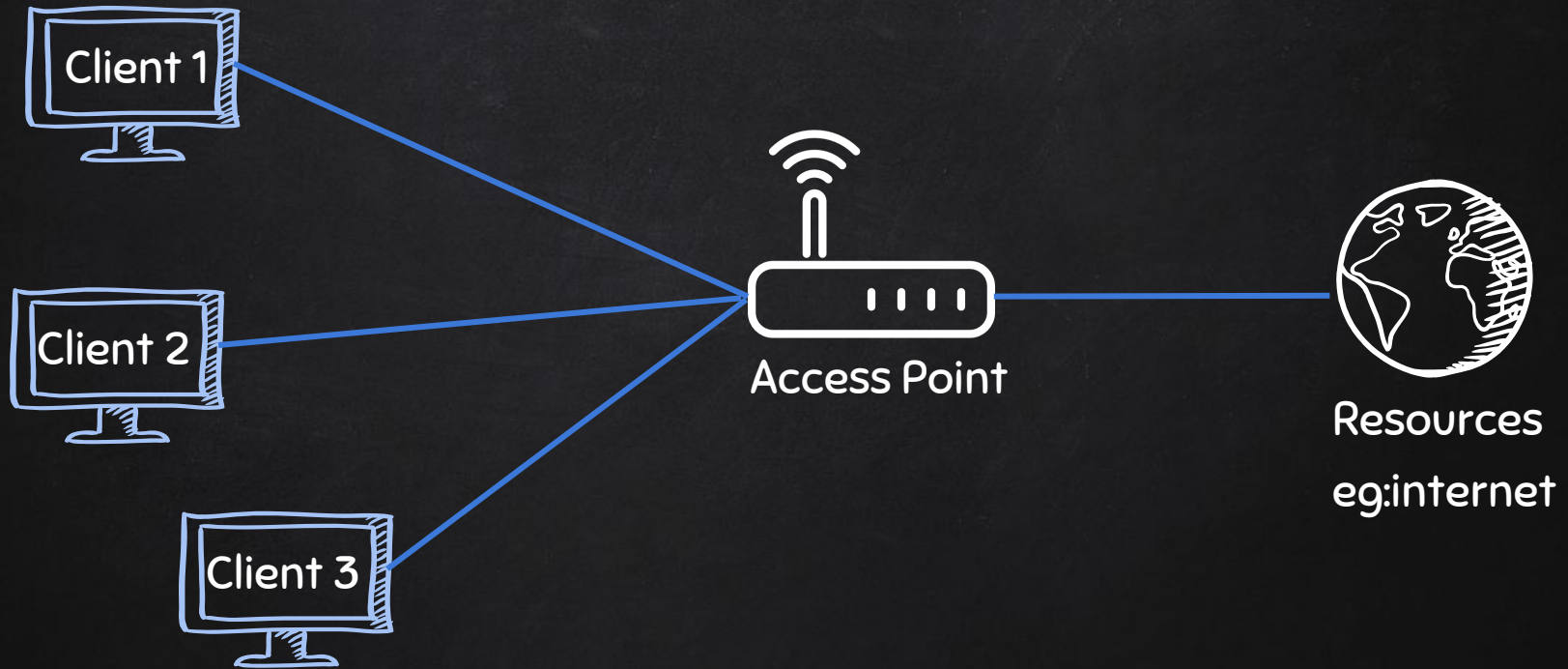


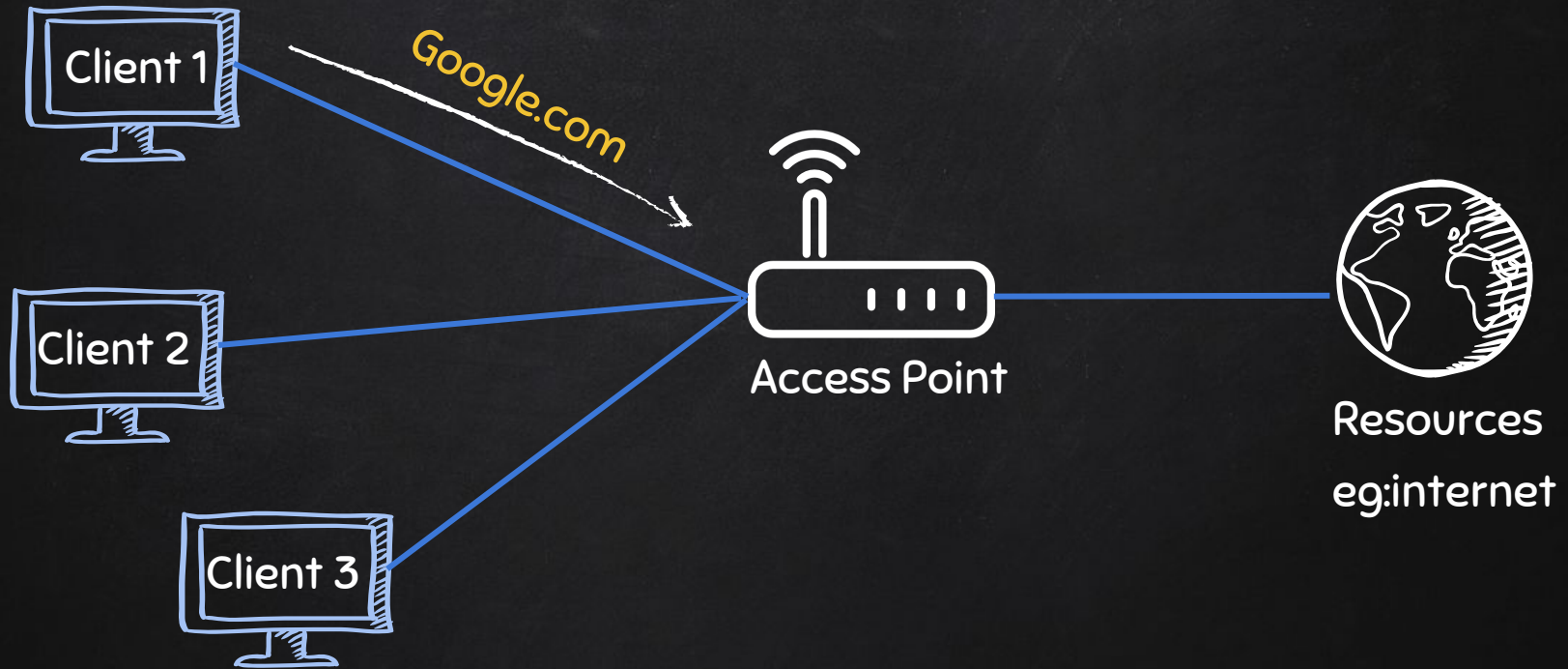
# TYPICAL NETWORK



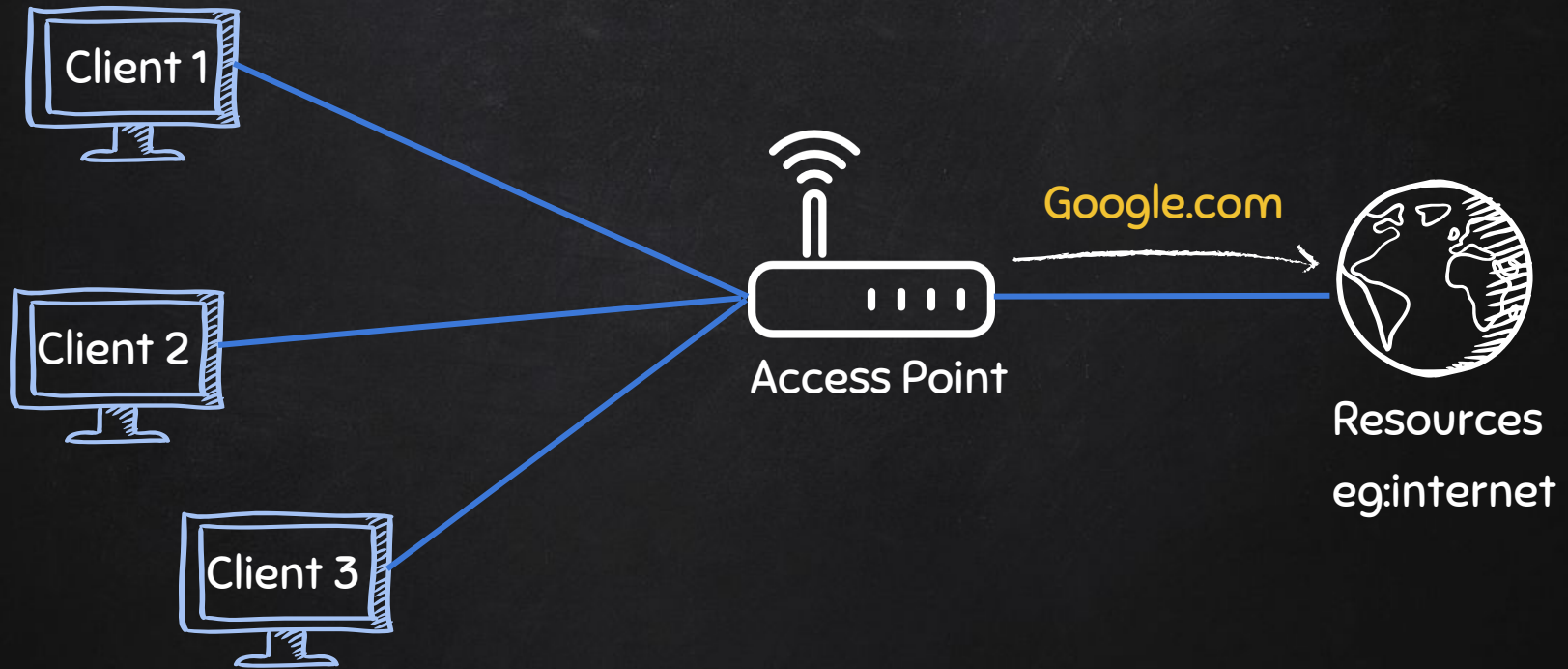
# TYPICAL NETWORK



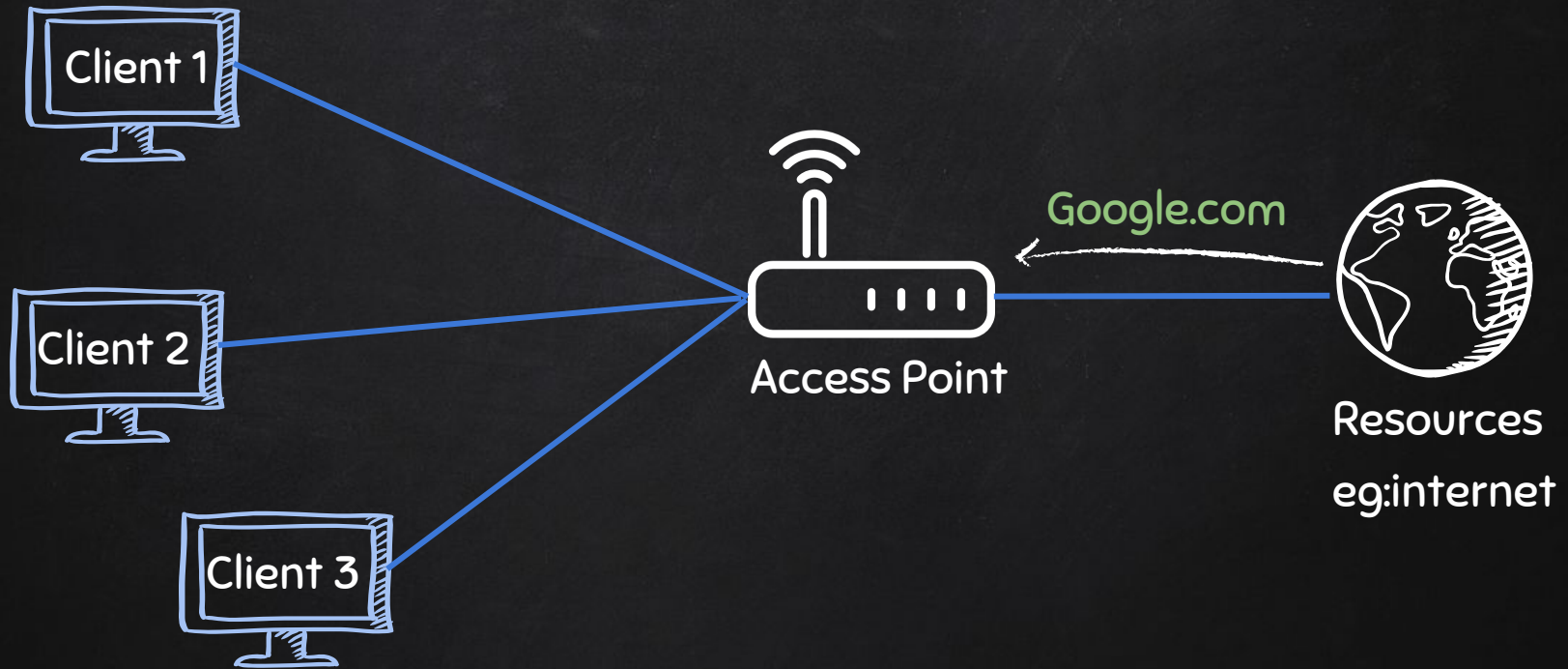
# TYPICAL NETWORK



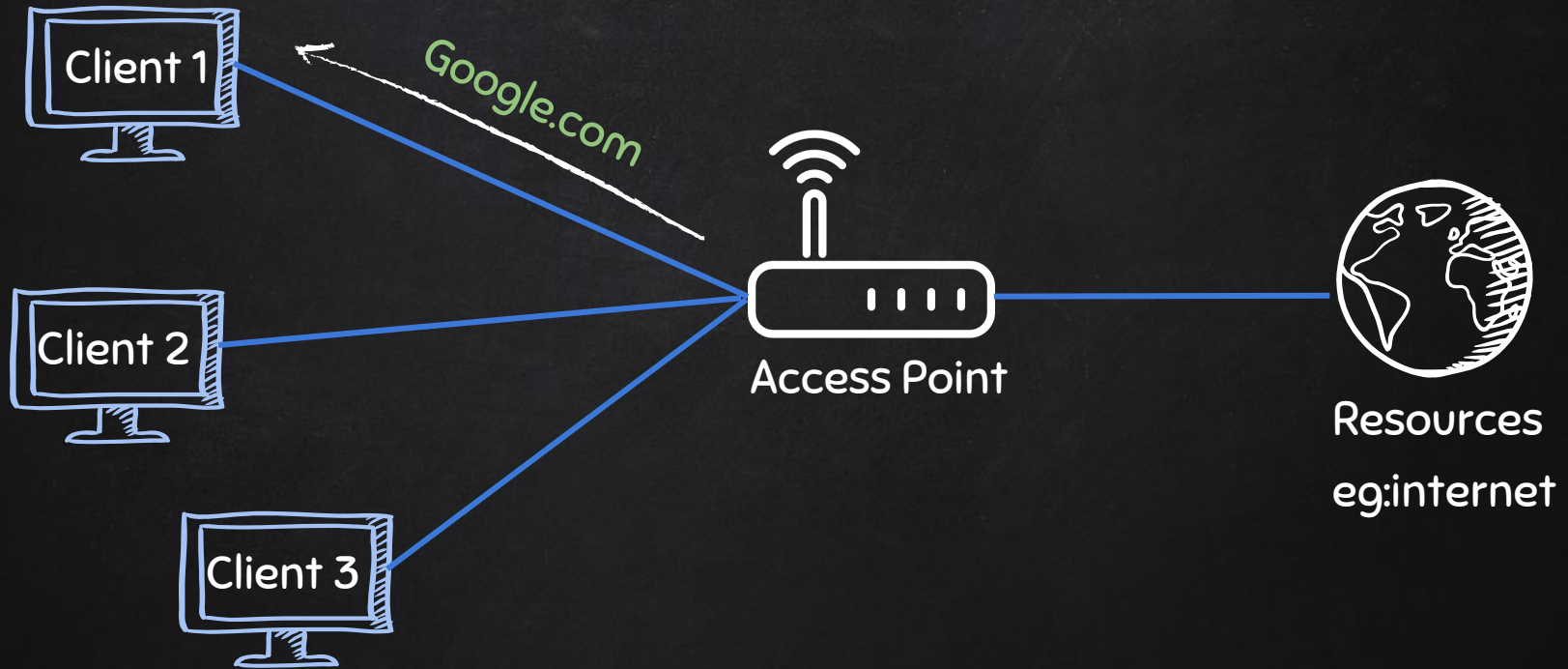
# TYPICAL NETWORK



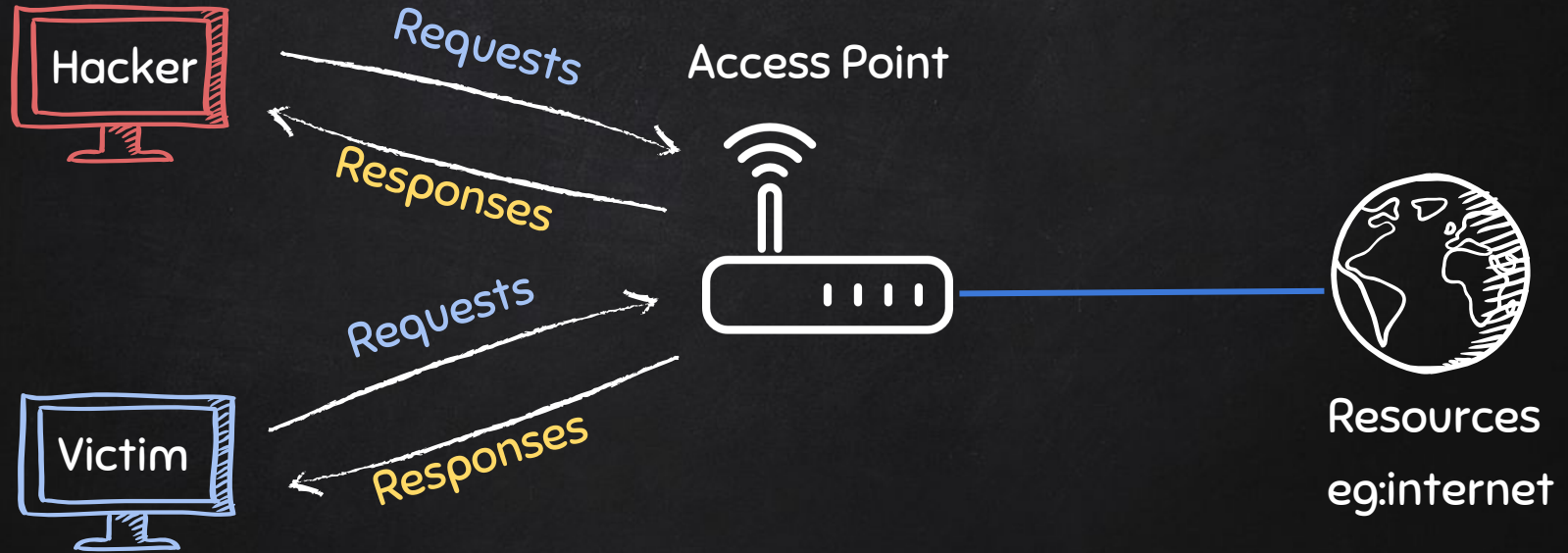
# TYPICAL NETWORK



# TYPICAL NETWORK



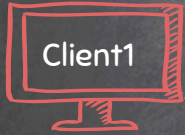
# TYPICAL NETWORK



## WHY CHANGE THE MAC ADDRESS?

1. Increase **anonymity**.
2. **Impersonate** other devices.
3. **Bypass** filters.

Source Mac: 00:11:11:11:11:11  
Destination Mac: 00:22:22:22:22:22



Client1



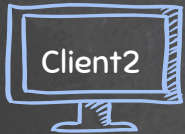
Access Point



Resources  
eg:internet

Mac = 00:11:11:11:11:11

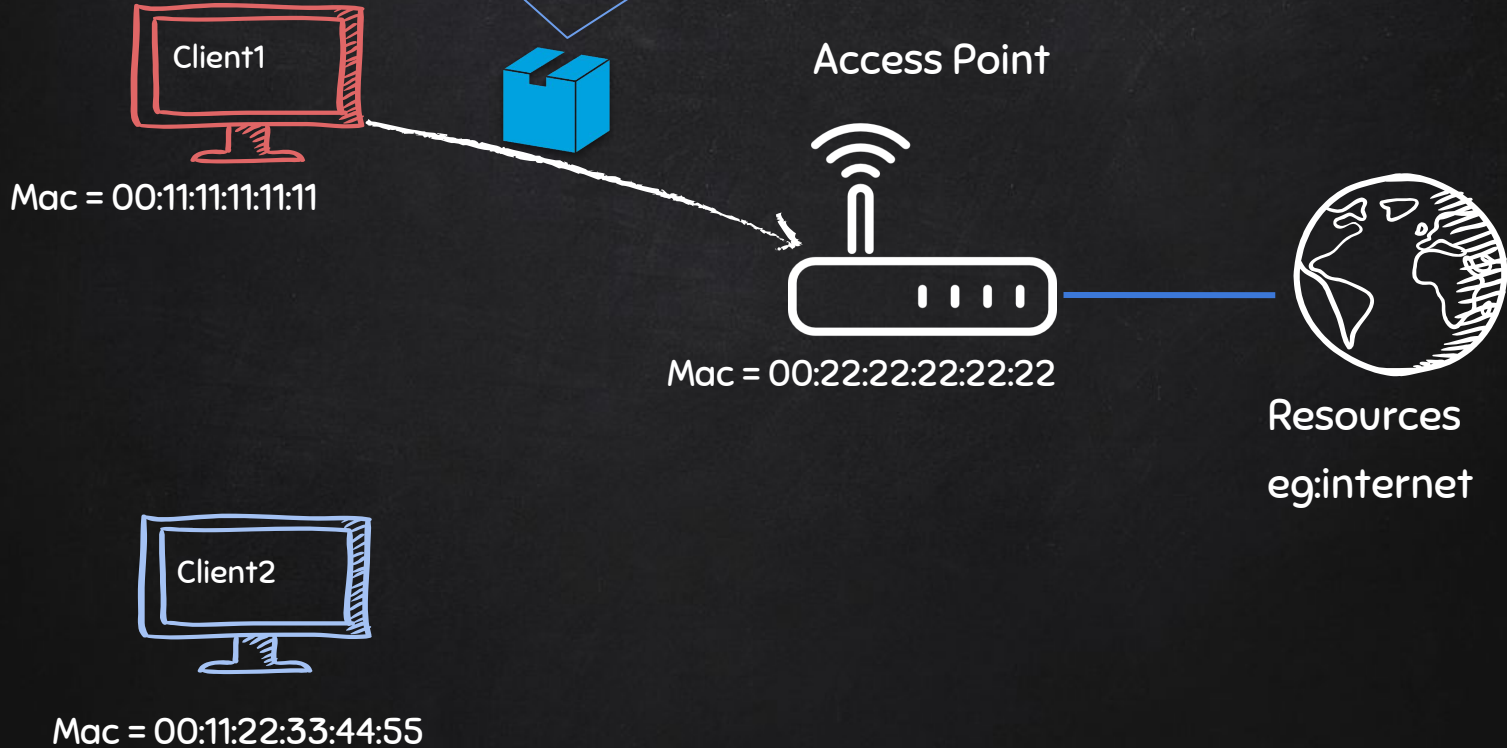
Mac = 00:22:22:22:22:22



Client2

Mac = 00:11:22:33:44:55

Source Mac: 00:11:11:11:11:11  
Destination Mac: 00:22:22:22:22:22



# PACKET SNIFFING

## USING AIRODUMP-NG

- Part of the aircrack-ng suit.
- Airodump-ng is a packet sniffer;
- Used to capture all packets within range.
- Display detailed info about networks around us.
- Connected clients ....etc

Use:

```
airodump-ng [MonitorModeInterface]
```



# PACKET SNIFFING

## USING AIRODUMP-NG

- Part of the aircrack-ng suit.
- Airodump-ng is a packet sniffer;
- Used to capture all packets within range.
- Display detailed info about networks around us.
- Connected clients ....etc

Use:

```
airodump-ng [MonitorModeInterface]
```



# DEAUTHENTICATION ATTACK



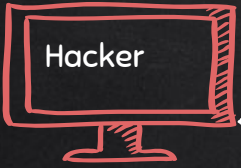
→ Disconnect **any** client from **any** network

- Works on encrypted networks (WEP, WPA & WPA2).
- No need to know the network key.
- No need to connect to the network.

Use:

```
aireplay-ng --deauth [#DeauthPackets] -a [NetworkMac] -c [TargetMac] [Interface]
```

Source Mac: 00:11:22:33:44:55  
Destination Mac: 00:22:22:22:22:22  
Message: I want to disconnect



Mac = 00:11:11:11:11:11



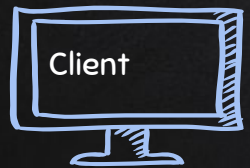
Access Point



Mac = 00:22:22:22:22:22



Resources  
eg: internet



Mac = 00:11:22:33:44:55

