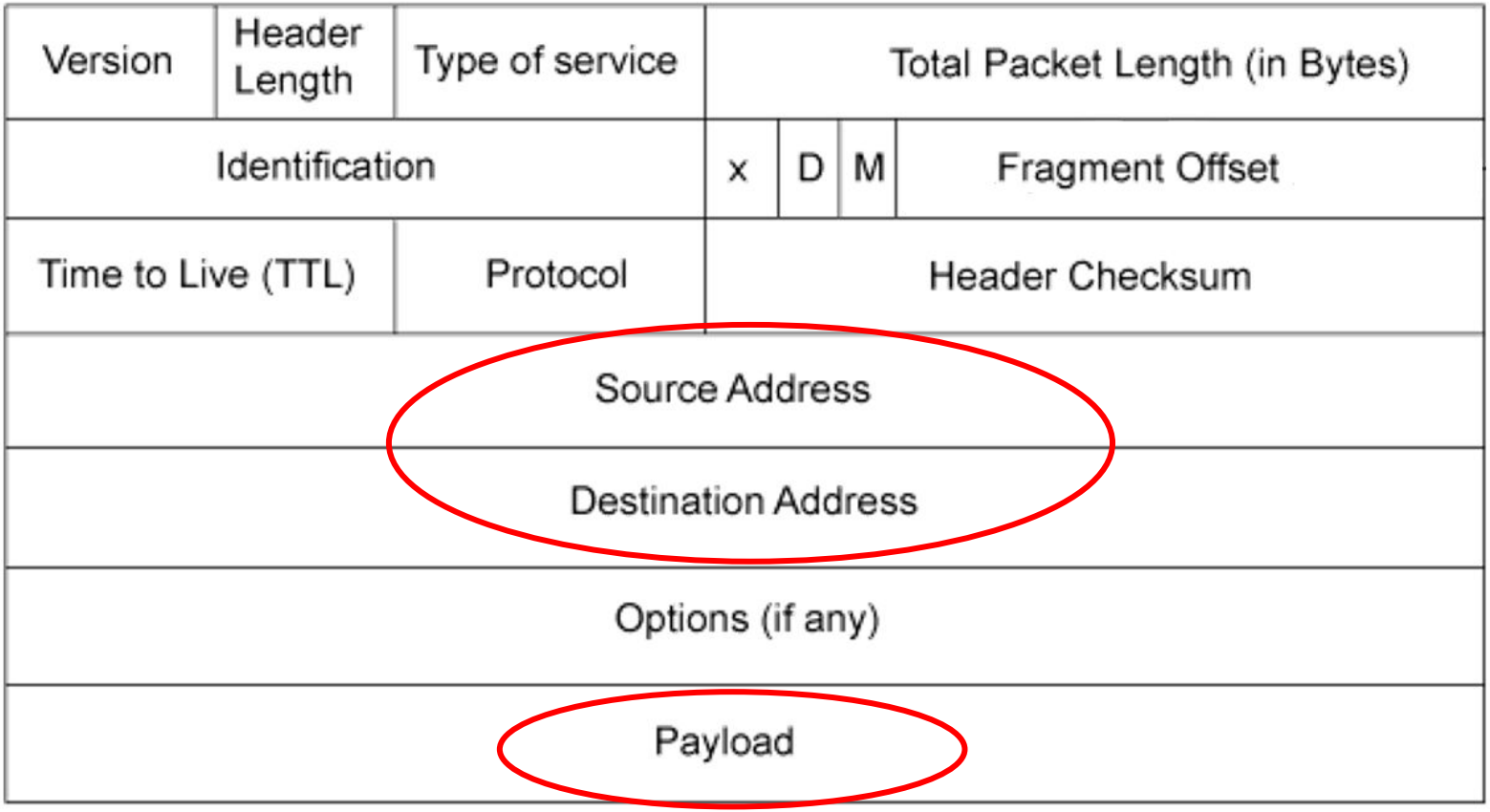


Note: Wireless (IEEE 802.11) is similar

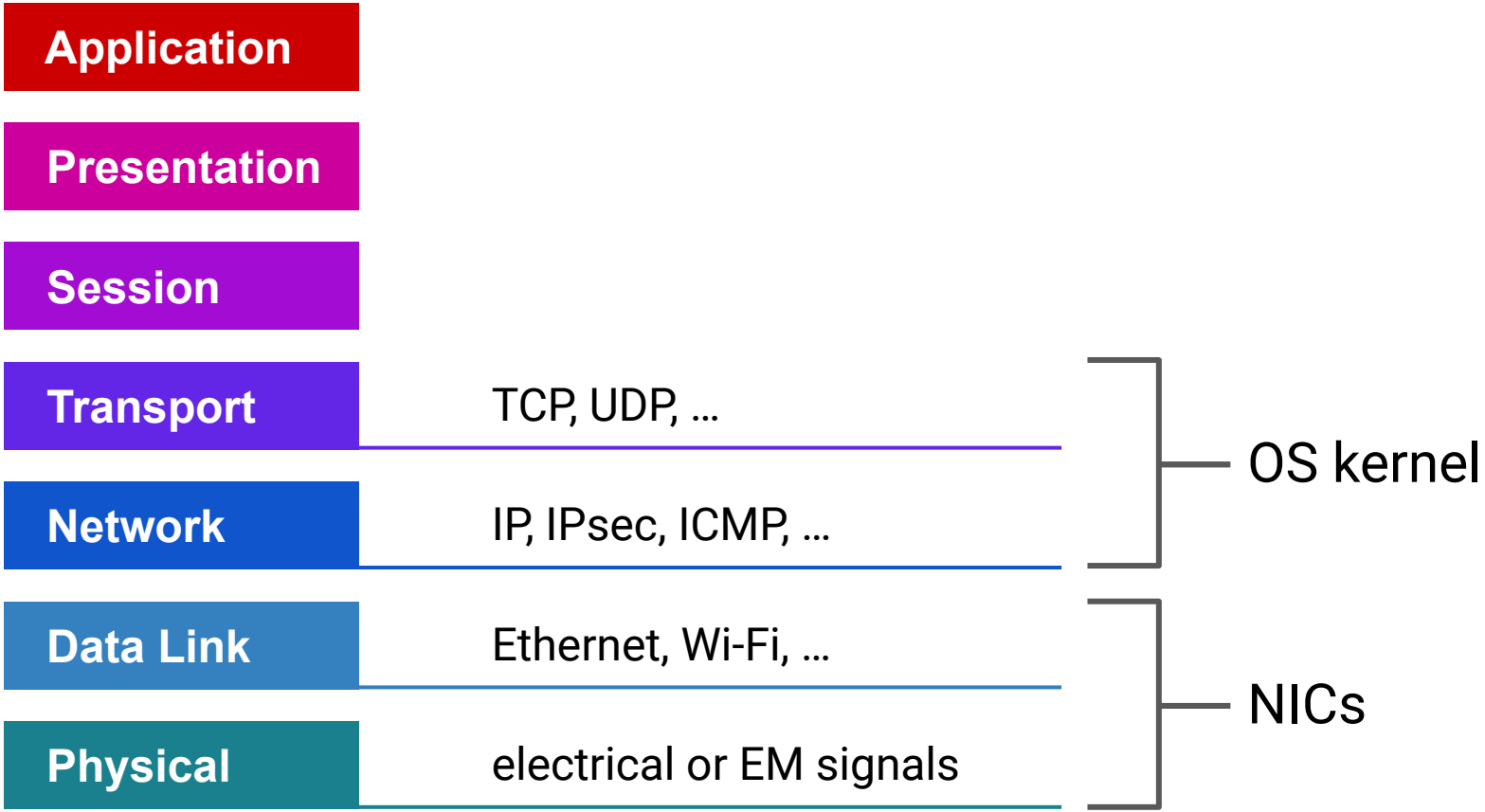
The OSI layers



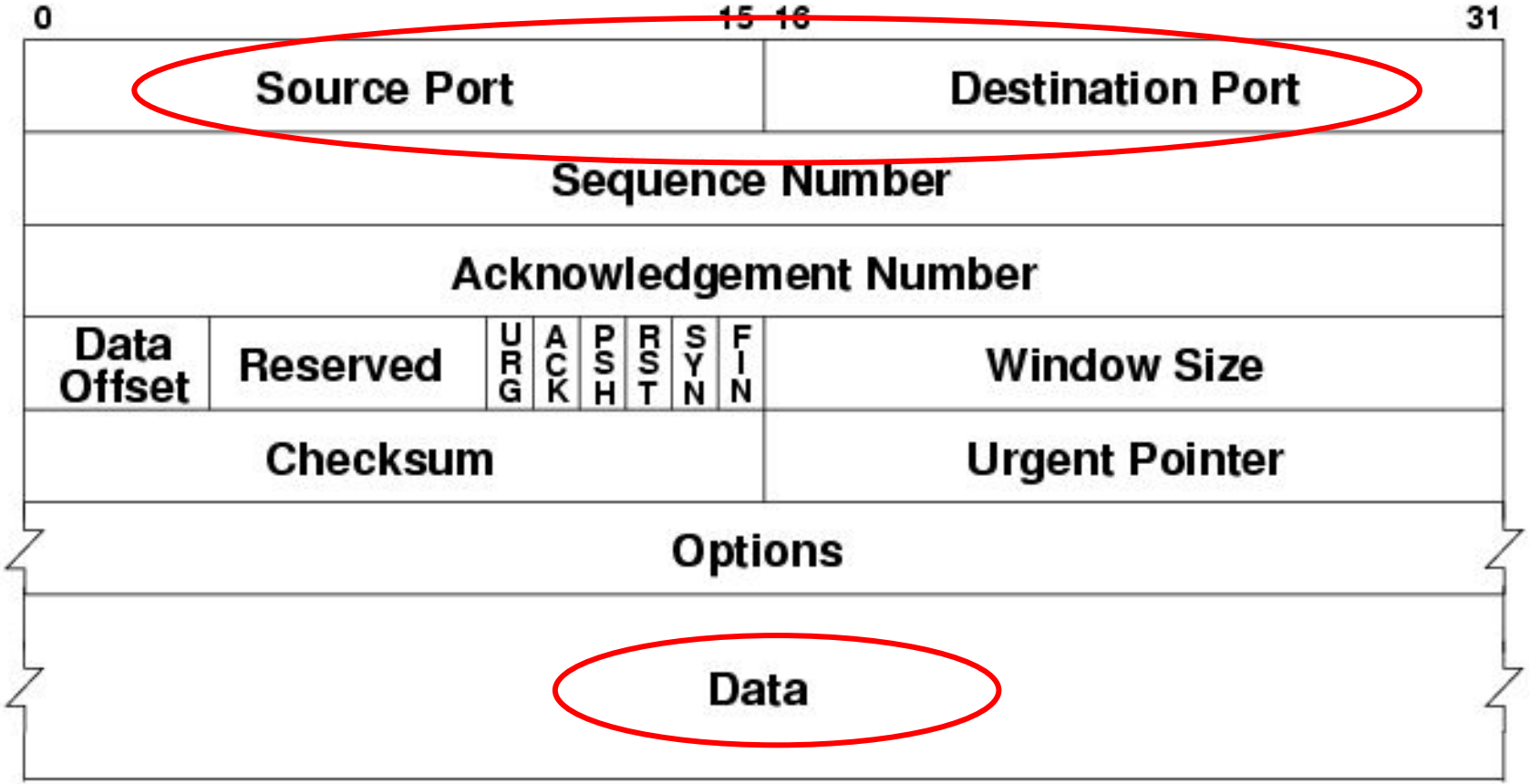
IP frame


Version
Header Length
Type of service
Total Packet Length (in Bytes)
Identification
x
D
M
Fragment Offset
Time to Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options (if any)
Payload

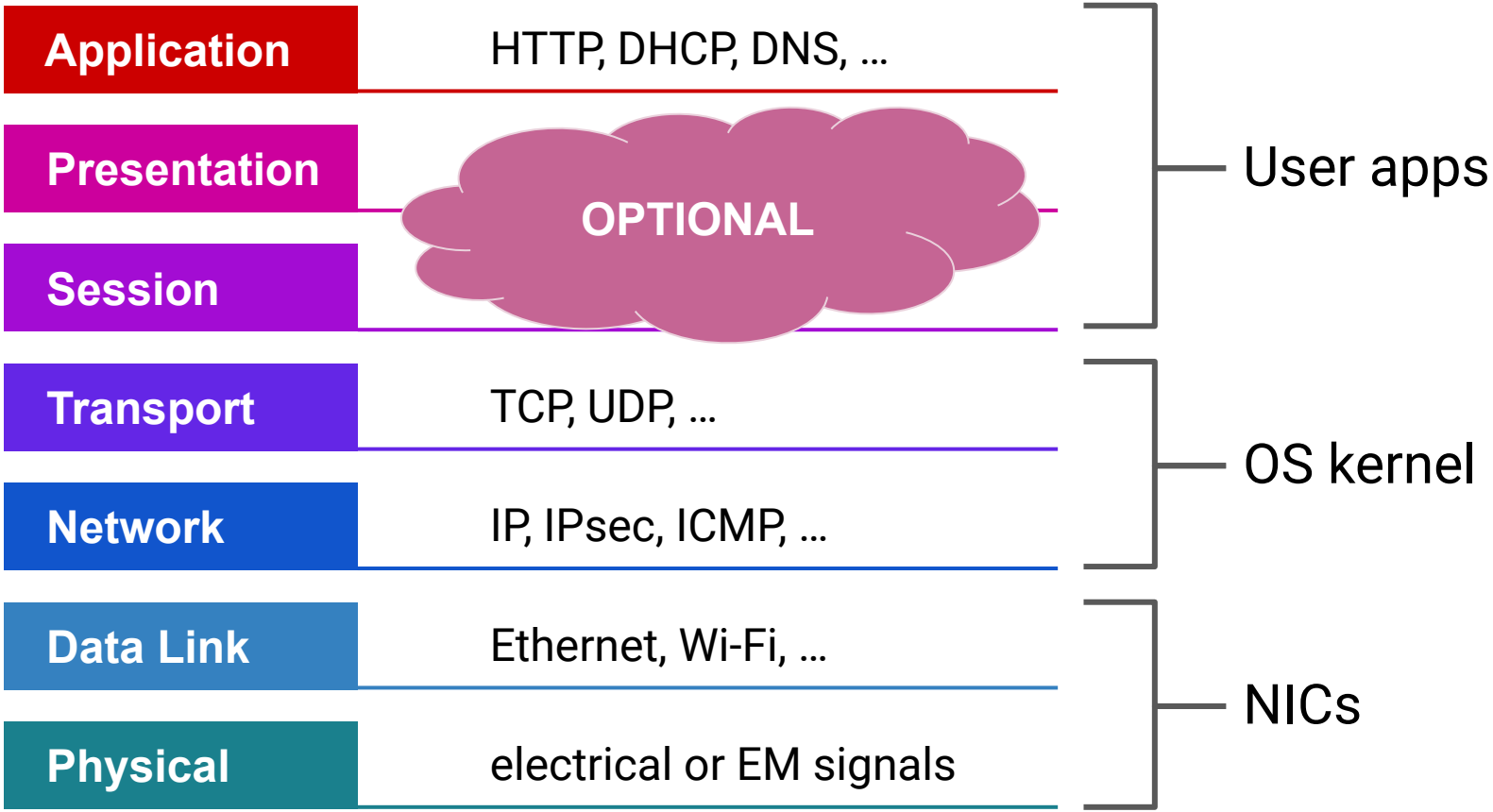
The OSI layers



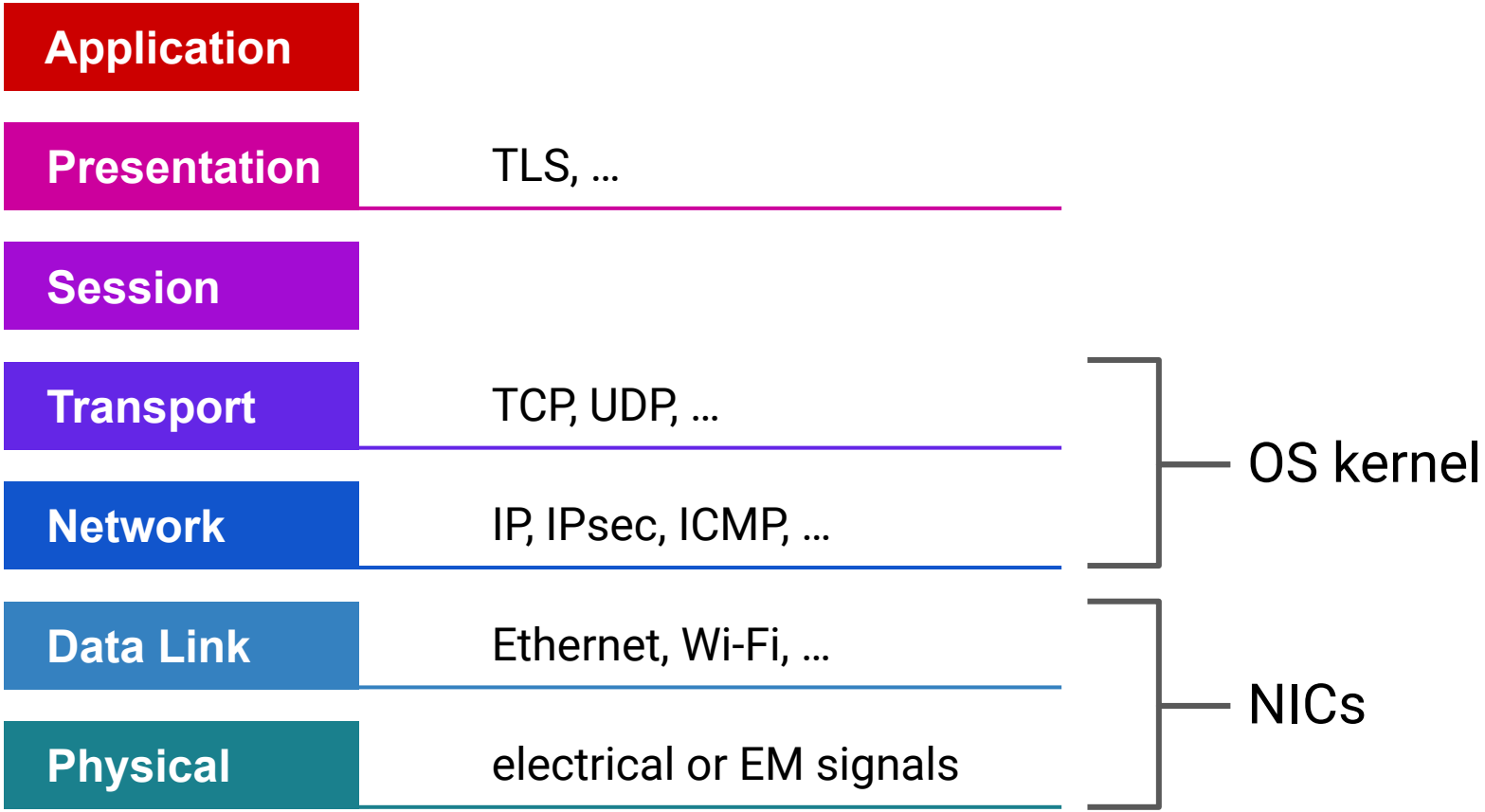
TCP frame


0
15 16
31
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window Size
Checksum
Urgent Pointer
Options
Data

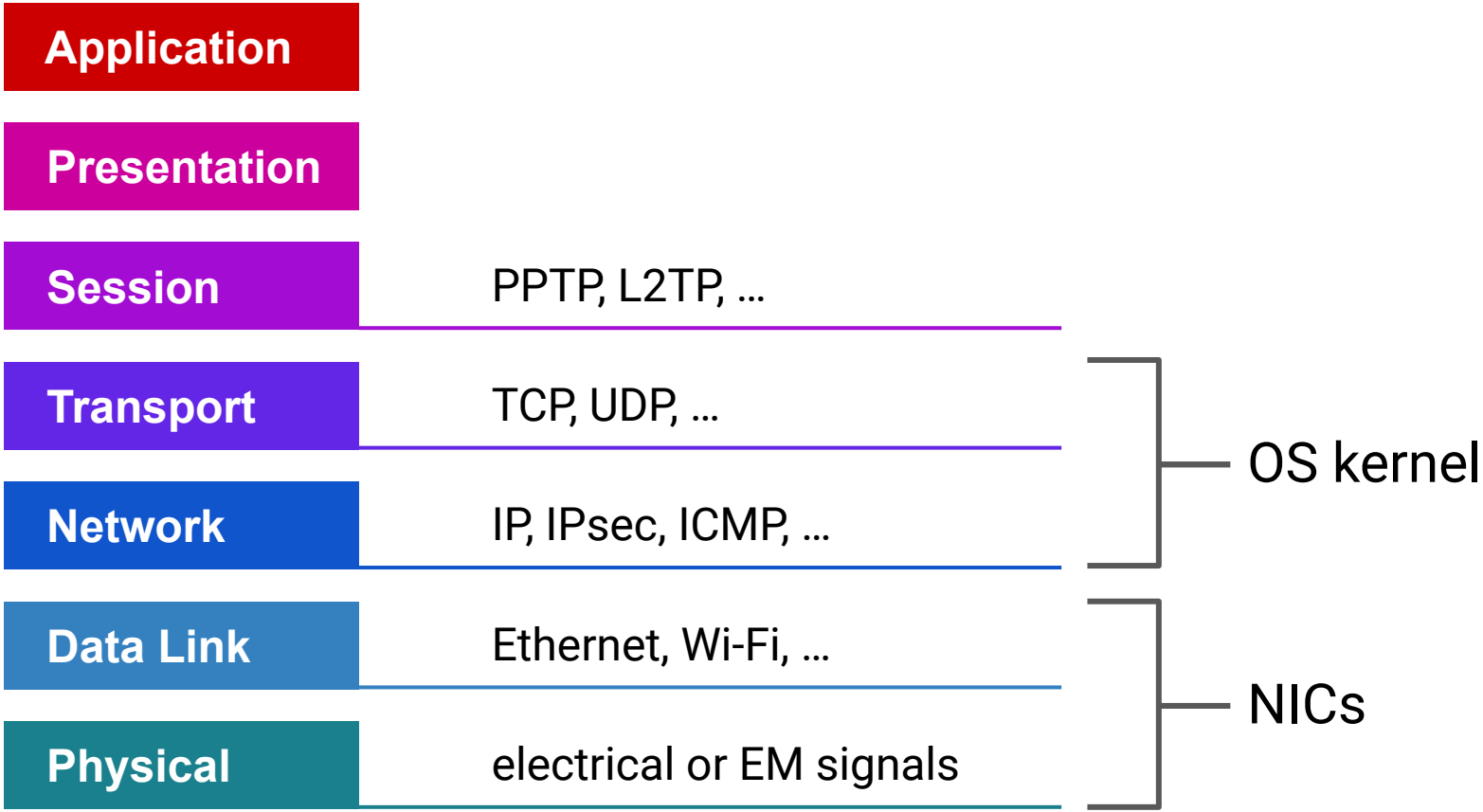
The OSI layers



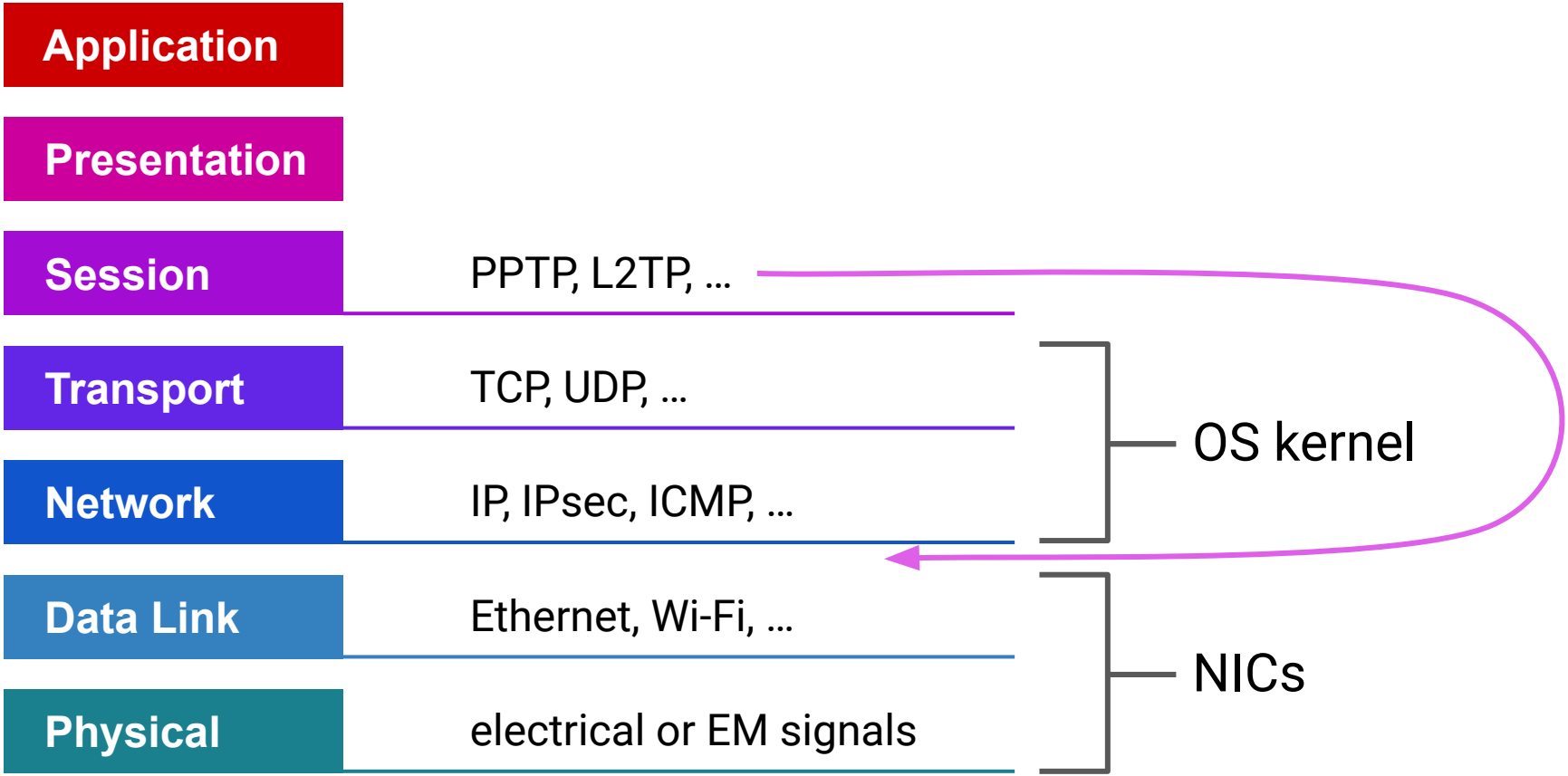
The OSI layers



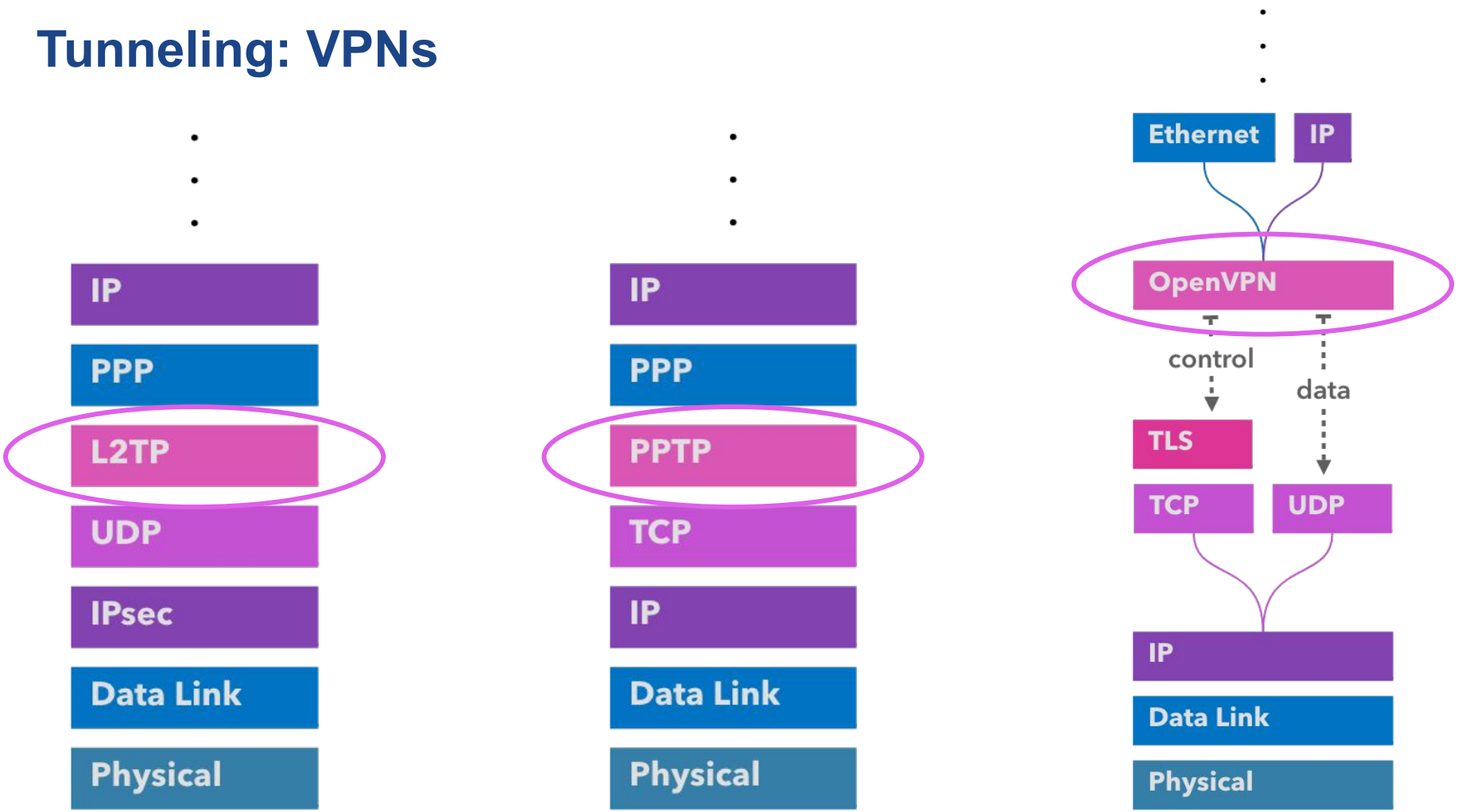
The OSI layers



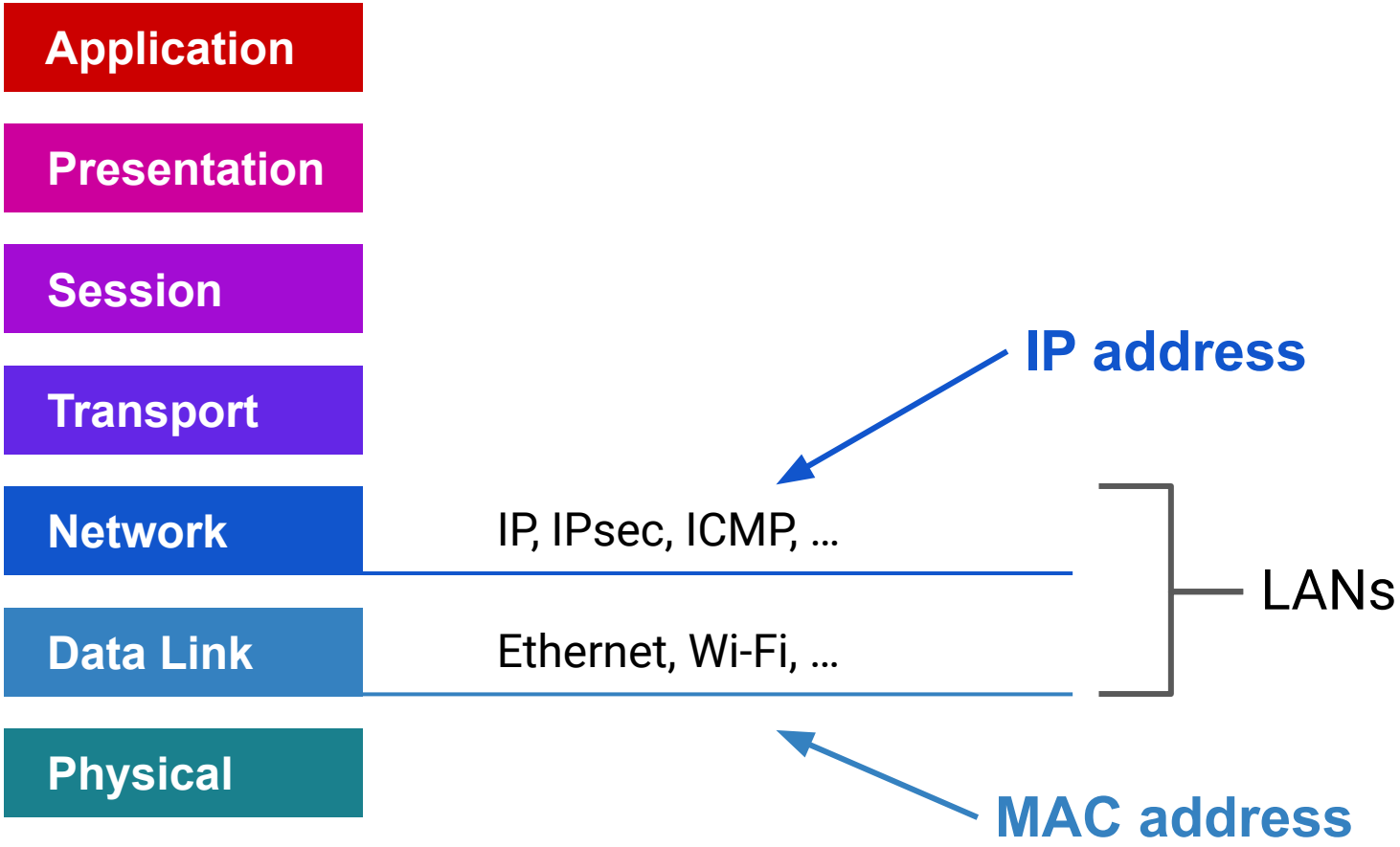
The OSI layers

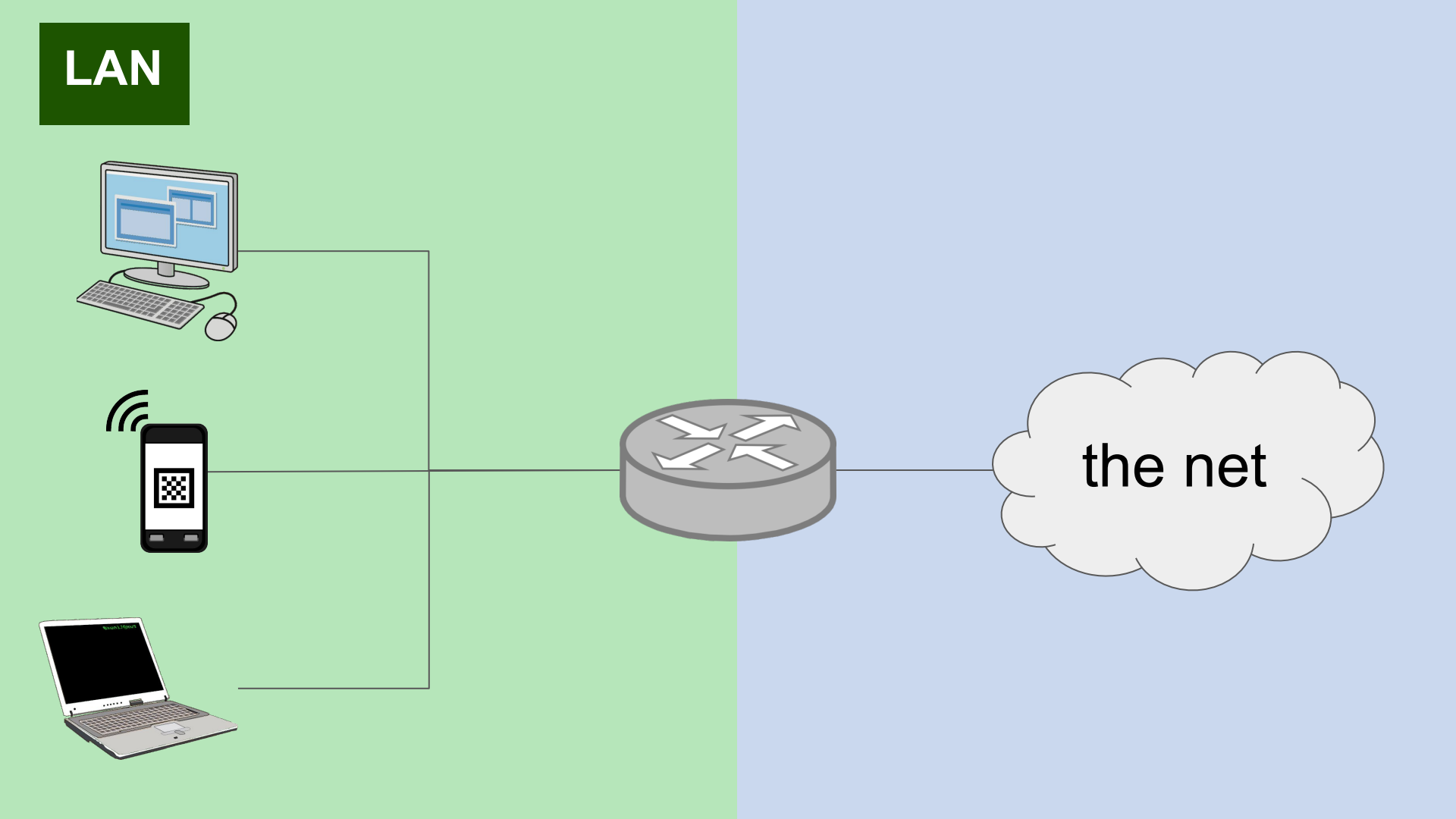


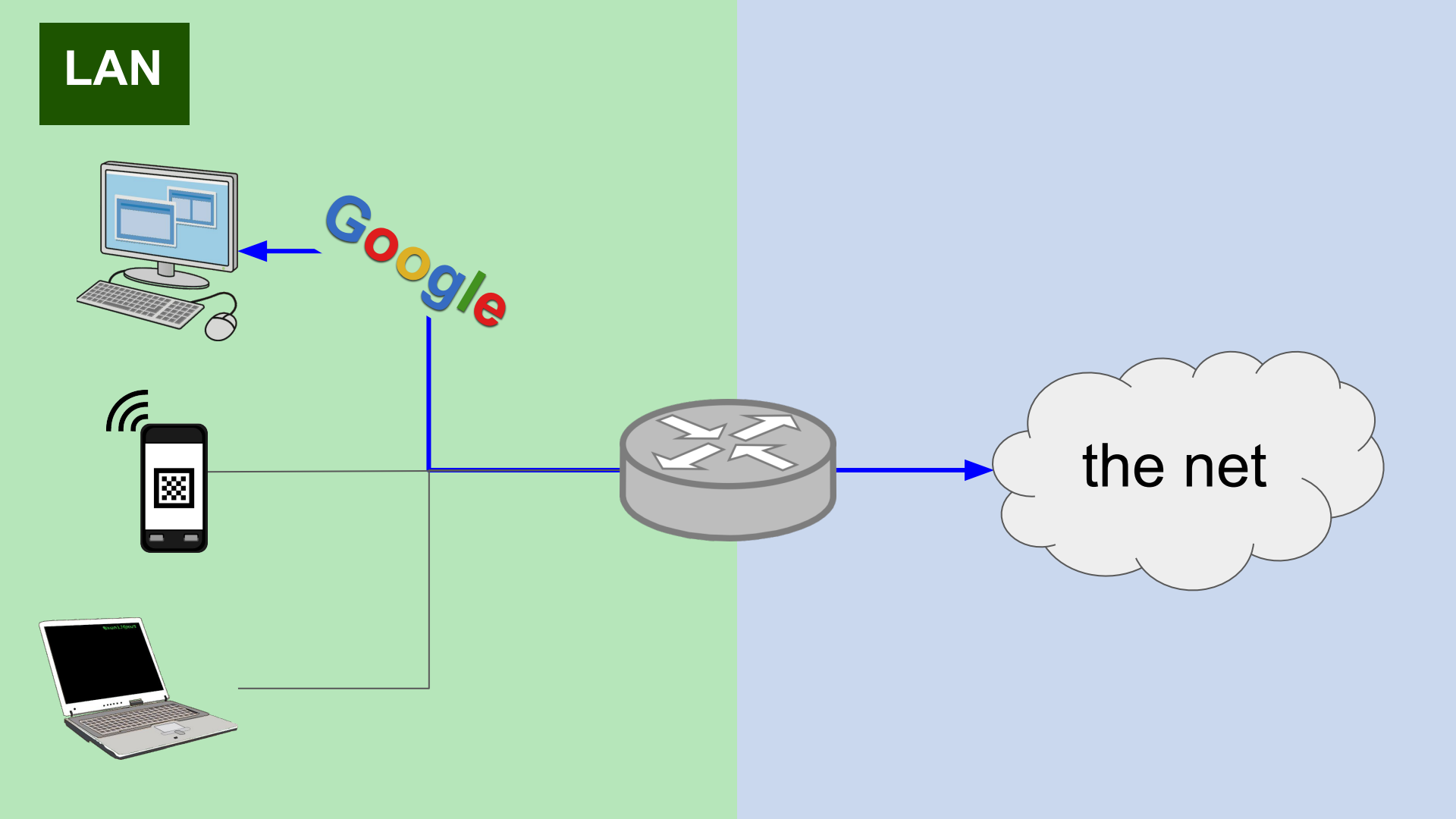
Tunneling: VPNs

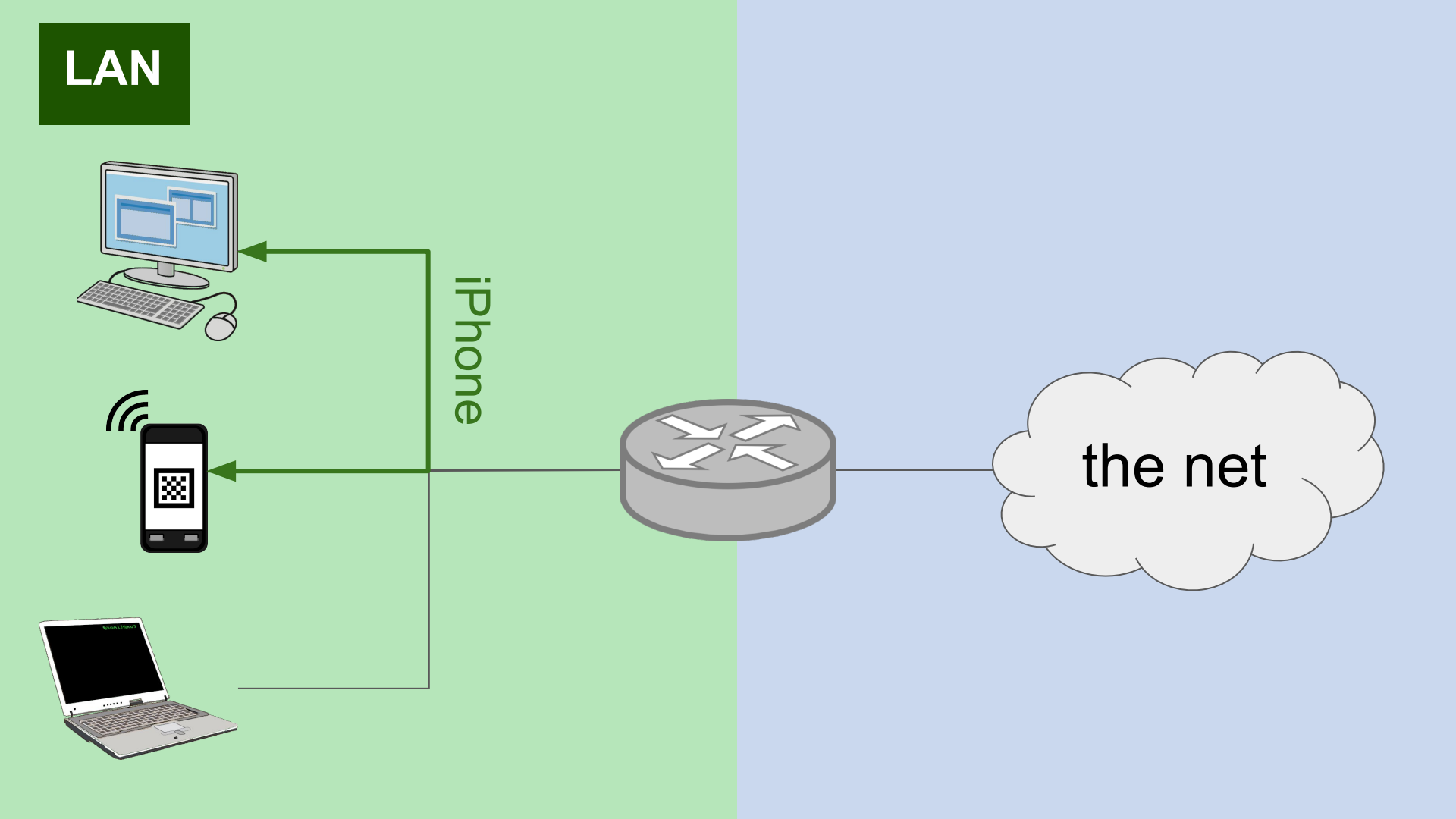


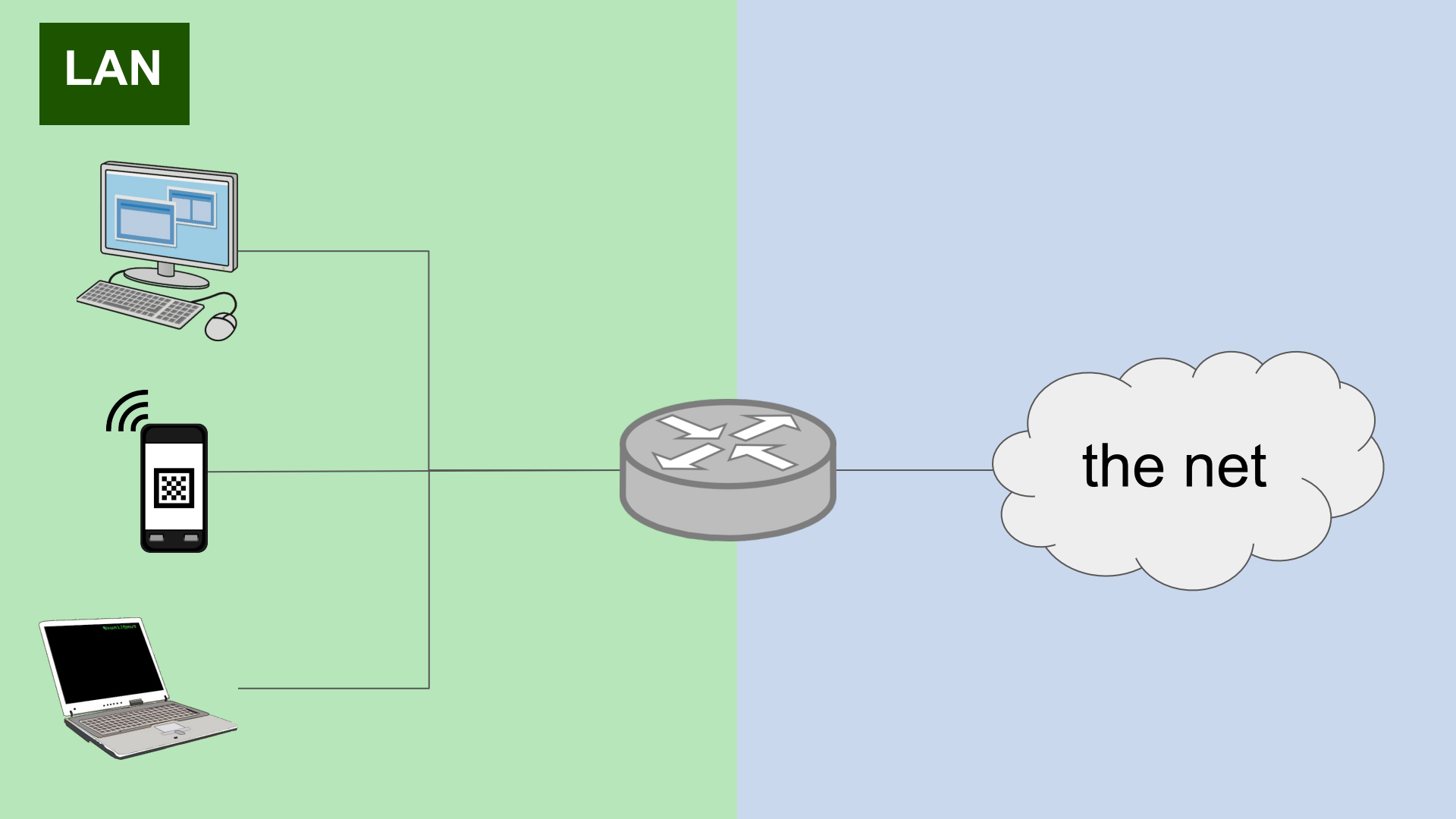
The OSI layers

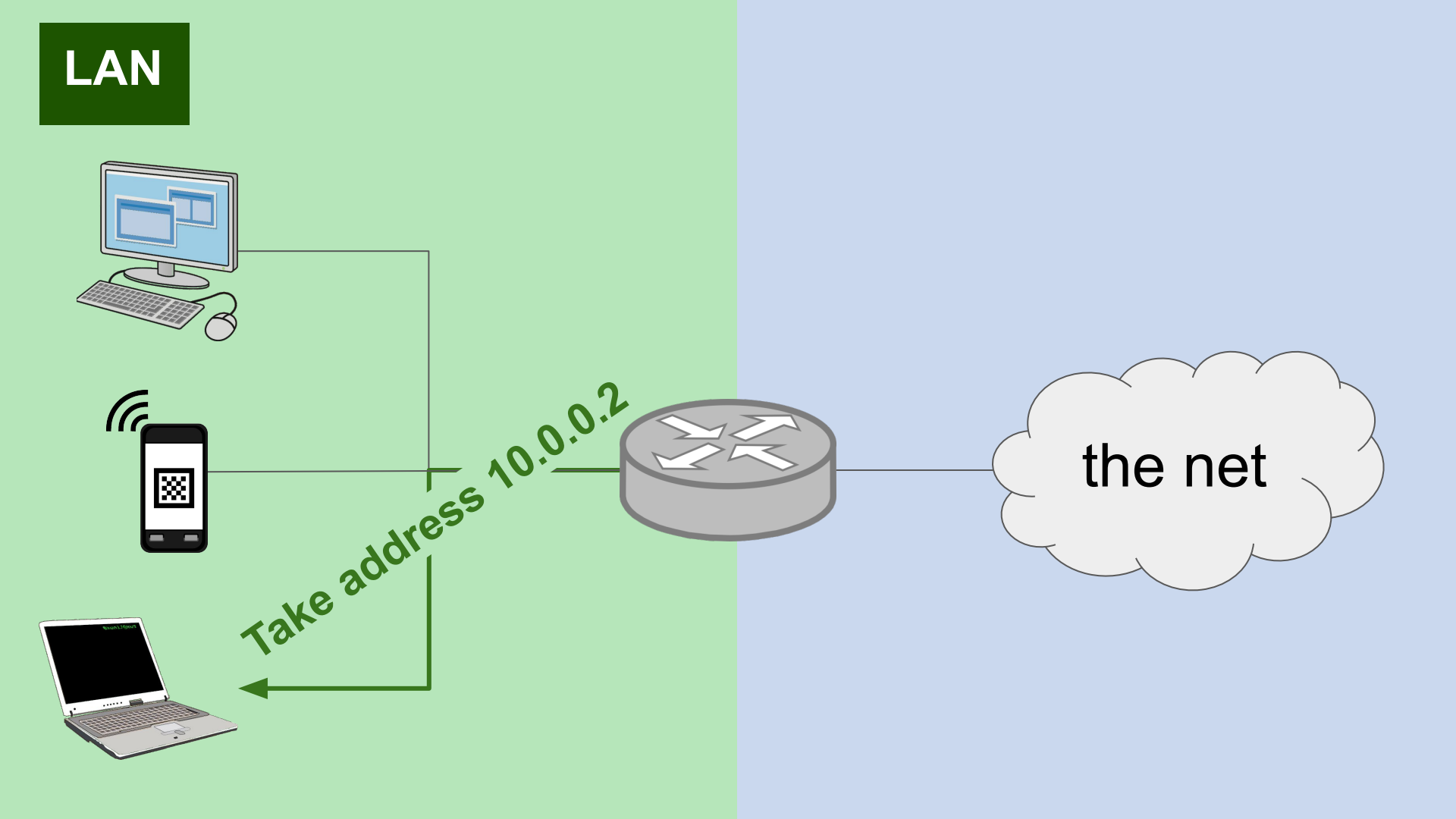


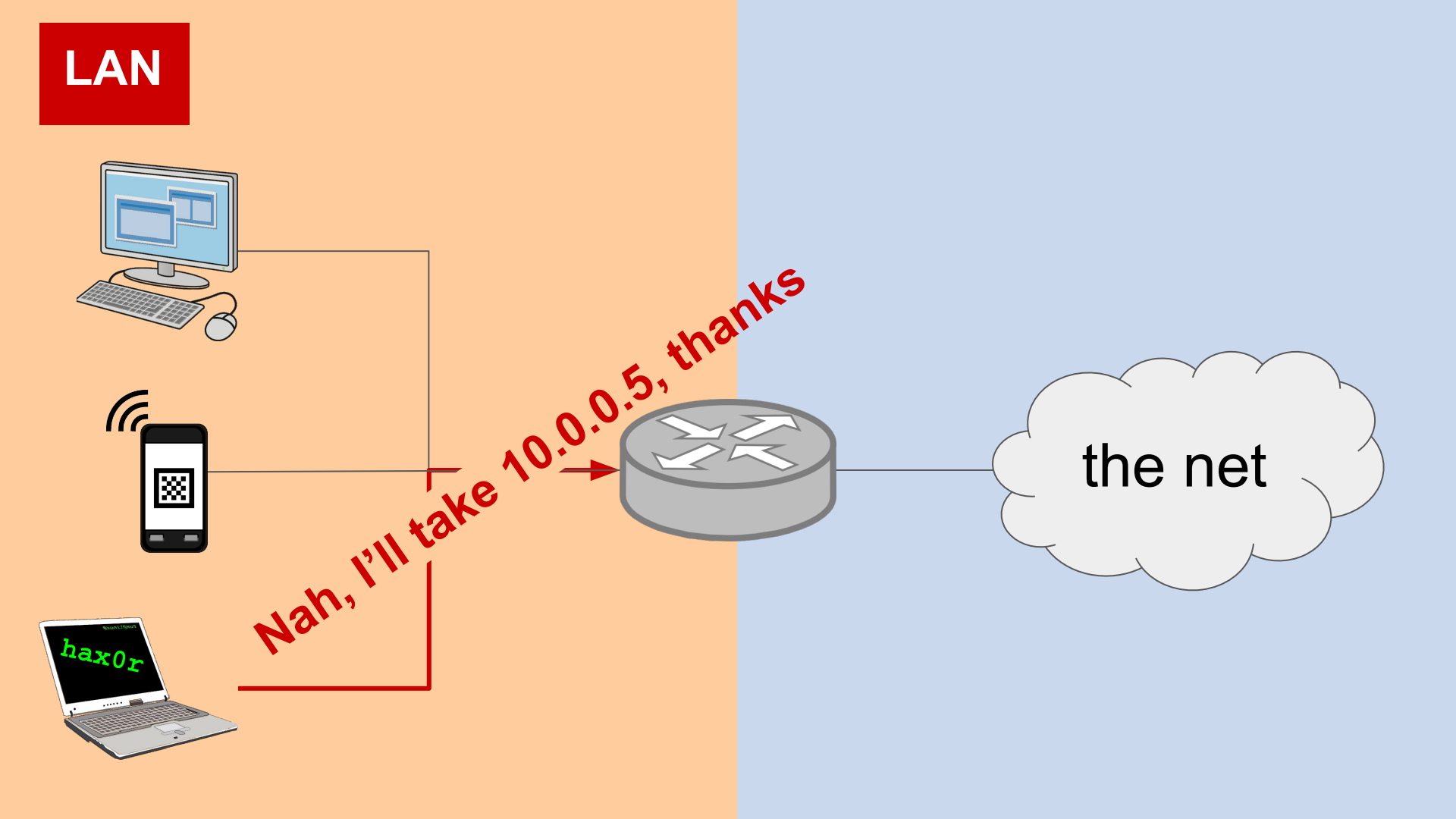

LAN
the net


LAN
Google
the net


LAN
iPhone
the net

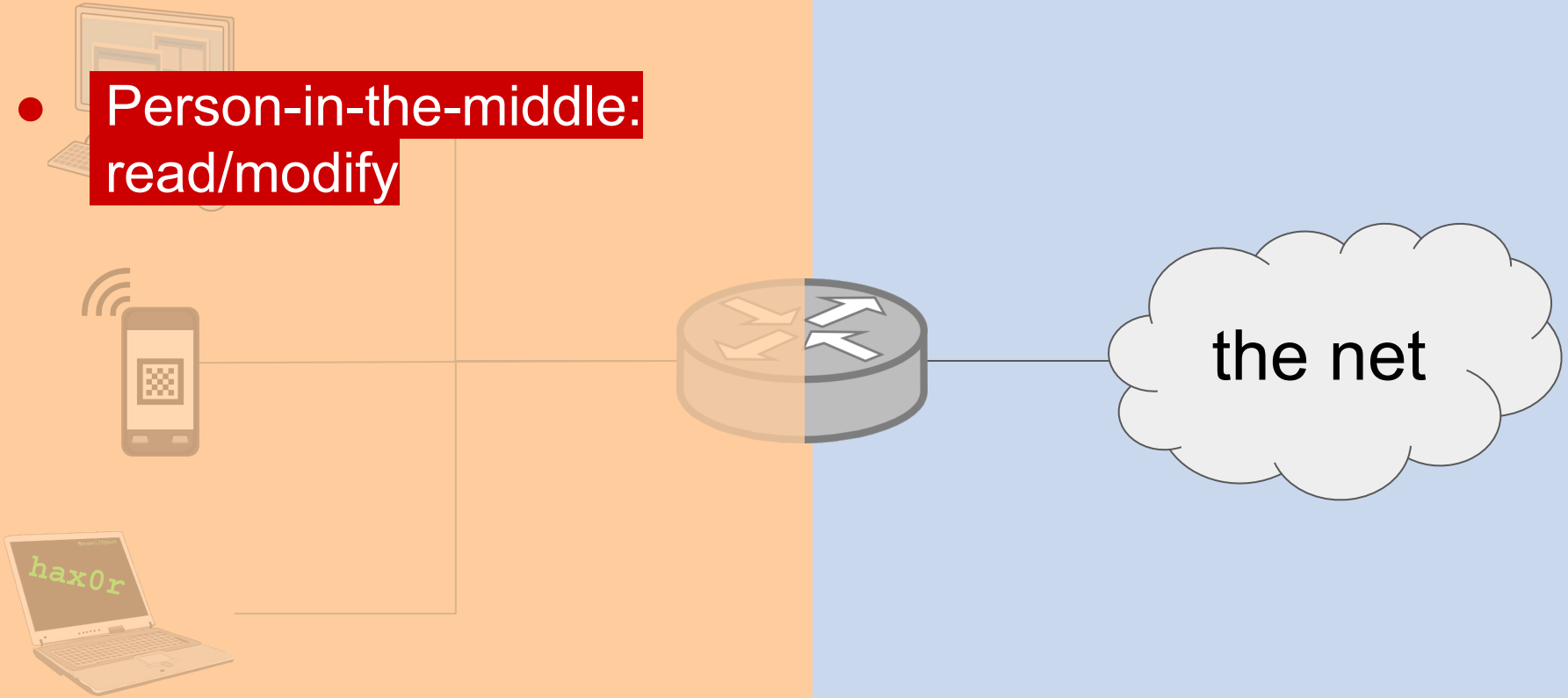

LAN
the net


LAN
Take address 10.0.0.2
the net


LAN
Nah, I'll take 10.0.0.5, thanks
haxOr
the net

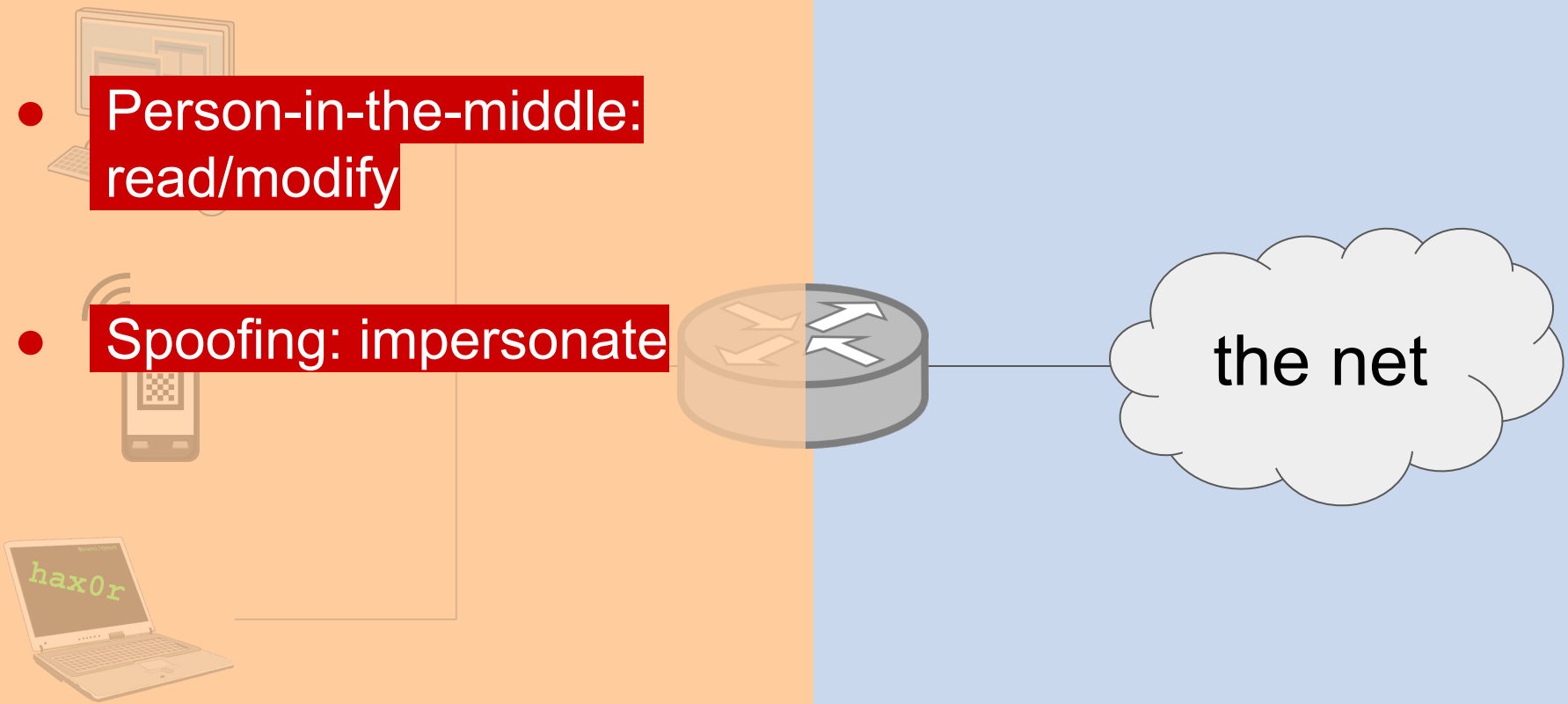
LAN

- Person-in-the-middle: read/modify



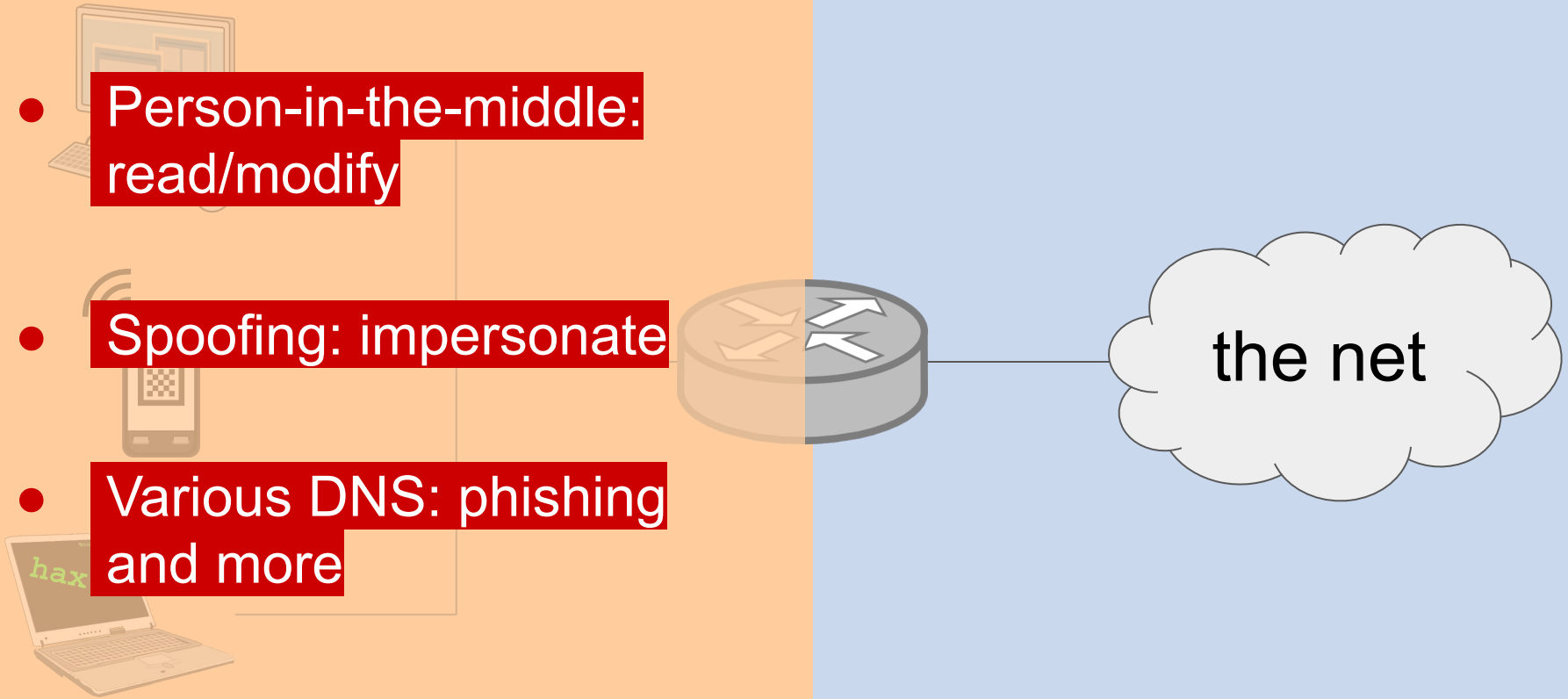
LAN

- Person-in-the-middle: read/modify
- Spoofing: impersonate



LAN

- Person-in-the-middle: read/modify
- Spoofing: impersonate
- Various DNS: phishing and more



To do

To do

To do

To do

The OSI layers

Application	HTTP, DHCP, DNS, …
Presentation	TLS, …
Session	
Transport	TCP, UDP, …
Network	IP, IPsec, ICMP, …
Data Link	Ethernet, Wi-Fi, …
Physical	electrical or EM signals

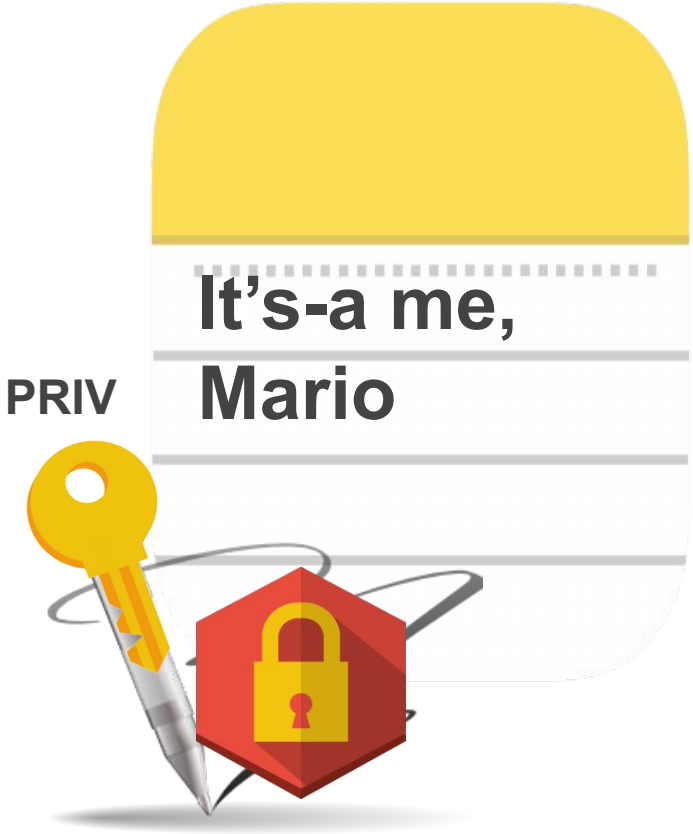
Encryption: a) privacy

Encryption: a) privacy

Encryption: b) authentication

Encryption: b) authentication

Encryption: b) authentication



Encryption: b) authentication

Encryption: b) authentication

Encryption: b) authentication and integrity

Encryption: b) authentication and integrity ⇒ TRUST

Encryption protocols:

Encryption protocols: SSL/TLS

Encryption protocols: SSL/TLS, PGP

Encryption protocols: SSL/TLS, PGP, ???

Encryption protocols: SSL/TLS, ~~PGP, ???~~

CLIENT

SERVER

SSL/TLS

CLIENT

SERVER

SSL/TLS

Here’re my KEX algorithms, give me your cert

CLIENT

SERVER

SSL/TLS

PUB

PRIV

Here’re my KEX algorithms, give me your cert

Here’s my cert and public key, send me the PMK

CLIENT

SERVER

SSL/TLS

PUB

PRIV

Here’re my KEX algorithms, give me your cert

Here’s my cert and public key, send me the PMK

SSL/TLS

CLIENT

SERVER

PUB

PRIV

Here’re my KEX algorithms, give me your cert

Here’s my cert and public key, send me the PMK

Here’s the encrypted PMK, decrypt it with your private key

CLIENT

SERVER

SSL/TLS

PUB

PRIV

Here’re my KEX algorithms, give me your cert

Here’s my cert and public key, send me the PMK

Here’s the encrypted PMK, decrypt it with your private key

CLIENT

SERVER

SSL/TLS

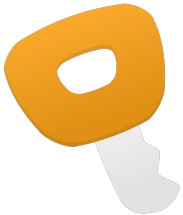
PUB

PRIV

Here’re my KEX algorithms, give me your cert

Here’s my cert and public key, send me the PMK

Here’s the encrypted PMK, decrypt it with your private key



Shared secret

Shared secret

SSL/TLS

CLIENT

SERVER

PUB

PRIV

Here're my KEX algorithms, give me your cert

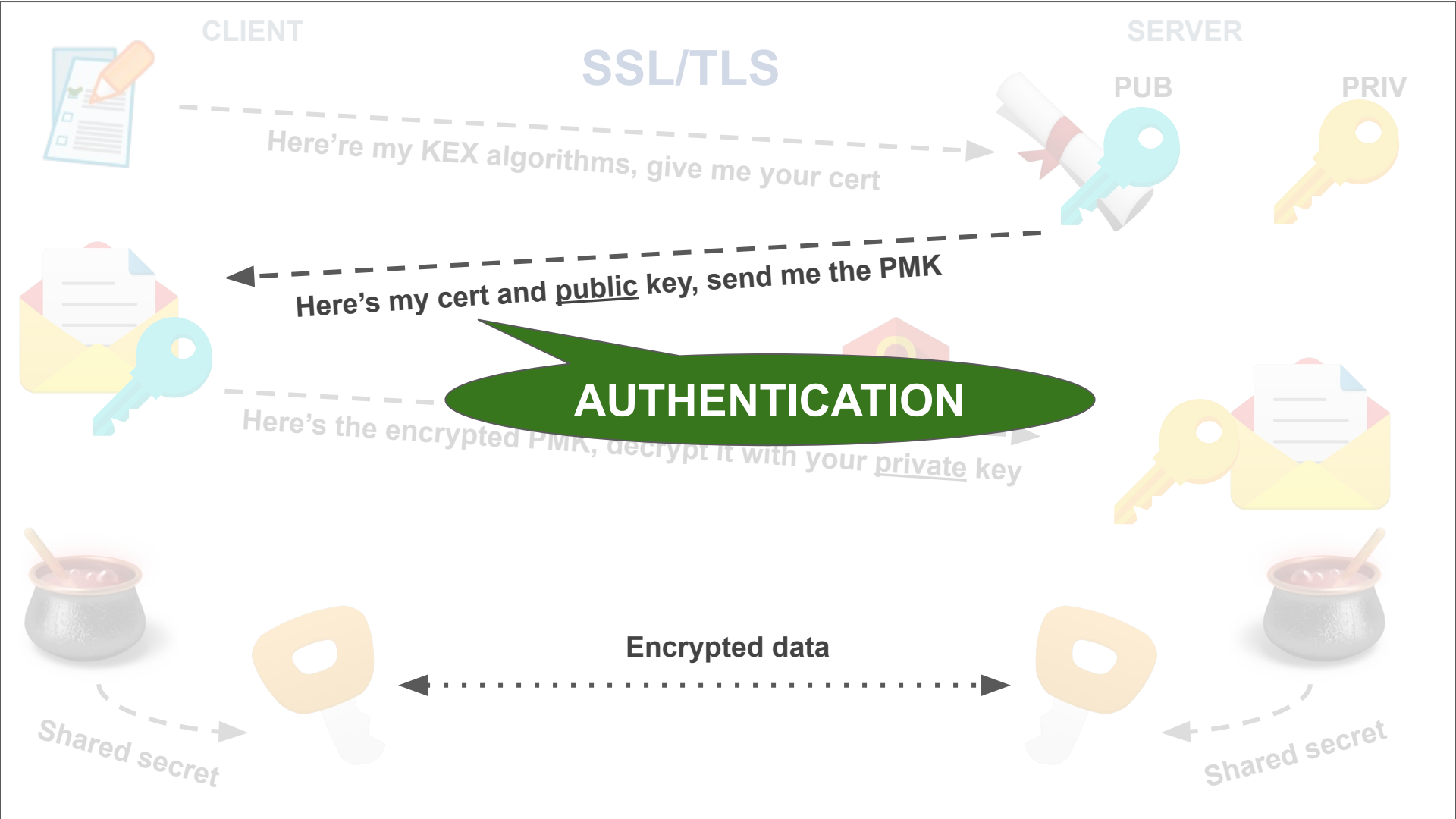
Here's my cert and public key, send me the PMK

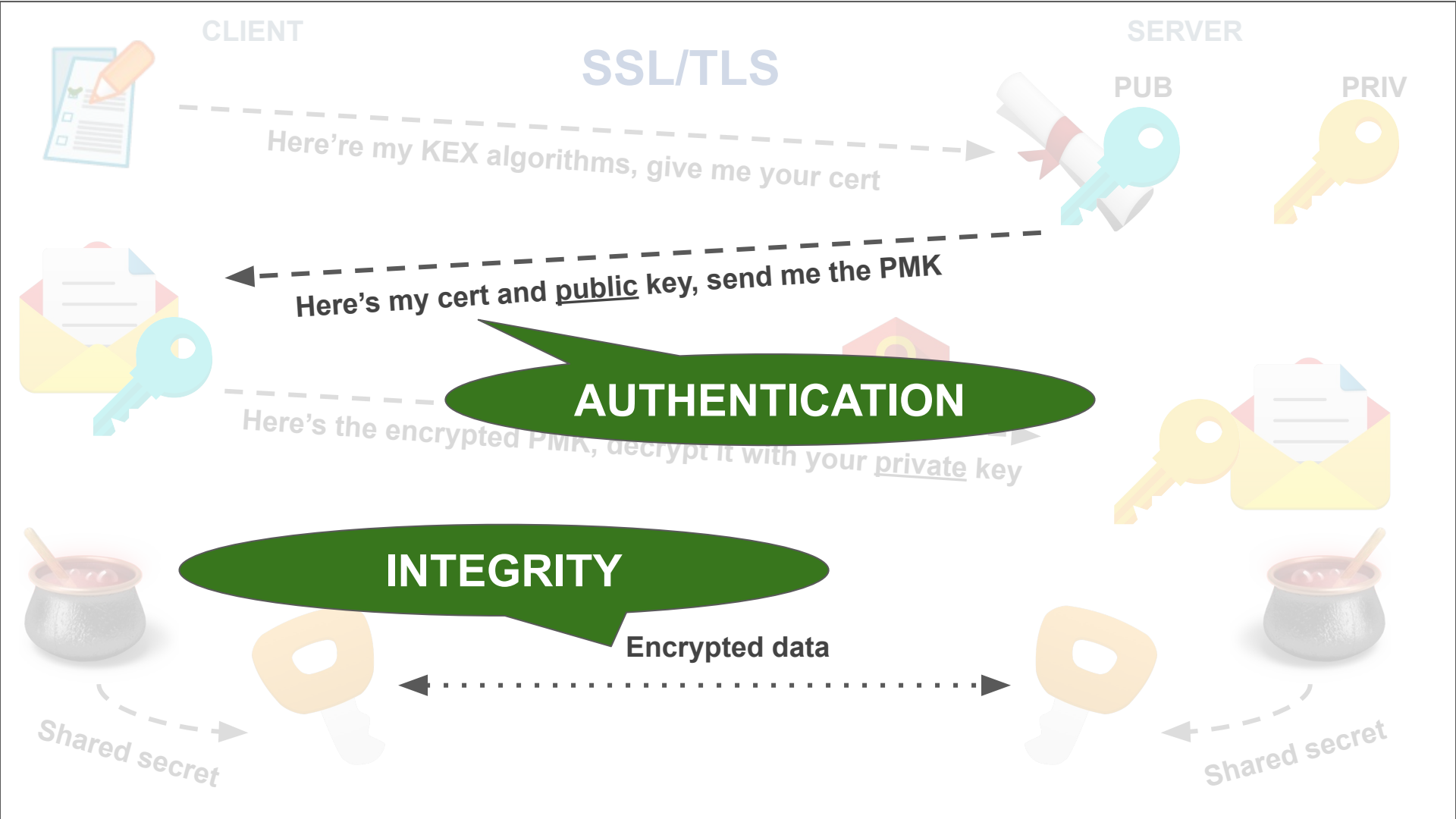
Here's the encrypted PMK, decrypt it with your private key

Encrypted data

Shared secret

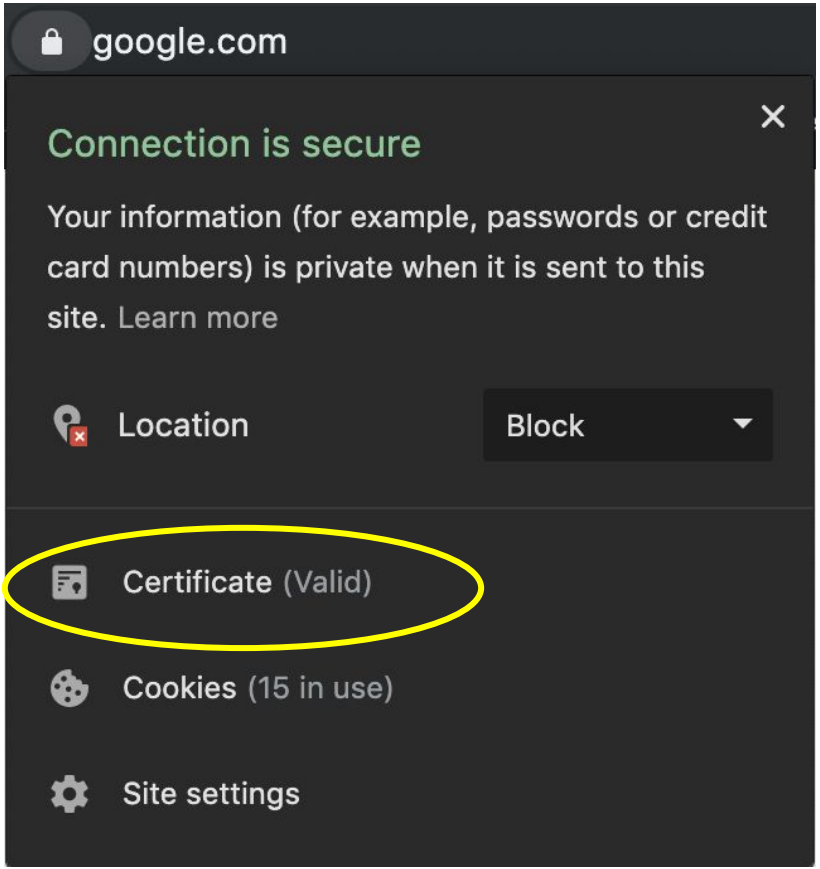
Shared secret


CLIENT
SERVER
SSL/TLS
PUB
PRIV
Here're my KEX algorithms, give me your cert
Here's my cert and public key, send me the PMK
AUTHENTICATION
Here's the encrypted PMK, decrypt it with your private key
Encrypted data
Shared secret
Shared secret


CLIENT
SERVER
SSL/TLS
PUB
PRIV
Here're my KEX algorithms, give me your cert
Here's my cert and public key, send me the PMK
AUTHENTICATION
Here's the encrypted PMK, decrypt it with your private key
INTEGRITY
Encrypted data
Shared secret
Shared secret

SSL/TLS certificates

SSL/TLS certificates



SSL/TLS certificates

Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to secure.bank because this website requires a secure connection.

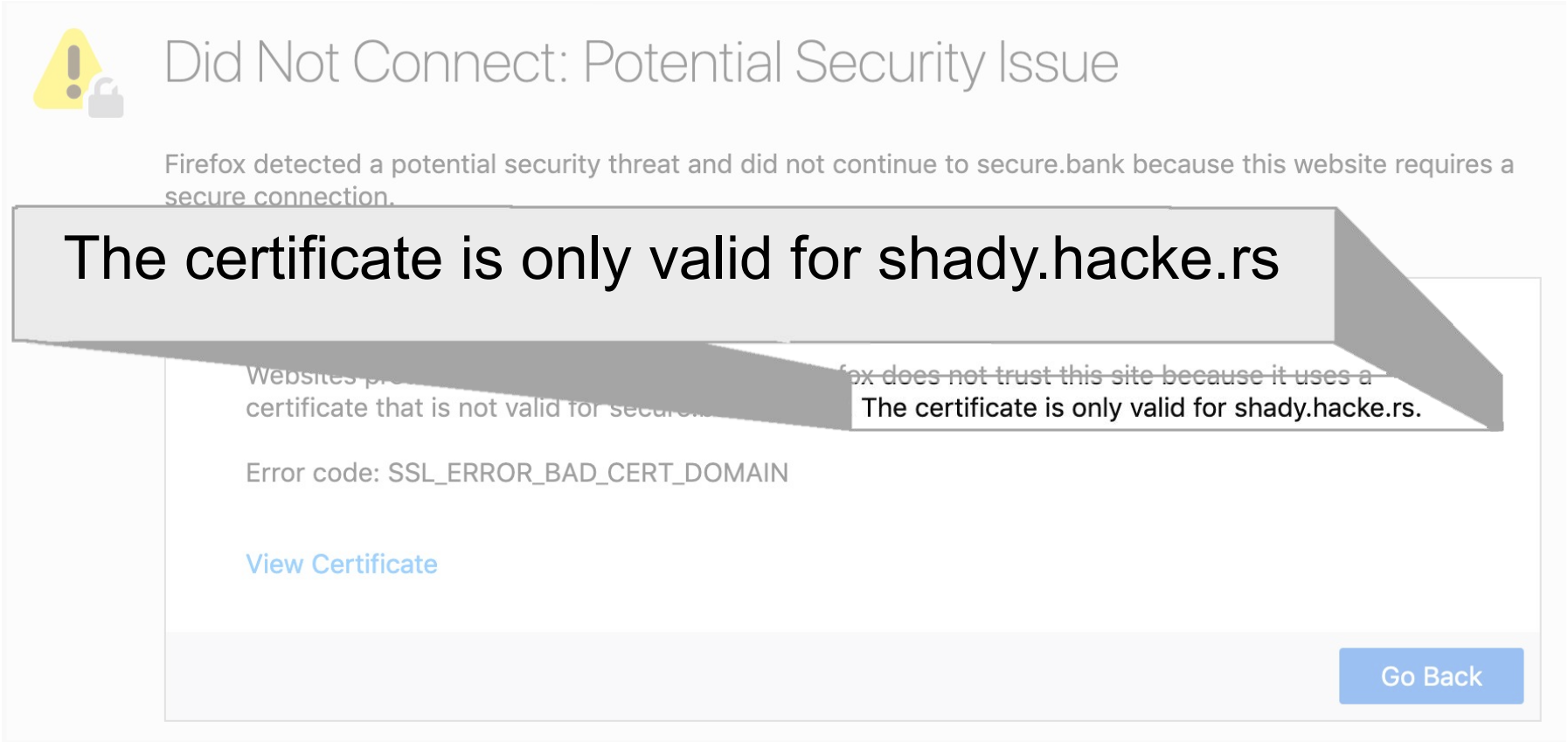
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for secure.bank:58443. The certificate is only valid for shady.hacke.rs.

Error code: SSL_ERROR_BAD_CERT_DOMAIN

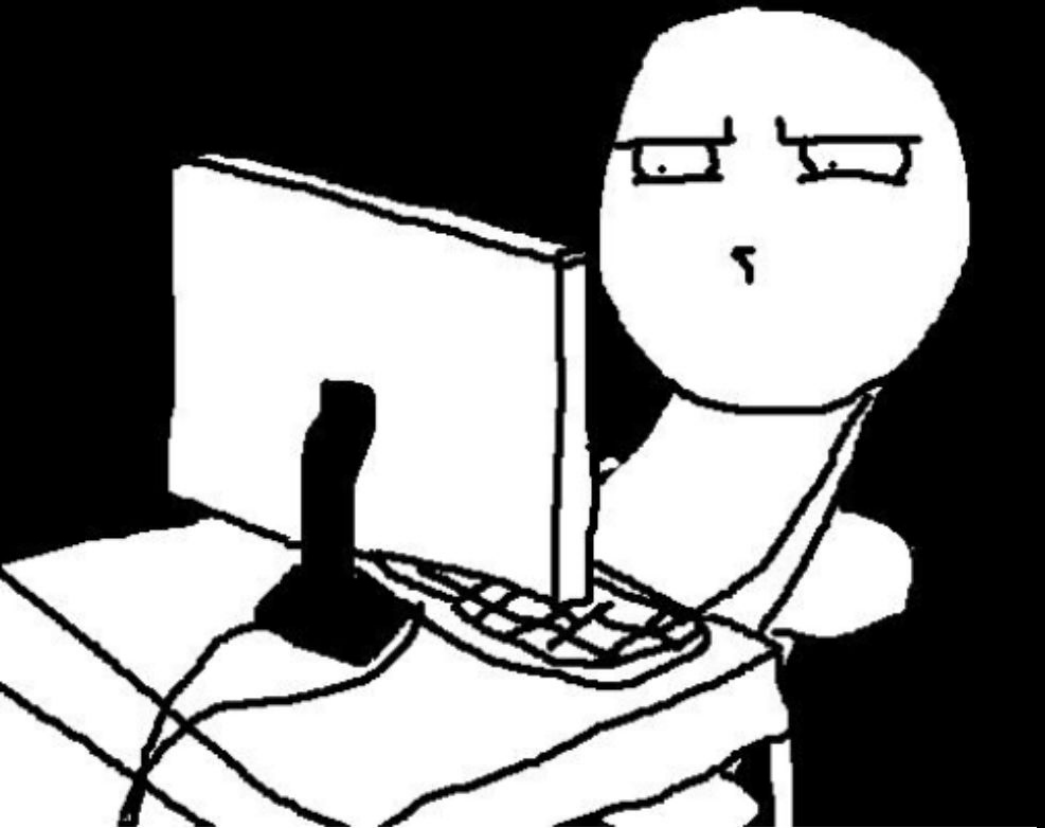
View Certificate

Go Back

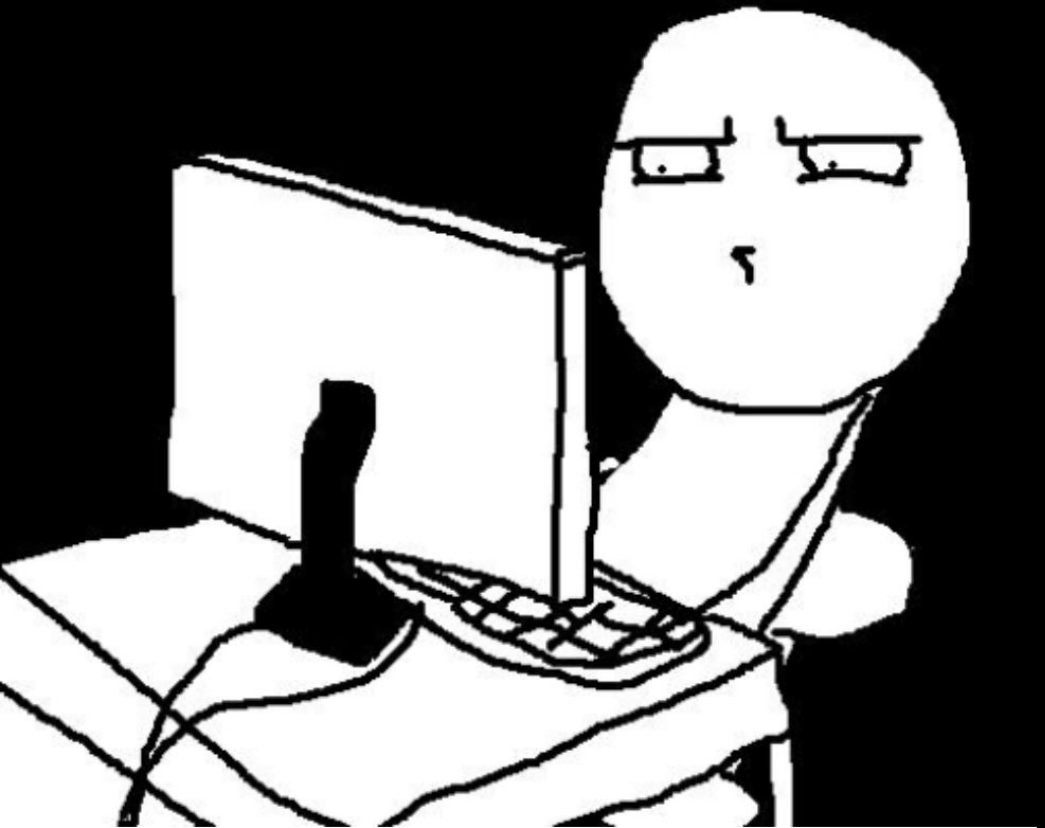
SSL/TLS certificates



WHAT HAPPENED HERE?!

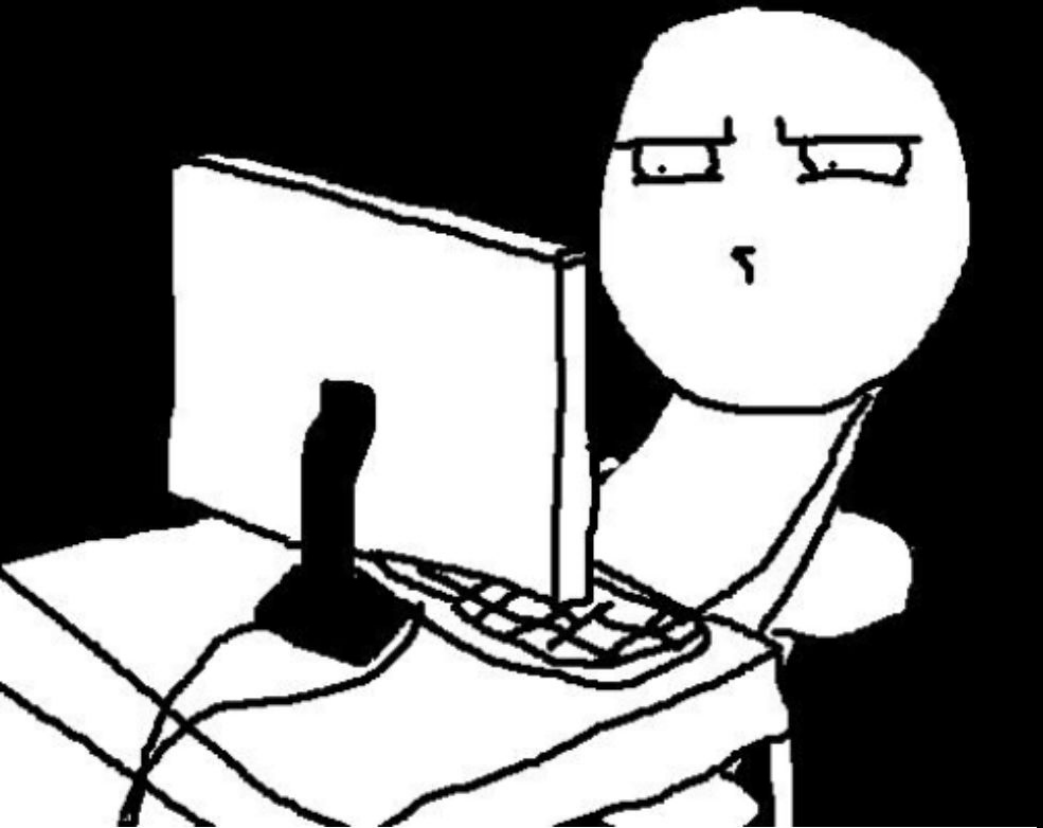


WHAT HAPPENED HERE?!



- ALIEN-IN-THE-MIDDLE

WHAT HAPPENED HERE?!



- ALIEN-IN-THE-MIDDLE
- SECURE.BANK WAS HAXED BY ALIENS

WHAT HAPPENED HERE?!

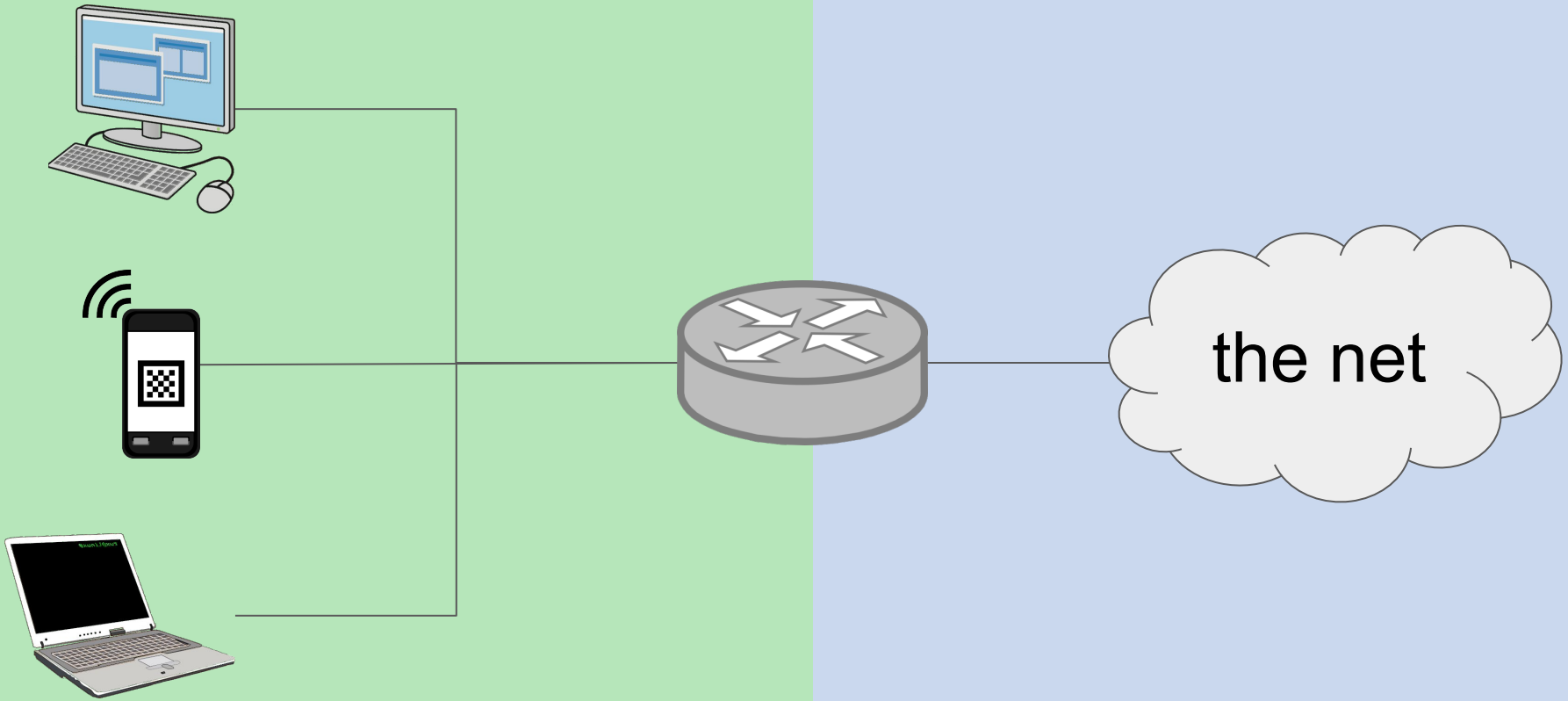
- Russian or Chinese gov
- 12-yo accidentally found the admin portal

- ALIEN-IN-THE-MIDDLE
- SECURE.BANK WAS HAXED BY ALIENS

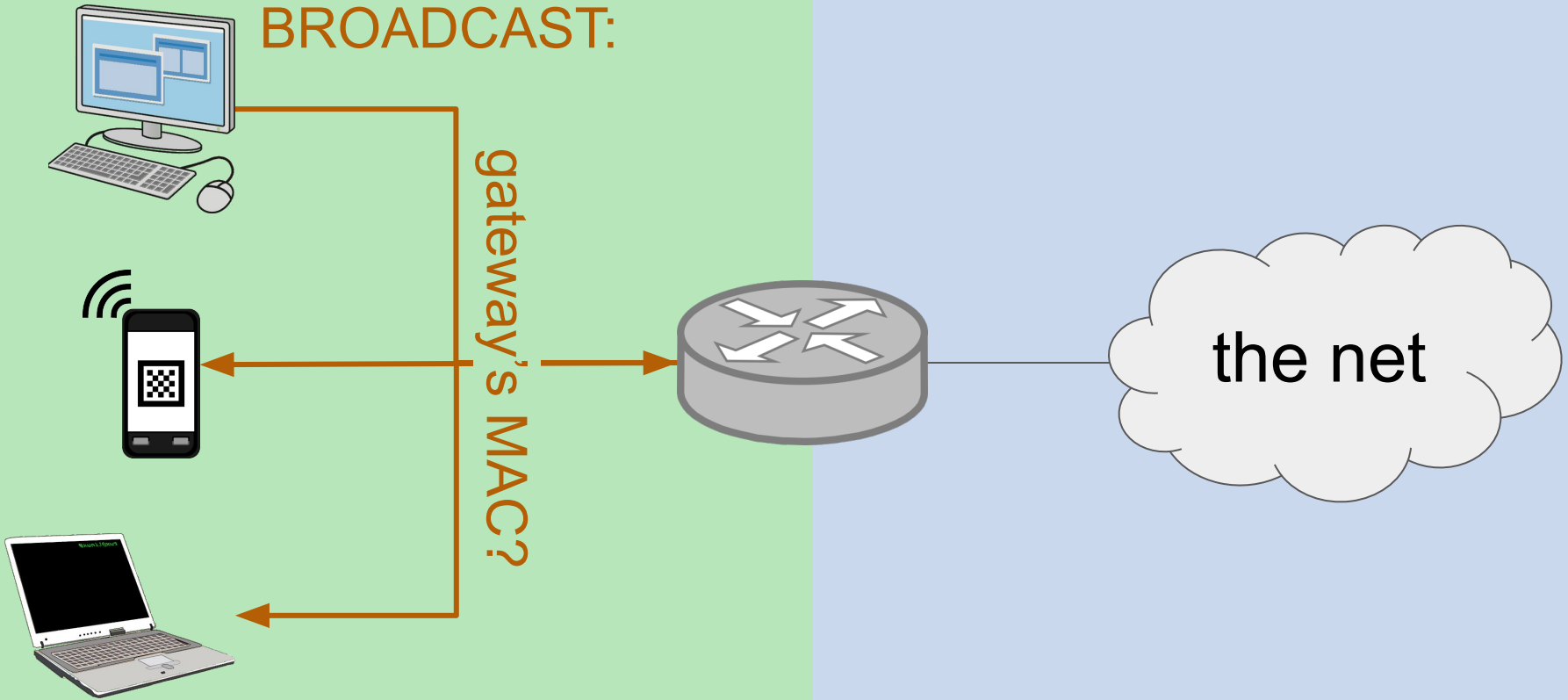
WHAT HAPPENED HERE?!

- ALIEN-IN-THE-MIDDLE
- SECURE.BANK WAS HAXED BY ALIENS

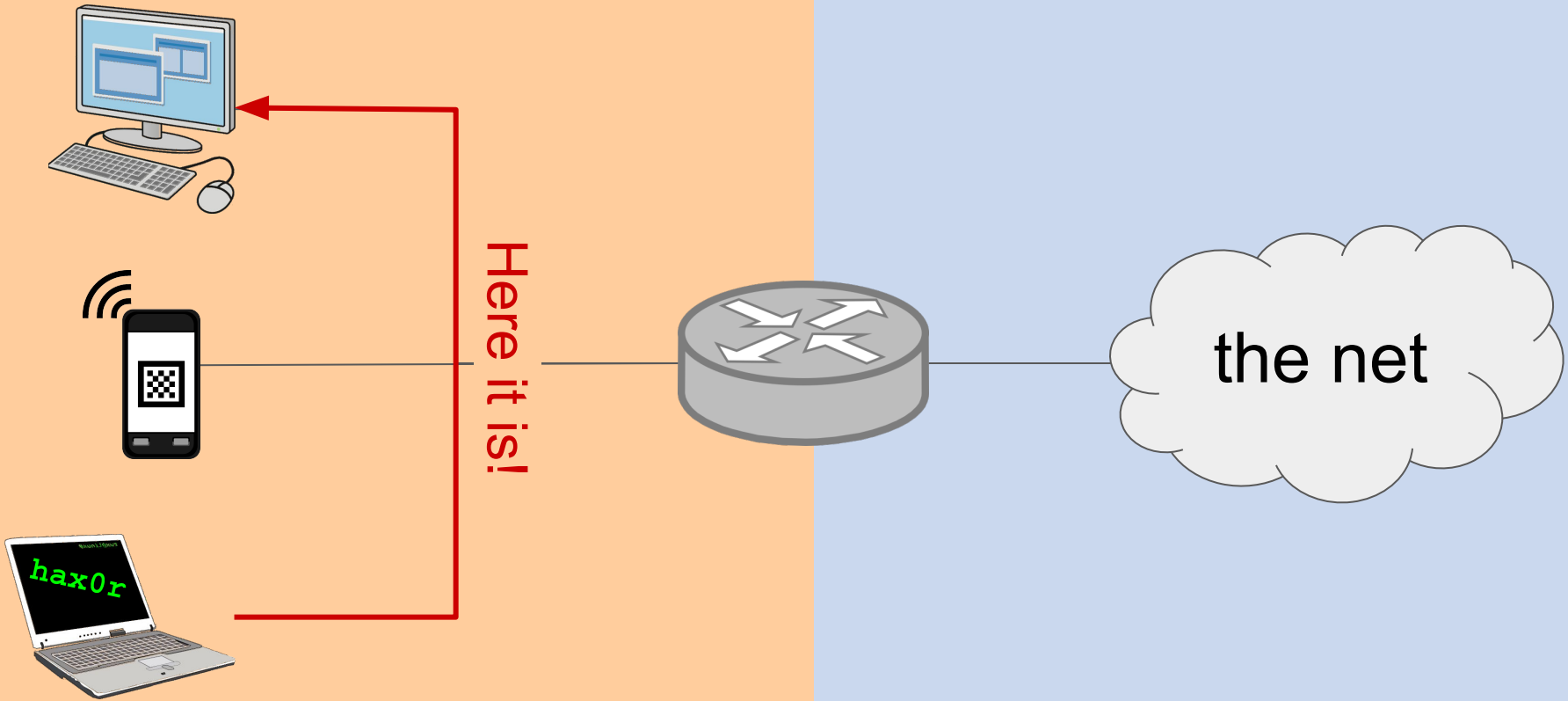
Person-in-the middle: ARP spoofing



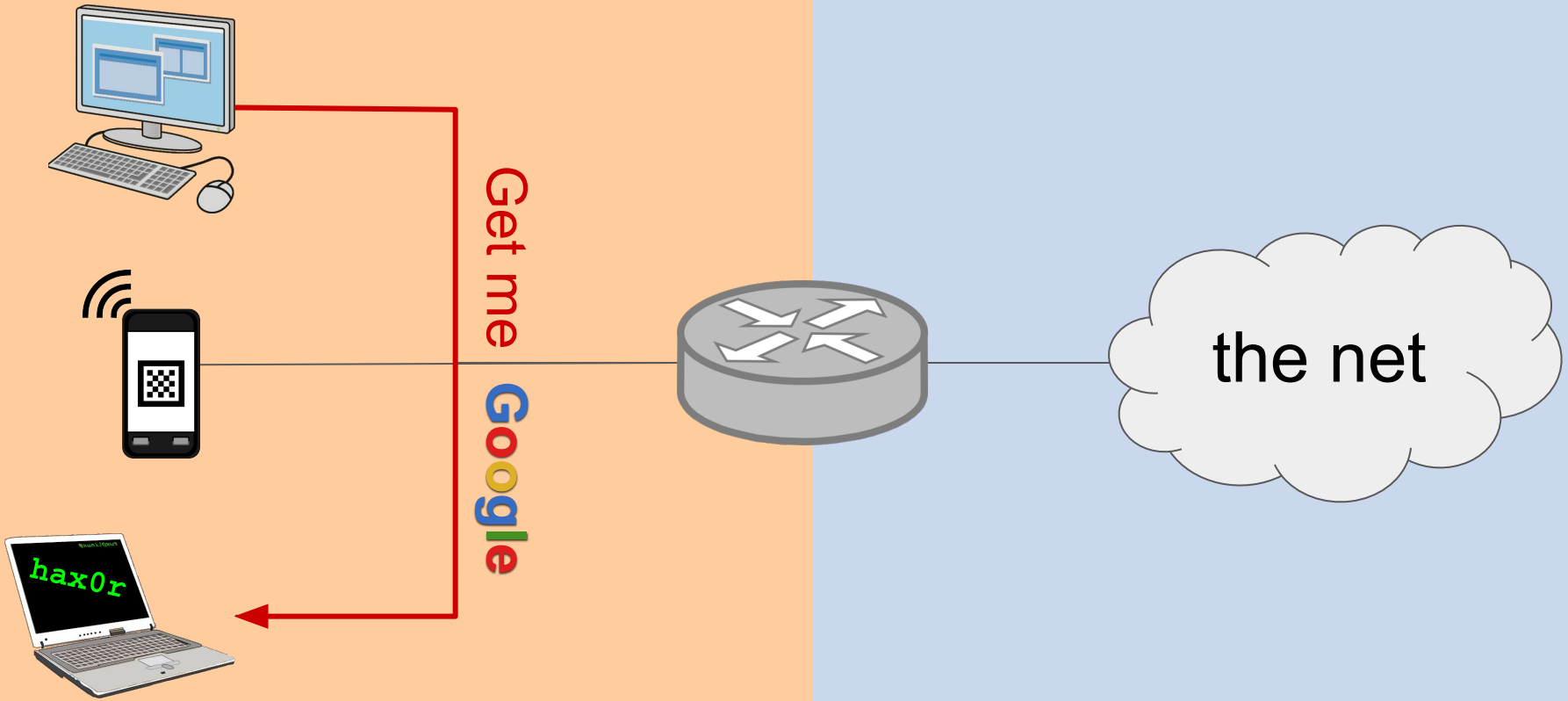
Person-in-the middle: ARP spoofing



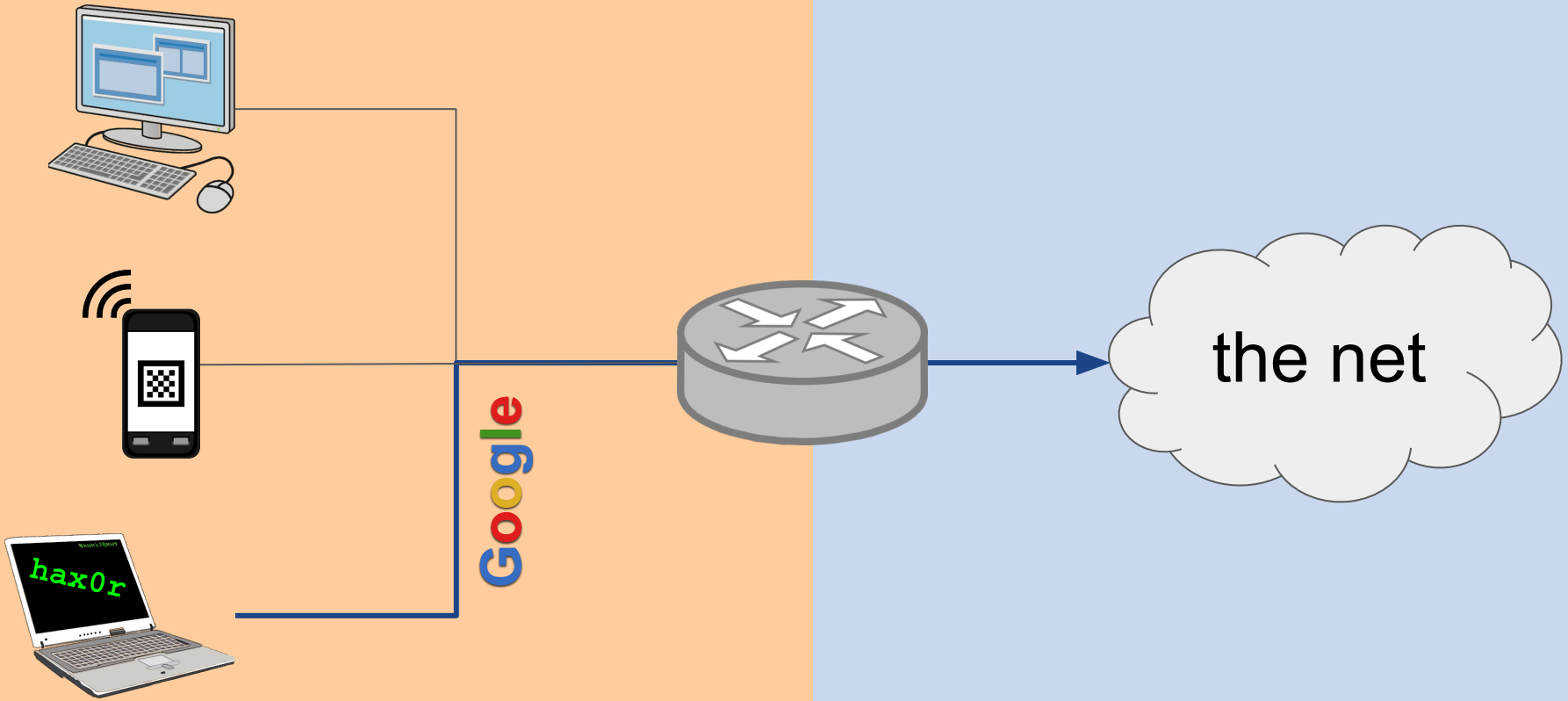
Person-in-the middle: ARP spoofing



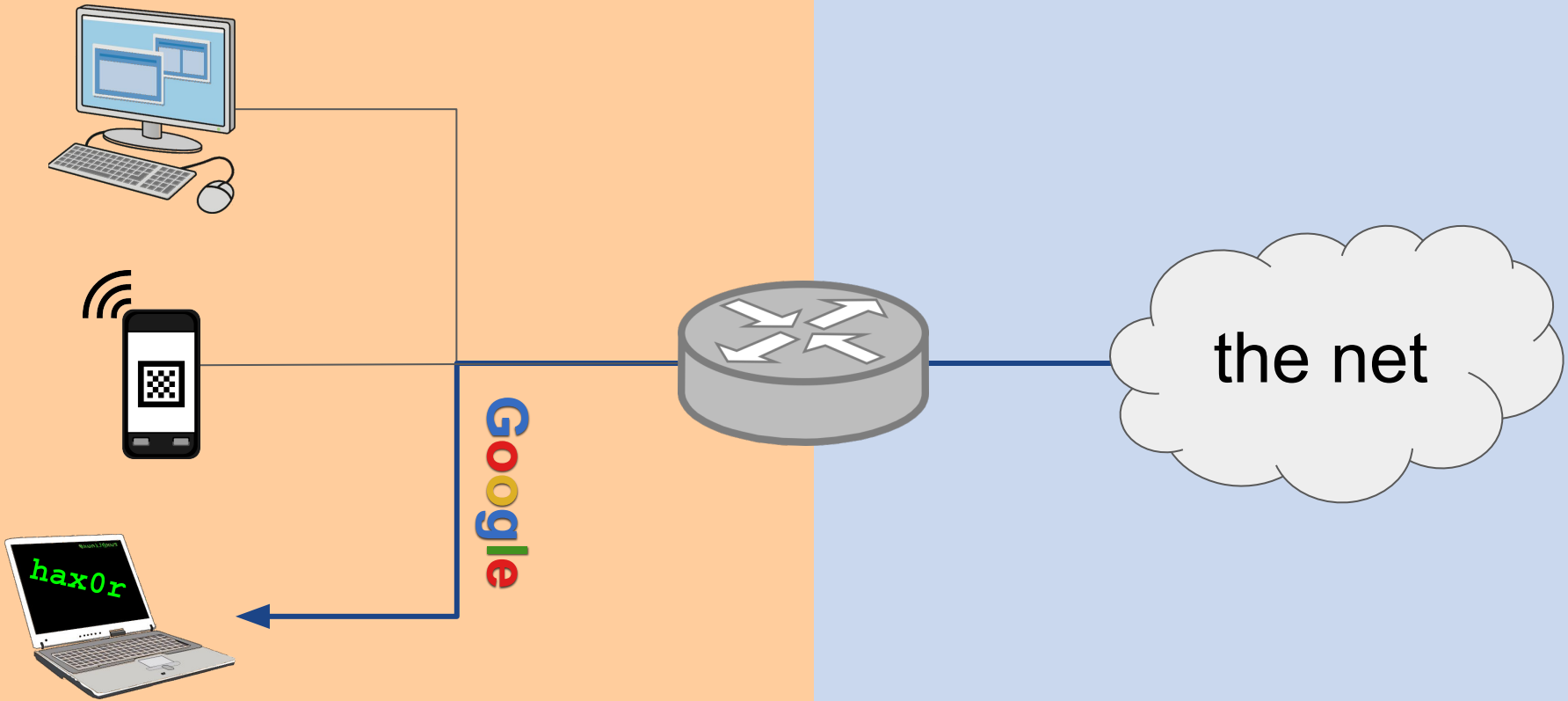
Person-in-the middle: ARP spoofing



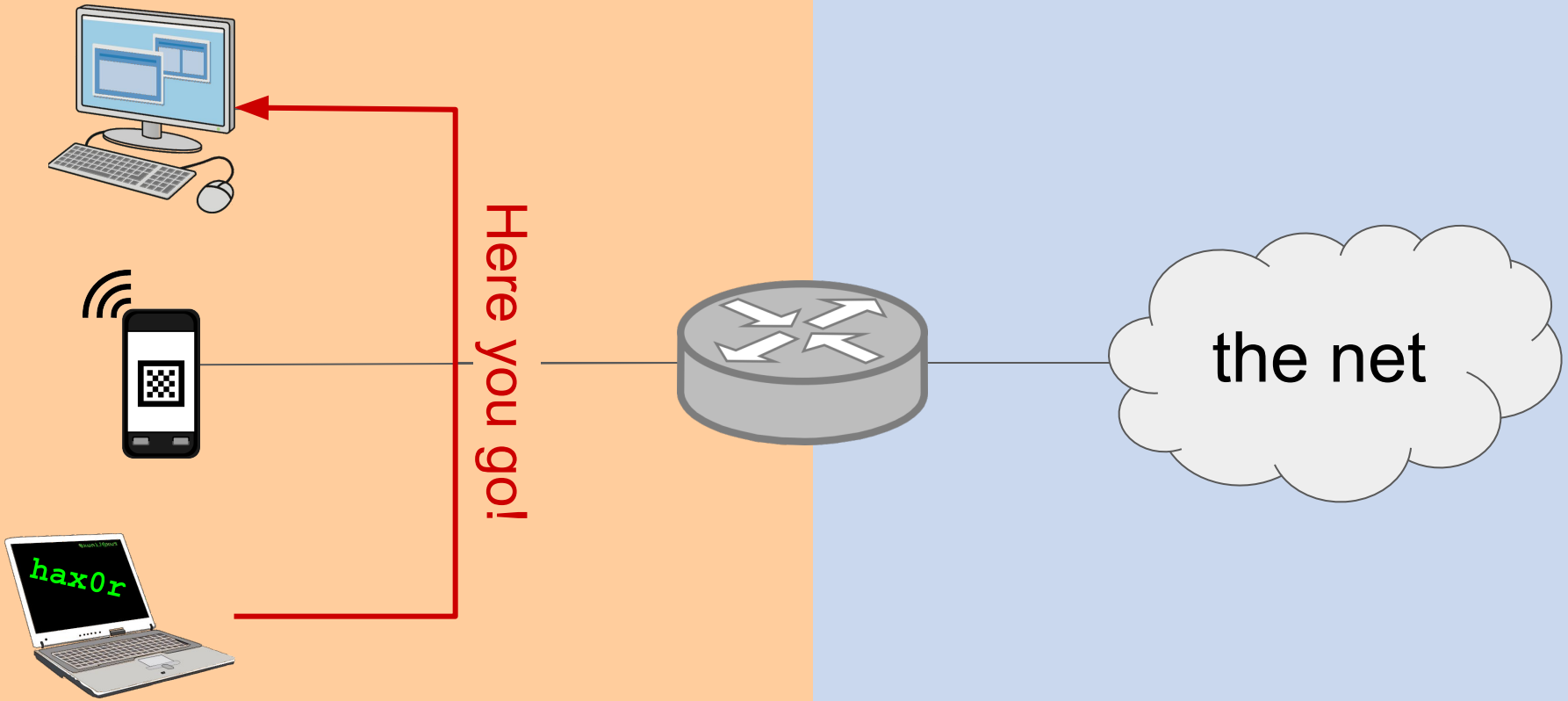
Person-in-the middle: ARP spoofing



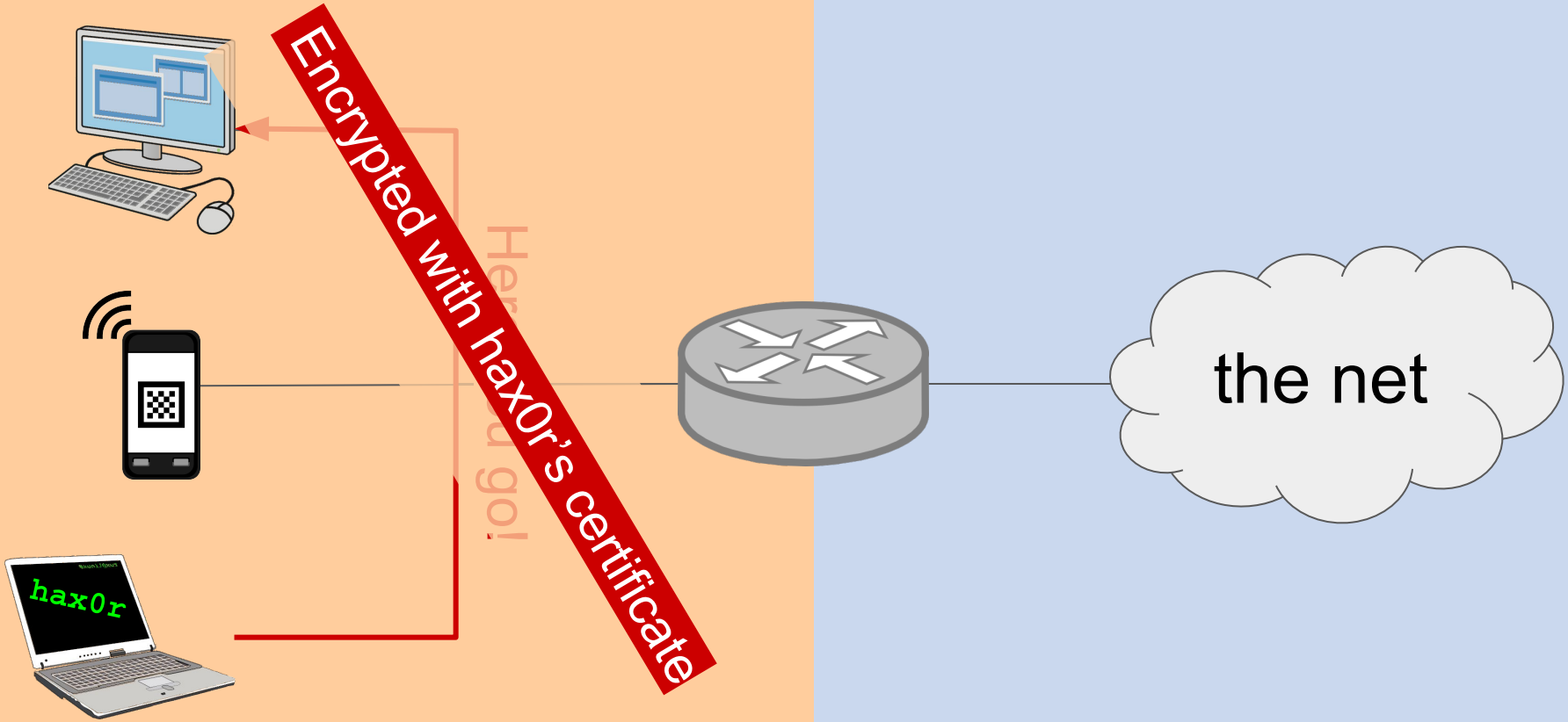
Person-in-the middle: ARP spoofing



Person-in-the middle: ARP spoofing

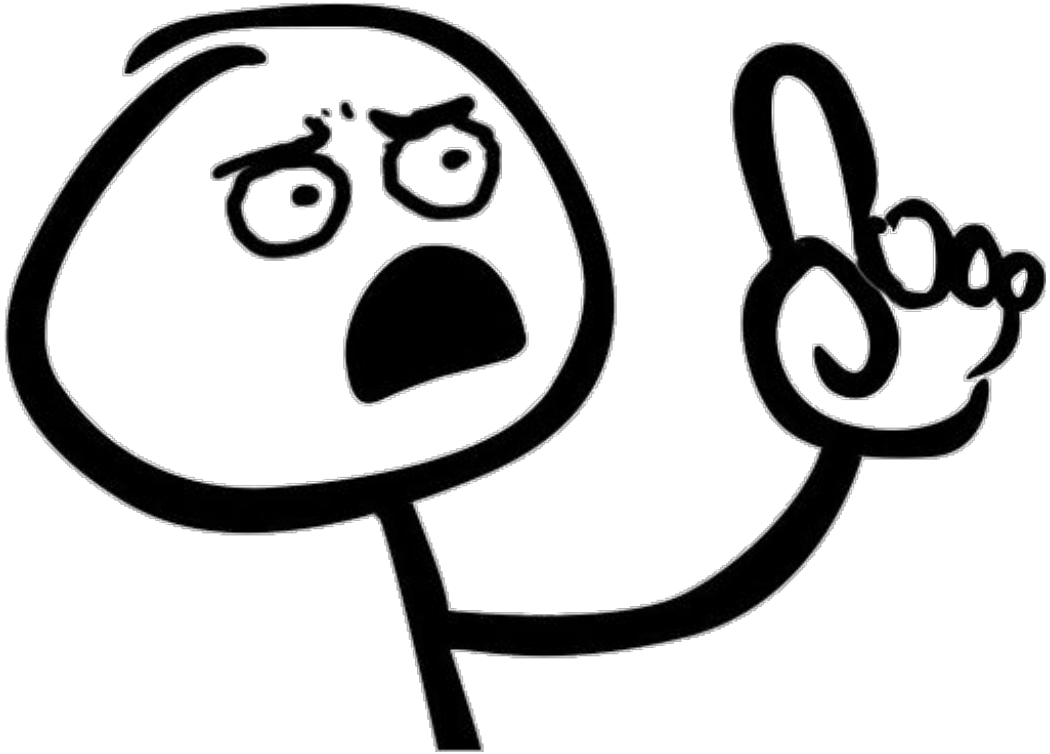


Person-in-the middle: ARP spoofing



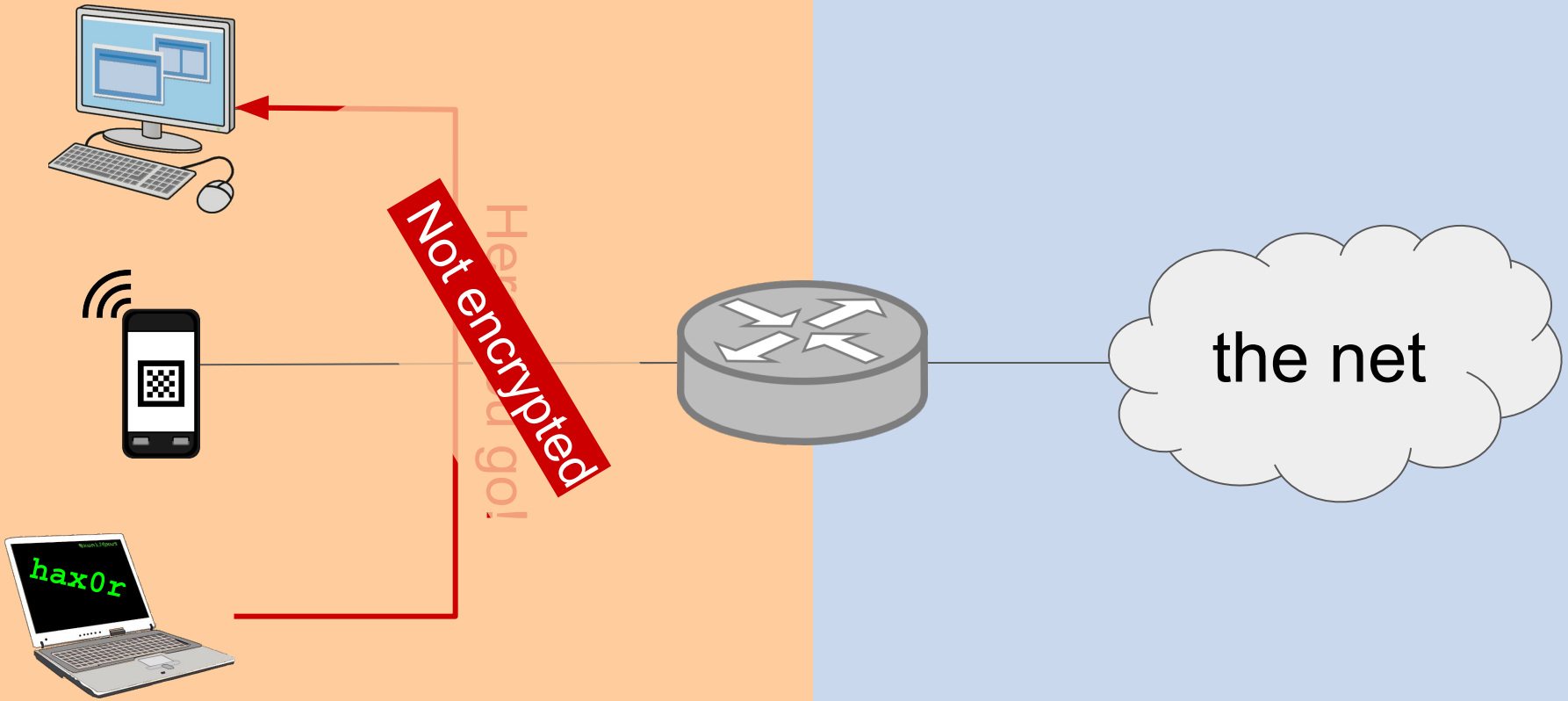
To do

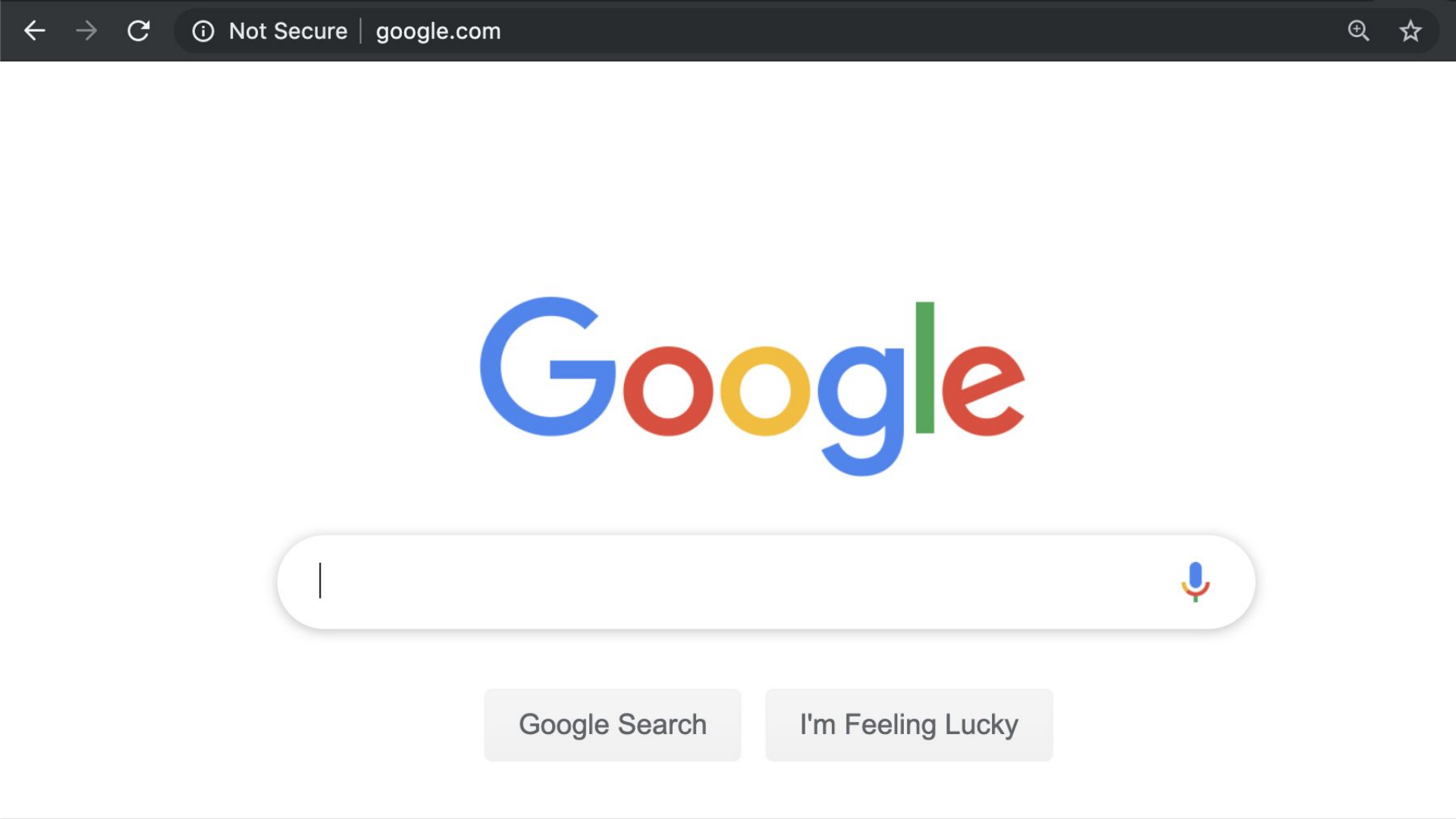
To do

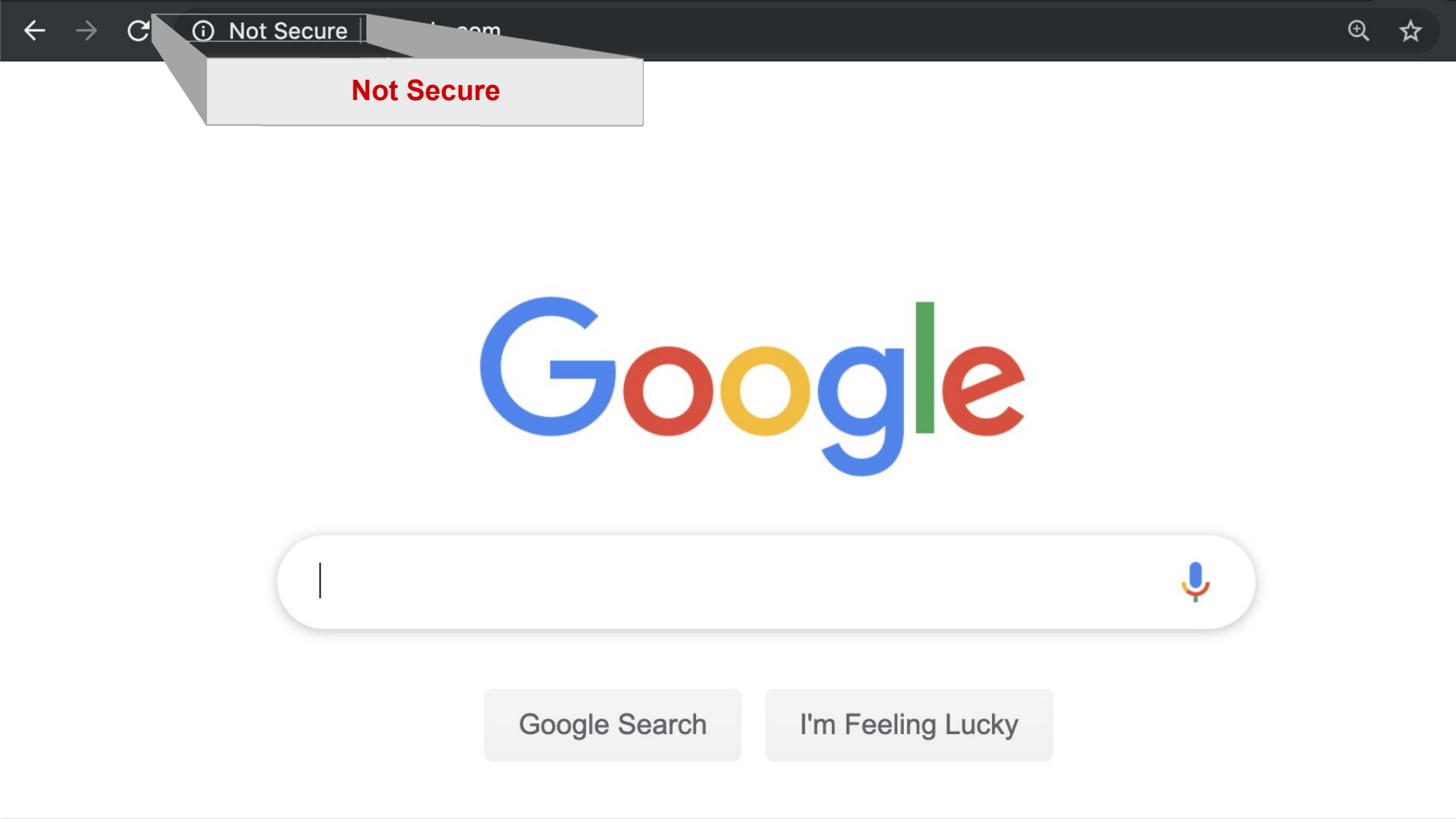


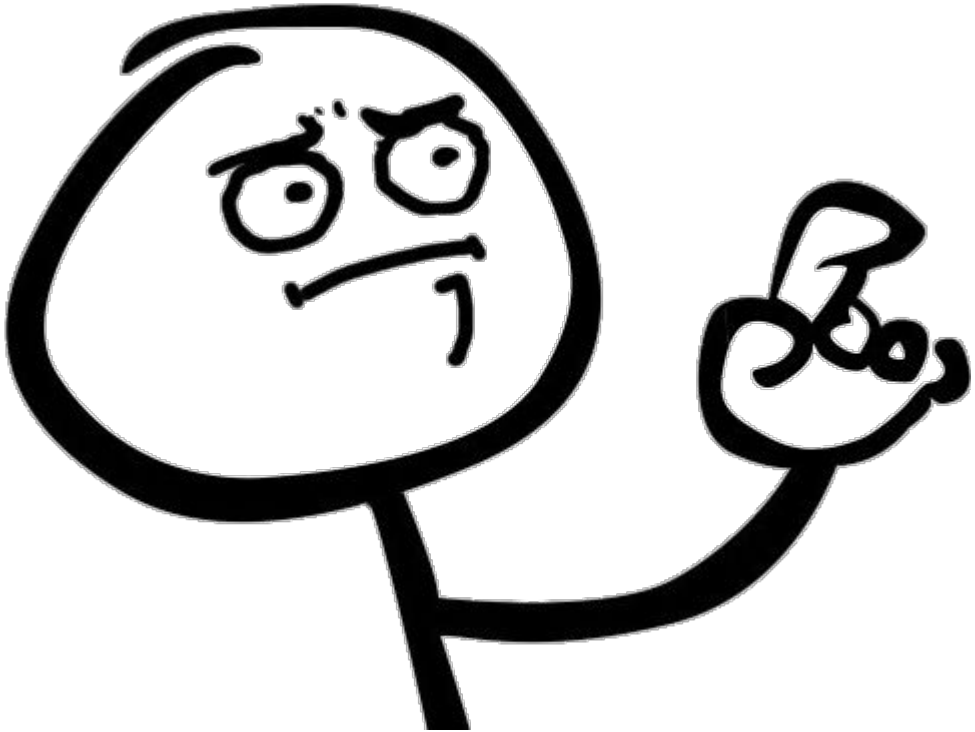
I NEVER IGNORE CERTIFICATE WARNINGS

Person-in-the middle: ARP spoofing




Not Secure
google.com
Google
Google Search
I'm Feeling Lucky


Not Secure
Not Secure
Google
Google Search
I'm Feeling Lucky

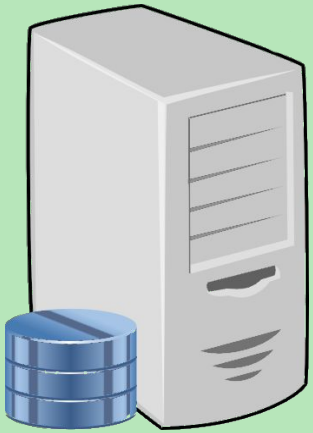


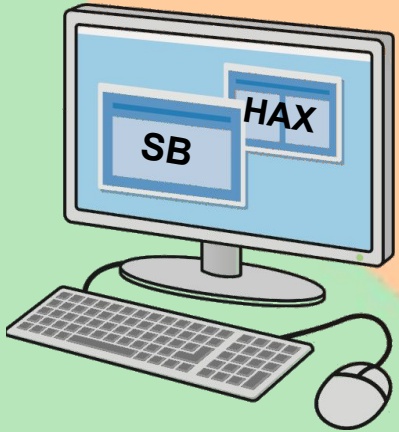
To do

WHAT IF THERE'S ANOTHER WAY TO GET HACKED?

Cross-site request forgery (CSRF)

Cross-site request forgery (CSRF)

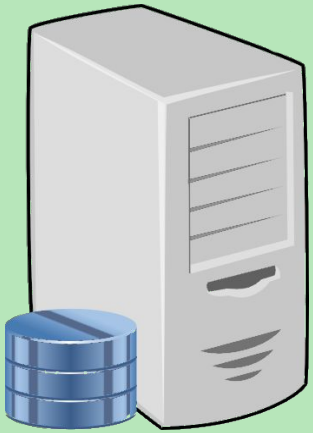


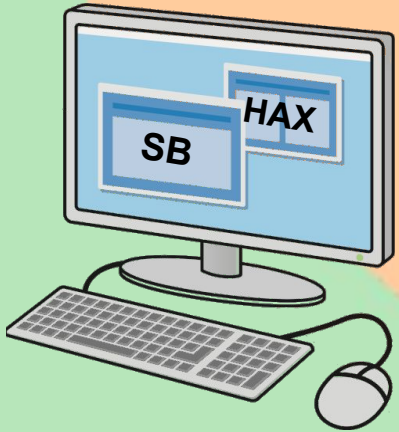


secure.bank

hacke.rs

Cross-site request forgery (CSRF)



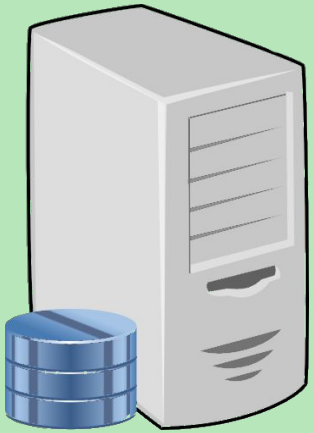


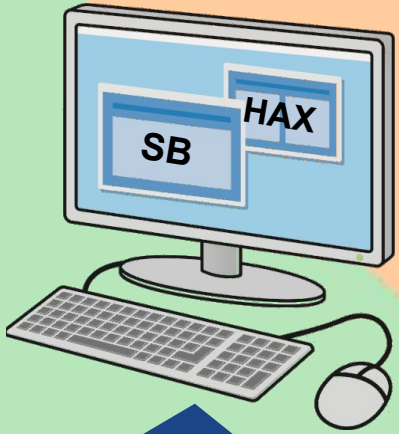
Psst, tell him to send some $$$

secure.bank

hacke.rs

Cross-site request forgery (CSRF)



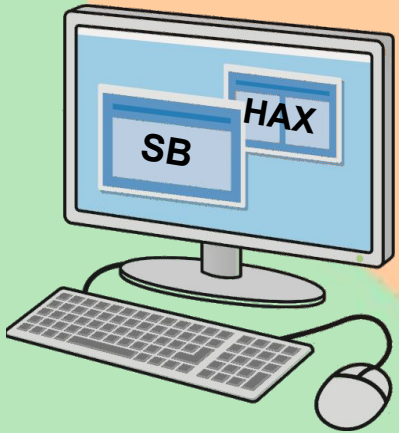


secure.bank

Hey, send him $$$

hacke.rs

Cross-site request forgery (CSRF)



secure.bank

hacke.rs

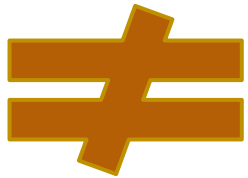
The web “Origin”

{hostname}:{port}

The web “Origin”

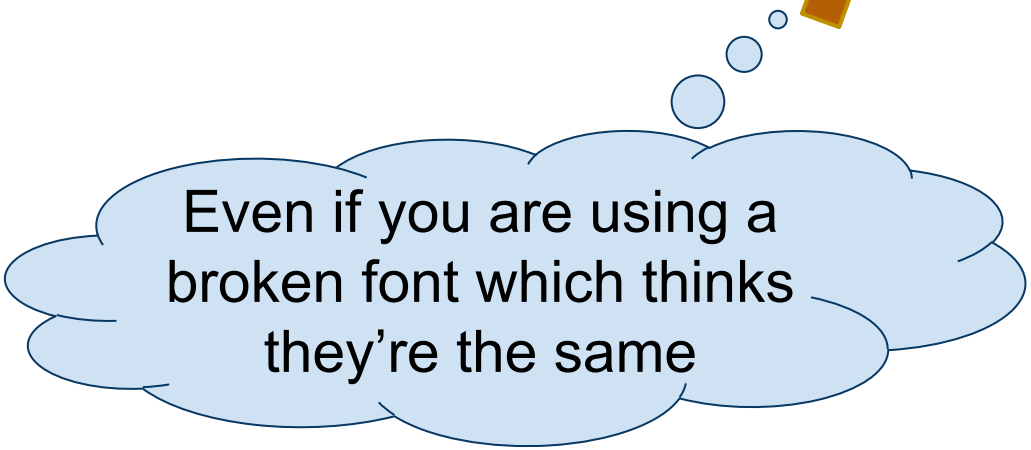
≠

The web “Origin”

paypal.com  paypa1.com

The web “Origin”

paypal.com ≠ paypa1.com

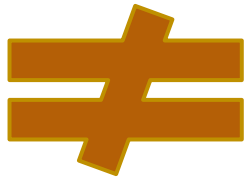


The web “Origin”

`paypal.com`  `paypa1.com`

And yes, even if they resolve to the same IP address

The web “Origin”

`secure.bank:443`  `secure.bank:8443`

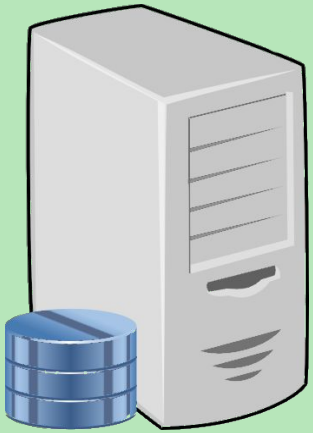
Same-origin policy (SOP)

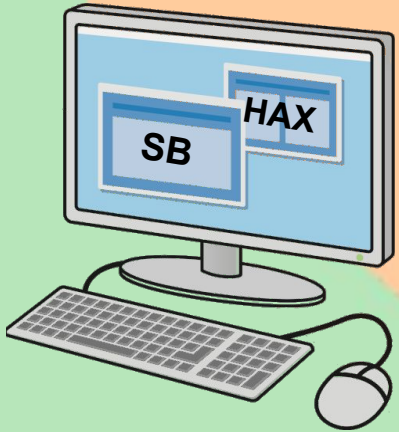
Same-origin policy (SOP)

SOP: it was never gonna work

Cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS)

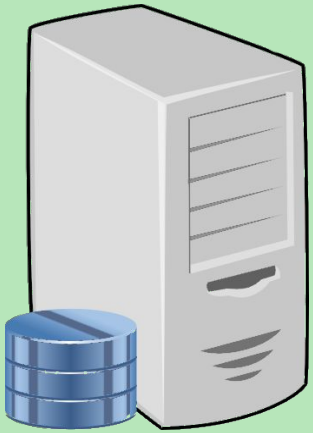


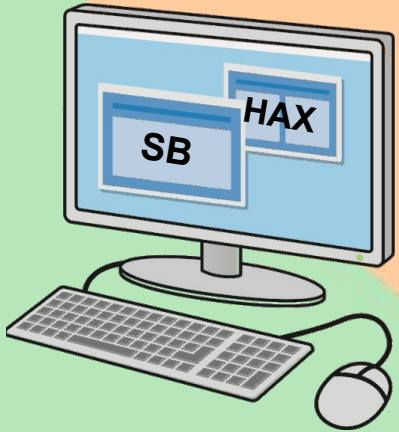


secure.bank

hacke.rs

Cross-origin resource sharing (CORS)



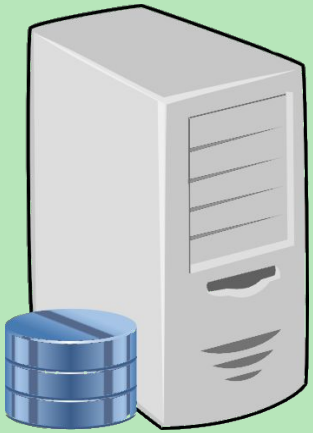


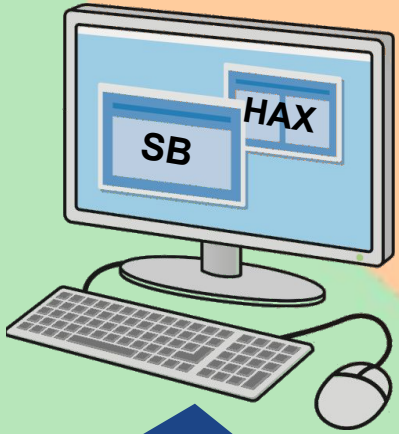
Psst, tell him to send some $$$

secure.bank

hacke.rs

Cross-origin resource sharing (CORS)



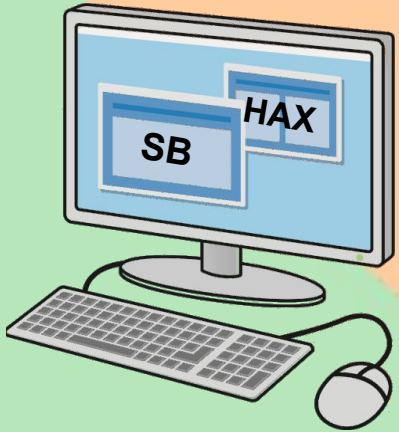


secure.bank

Hey, send him $$$

hacke.rs

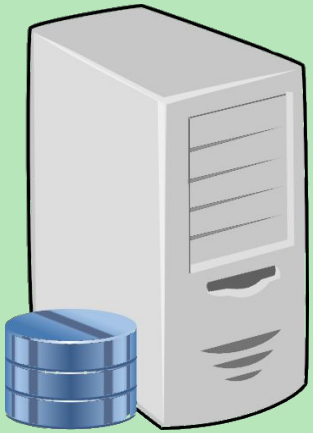
Cross-origin resource sharing (CORS)



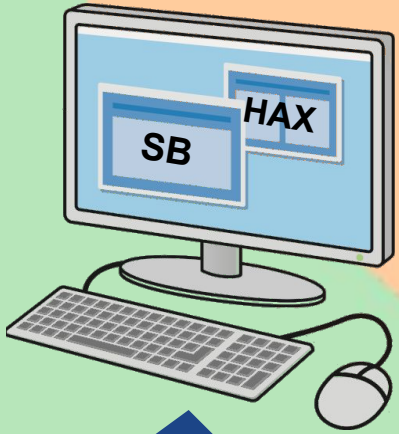
secure.bank

hacke.rs

Cross-origin resource sharing (CORS)



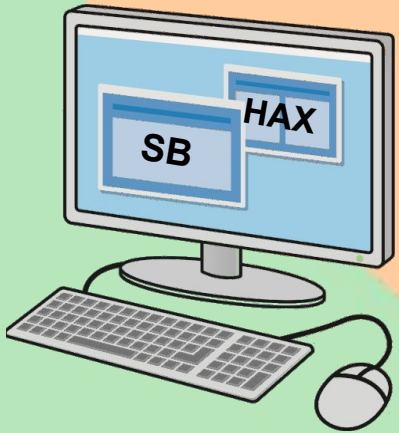
secure.bank



hacke.rs

hacke.rs

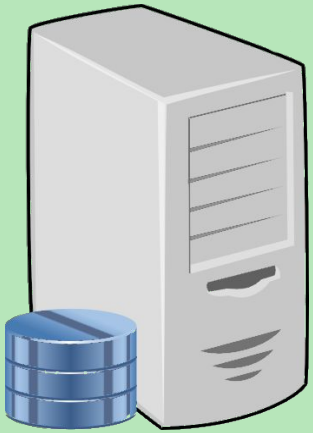
Cross-origin resource sharing (CORS)

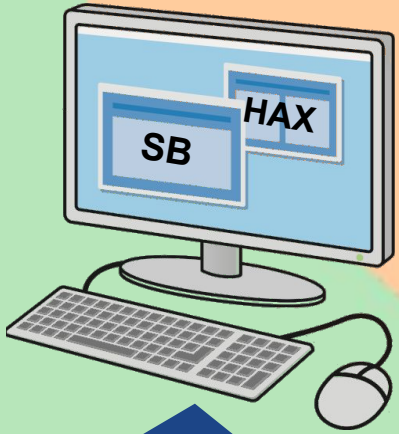


secure.bank

hacke.rs

Cross-origin resource sharing (CORS)





secure.bank

K, nevermind

hacke.rs

CORS and HTTP

CORS and HTTP

```
GET / HTTP/1.1
Host: secure.bank
Cookie: SESSION=xbatmanxwashingxhisxtights
```

CORS and HTTP

```
GET / HTTP/1.1
Host: secure.bank
Cookie: SESSION=xbatmanxwashingxhisxtights
```

```
HTTP/1.1 200 OK

...
```

CORS and HTTP

```
GET / HTTP/1.1
Host: secure.bank
Cookie: SESSION=xbatmanxwashingxhisxtights
Origin: hacke.rs
```

```
HTTP/1.1 200 OK


...
```

CORS and HTTP

```
GET / HTTP/1.1
Host: secure.bank
Cookie: SESSION=xbatmanxwashingxhisxtights
Origin: hacke.rs
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: secure.bank
Access-Control-Allow-Credentials: false
...
```

CORS and HTTP

```
GET / HTTP/1.1
Host: secure.bank
Cookie: SESSION=xbatmanxwashingxhisxtights
Origin: hacke.rs
```

hacke.rs tells the browser
whether to include cookies or not

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: secure.bank
Access-Control-Allow-Credentials: false
...
```

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	
	Yes	

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	
*	No	
	Yes	

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	
*	No	**Yes, if no cookies needed**
	Yes	

CORS: what should browsers do

Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	
*	No	**Yes, if no cookies needed**
	Yes	
{as requested}	No	
	Yes	

CORS: what should browsers do

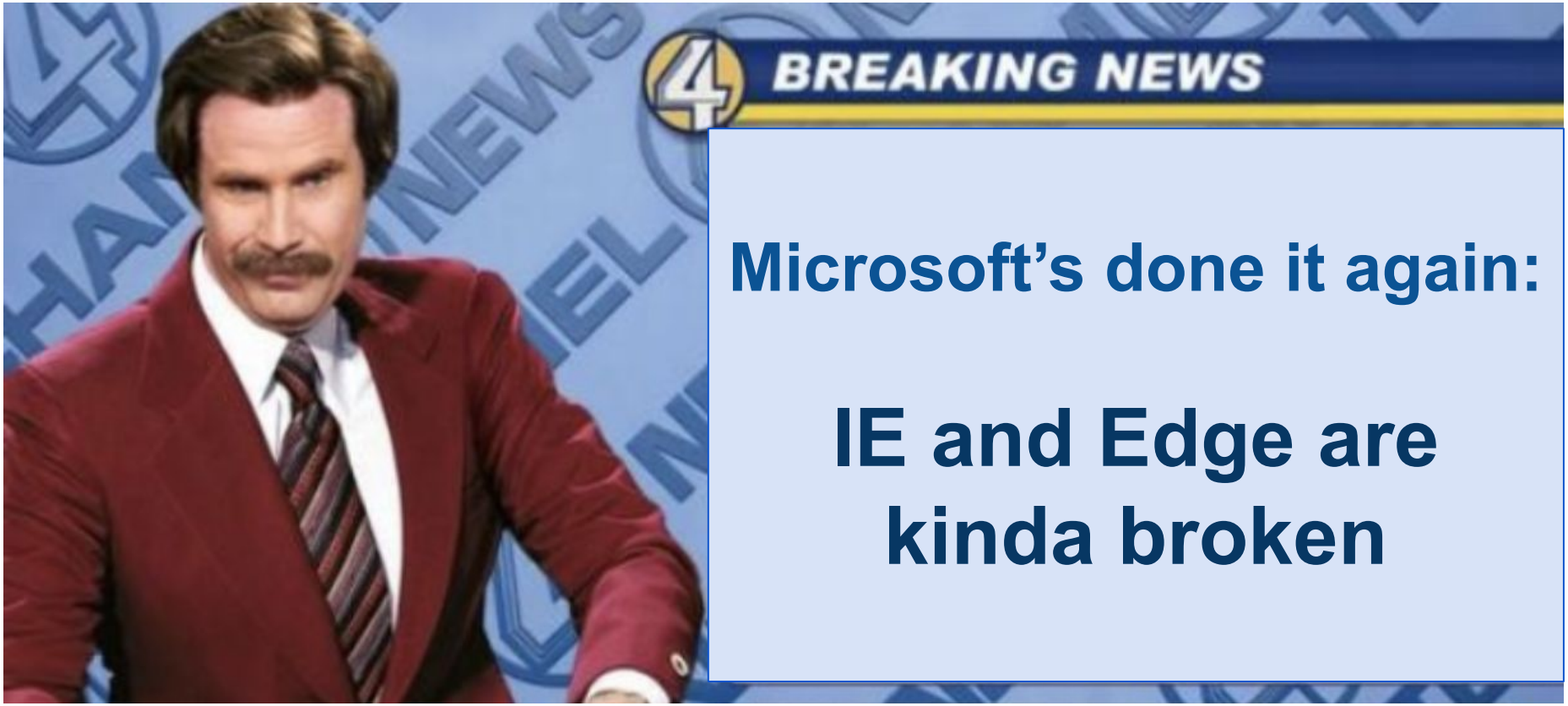
Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	
*	No	**Yes, if no cookies needed**
	Yes	
{as requested}	No	
	Yes	

CORS: what should browsers do

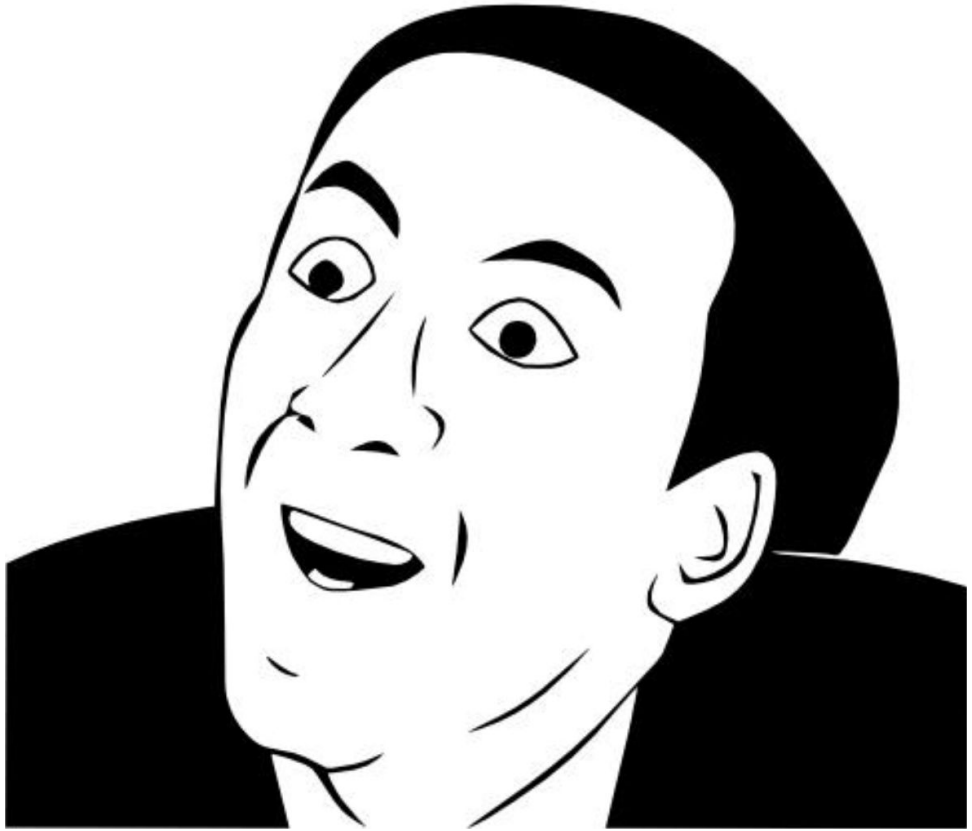
Server allows		Browser must
Origin	Credentials	Give JavaScript Access
{not as requested}	No	**No**
	Yes	
*	No	**Yes, if no cookies needed**
	Yes	
{as requested}	No	
	Yes	**Yes**

CORS: what do browsers actually do

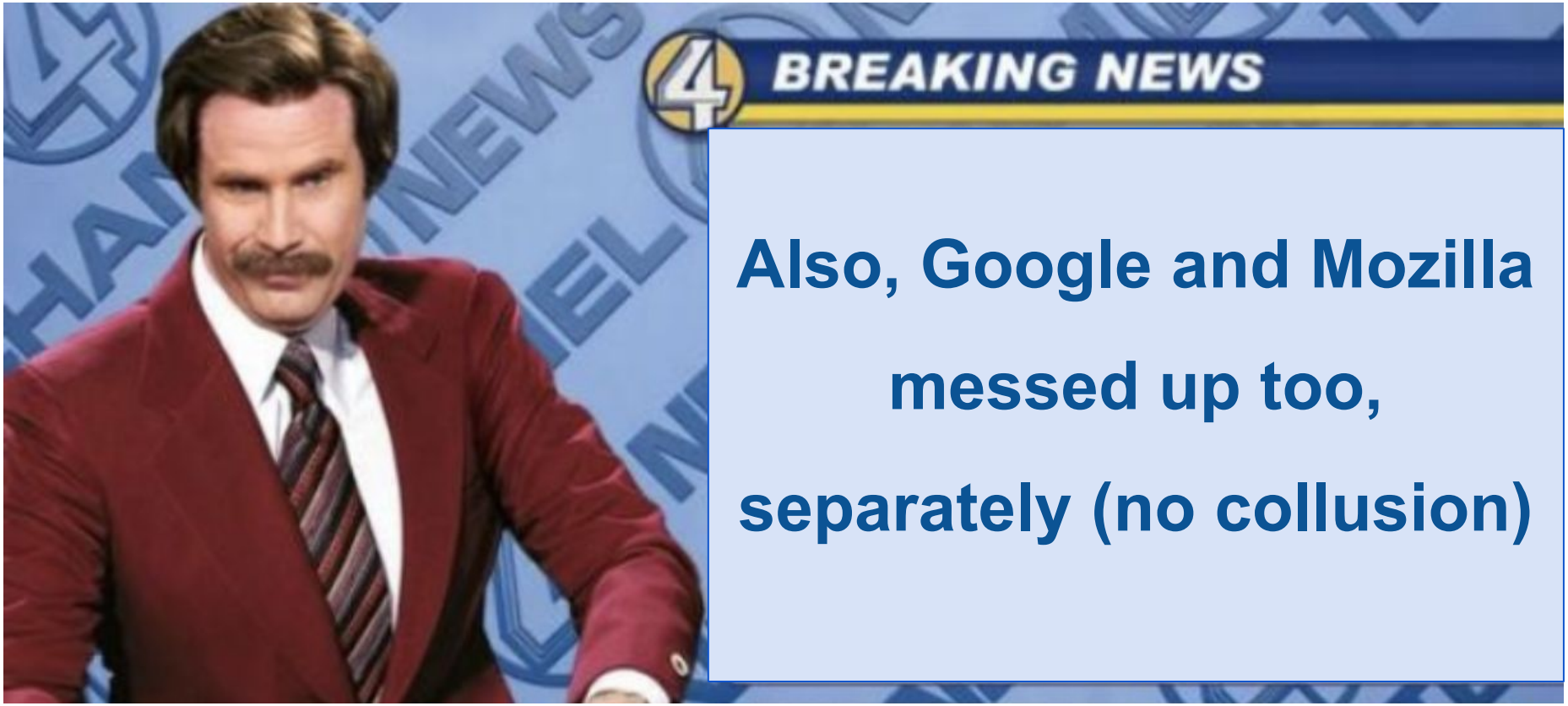
CORS: what do browsers actually do



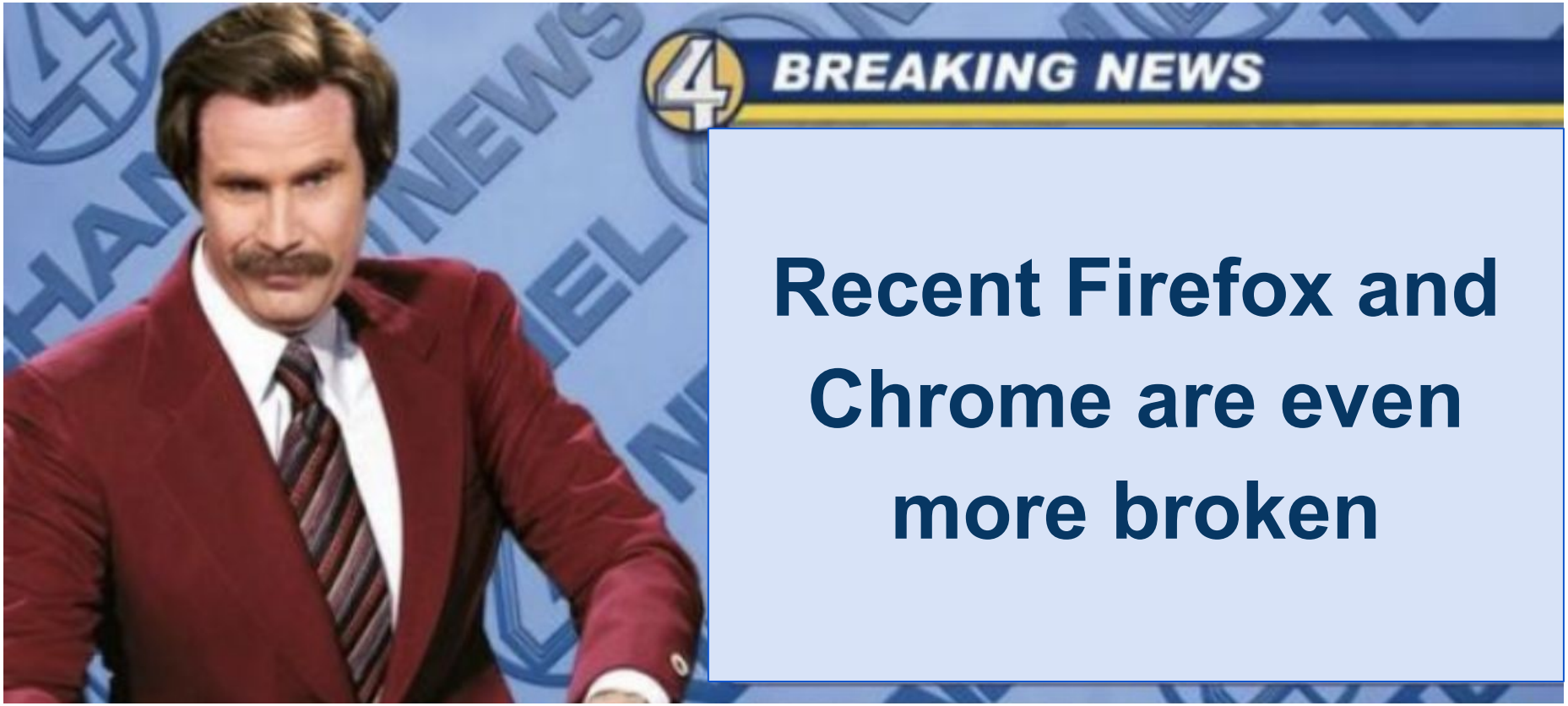
CORS: what do browsers actually do



CORS: what do browsers actually do



CORS: what do browsers actually do



CORS: what do browsers actually do

WAIT
WHAT?!

It’s a bug and...

It’s a bug and...

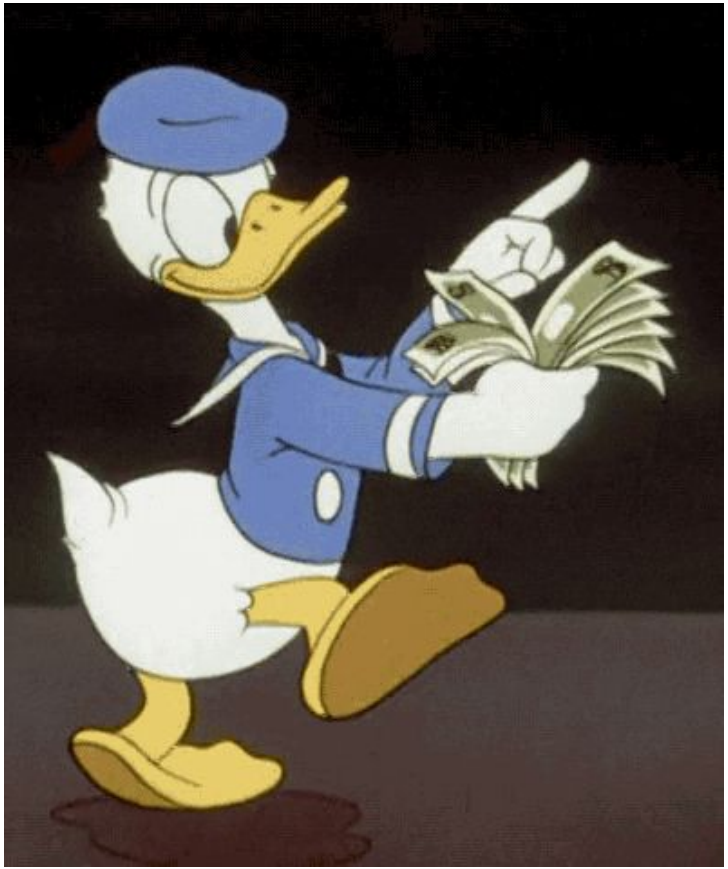
I FOUND IT, IT IS MINE!

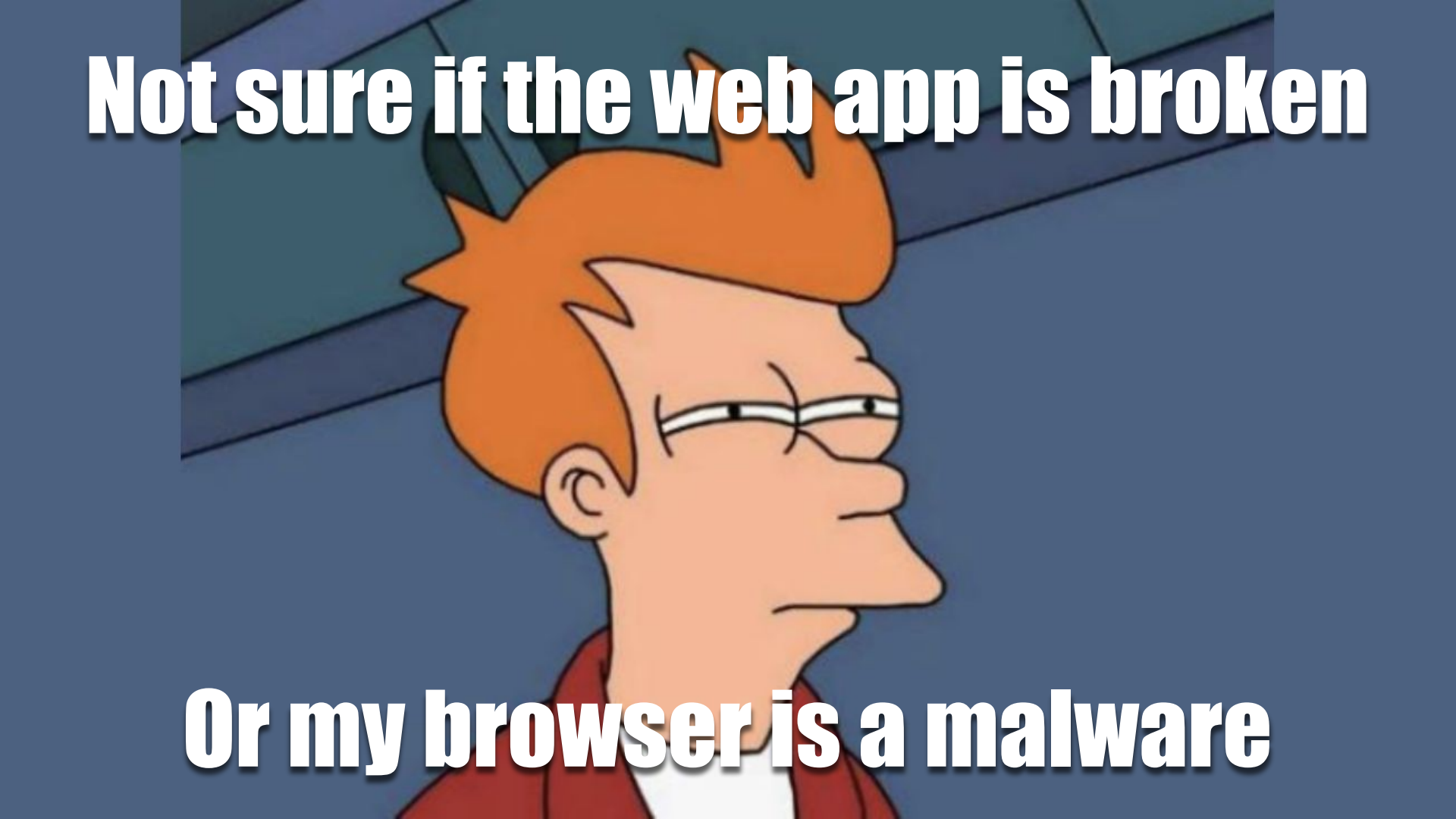
Now gimme moneyz

Chromium bug #930057	**CVE-2019-5814**	⇒	**US$1,000**
Mozilla bug #1526218	**CVE-2018-18511**	⇒	**US$3,000**

Now gimme moneyz

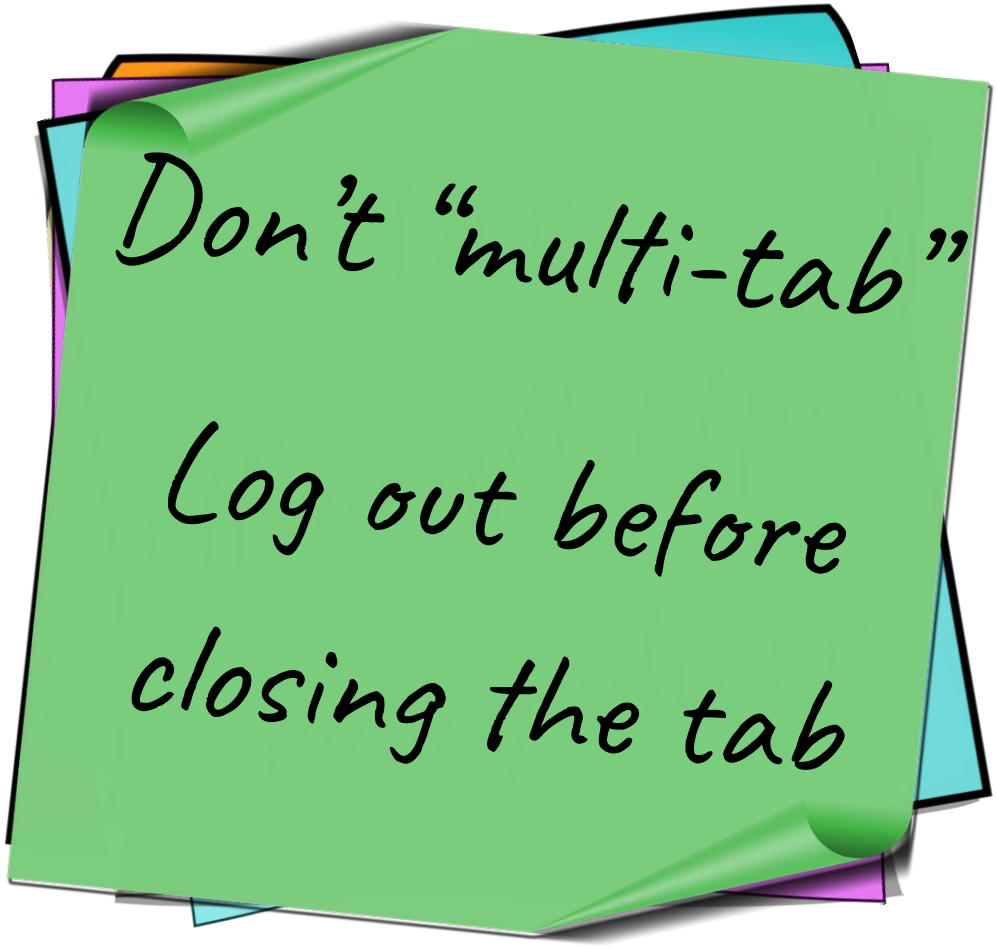
Chromium bug #930057	**CVE-2019-5814**	⇒	**US$1,000**
Mozilla bug #1526218	**CVE-2018-18511**	⇒	**US$3,000**
Mozilla bug #1528909	**CVE-2019-9797**	⇒	another **US$3,000**




Not sure if the web app is broken
Or my browser is a malware

To do

To do



SOP bypass

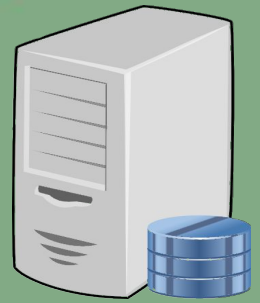
SOP bypass via DNS rebinding

In DNS we trust

DNS rebinding

hacke.rs: 1.3.3.7

evil
DNS server



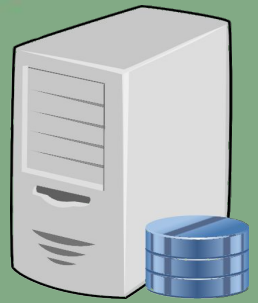
secure.bank: 1.2.3.4

DNS rebinding

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

evil DNS server



secure.bank: 1.2.3.4

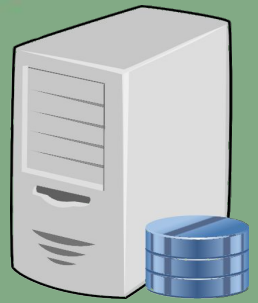
DNS rebinding

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

It's 1.2.3.4

evil DNS server

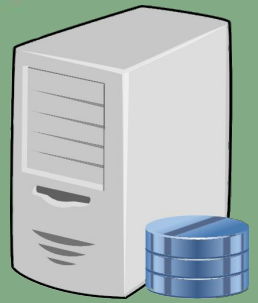


secure.bank: 1.2.3.4

DNS rebinding

hacke.rs: 1.3.3.7

evil
DNS server



Establish login session

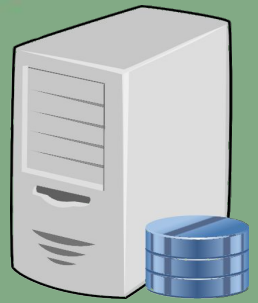
secure.bank: 1.2.3.4

DNS rebinding: later...

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

evil DNS server



secure.bank: 1.2.3.4

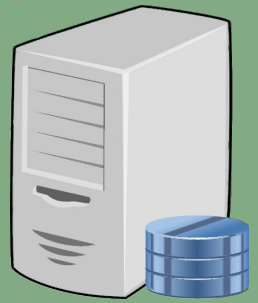
DNS rebinding: later...

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

It's 1.3.3.7

evil DNS server



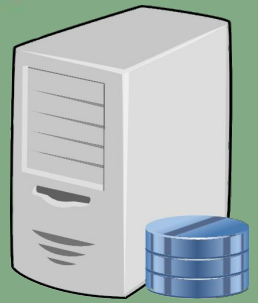
secure.bank: 1.2.3.4

DNS rebinding: later...

hacke.rs: 1.3.3.7

Get evil scripts

evil
DNS server



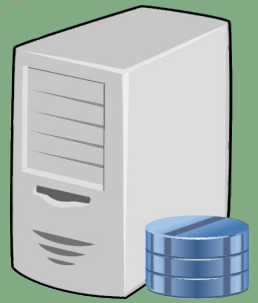
secure.bank: 1.2.3.4

DNS rebinding: laterer...

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

evil DNS server



secure.bank: 1.2.3.4

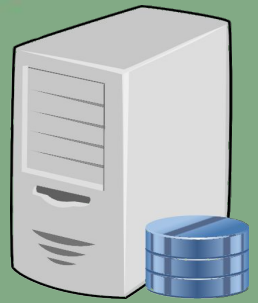
DNS rebinding: laterer...

hacke.rs: 1.3.3.7

What's the IP address of secure.bank ?

It's 1.2.3.4

evil DNS server

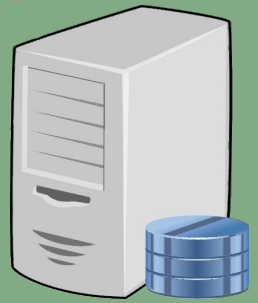


secure.bank: 1.2.3.4

DNS rebinding: laterer...

hacke.rs: 1.3.3.7

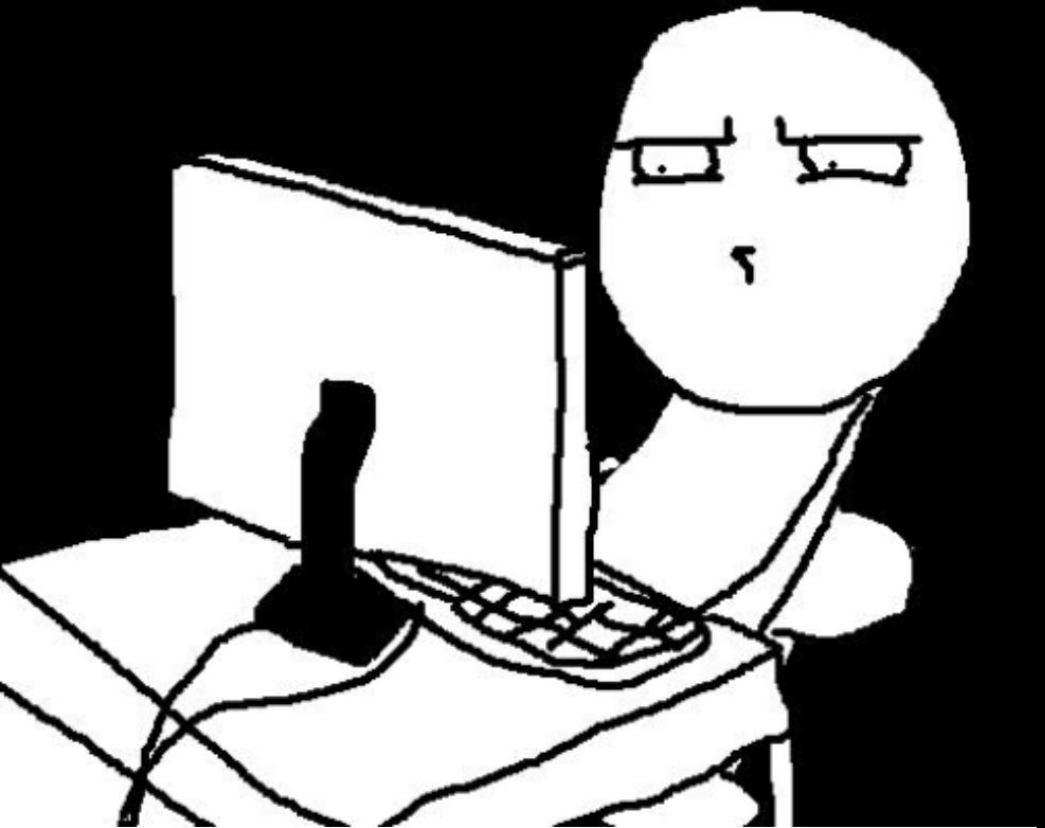
evil
DNS server



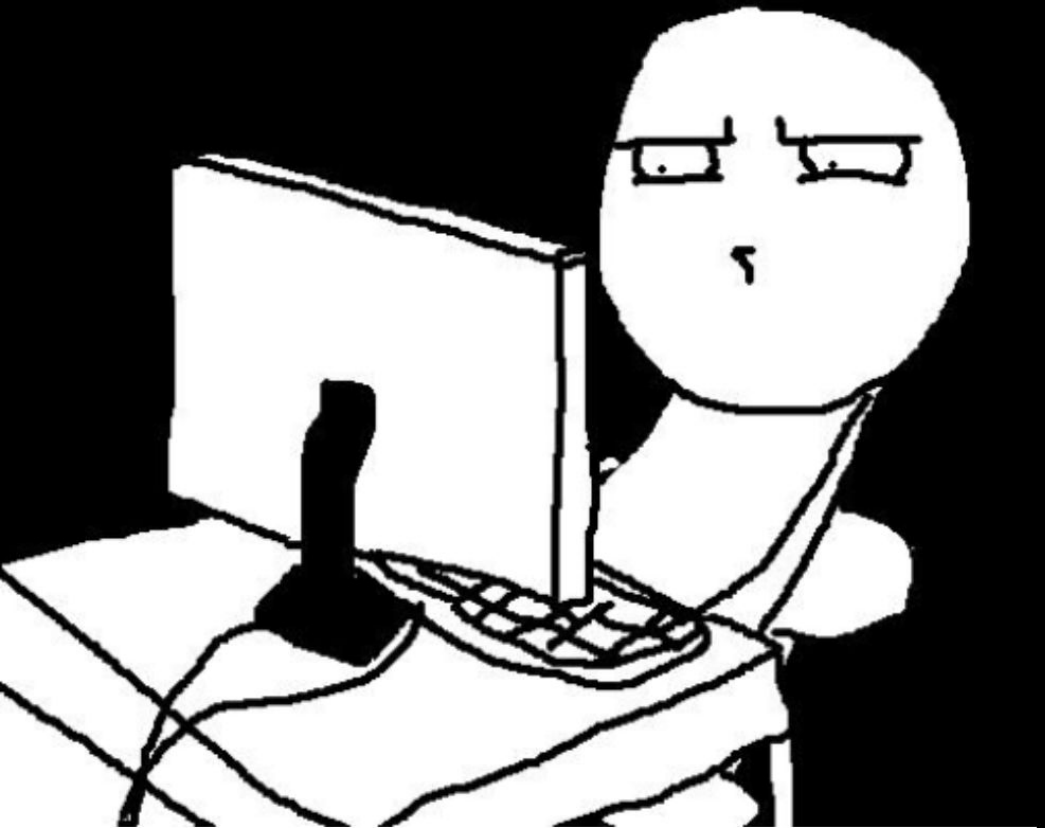
Evil scripts get private data

secure.bank: 1.2.3.4

WHAT HAPPENED HERE?!

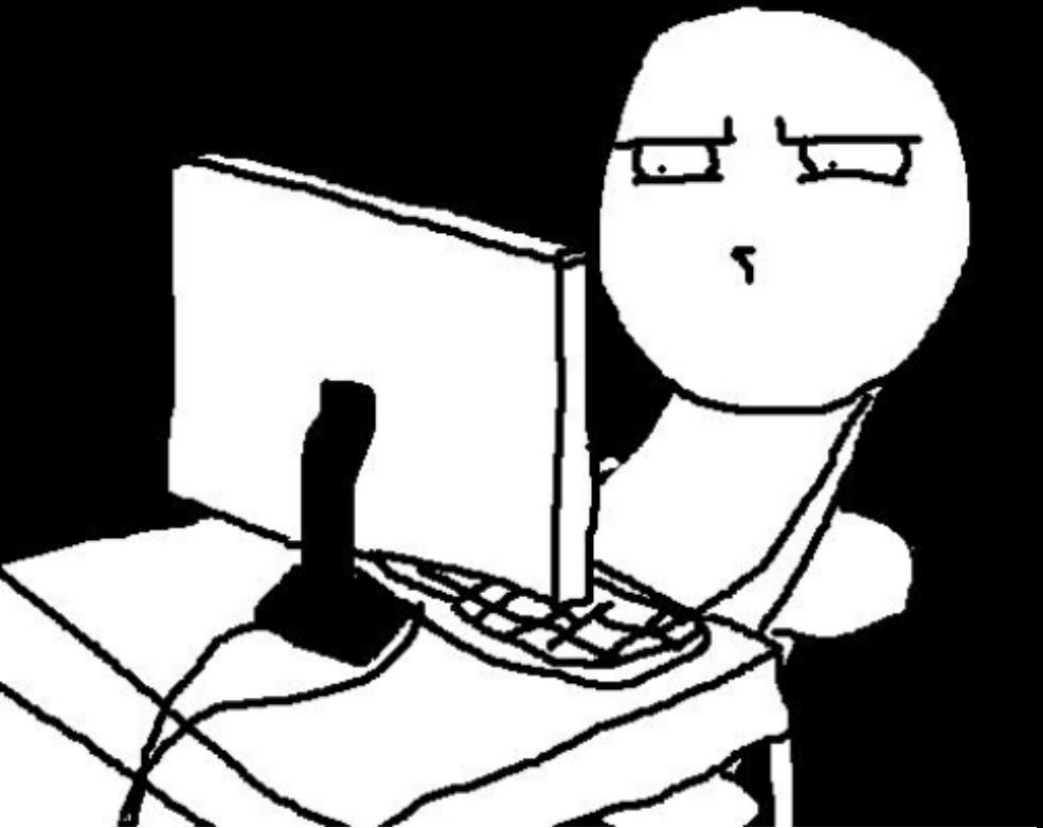


WHAT HAPPENED HERE?!



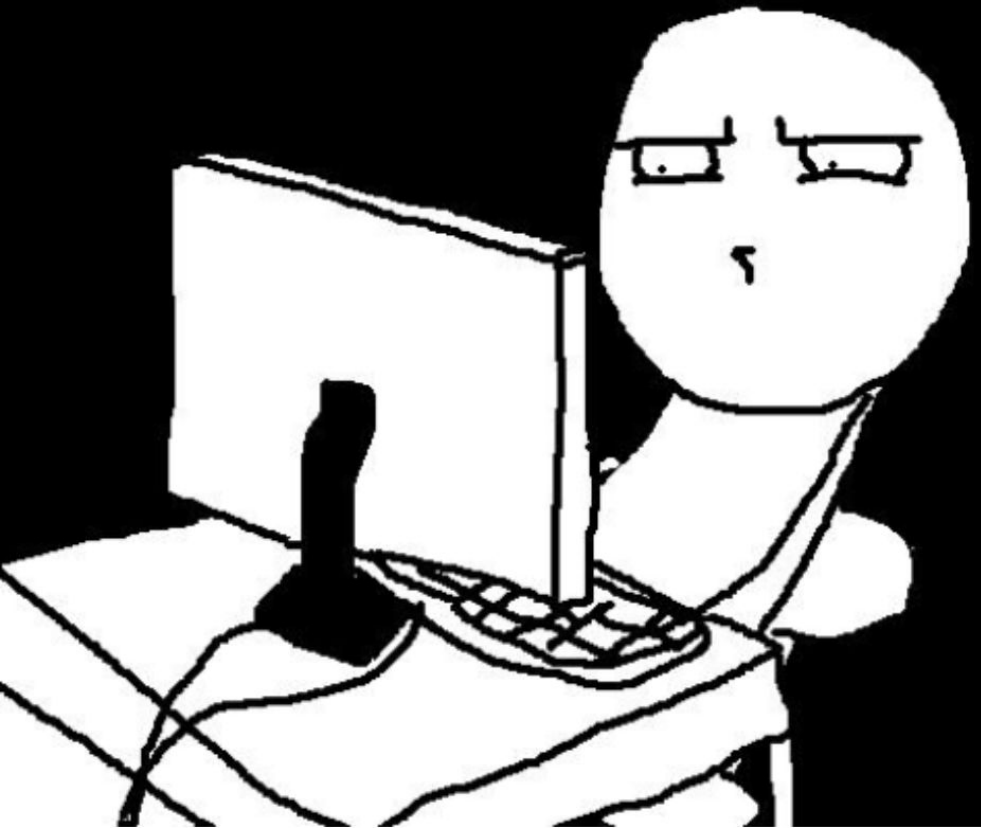
- Rogue DHCP server (setup by aliens)

WHAT HAPPENED HERE?!



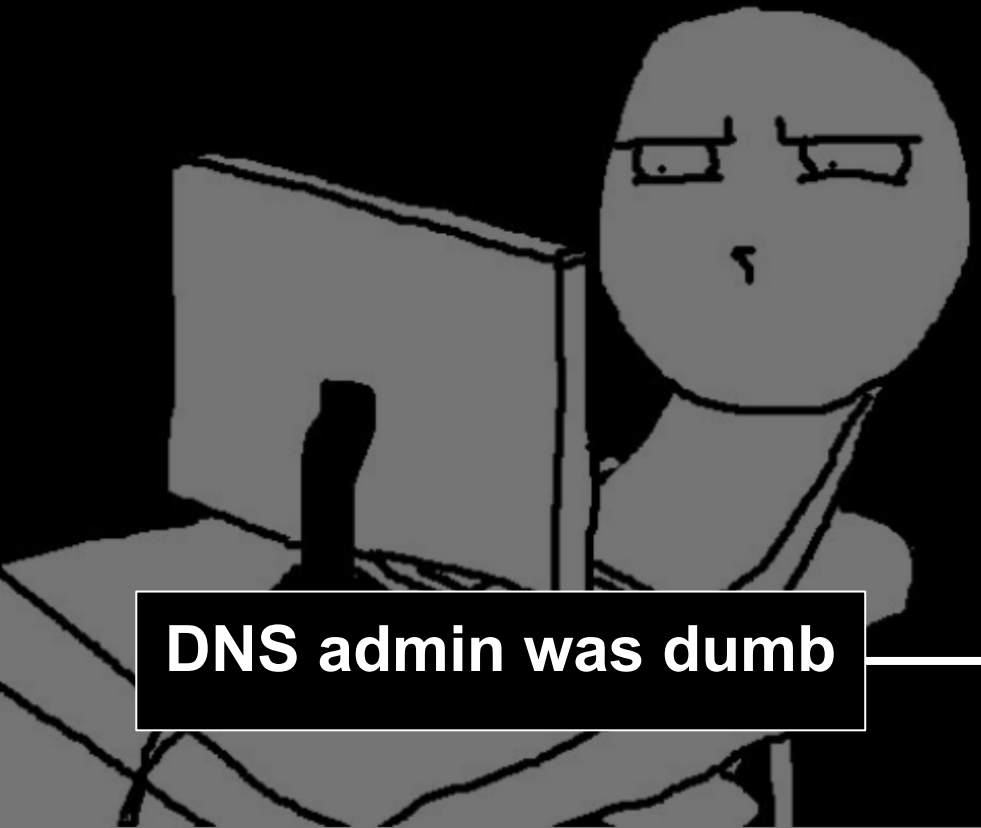
- Rogue DHCP server (setup by aliens)
- Multicast DNS or NetBIOS (invented by aliens)

WHAT HAPPENED HERE?!



- Rogue DHCP server (setup by aliens)
- Multicast DNS or NetBIOS (invented by aliens)
- DNS cache poisoning

WHAT HAPPENED HERE?!

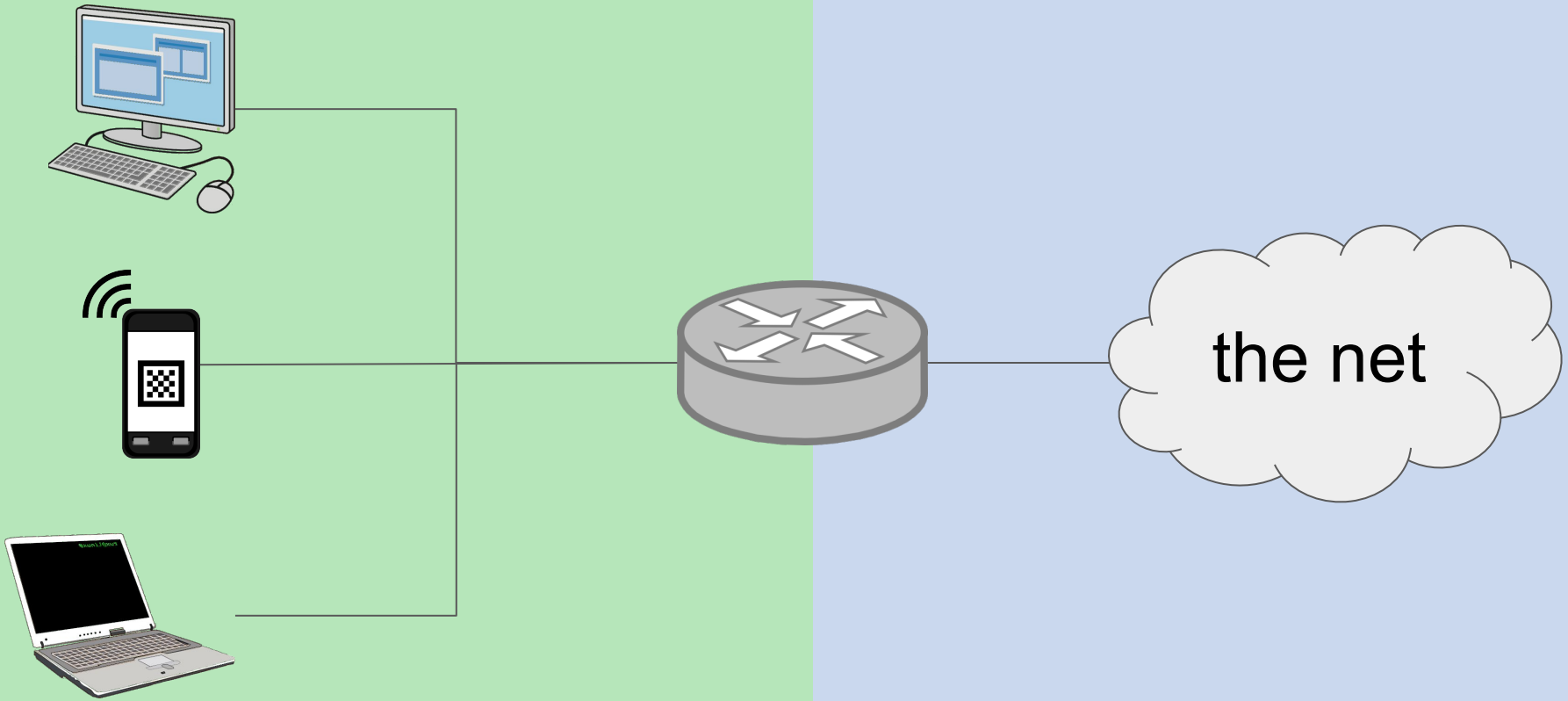


- Rogue DHCP server (setup by aliens)
- Multicast DNS or NetBIOS (invented by aliens)
- DNS cache poisoning

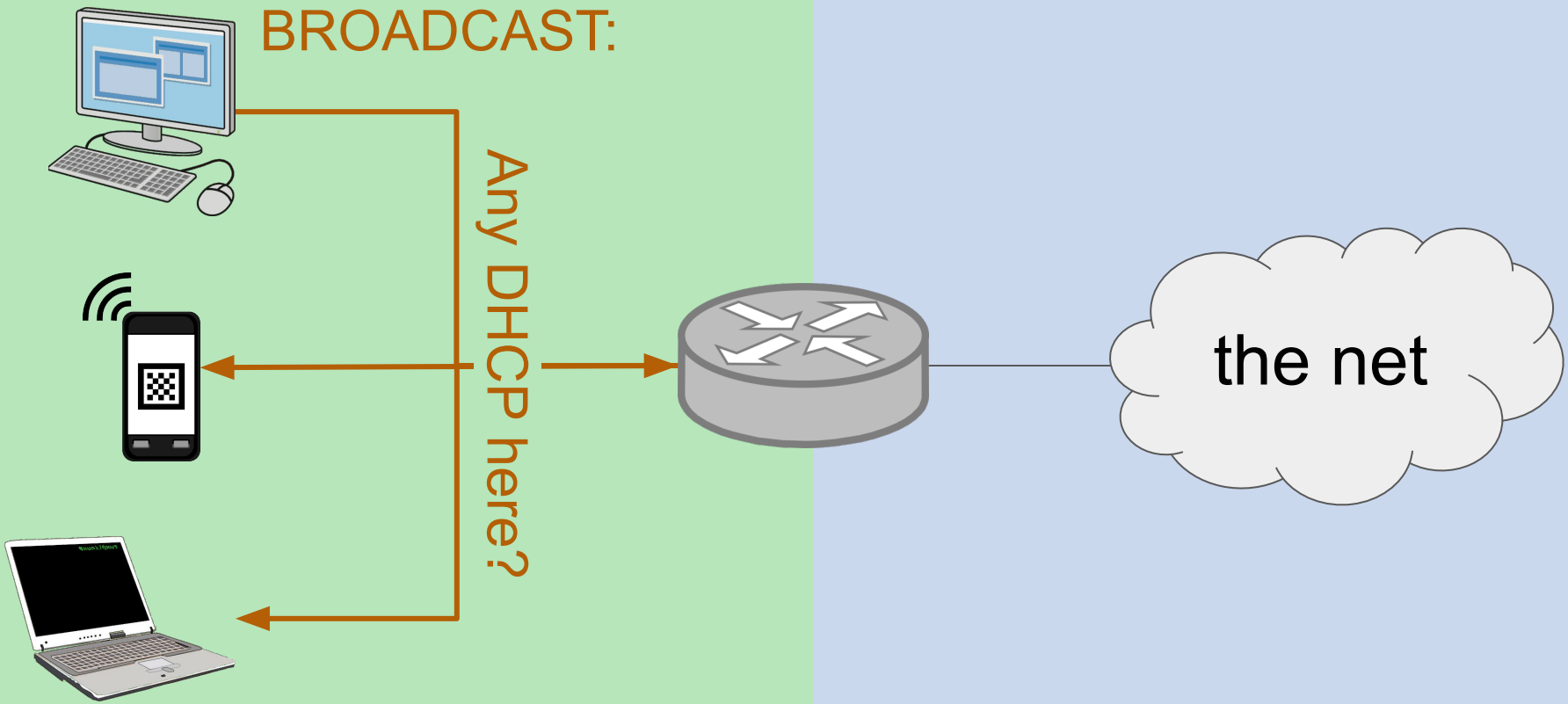
WHAT HAPPENED HERE?!

- Rogue DHCP server (setup by aliens)
- Multicast DNS or NetBIOS (invented by aliens)
- DNS cache poisoning

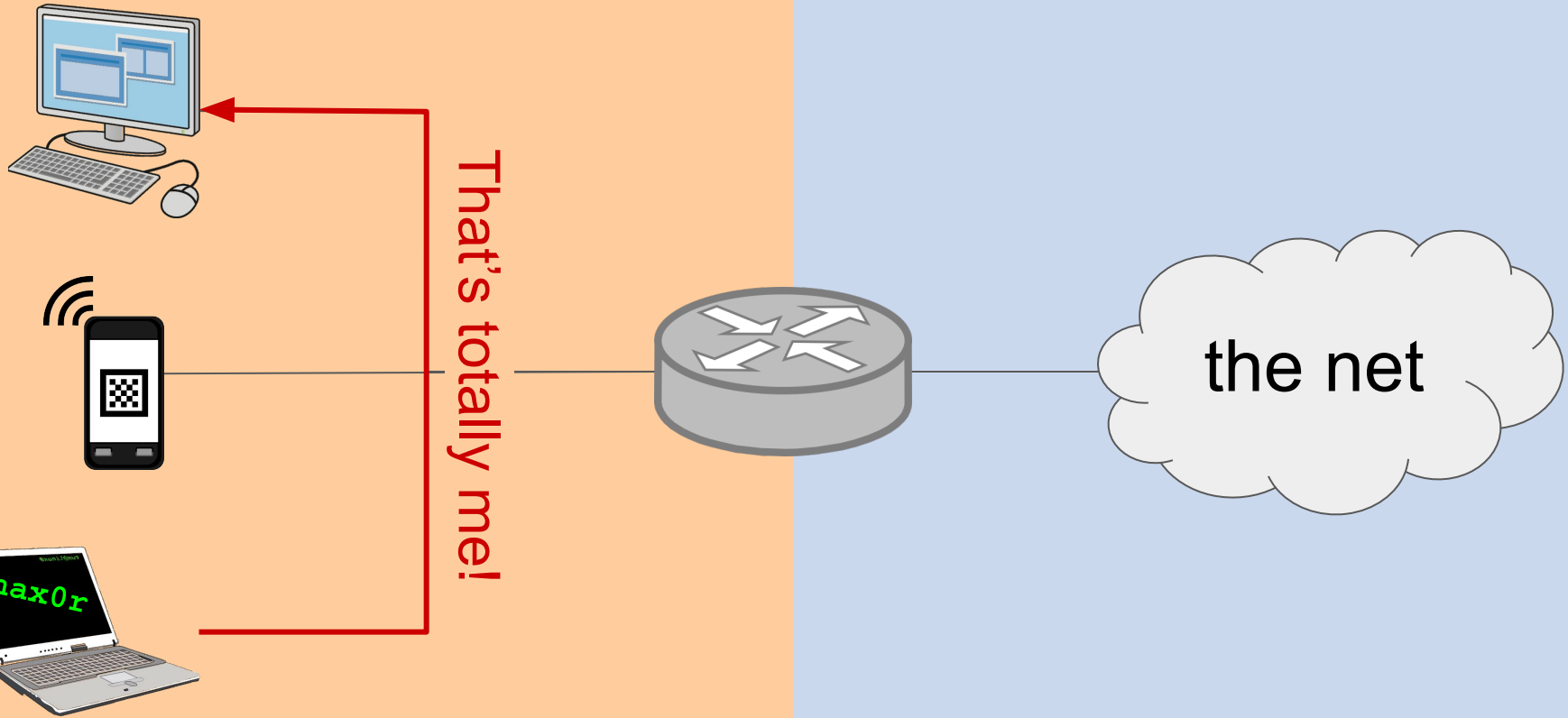
Rogue DHCP



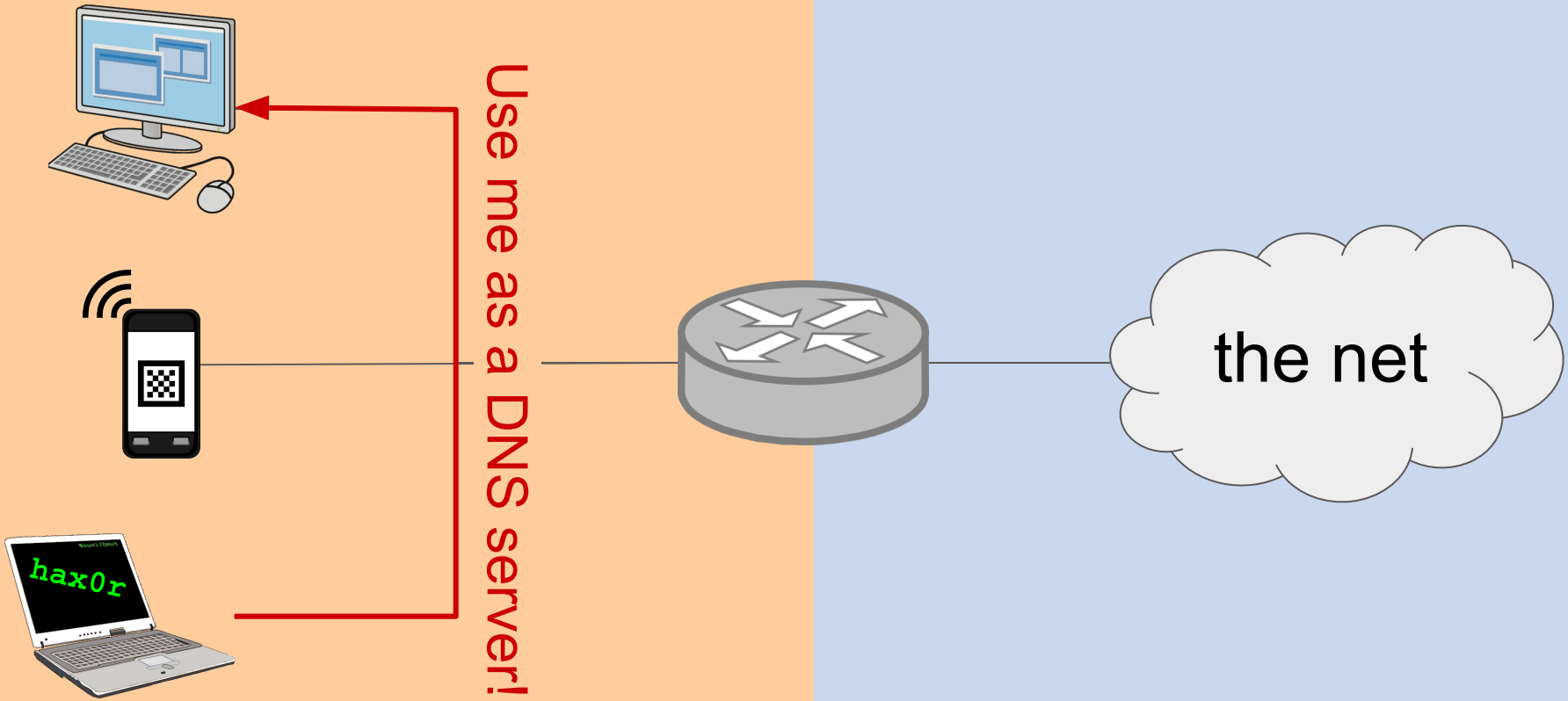
Rogue DHCP



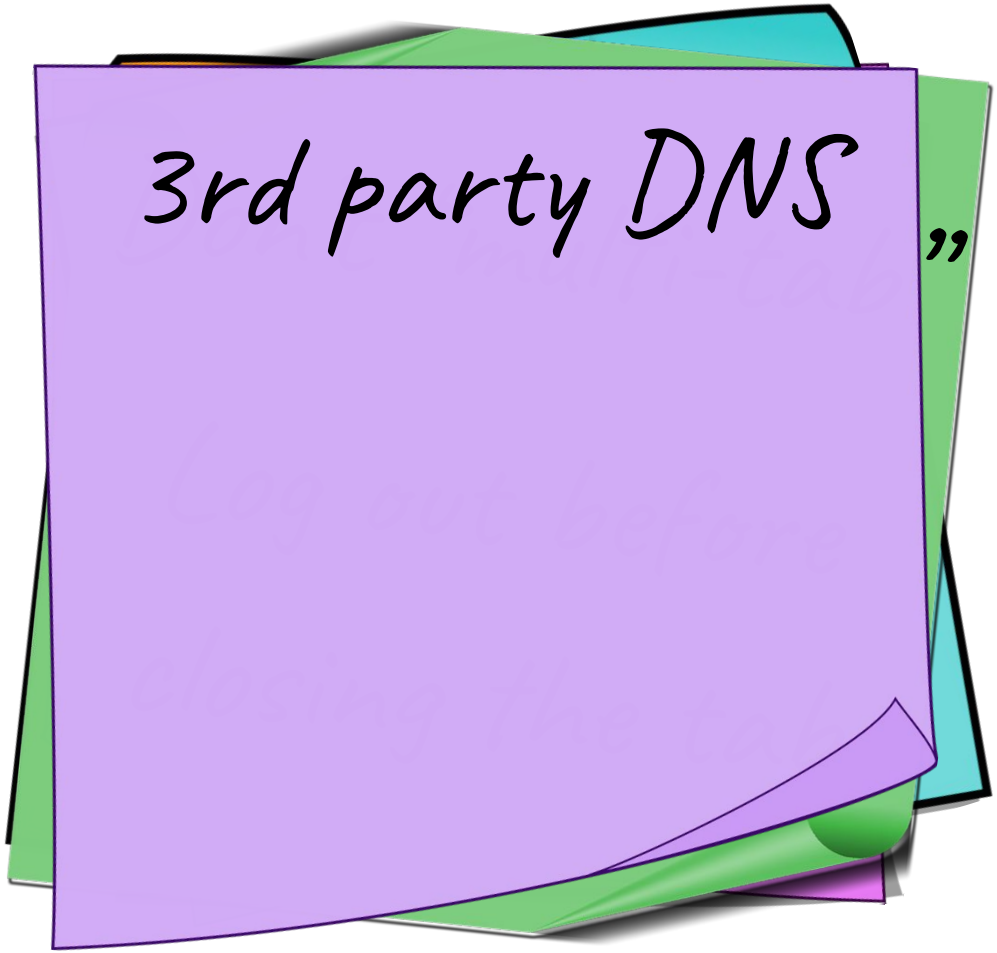
Rogue DHCP



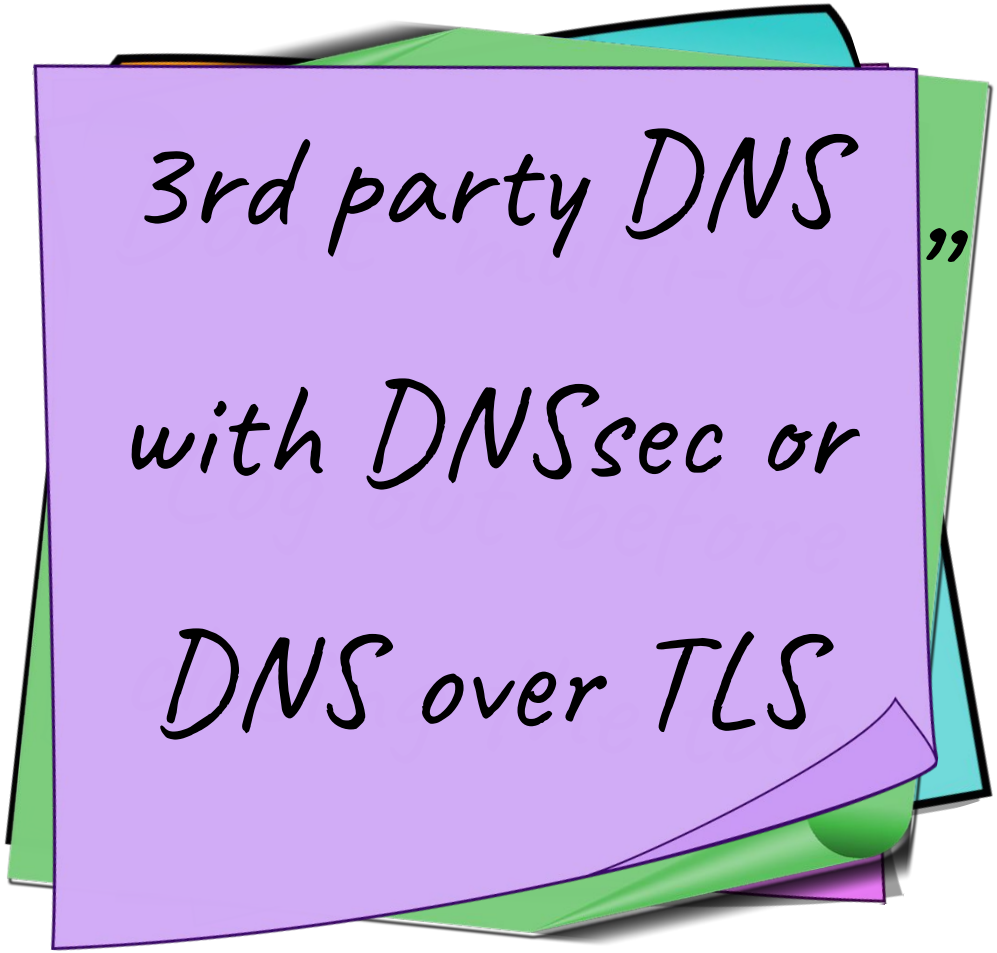
Rogue DHCP



To do



To do



ARE YOU

DONE YET

What happens when you type in the address bar?

What happens when you type in the address bar?

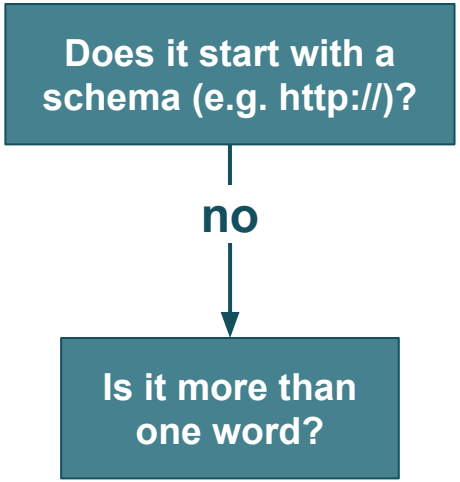
Use default search engine

Establish connection

Does it start with a schema (e.g. http://)?

Use default search engine

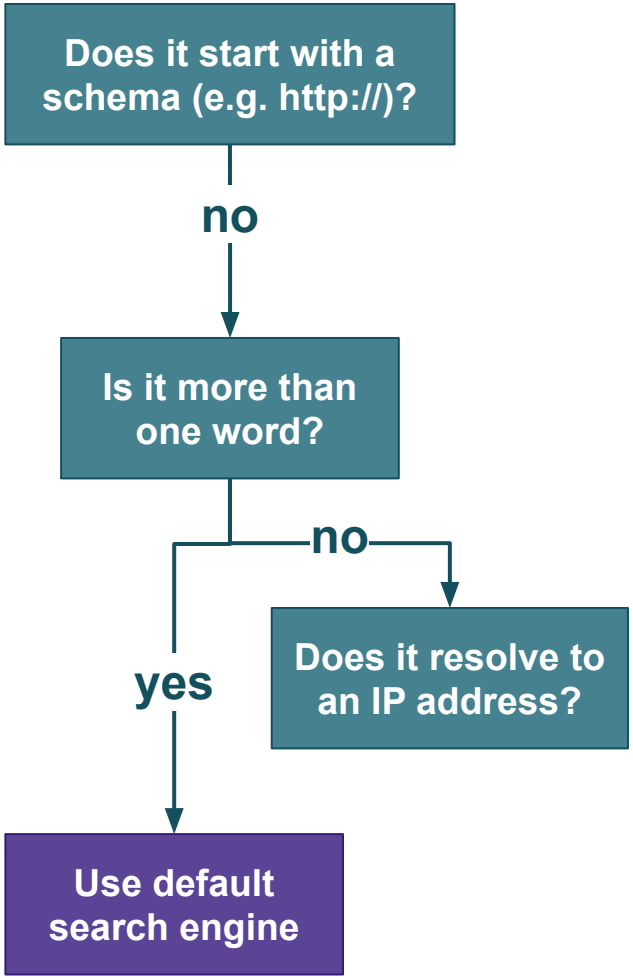
Establish connection



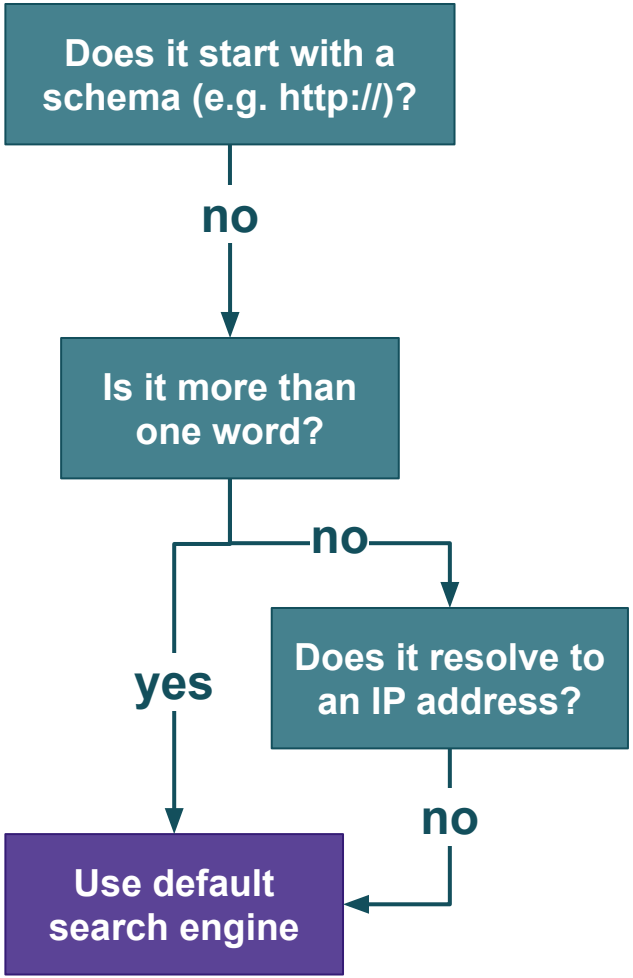
Use default search engine

Establish connection

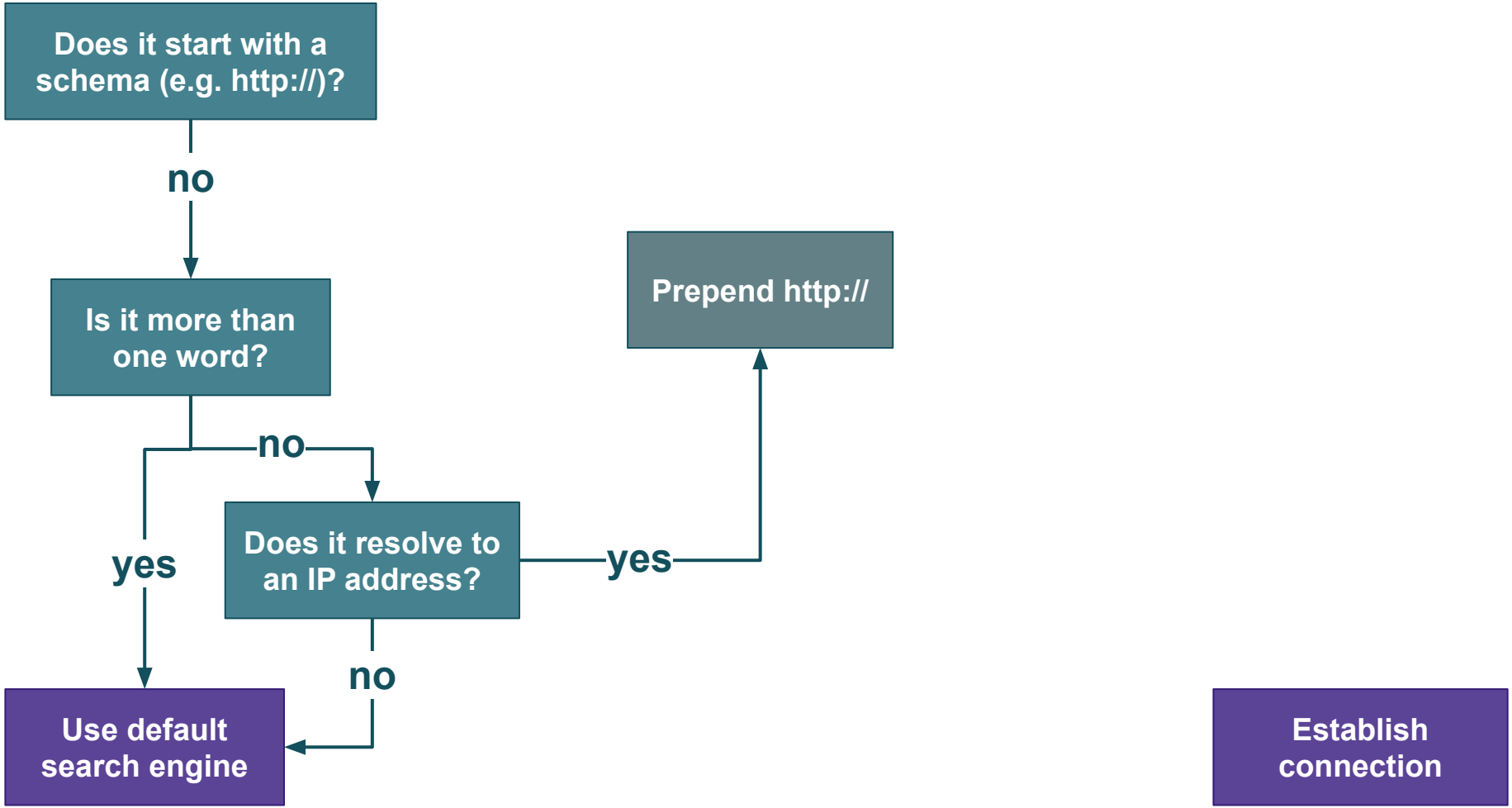

Does it start with a schema (e.g. http://)?
no
Is it more than one word?
yes
Use default search engine
Establish connection

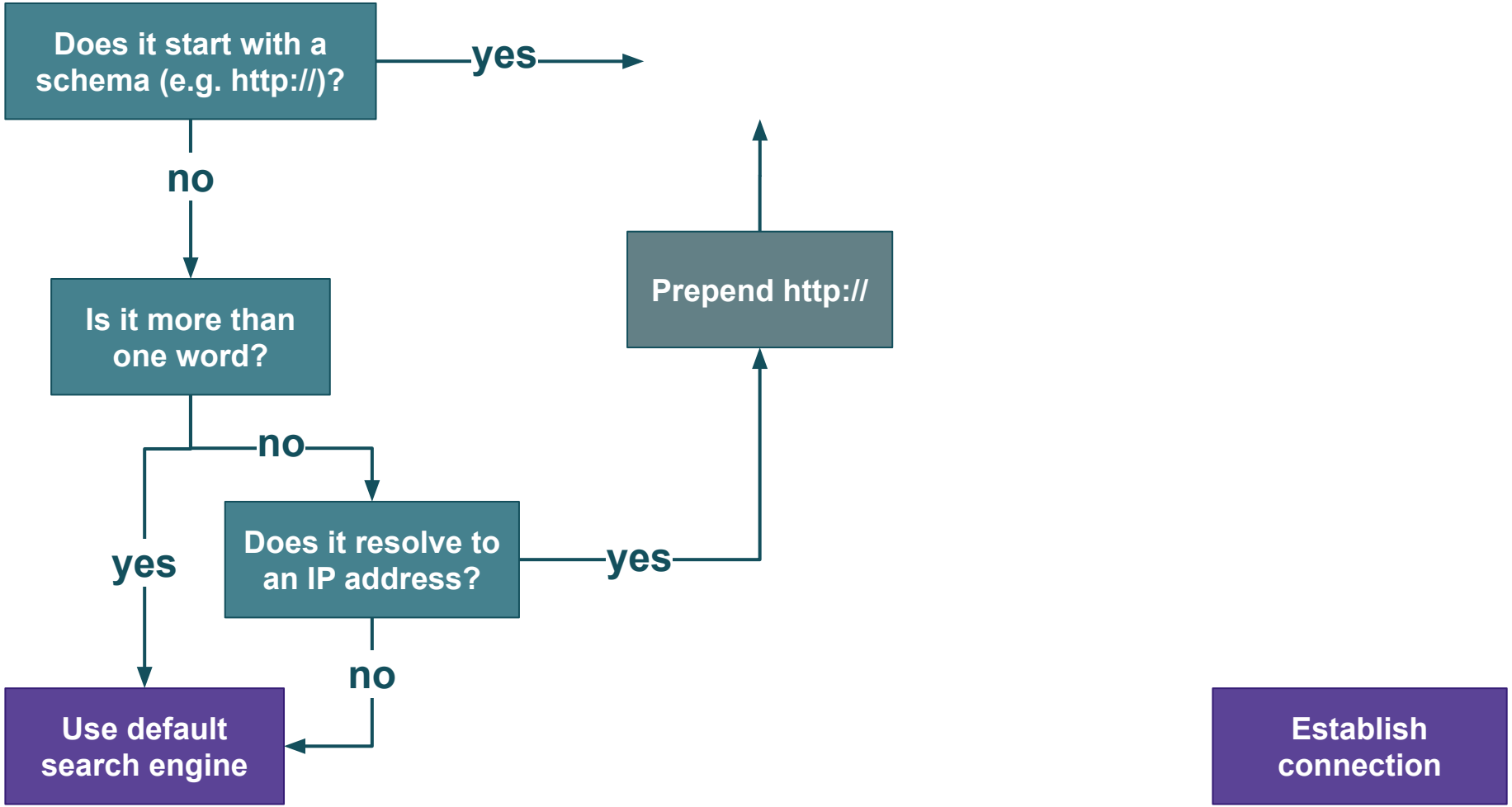


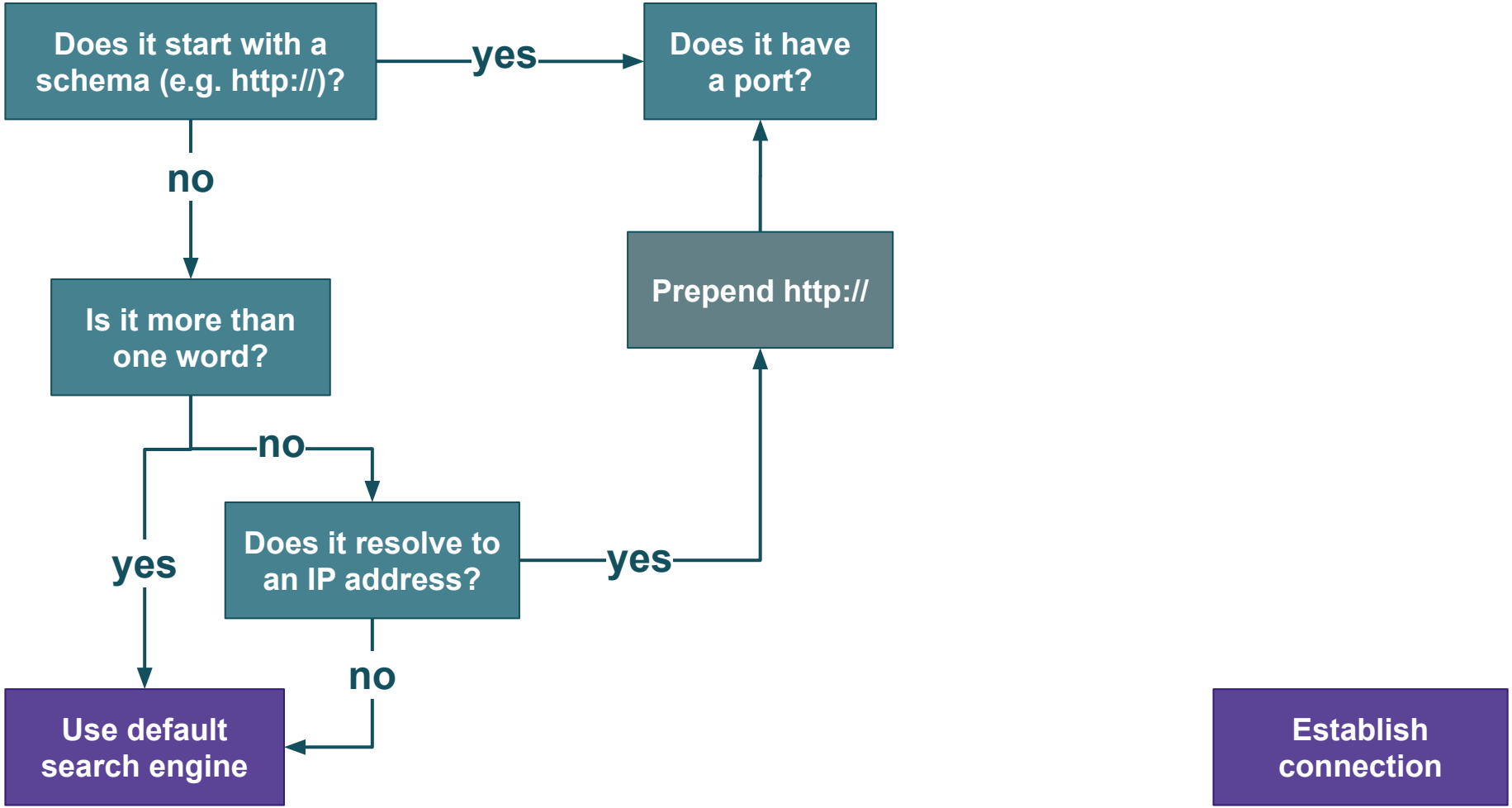
Establish connection

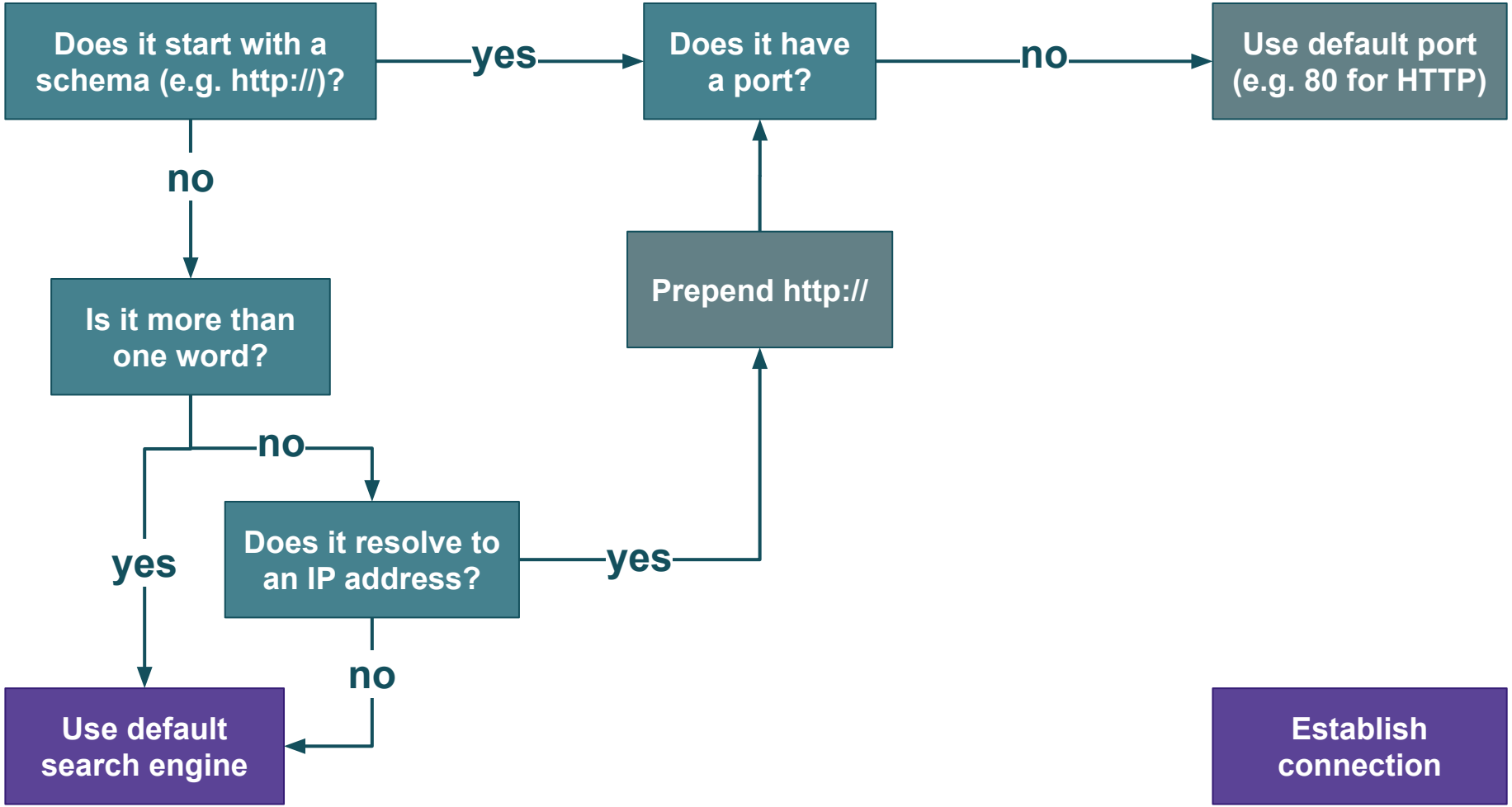


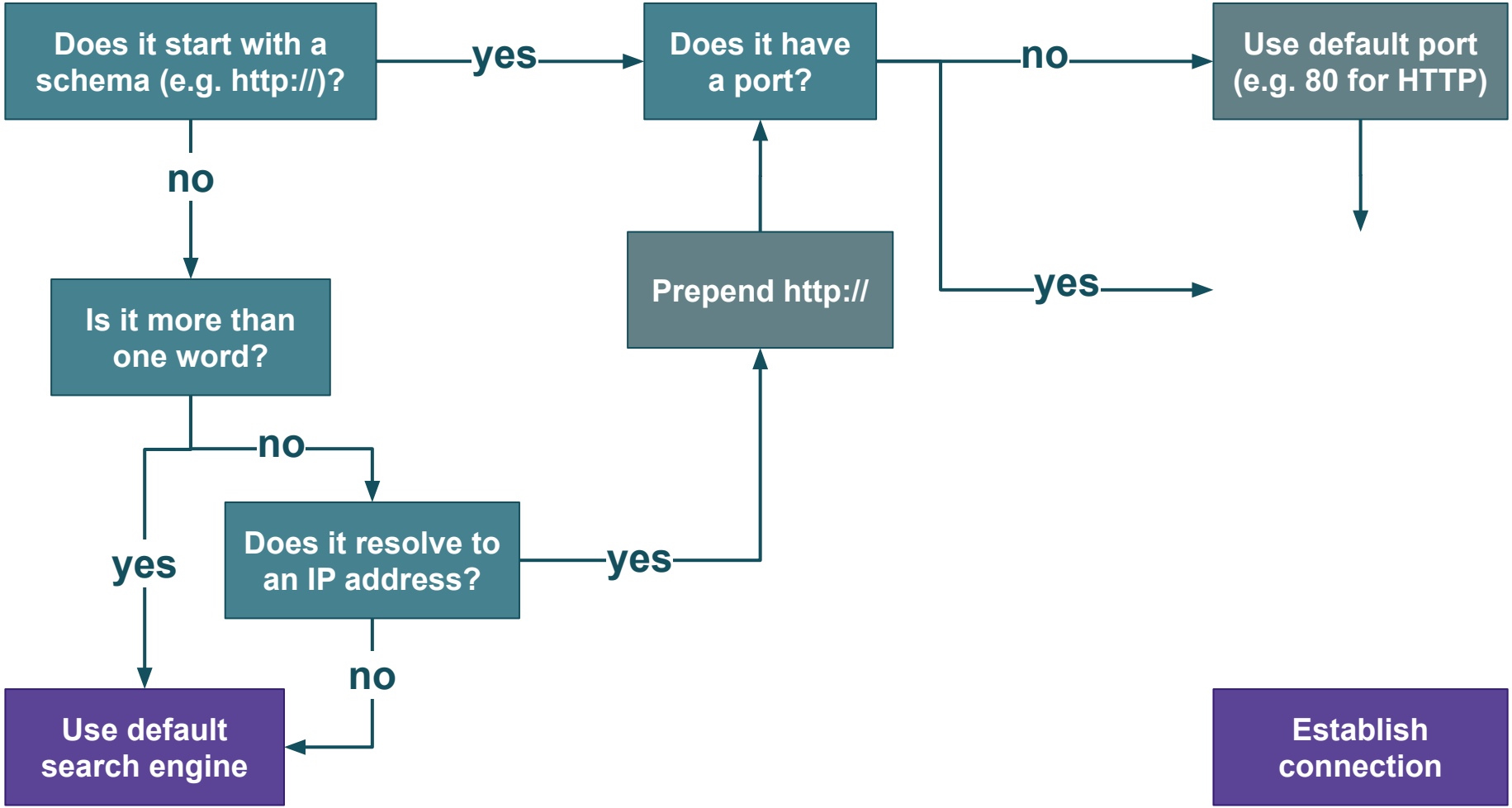
Establish connection

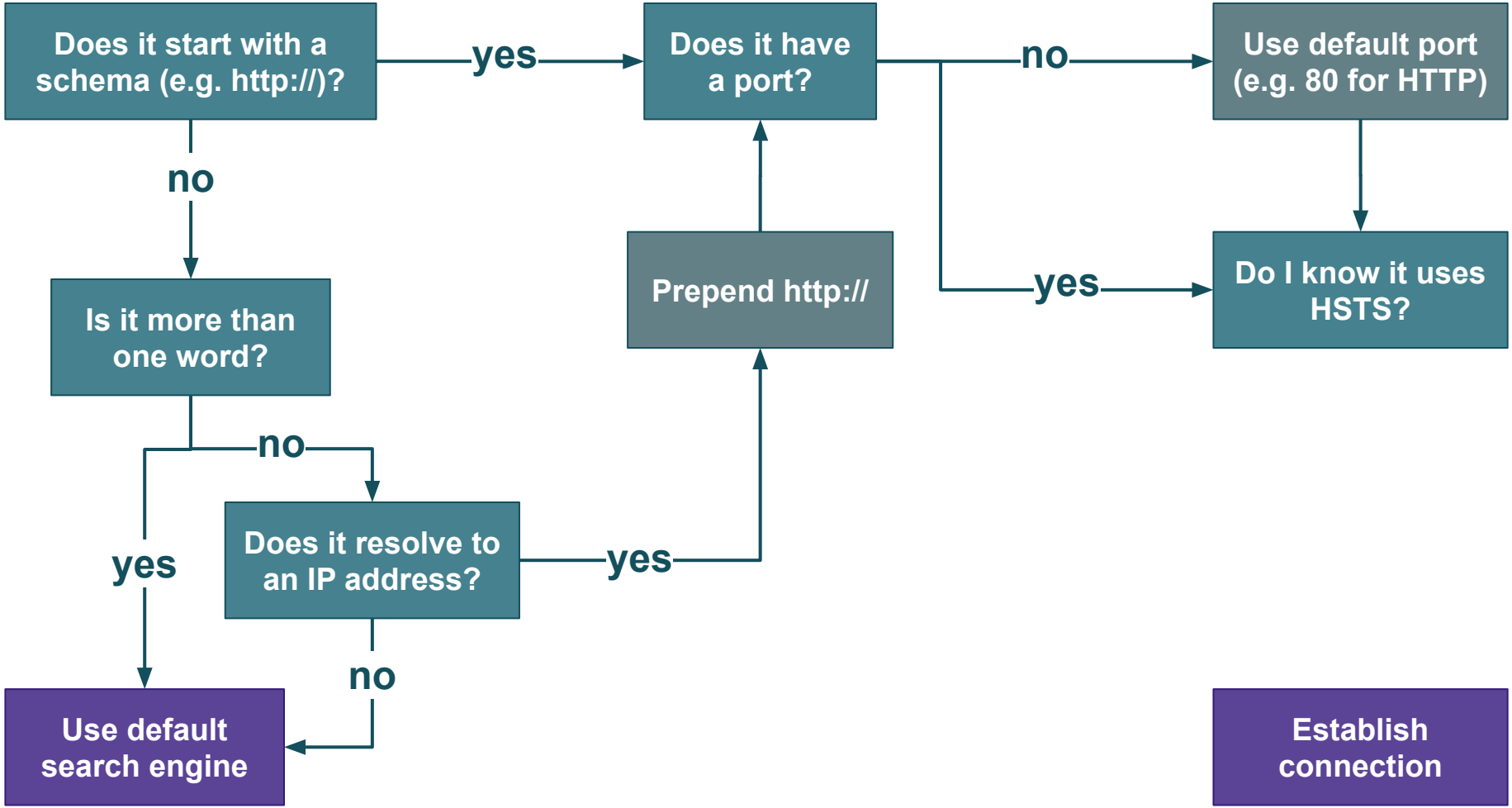

Does it start with a schema (e.g. http://)?
no
Is it more than one word?
no
yes
Does it resolve to an IP address?
yes
Prepend http://
no
Use default search engine
Establish connection

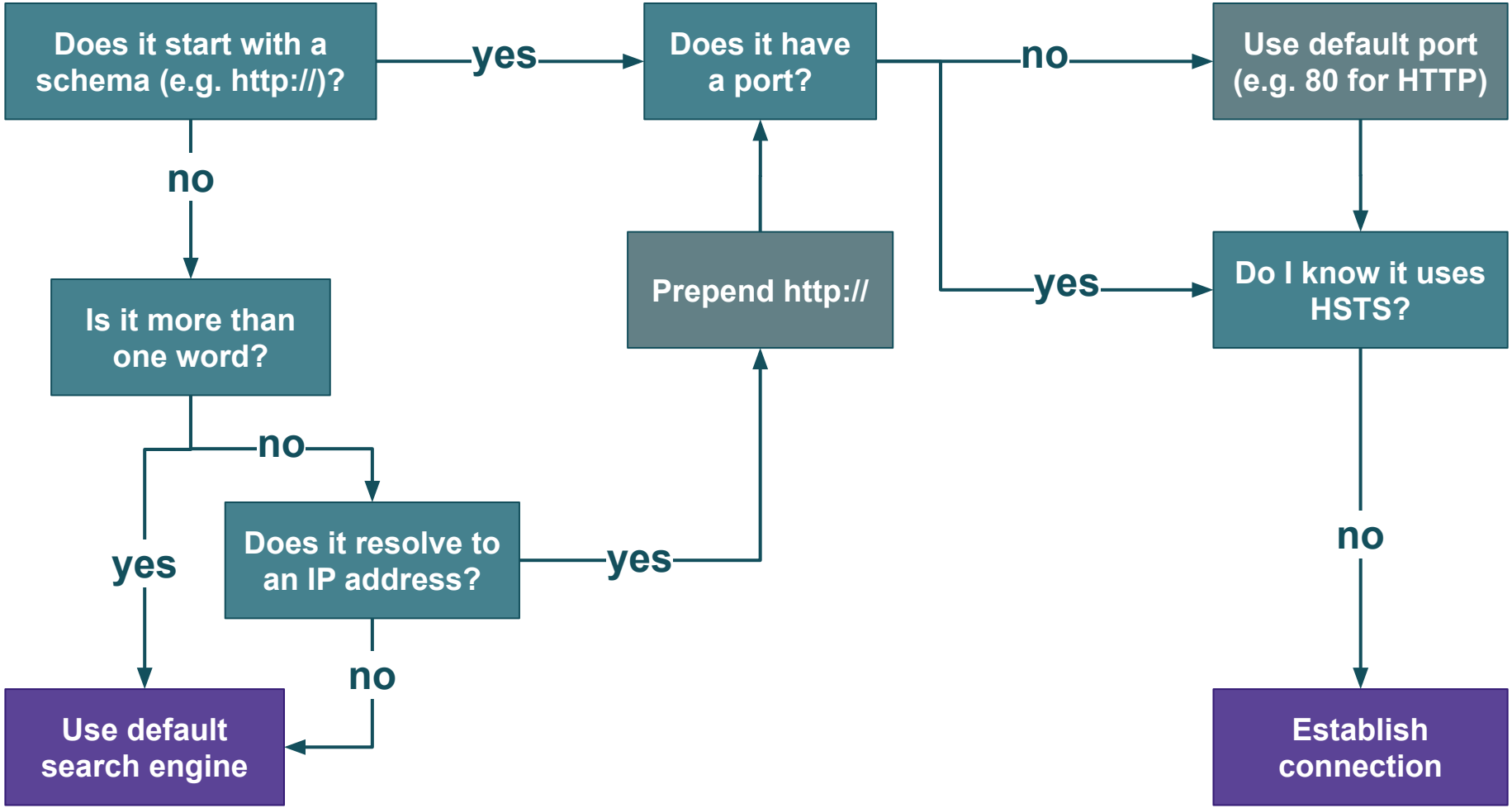

Does it start with a schema (e.g. http://)?
yes
no
Is it more than one word?
no
yes
Does it resolve to an IP address?
yes
no
Prepend http://
Use default search engine
Establish connection

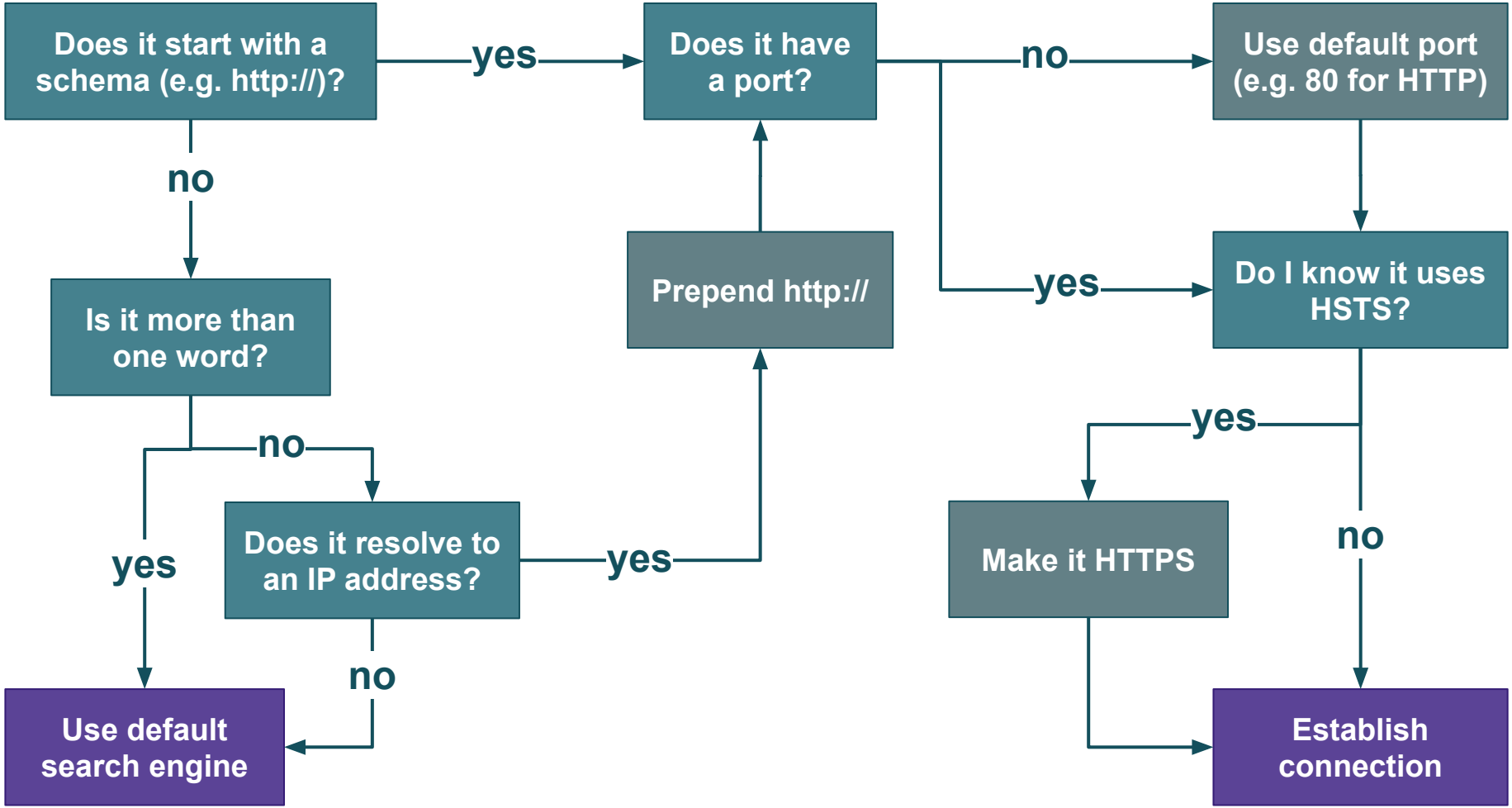

Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Prepend http://
Is it more than one word?
no
yes
Does it resolve to an IP address?
yes
no
Use default search engine
Establish connection

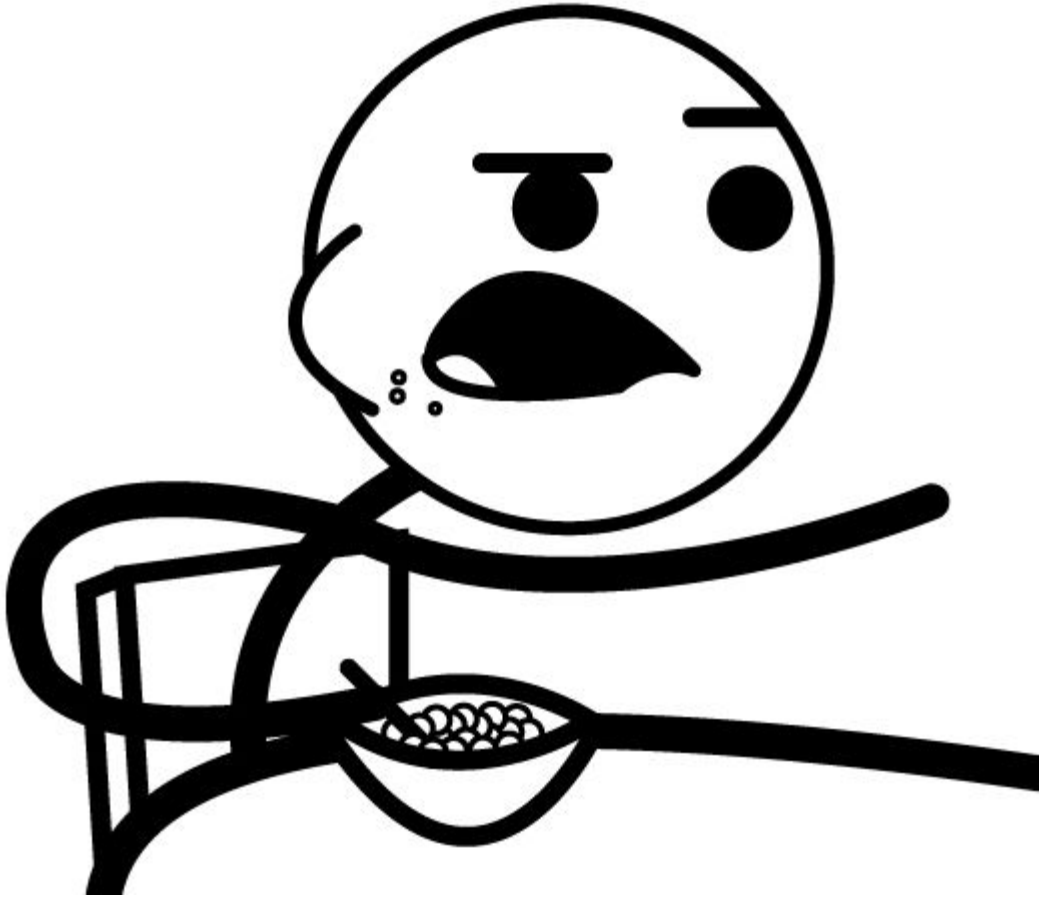

Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
Is it more than one word?
Prepend http://
no
yes
Does it resolve to an IP address?
yes
no
Use default search engine
Establish connection


Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
yes
Prepend http://
Is it more than one word?
no
yes
Does it resolve to an IP address?
yes
no
Use default search engine
Establish connection

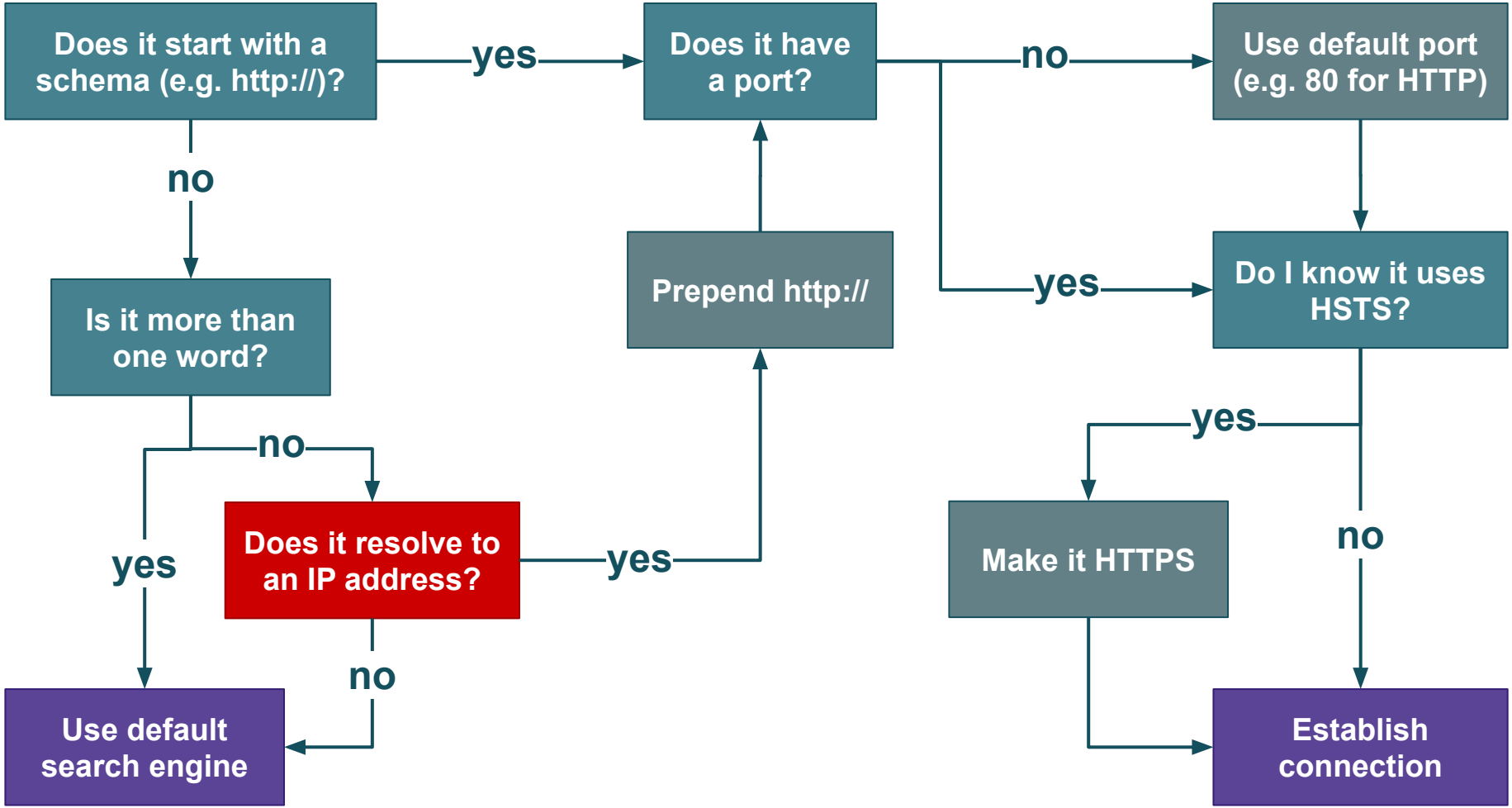

Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
Is it more than one word?
Prepend http://
yes
Do I know it uses HSTS?
no
yes
Does it resolve to an IP address?
yes
no
Use default search engine
Establish connection


Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
Is it more than one word?
Prepend http://
yes
Do I know it uses HSTS?
no
yes
Does it resolve to an IP address?
yes
yes
no
no
Use default search engine
Establish connection

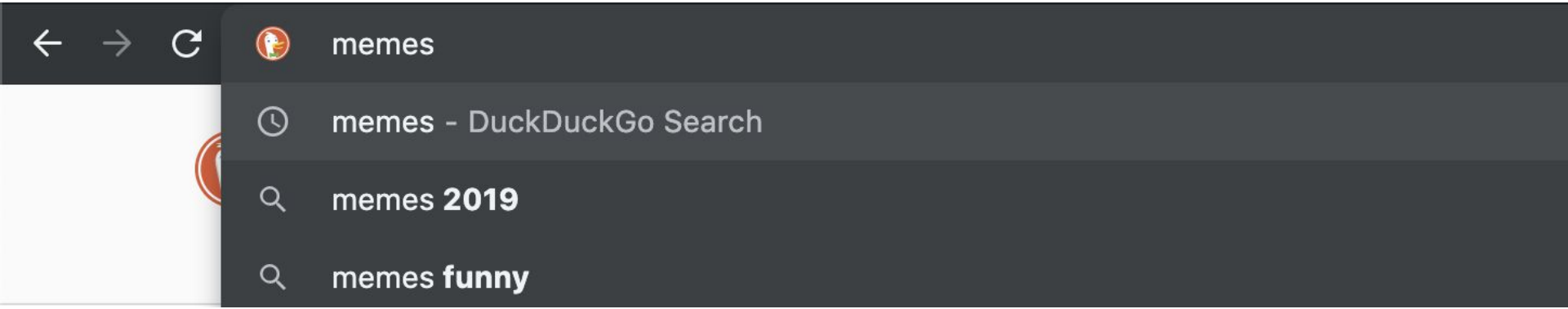

Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
Prepend http://
yes
Do I know it uses HSTS?
Is it more than one word?
no
yes
Does it resolve to an IP address?
yes
yes
Make it HTTPS
no
yes
no
Use default search engine
Establish connection



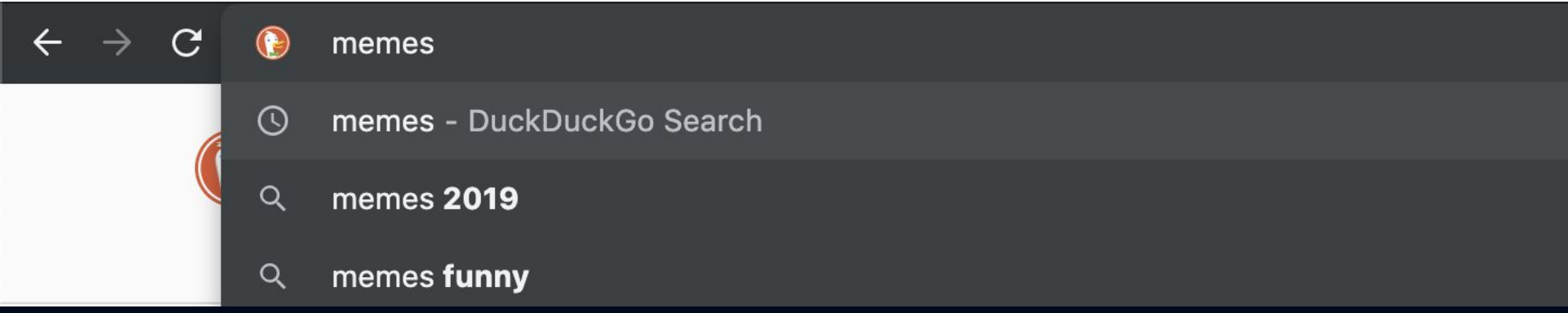
BLAH
BLAH
BLAH


Does it start with a schema (e.g. http://)?
yes
Does it have a port?
no
Use default port (e.g. 80 for HTTP)
no
Is it more than one word?
Prepend http://
yes
Do I know it uses HSTS?
no
yes
Does it resolve to an IP address?
yes
yes
Make it HTTPS
no
no
Use default search engine
Establish connection

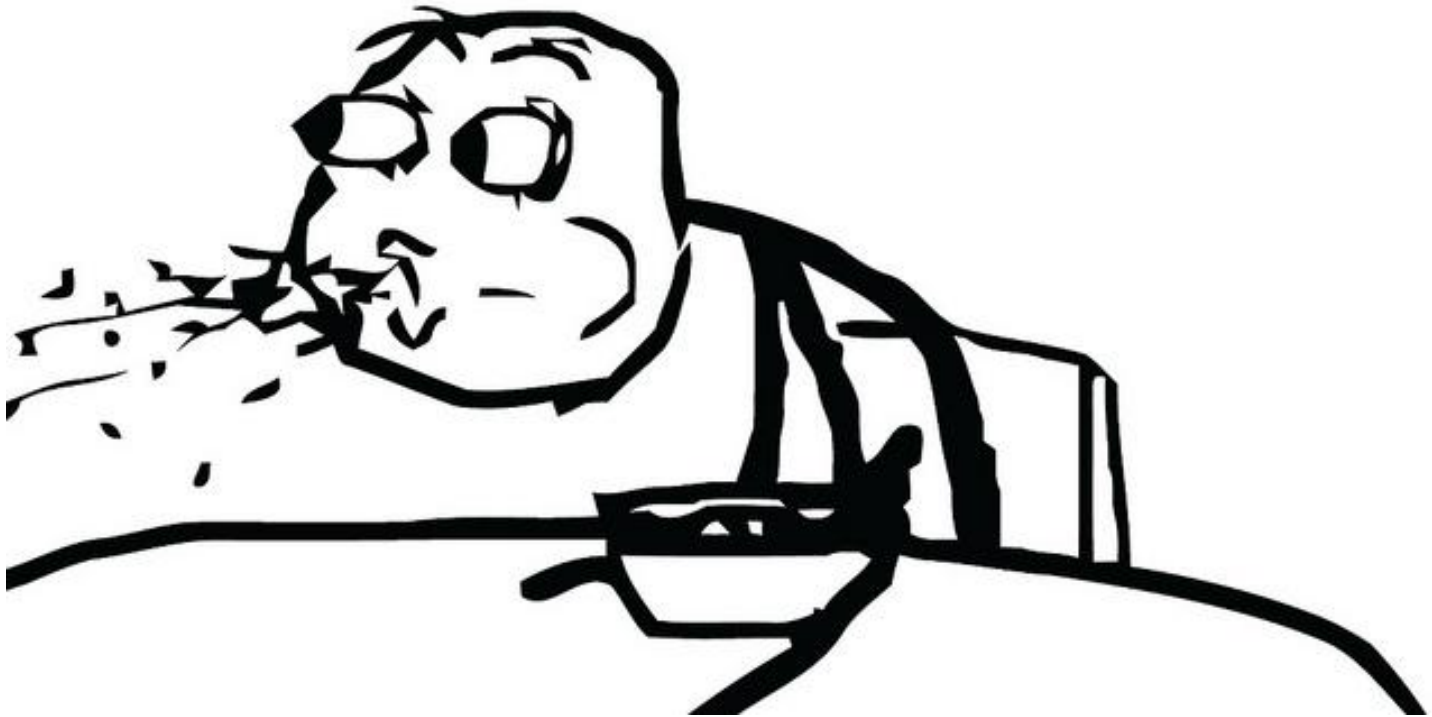
What happens when you type in the address bar?



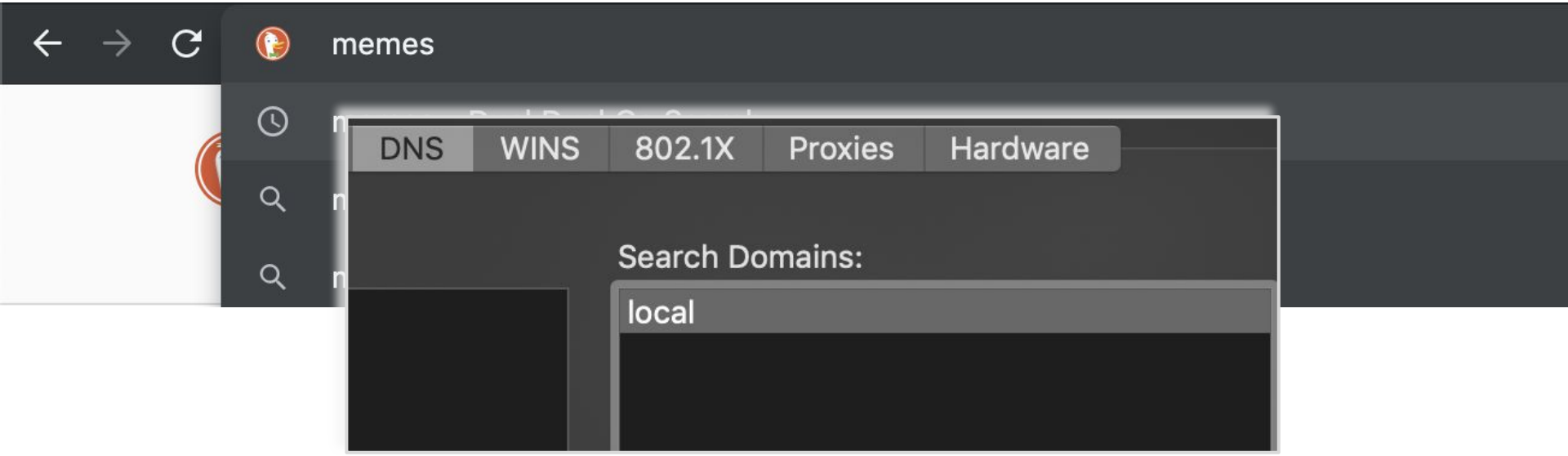
What happens when you type in the address bar?



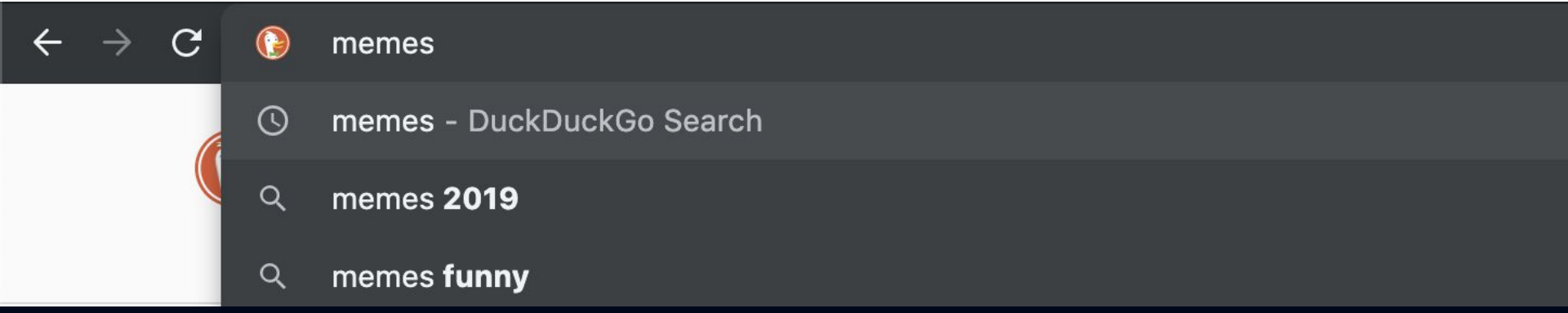

```
anikolova ttys009 ~ sudo tshark -i en0 dst port 53
Capturing on 'Wi-Fi'
    1   0.000000 192.168.1.121 → 192.168.1.1  DNS 65 Standard query 0xc9b0 A memes
```



What happens when you type in the address bar?



What happens when you type in the address bar?




```
anikolova ttys009 ~ sudo tshark -i en0 dst port 53
Capturing on 'Wi-Fi'
    1   0.000000 192.168.1.121 → 192.168.1.1  DNS 71 Standard query 0x969b A memes.local
    2   0.080878 192.168.1.121 → 192.168.1.1  DNS 71 Standard query 0x000f A memes.local
```

What happens when you type in the address bar?

To do

TL;DR: (Dis)trust on the LAN

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address:

⇒ impersonate a machine we trust

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address:

⇒ impersonate a machine we trust

⇒ person-in-the-middle

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address:

- ⇒ impersonate a machine we trust
  - ⇒ person-in-the-middle
- ⇒ DNS rebinding

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address:

- ⇒ impersonate a machine we trust
  - ⇒ person-in-the-middle
- ⇒ DNS rebinding
- ⇒ DNS hijiacking

TL;DR: (Dis)trust on the LAN

Any machine can choose its IP or MAC address:

- ⇒ impersonate a machine we trust
  - ⇒ person-in-the-middle
- ⇒ DNS rebinding
- ⇒ DNS hijiacking

(If wireless) any machine can read the traffic of any other

TL;DR: (Dis)trust on the net

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous!

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don’t enter PPI)!

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don’t enter PPI)!

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don’t enter PPI):

⇒ phishing

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

⇒ phishing

⇒ hack accounts on other sites

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

- ⇒ phishing
  - ⇒ hack accounts on other sites
  - ⇒ install evil browser extensions or other software

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

- ⇒ phishing
  - ⇒ hack accounts on other sites
  - ⇒ install evil browser extensions or other software
  - ⇒ attack other machines on the LAN

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

- ⇒ phishing
  - ⇒ hack accounts on other sites
  - ⇒ install evil browser extensions or other software
  - ⇒ attack other machines on the LAN
- ⇒ hack accounts on vulnerable sites

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

- ⇒ phishing
  - ⇒ hack accounts on other sites
  - ⇒ install evil browser extensions or other software
  - ⇒ attack other machines on the LAN
- ⇒ hack accounts on vulnerable sites

because

Good sites *can* be vulnerable

TL;DR: (Dis)trust on the net

Bad sites *can* be dangerous (even if you don't enter PPI):

- ⇒ phishing
  - ⇒ hack accounts on other sites
  - ⇒ install evil browser extensions or other software
  - ⇒ attack other machines on the LAN
- ⇒ hack accounts on vulnerable sites

Good sites *can* be vulnerable

- ⇒ distribute malware

TL;DR: As a good user, you:

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings
- Use HTTPS everywhere

TL;DR: As a good user, you:

- Get off your flatmate's wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings
- Use HTTPS everywhere
- Log out of sites (or automatic cookie clearing)

TL;DR: As a good user, you:

- Get off your flatmate's wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings
- Use HTTPS everywhere
- Log out of sites (or automatic cookie clearing)
- Use 3rd party DNS with DNSsec or DNS over TLS

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings
- Use HTTPS everywhere
- Log out of sites (or automatic cookie clearing)
- Use 3rd party DNS with DNSsec or DNS over TLS
- Don’t use address bar search

TL;DR: As a good user, you:

- Get off your flatmate’s wi-fi (or hack their router and take control)
- Do not connect to untrusted networks
- Do not use untrusted devices
- Do not ignore certificate warnings
- Use HTTPS everywhere
- Log out of sites (or automatic cookie clearing)
- Use 3rd party DNS with DNSsec or DNS over TLS
- Don’t use address bar search
- Keep your browser up to date, duh

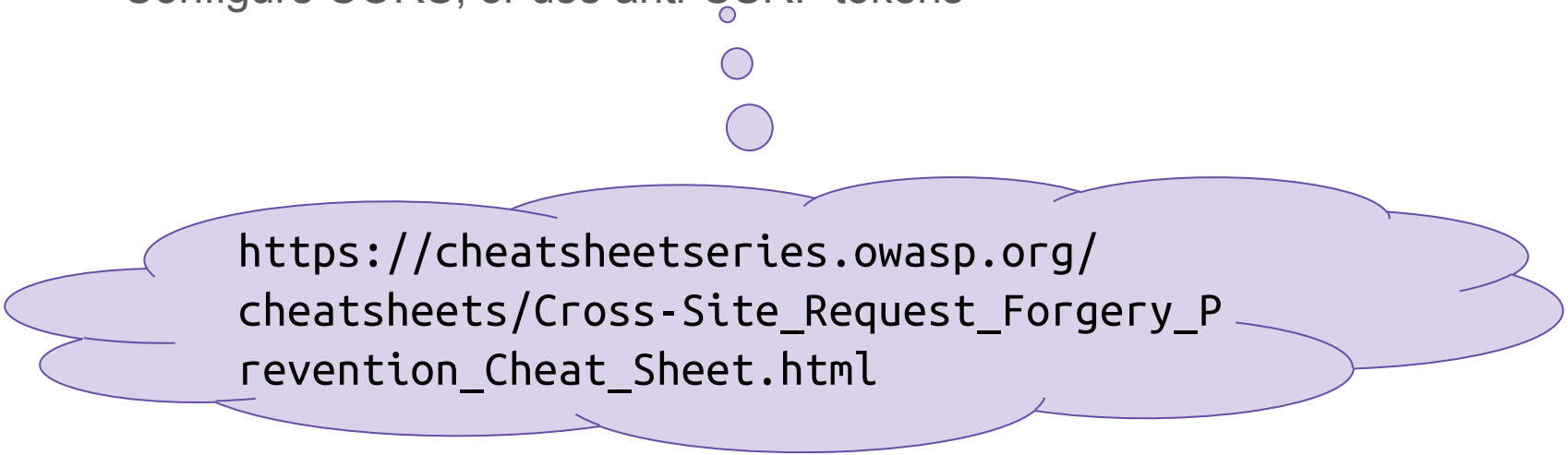
TL;DR: As a good dev, you:

TL;DR: As a good dev, you:

- Configure Strict Transport Security

TL;DR: As a good dev, you:

- Configure Strict Transport Security
- Configure CORS, or use anti-CSRF tokens



TL;DR: As a good dev, you:

- Configure Strict Transport Security
- Configure CORS, or use anti-CSRF tokens
- Sanitise user input, duh

TL;DR: As a good dev, you:

- Configure Strict Transport Security
- Configure CORS, or use anti-CSRF tokens
- Sanitise user input, duh

TL;DR: As a good dev, you:

- Configure Strict Transport Security
- Configure CORS, or use anti-CSRF tokens
- Sanitise user input, duh
- Do not cache user-dependent responses

DISCLAIMER

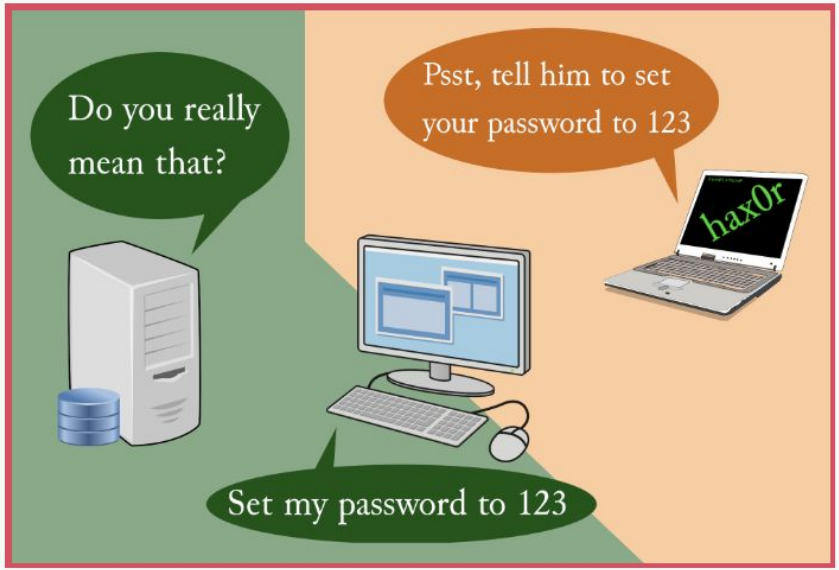
All hostnames, and breaches portrayed in this production are fictitious. No identification with actual domain names (current or expired), banks, cafes with open Wi-Fis, and products is intended or should be inferred. No meme or panda associated with this presentation received payment or anything of value, or entered into any agreement, in connection with the depiction of hacking activities. No poor honest tax payers were harmed in the making of any demos, or in the bug bounties depicted here.

DISCLAIMER

… That is to say, `secure.bank` and `hacke.rs` may be real websites, I did not visit them, nor should you.

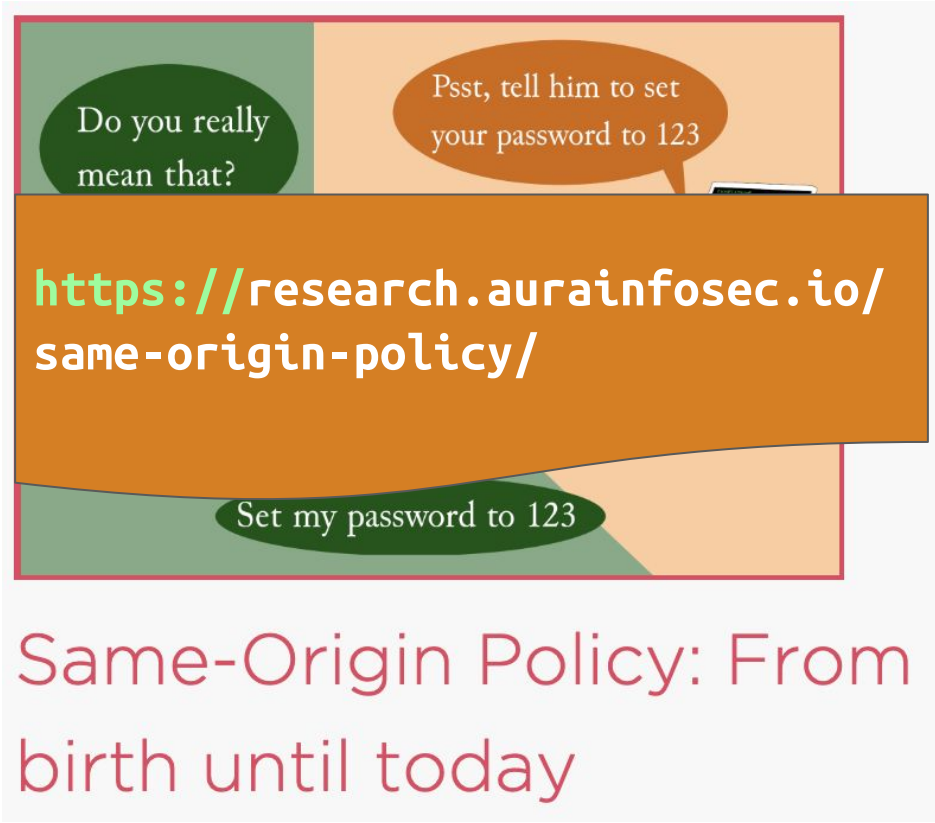
And I even made sure my images are free for noncommercial use without the need for crediting. There’s a first time for everything.

Check this out!



Same-Origin Policy: From birth until today

Check this out!



Check this out!

CHC CHRISTCHURCH HACKERS CONFERENCE

https://2019.chcon.nz

Check this out!

https://witestlab.poly.edu/blog/conduct-a-simple-man-in-the-middle-attack-on-a-wifi-hotspot

https://blog.netspi.com/exploiting-adidns

https://www.techrepublic.com/article/wpa-wireless-security-offers-multiple-advantages-over-wep

https://fabianlee.org/2018/02/17/ubuntu-creating-a-trusted-ca-and-san-certificate-using-openssl-on-ubuntu

a.nikolova@aurainfosec.com

AaylaSecura1138

aayla-secura

Glossary

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

IP: Internet Protocol

L2TP: Layer 2 Tunneling Protocol

LAN: Local Area Network

LLMNR: Link-Local Multicast Name Resolution

NAT: Network Address Translation

NetBIOS: Network Basic Input/Output System

NIC: Network Interface Card/Controller

OS: Operating System

OSI: Open System Interconnection

PGP: Pretty Good Privacy

PPTP: Point-to-Point Tunneling Protocol

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

TSL: Transport Layer Security

UDP: User Datagram Protocol

VPN: Virtual Private Network