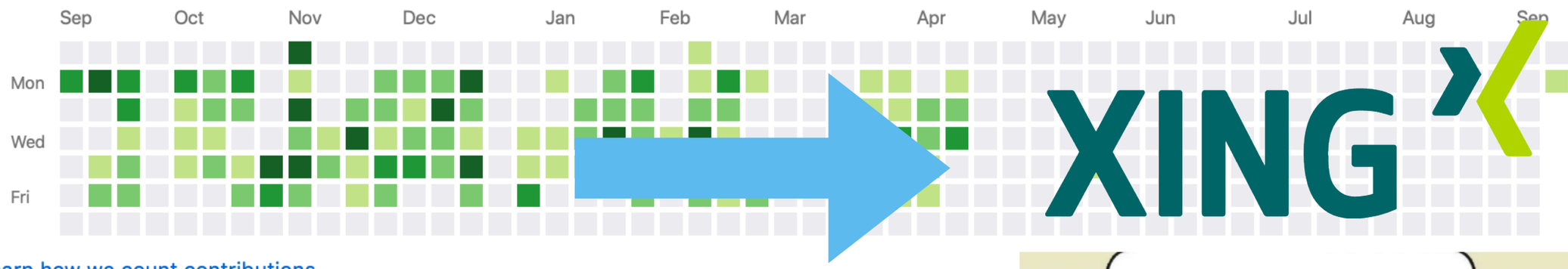
Bettercap Workshop

@zeitgeist_y2k

Who am I?

941 contributions in the last year

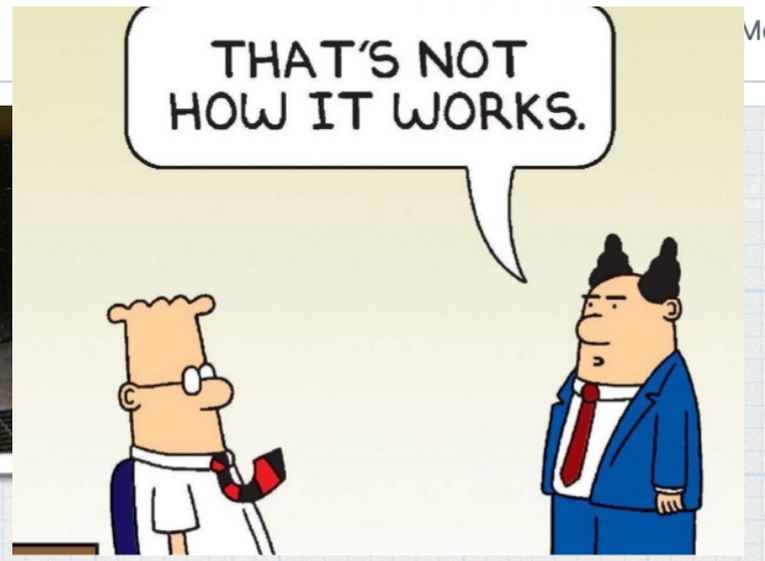
Contribution settings



XING

Learn how we count contributions.

More



@zeitgeist_y2k

Who are you?

- Why are you here?
- Why are you in this workshop?

Bettercap

- MITM attack framework
- Original idea: Ettercap from 2001
- Current version re-implemented 2018 in Go (after first version in Ruby)
- Ethernet, 802.11, BLE, HID hijacking…
- Simone Margaritelli
- @evilsocket

Theory Recap

OSI/ISO

Application Layer

Presentation Layer

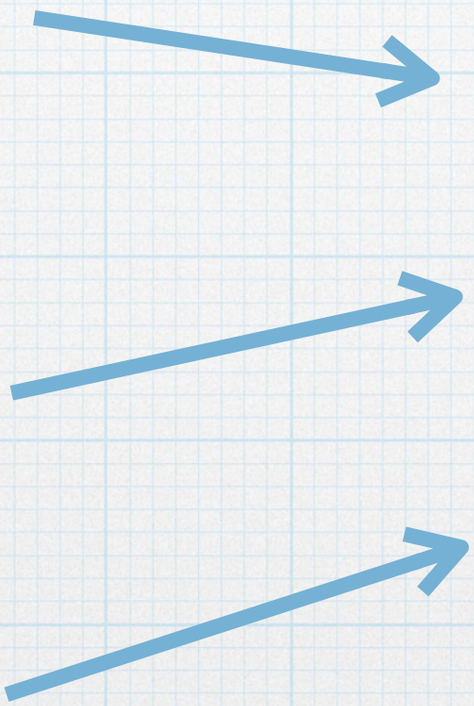
Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer



Ethernet

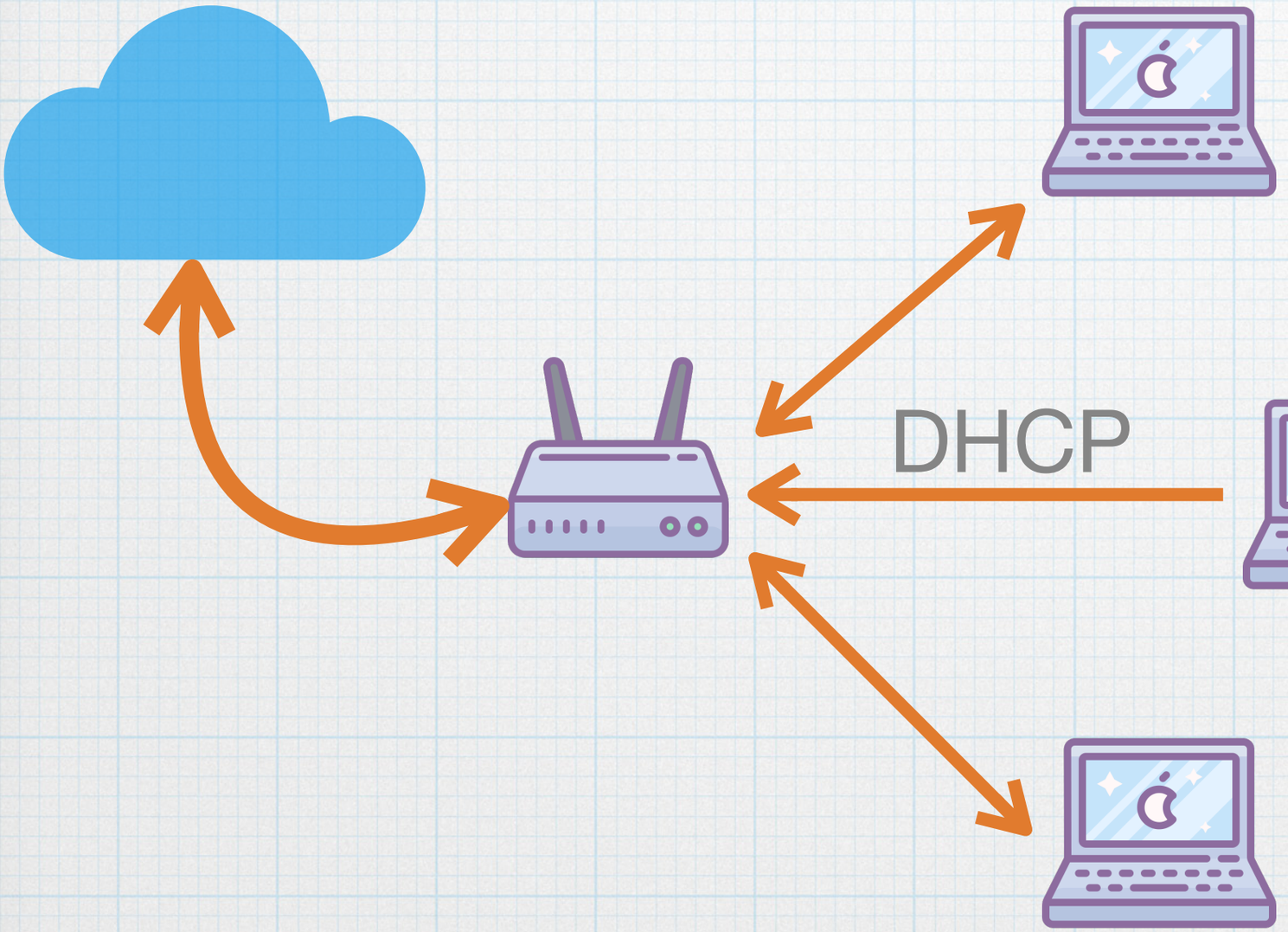
HTTP | SMTP | …

TCP / UDP

IP

Ethernet

Ethernet Networks



- No IP address
- No DNS
- No default route

MAC address

OSI/ISO

```
Christophs-MacBook-Pro:~ ceicke$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f4:5c:89:b4:10:23
        inet6 fe80::1c1b:1cda:b51a:5085%en0 prefixlen 64 secured scopeid 0x5
        inet 192.168.0.124 netmask 0xffffff00 broadcast 192.168.0.255
        inet6 2a04:4540:6b05:9f01:8dc:524:dcb7:2c70 prefixlen 64 autoconf secured
        inet6 2a04:4540:6b05:9f01:c0d:88e:d9f6:1e77 prefixlen 64 autoconf temporary
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Data Link Layer

Physical Layer

IEEE 802.3 (Ethernet)

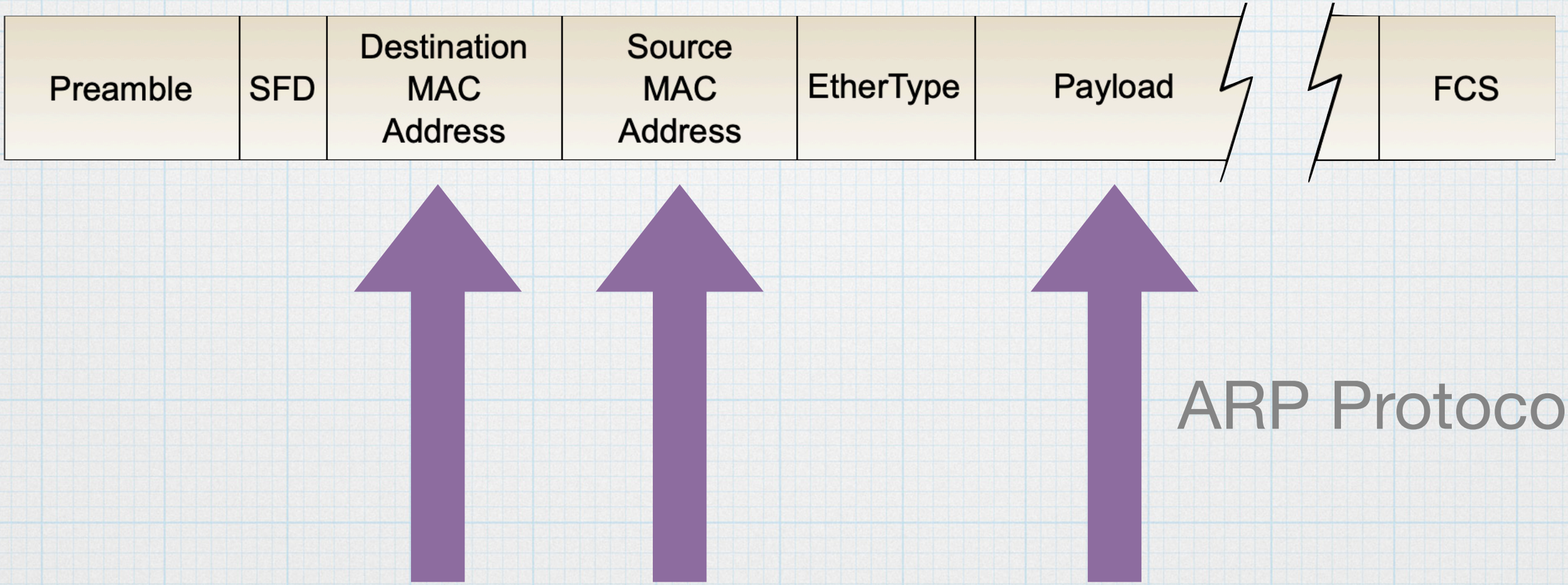
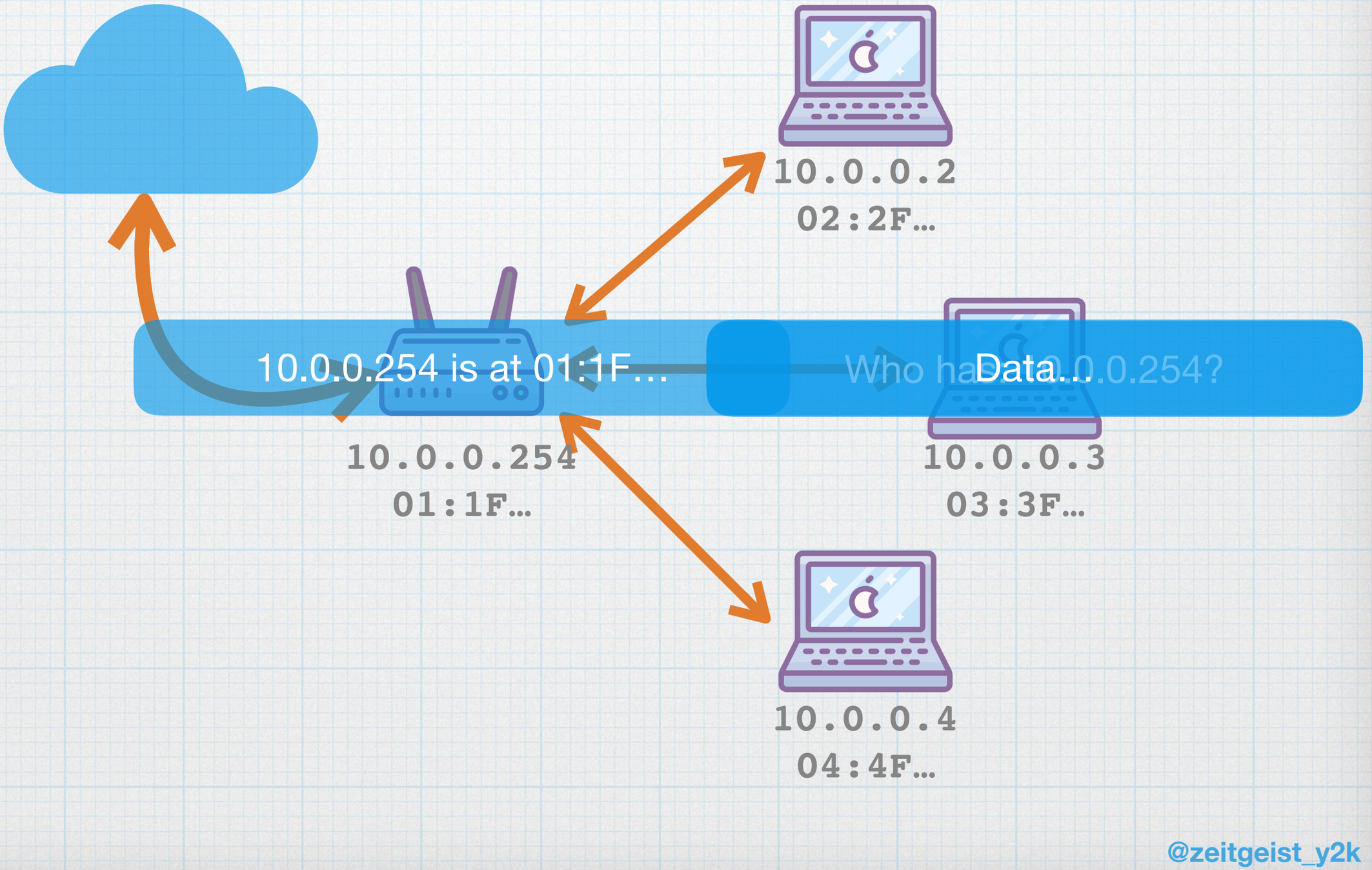
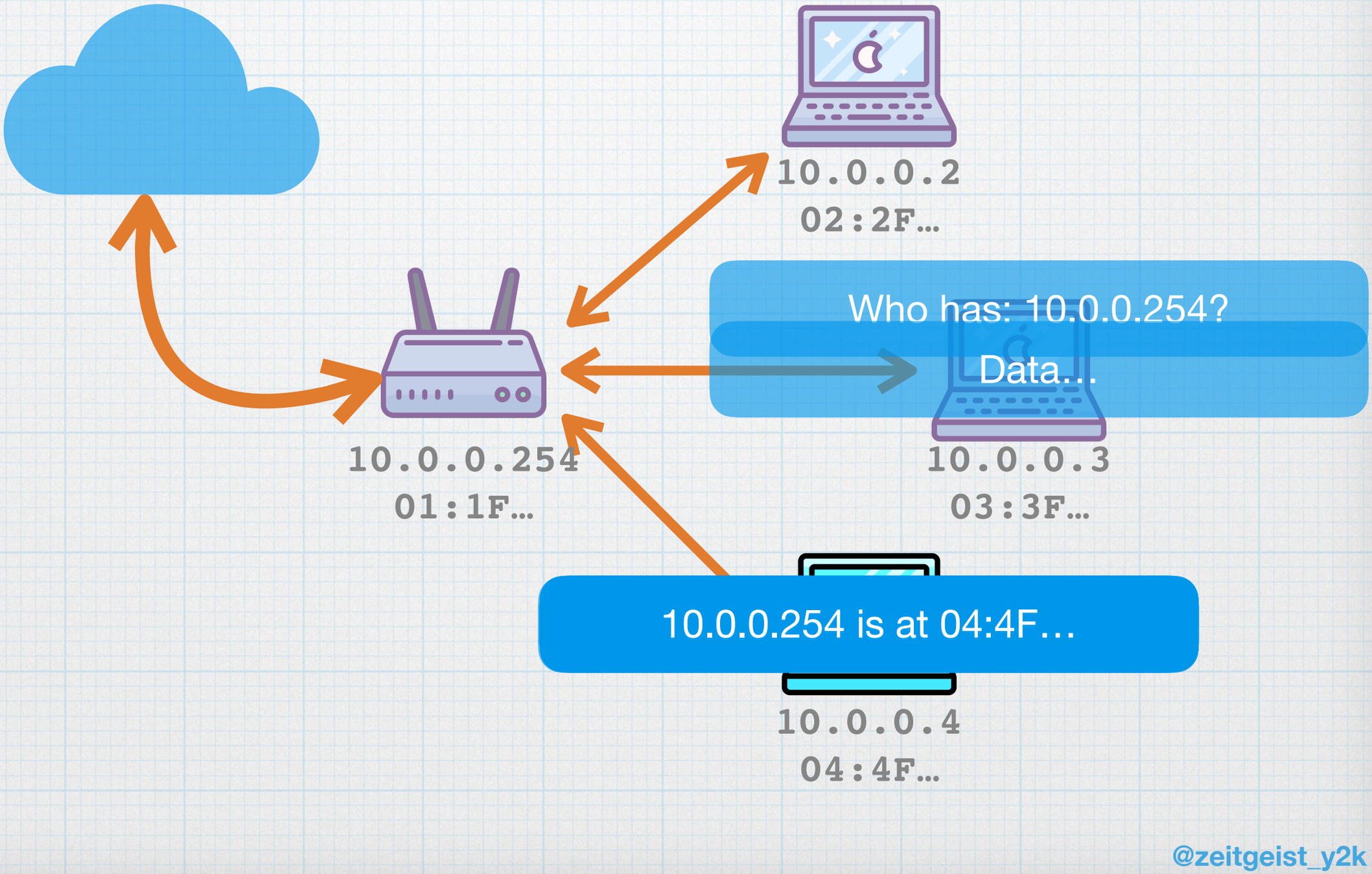


Image: Self-made [Public domain] via Wikimedia Commons

ARP
(Address Resolution Protocol)



ARP Spoofing



Installation

- Go >= 1.8
- libpcap-dev
- libnetfilter-queue-dev

Installation

```
$ sudo apt-get install libpcap-dev libnetfilter-queue-dev
```

```
$ go get github.com/bettercap/bettercap
```

```
$ sudo bettercap
```

Basic Usage

```
>> help
```

```
>> help arp.spoof
```

```
>> arp.spoof on
```

```
>> arp.spoof off
```

```
>> get arp.spoof.internal
```

```
>> set arp.spoof.internal true
```

Demo

Thanks!

https://github.com/ceicke/bettercap-elbsides

@zeitgeist_y2k