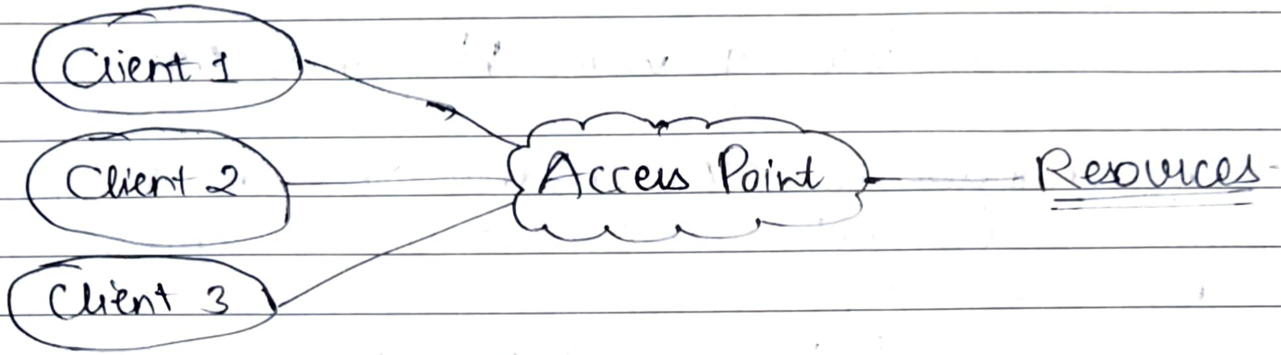
Network Hacking

↳ client connects to a network to share resources; such as internet.

↳ clients are connected to a router/access point which has access to resource.

→ No client can directly access resources.



☆ You need an access point to access resources.

→ Data is transmitted as packets.

☆ Moving forword, you must have wireless adapter

(~~Skipping Wireless Adapters for now~~). (~~Lec 11 To 28~~)

☆ MAC Address (Media Access Control) are unique, permanent & physical addresses for each device. They are assigned by manufacturers.

→ MAC addresses are used to transfer data from source to destination.

Why to change MAC address?

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

To change it:→ go to 'ifconfig' on terminator:

→ for each virtual interface, 'ather' (ether) shows you its MAC address

→ for your wireless adapter, there is an ether too.

→ To change the MAC address, disable the interface first

→ To disable:

```
# ifconfig {name} down
           (eg wlan0)
```

→ Now change ether:

```
                    (hardware)
# ifconfig wlan0 hw ether 00:11:22:33:44:55
```

→ This changes the MAC address. You can choose any address you want, but just start it with 00.

→ Now enable it:

```
# ifconfig wlan0 up
```

★ The MAC address reverts back to original one when you ~~reset~~ (restart) the pc.

★ Since every data has a source MAC & destination MAC, it is easy for us to trace them. We can get in between the transmission.

→ if we write 'iwconfig', it will show you the wireless configurations.

→ for wlan0, current Mode: managed. It is by default.

- which means ~~all~~ this device will capture packets that has the destination mac of this device.
- but we need to capture all packets that are not directed to us.

∴ change mode to monitored.

∴ • disable wlan0

• kill any interfering processes using:

```
# airmon-ng check kill
```

★ You might lose internet access for some time. This is a preconnection step.

→ enable monitor mode:

```
# iwconfig wlan0 mode monitor
```

→ enable wlan.

★ Now you can capture packets within range.