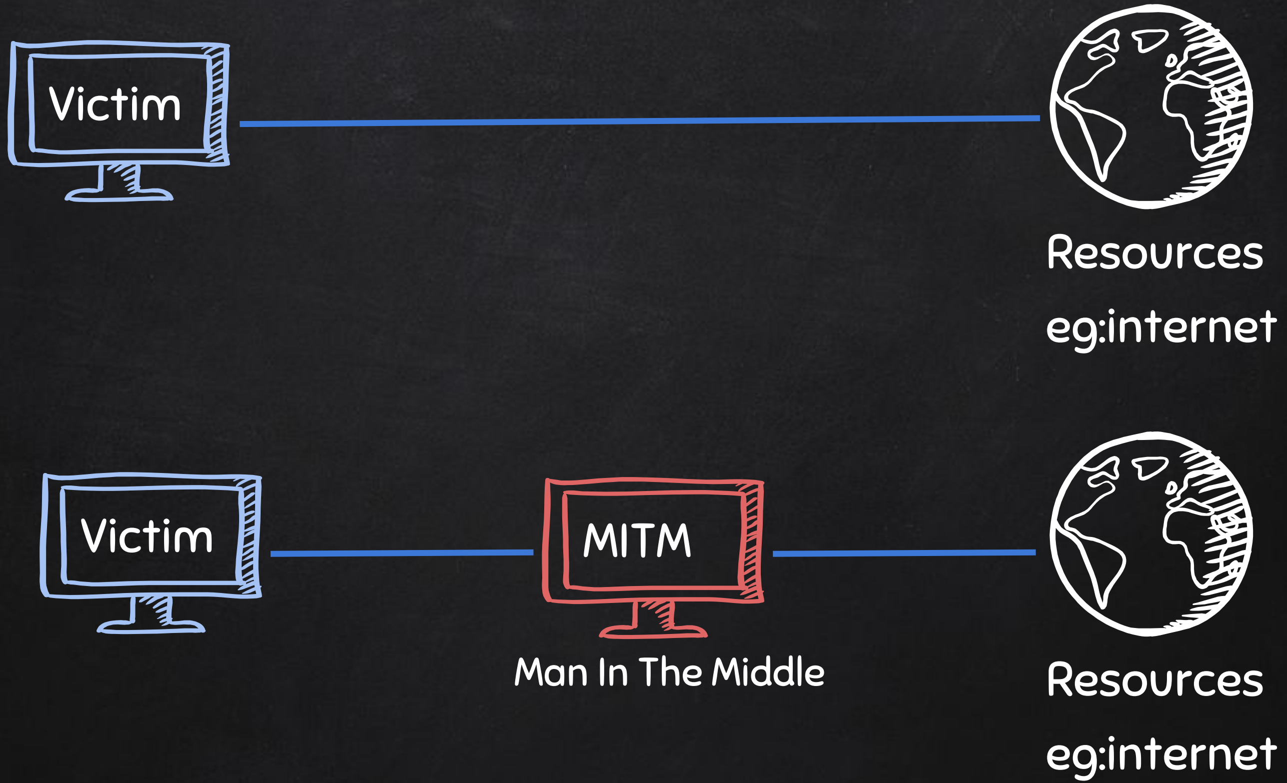
Network Mapping

Nmap / Zenmap

- HUGE security scanner.
- From an IP/IP range it can discover:
    - Open ports.
    - Running services.
    - Operating system.
    - Connected clients.
    - + more

MITM Attacks

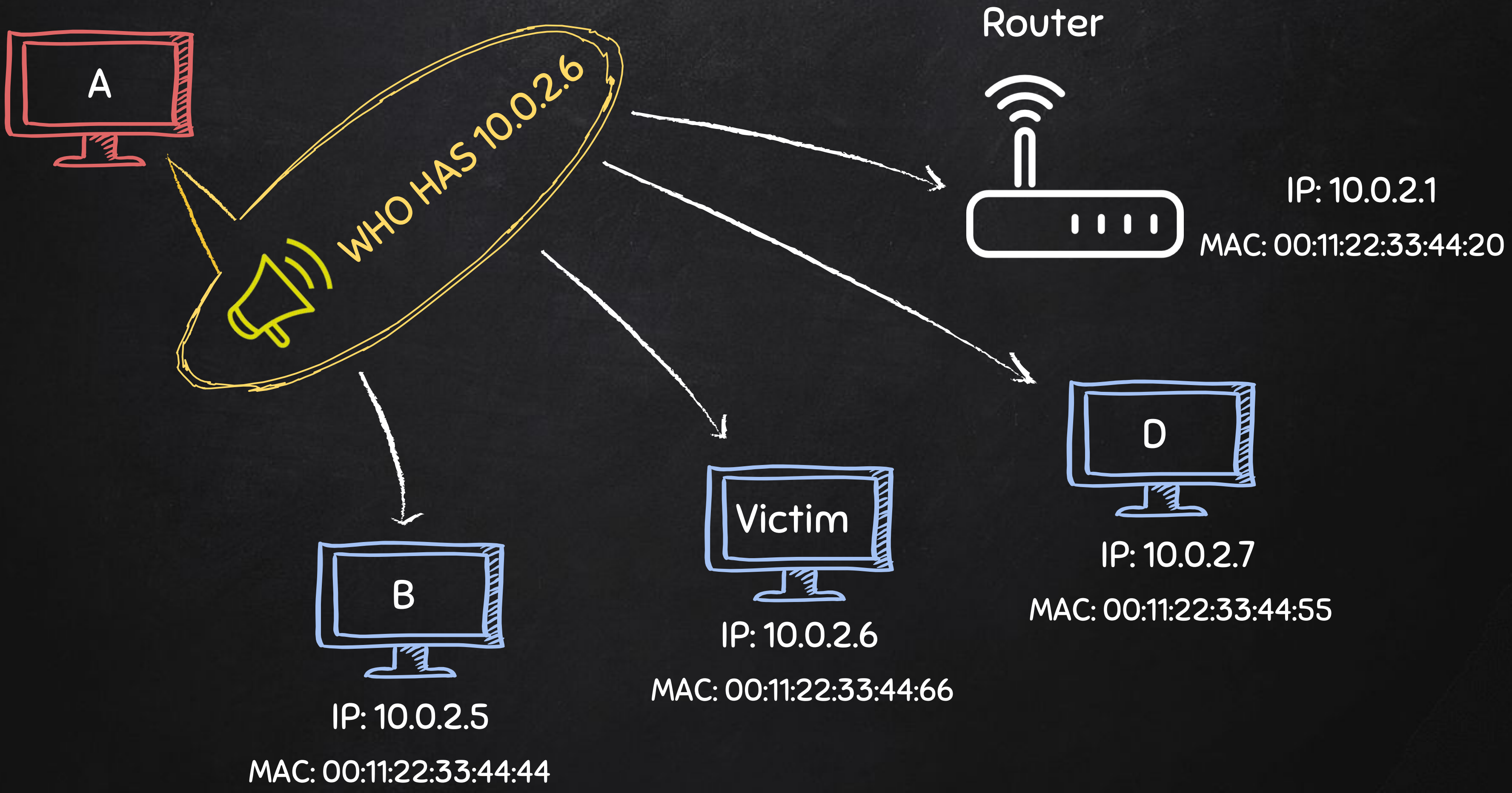


Address Resolution Protocol

(ARP)

→ Simple protocol used to map IP Address of a machine to its MAC address.

ARP Request



A

WHO HAS 10.0.2.6

Router

IP: 10.0.2.1

MAC: 00:11:22:33:44:20

B

IP: 10.0.2.5

MAC: 00:11:22:33:44:44

Victim

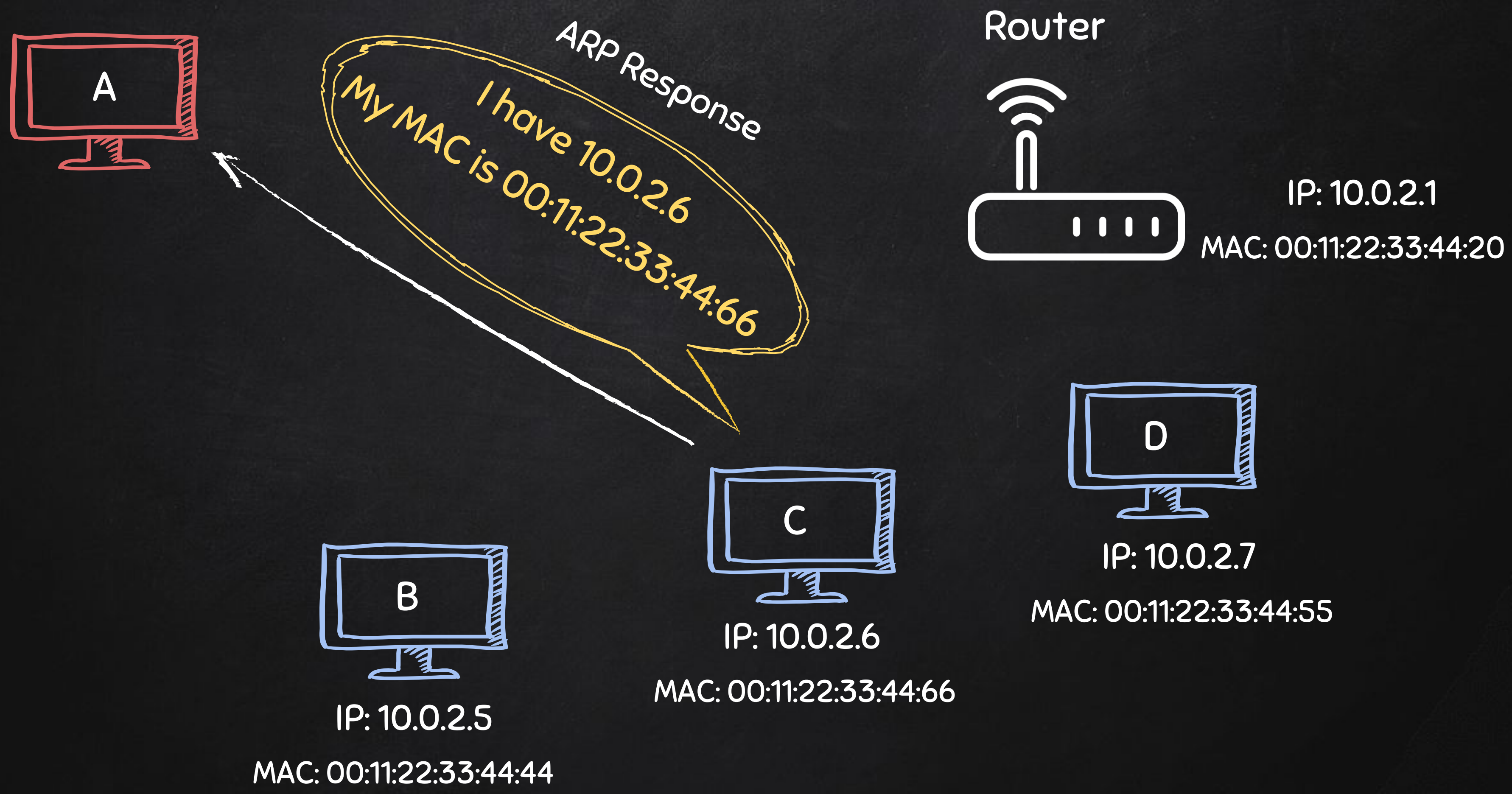
IP: 10.0.2.6

MAC: 00:11:22:33:44:66

D

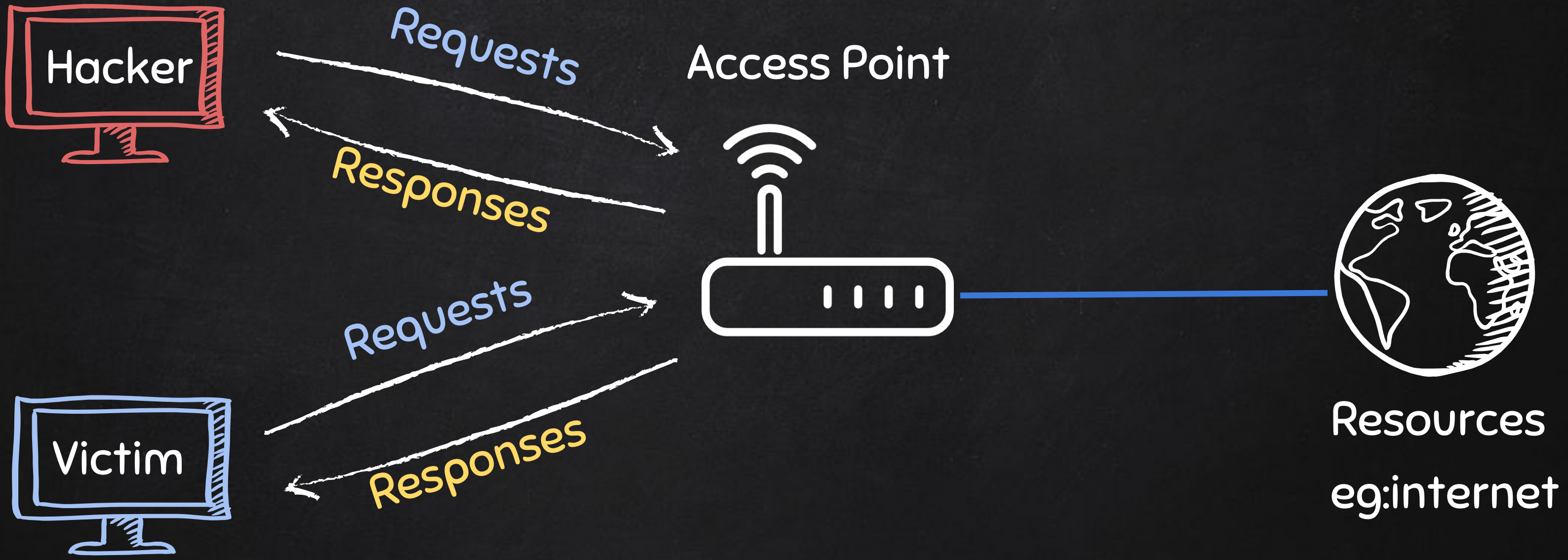
IP: 10.0.2.7

MAC: 00:11:22:33:44:55



A
ARP Response
I have 10.0.2.6
My MAC is 00:11:22:33:44:66
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55
C
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44

Typical Network



Hacker

Requests

Responses

Access Point

Requests

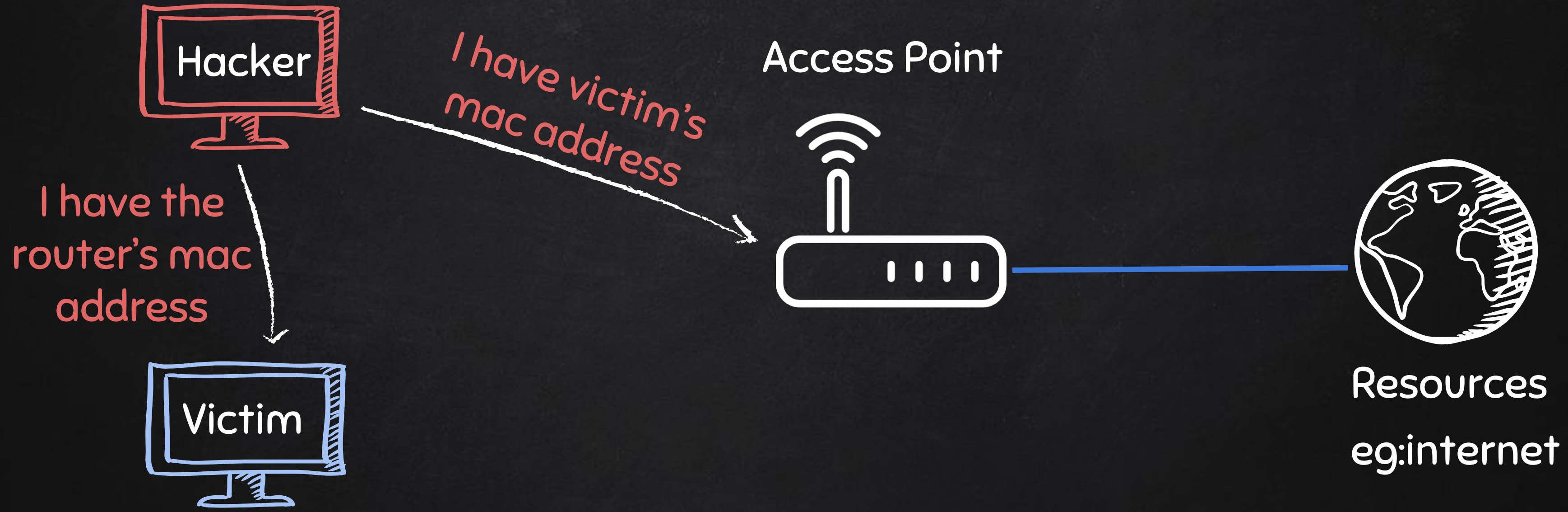
Responses

Victim

Resources

eg:internet

ARP Spoofing



Hacker

I have victim's mac address

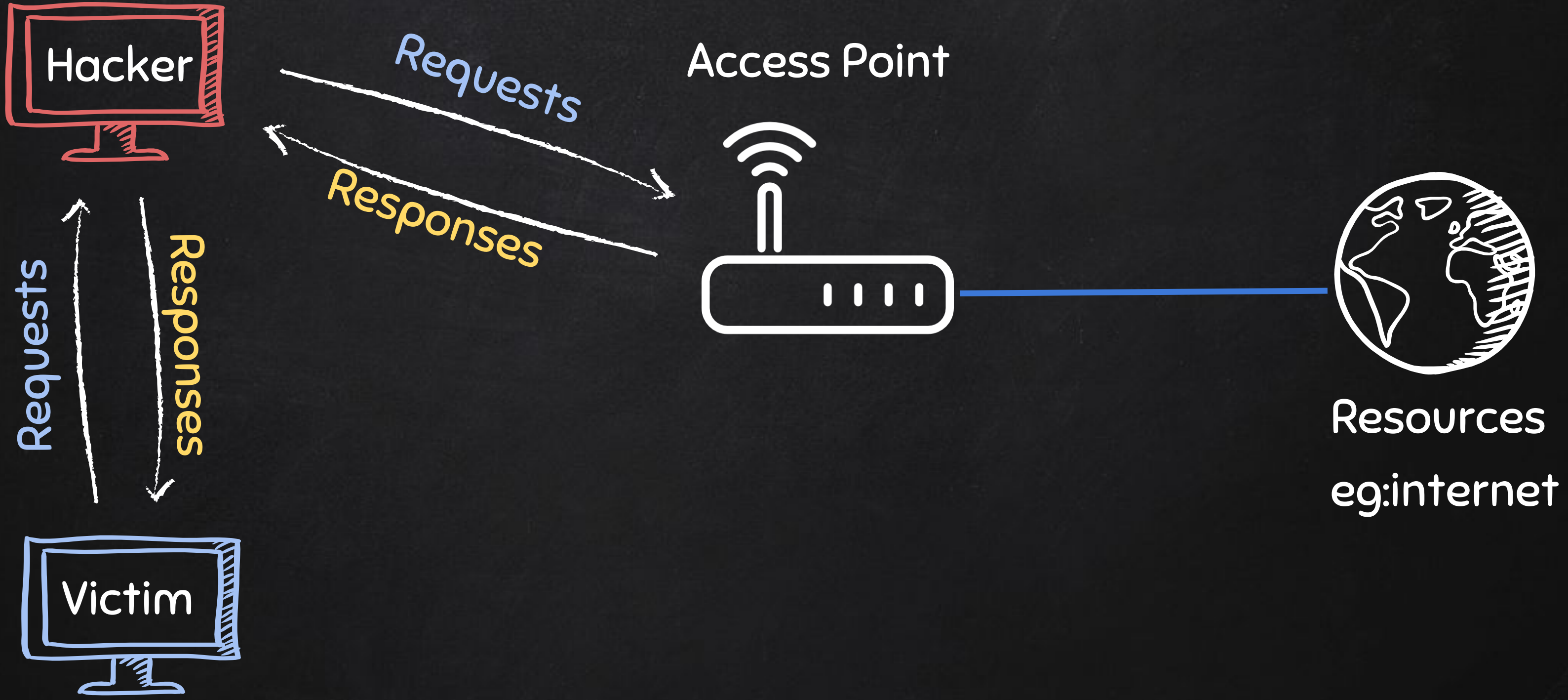
Access Point

I have the router's mac address

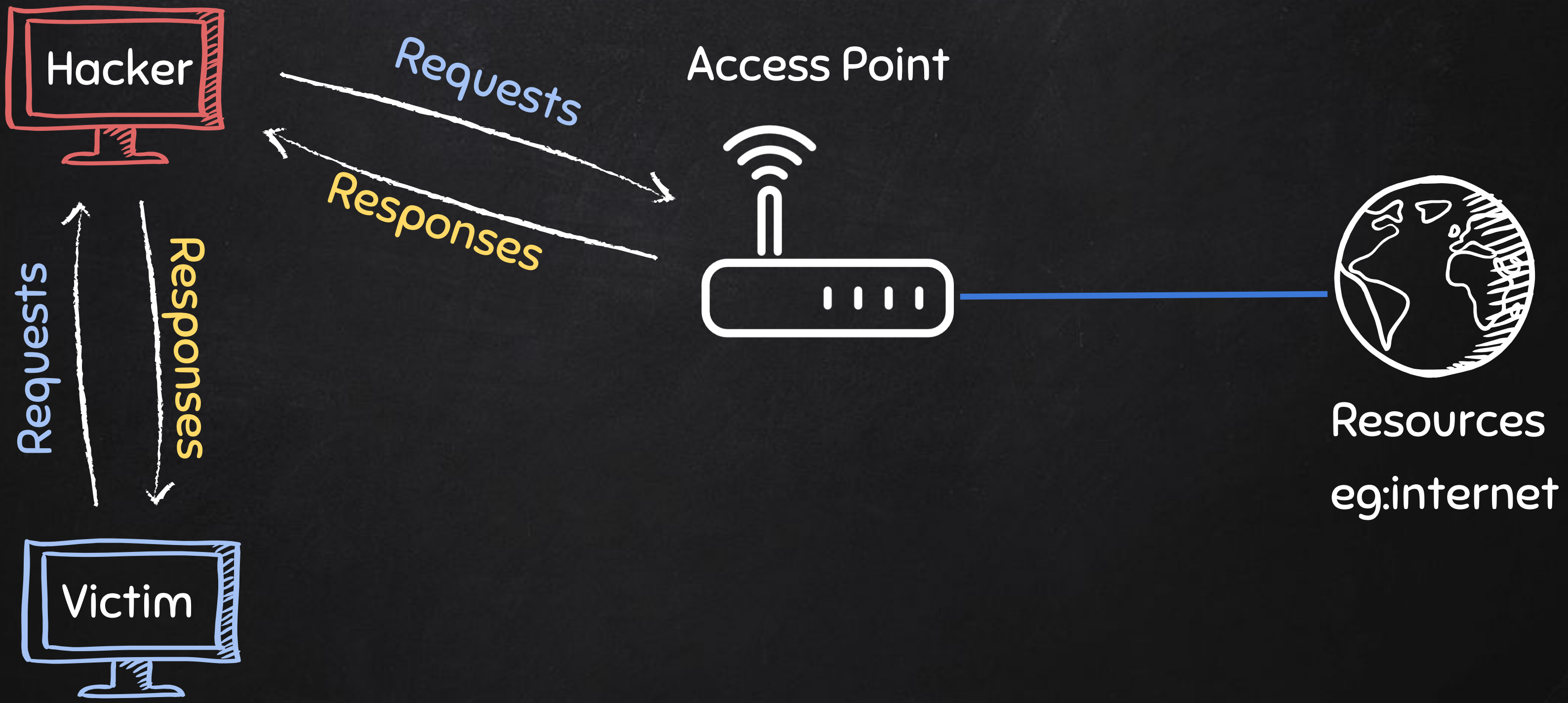
Victim

Resources eg:internet

ARP Spoofing



ARP Spoofing



ARP Spoofing

Using arpspoof

- arpspoof tool to run arp spoofing attacks.
- Simple and reliable.
- Ported to most operating systems including Android and iOS.
- Usage is always the same.

use:

```
arpspoof -i [interface] -t [clientIP] [gatewayIP]
arpspoof -i [interface] -t [gatewayIP] [clientIP]
```

ARP Spoofing Using MITMf

- Framework to run MITM attacks.
- Can be used to :
  - ○ ARP Spoof targets (redirect the flow of packets)
  - ○ Sniff data (urls, username passwords).
  - ○ Bypass HTTPS.
  - ○ Redirect domain requests (DNS Spoofing).
  - ○ Inject code in loaded pages.
  - ○ And more!

use:

```
mitmf --arp --spoof -i [interface] --target [clientIP] --gateway [gatewayIP]
```

HTTPS

Problem:

- Data in HTTP is sent as plain text.
- A MITM can read and edit requests and responses.

→ not secure

Solution:

- Use HTTPS.
- HTTPS is an adaptation of HTTP.
- Encrypt HTTP using TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

Bypassing HTTPS

Problem:

- Most websites use HTTPS

→ Sniffed data will be encrypted.

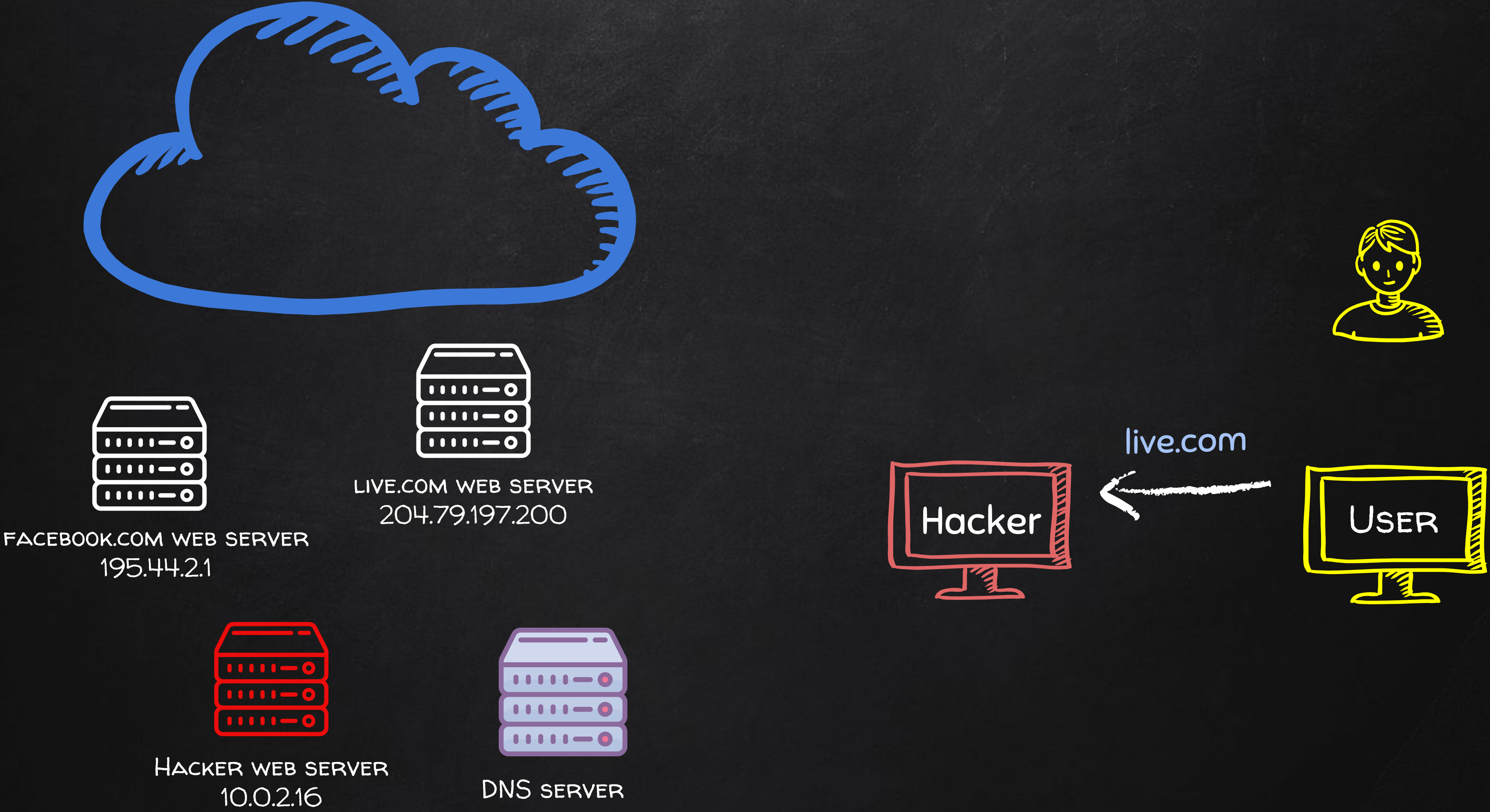
Solution:

- Downgrade HTTPS to HTTP.

DNS Spoofing

- DNS → Domain Name System.
- Translates domain names to IP addresses.
- Eg: links www.google.com to the IP of Google's server.

bing.com	A	204.79.197.200
facebook.com	A	195.44.2.1
zsecurity.org	A	104.27.153.174
……..etc		



FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200

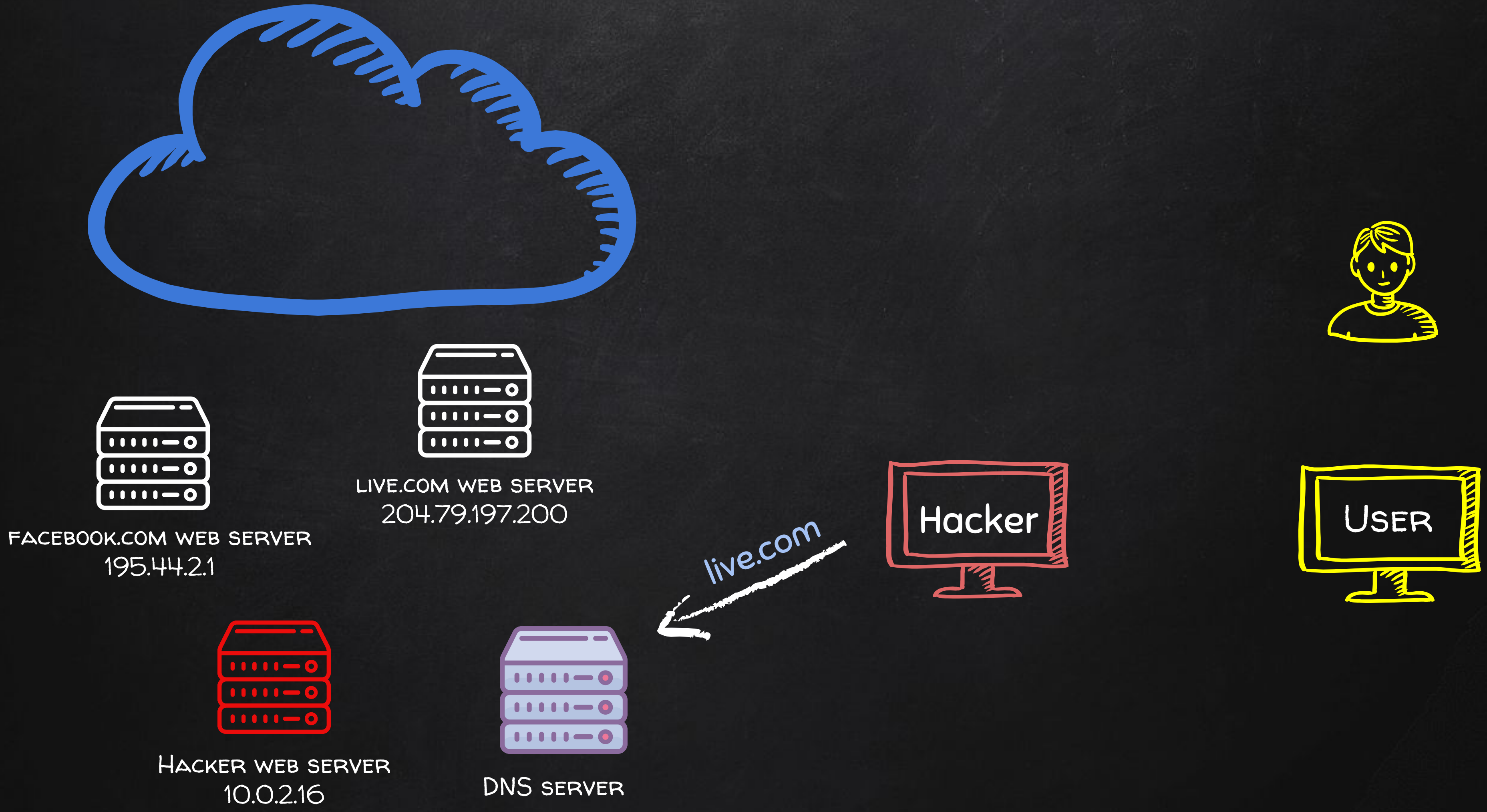
HACKER WEB SERVER
10.0.2.16

DNS SERVER

Hacker

live.com

USER

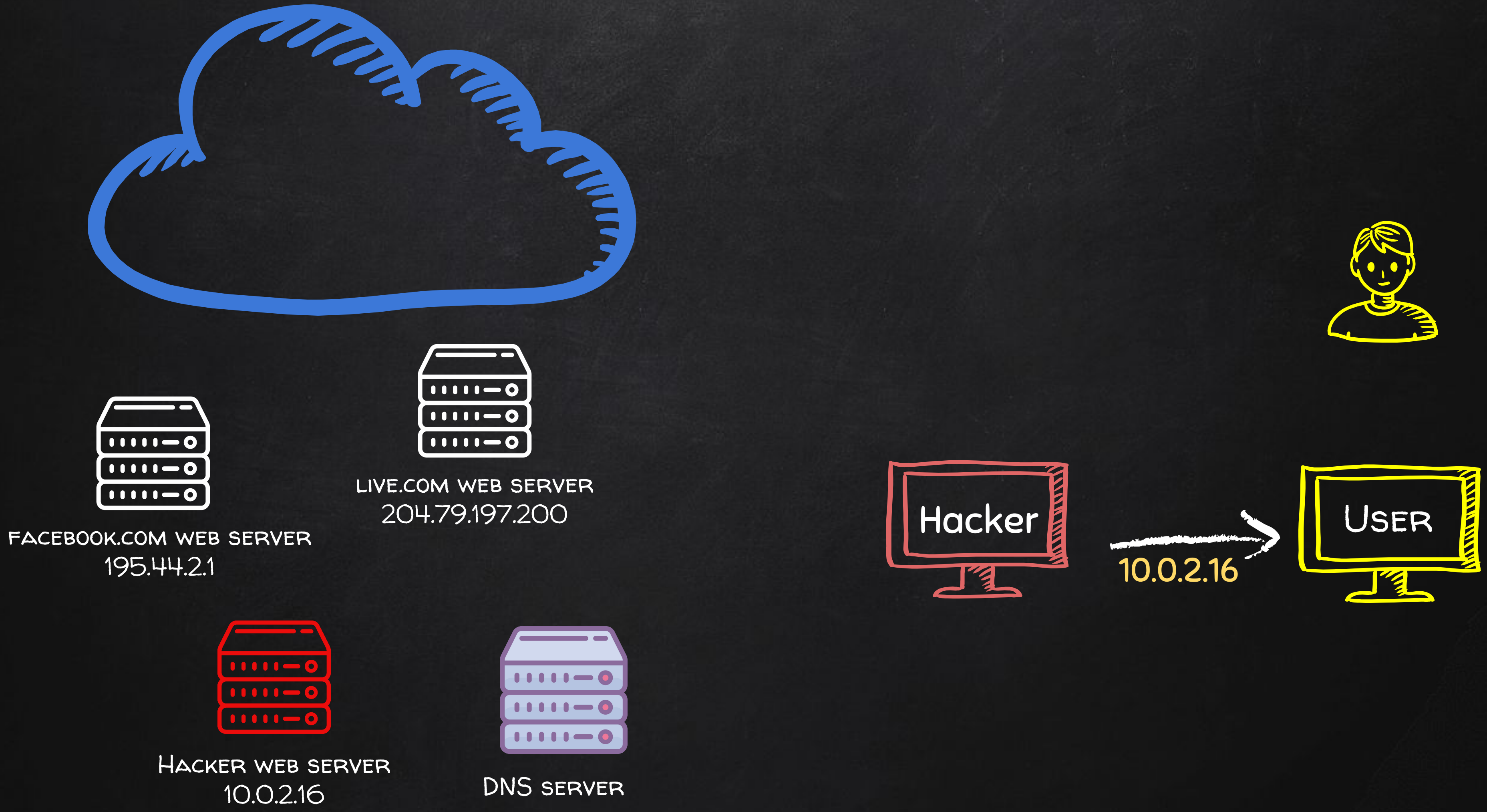


FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200

HACKER WEB SERVER
10.0.2.16

DNS SERVER



FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200

HACKER WEB SERVER
10.0.2.16

DNS SERVER

Hacker

10.0.2.16

USER

MITM

Code Injection

- Inject Javascript/HTML code.
- Code gets executed by the target browser

→ use the `--inject` plugin

Code can be

1. Stored in a file `--js-file` or `--html-file`
2. Stored online `--js-url` or `--html-url`
3. Supplied through the command line `--js-payload` or `--html-payload`

Creating a Fake Access Point Using Mana-Toolkit

- Tools run rogue access point attacks.
- It can:
  - Automatically configure and create fake AP.
  - Automatically sniff data.
  - Automatically bypass https.
  - ....etc

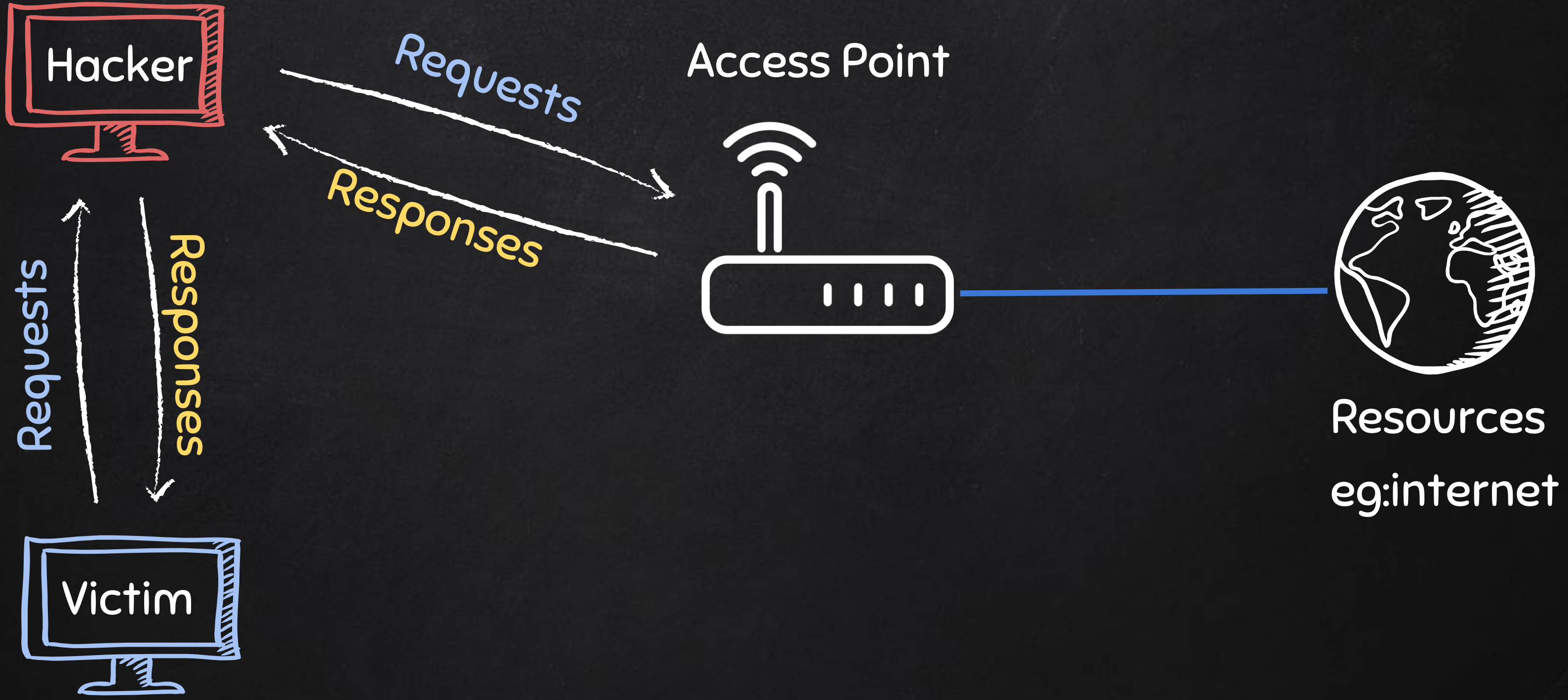
Creating a Fake Access Point Using Mana-Toolkit

- Tools run rogue access point attacks.
- It can:
  - Automatically configure and create fake AP.
  - Automatically sniff data.
  - Automatically bypass https.
  - ....etc

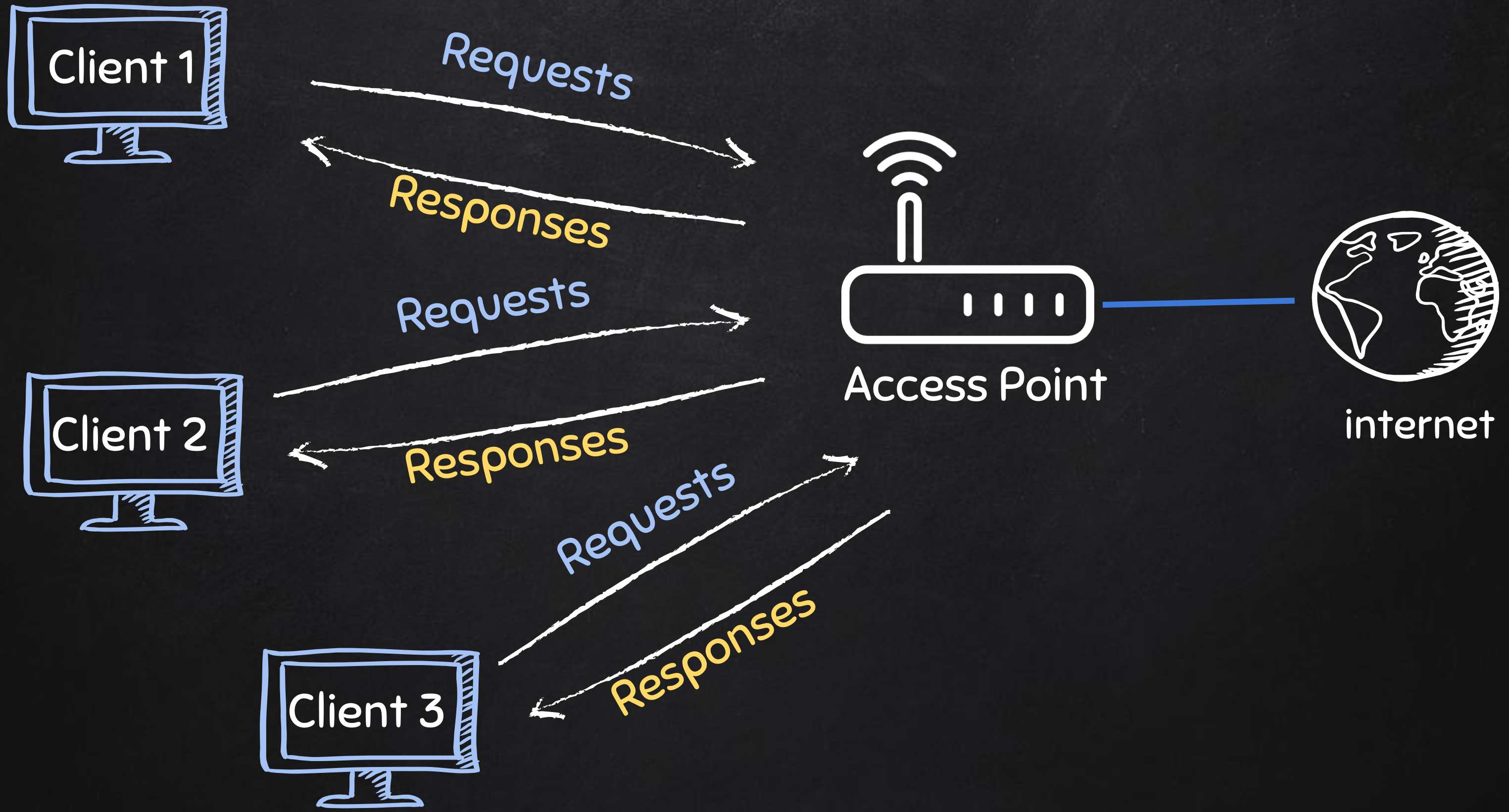
Mana has 3 main start scripts:

1. start-noupstream.sh – starts fake AP with no internet access.
2. start-nat-simple.sh – starts fake AP with internet access.
3. start-nat-full.sh – starts fake AP with internet access, and automatically starts sniffing data, bypass https.

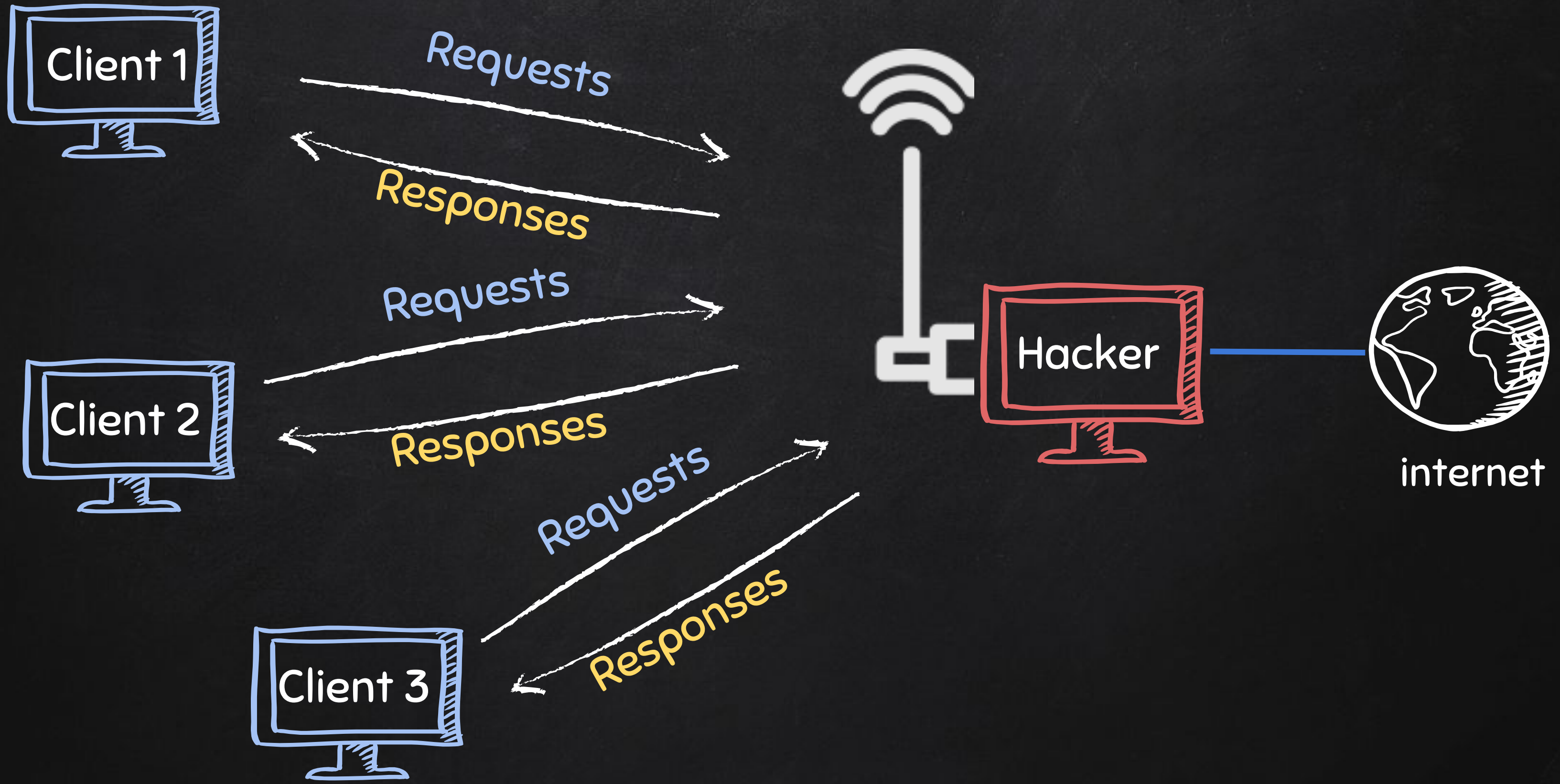
ARP Spoofing



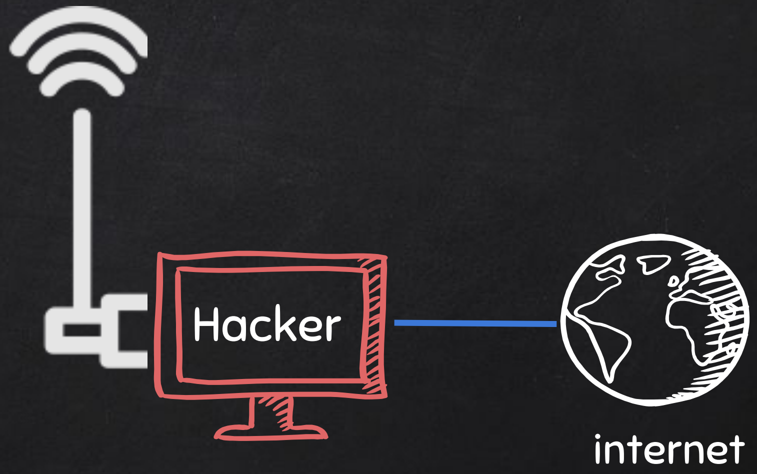
Typical Network



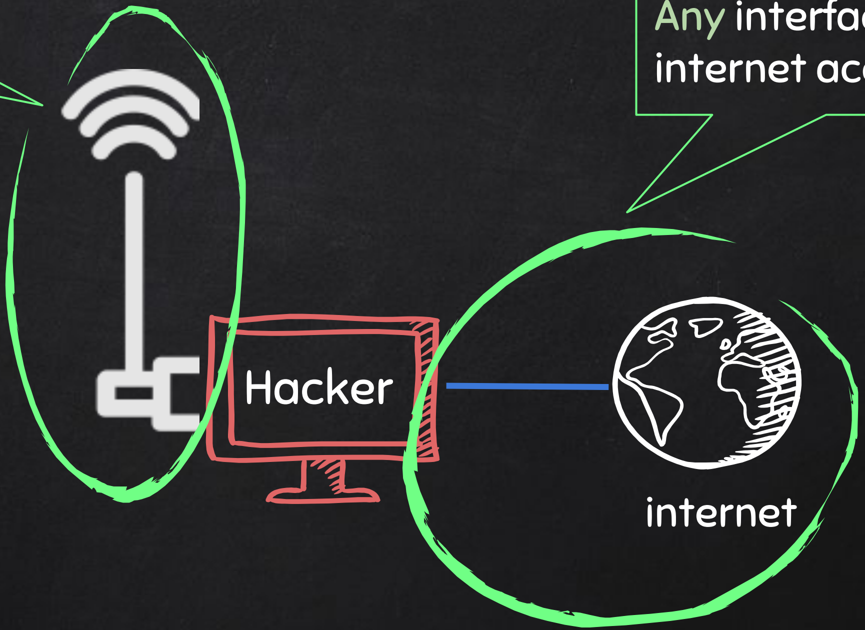
Creating a Fake Access Point



Creating a Fake Access Point



Creating a Fake Access Point



Wireless adapter that supports AP mode

Any interface with internet access