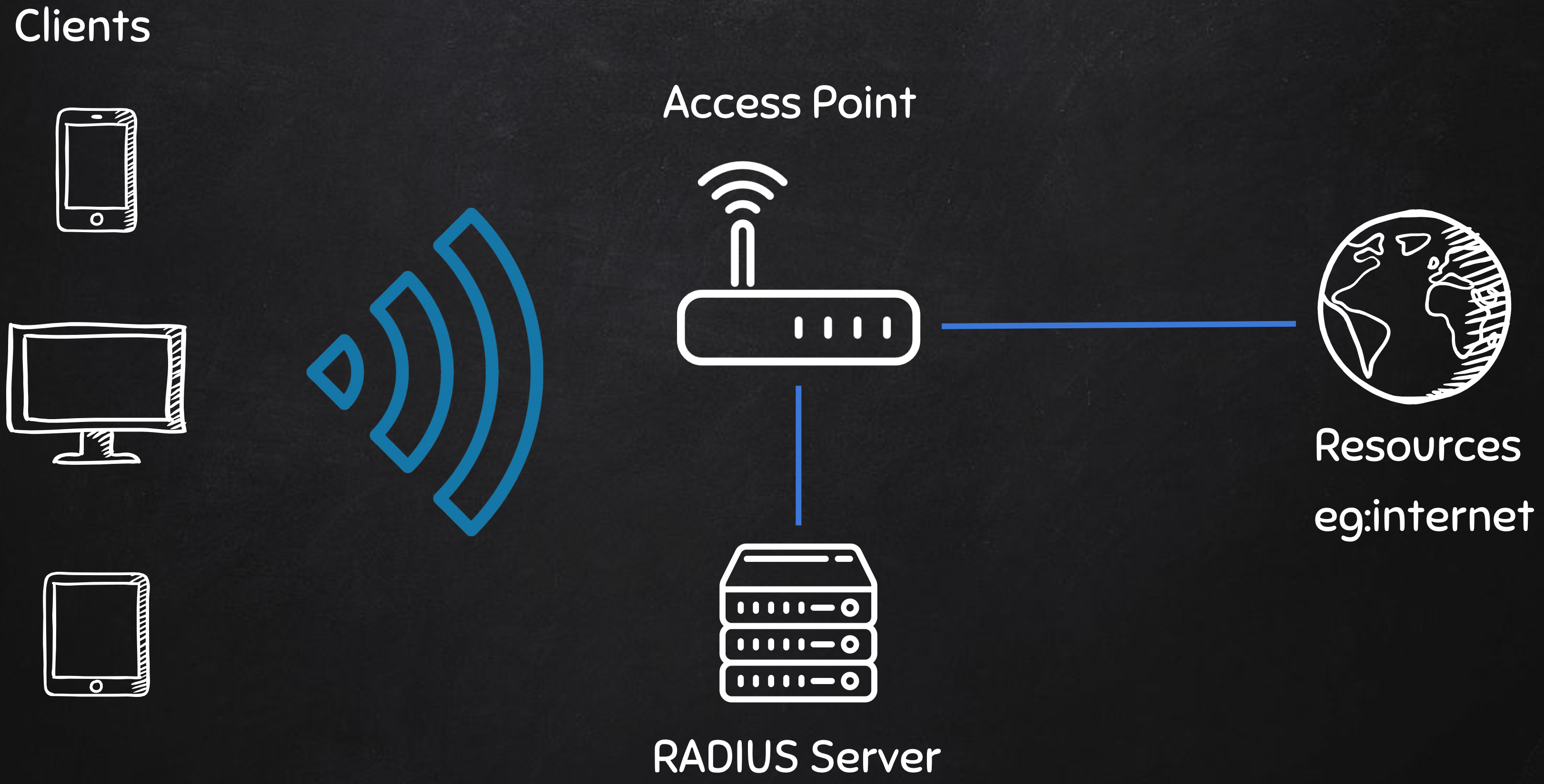
WPA Enterprise

- All WPA/WPA2 networks we seen so far use PSK authentication.
- A shared key is used to authenticate users.
- One key per network.
- Router manages authentication.

- WPA Enterprise is another form of authentication.
- Each user get their own key to connect to the network.
- Authentication is managed through a central server (RADIUS Server).

WPA Enterprise



Clients

Access Point

Resources

eg:internet

RADIUS Server

Hacking WPA Enterprise

Problems:

1. Encryption is used, so can't sniff credentials in monitor mode.
2. Can't use ARP spoofing because we need to connect first.

The only solution is to run an evil twin attack, 2 ideas:

1. Using the traditional method, just use a page that looks like login box.
2. Create a fake AP that uses WPA enterprise.

Hacking WPA Enterprise

Using Traditional Fake AP

Drawbacks:

1. Has to be an open network when users know their network use WPA/WPA2.
2. They have to enter password in a web page.

Advantages:

- Password is sent in plain text.
- No need to decrypt it.

Hacking WPA Enterprise

Using a Fake WPA Enterprise AP

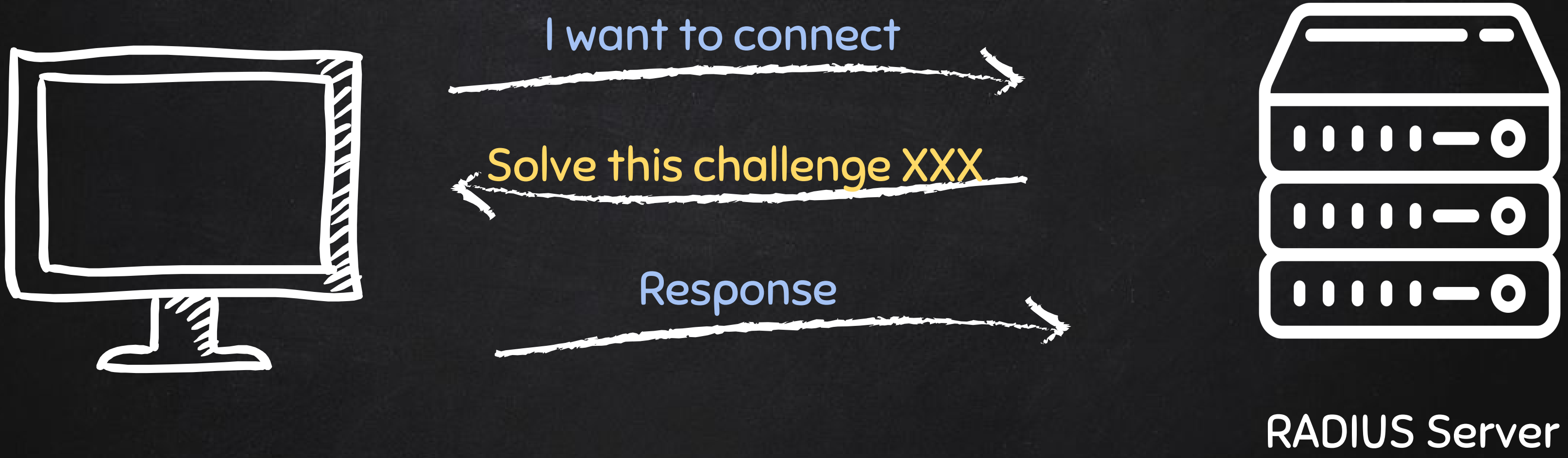
Drawbacks:

- Captured password will be encrypted.

Advantages:

- Looks and behaves exactly like a real WPA-Enterprise network.

Challenge Response Authentication



I want to connect

Solve this challenge XXX

Response

RADIUS Server