WiFi

Ethernet is wired
    information is carried through a wire (copper)
fiber optic is wired
    information is carried through a wire, but using light
wireless is not wired
    information is carried on top of a wave
    the wave is a carrier signal
    we must encode the information on this carrier signal → modulation
    the other side (receiver) must extract the information → demodulation
    waves have a frequency (width) and amplitude (height)
        frequency is usually 2.4GHz or 5GHz

wired vs wireless
    wired requires physical proximity and access to ports
    wireless doesn't: we can be close enough
        or have really large antennas
        so I can be concealed
        this motivates encryption of the information being carried on the carrier signal

wifi best practices
    a live demo of the following may occur
    when setting up a wifi network (e.g., in our homes), we give it a name: ssid
        it is repeatedly broadcasted (our wifi interfaces pick this up)
    we can hide it if we wish (i.e., tell the wifi router to stop broadcasting the ssid)
        but this can still be easily discovered with sniffers
        note that most defensive tactics don't prevent pros
            we can only delay them...perhaps
        in the end, hiding the ssid doesn't really make your network any safer
            it's just an illusion
    each physical network device has an address (mac address)
        we can specify white lists (who do we allow on our wifi network)
            everyone else is blocked
        we can specify black lists (who do we block from our wifi)
            everyone else is allowed
        these lists are just mac addresses of wifi interfaces
        guess what? we can spoof mac addresses!
            I can sniff the network for a while (even if it is encrypted)
            and discover packet header information which contains mac addresses
            then, I just spoof one
            this kicks off the legitimate interface, letting me in
            if course, the legitimate interface may automatically try to reconnect
            which kicks me off
            ...and so on...
            but maybe I can find one that doesn't try to reconnect
            and now, I'm in!
        in the end, having white lists (or black lists) makes sense
            but it's a hassle if you constantly have new wifi interfaces needing wifi access
                think guests in your home

    we can encrypt the information over the wifi network!

in fact, this is absolutely recommended
there are several encryption methods
WEP: wired equivalent privacy (weak and easily defeated)
WPA/WPA2: wifi protected access (stronger, but depends on the strength of a passphrase)
more about these later

spoofing mac addresses (a brief tutorial)

****a live demo of the following may occur****

text in `Courier New` are commands to enter in bash

open a terminal
first, we need to get **macchanger**

```
sudo apt-get install macchanger
```

next, disconnect and reconnect wifi interface
and check for the name of the wifi interface via ifconfig

```
ifconfig
```

mine is **wlan0**
let's store this in a variable

```
int=wlan0
```

while we're at it, let's note the mac address of wlan0 so we see it changed later

now, bring wlan0 down

```
sudo ifconfig $int down
```

finally, change the mac address

```
sudo macchanger -m 00:02:04:06:08:10 $int
```

let's bring wlan0 back up

```
sudo ifconfig $int up
```

and check the interface via ifconfig

```
ifconfig
```

it should have the new mac address

to undo this and restore the original mac address
well, you could just reboot
or instead bring wlan0 down

```
sudo ifconfig $int down
```

and now restore the original mac address

```
sudo macchanger -p wlan0
```

and finally bring wlan0 back up

```
sudo ifconfig $int up
```

and check the interface via ifconfig

```
ifconfig
```

it should have the old mac address