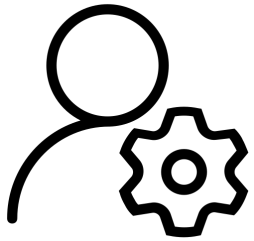
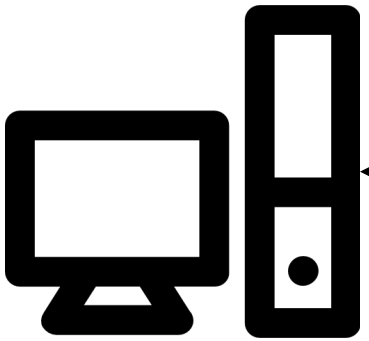
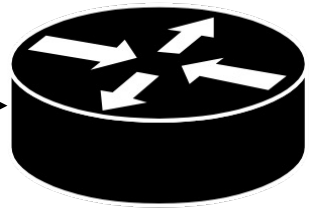
Example Authentication Setup



Network admin
- Monitors the legitimacy of the client
- Listens + collects in-air frames
- Collects CSI



Client:
- Generates traffic (surfs web)

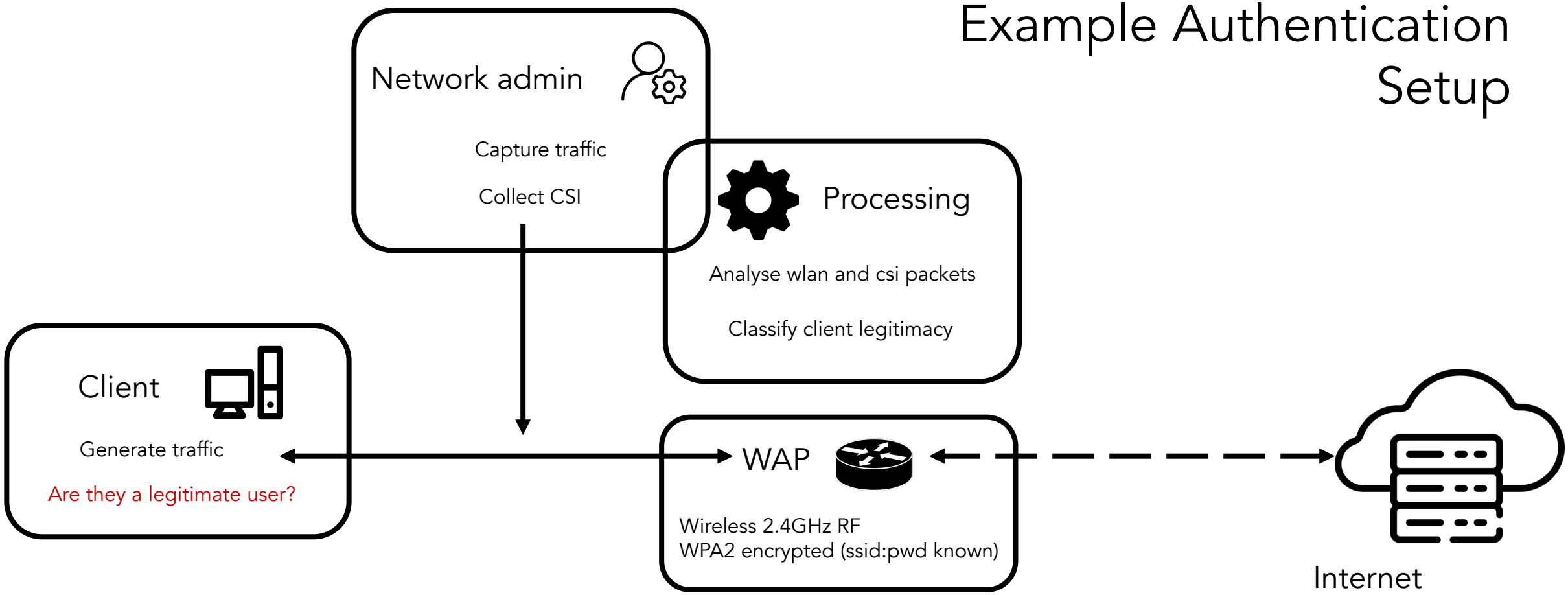


WAP
- For wireless communication on network

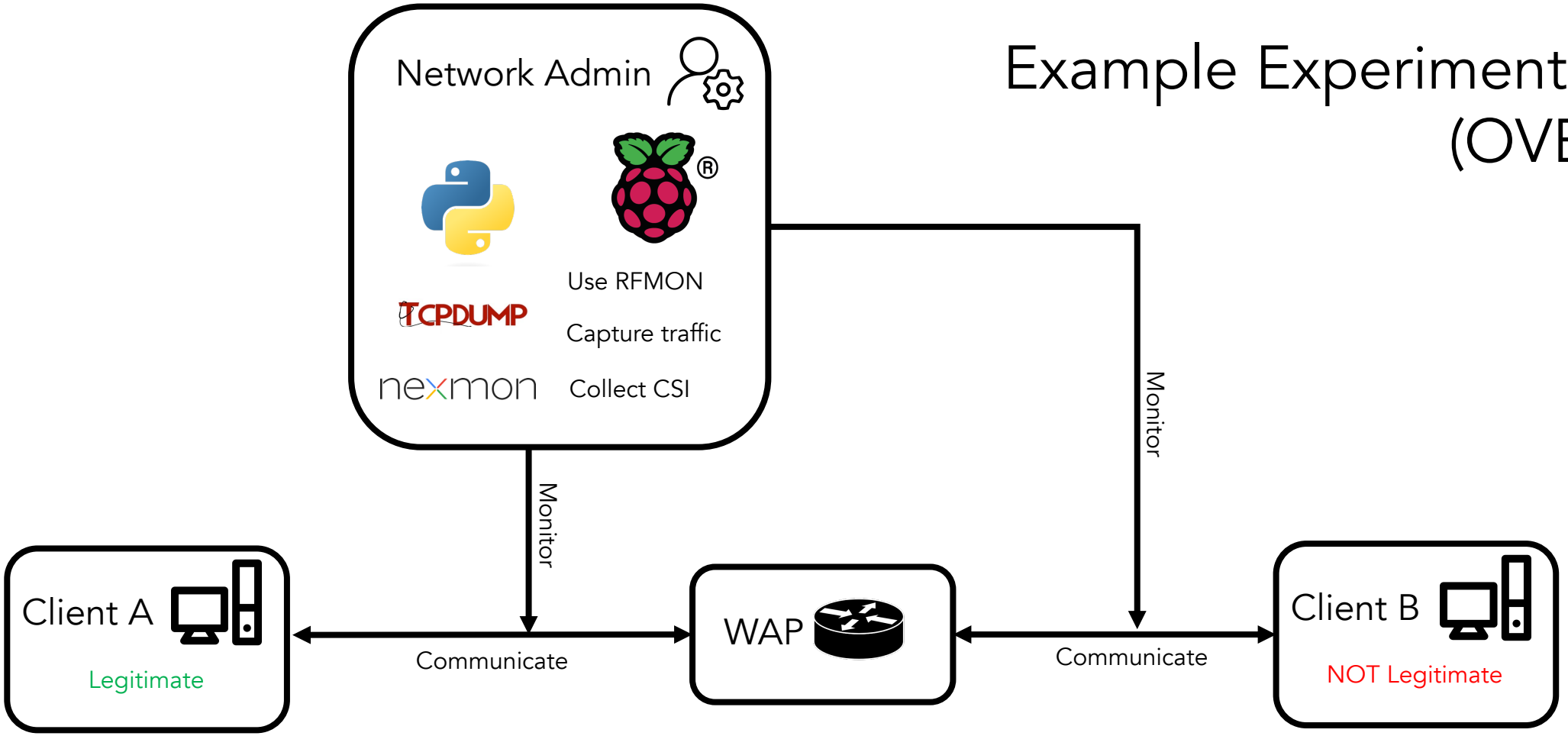
Internet
- Visited streaming servers are YouTube, Netflix, Stan, etc.
- Also plan to visit websites

Network admin wants to determine whether the client is legitimate and working legitimately

Example Authentication Setup



Example Experiment Setup (OVERALL)



Three independent variables:

a) Different traffic (detect anted activity)
b) Different devices (detect masquerading)
c) Different device locations (detect intrusion or unauthorised location)

Example Experiment Setup (INDEPENDENT VARS)

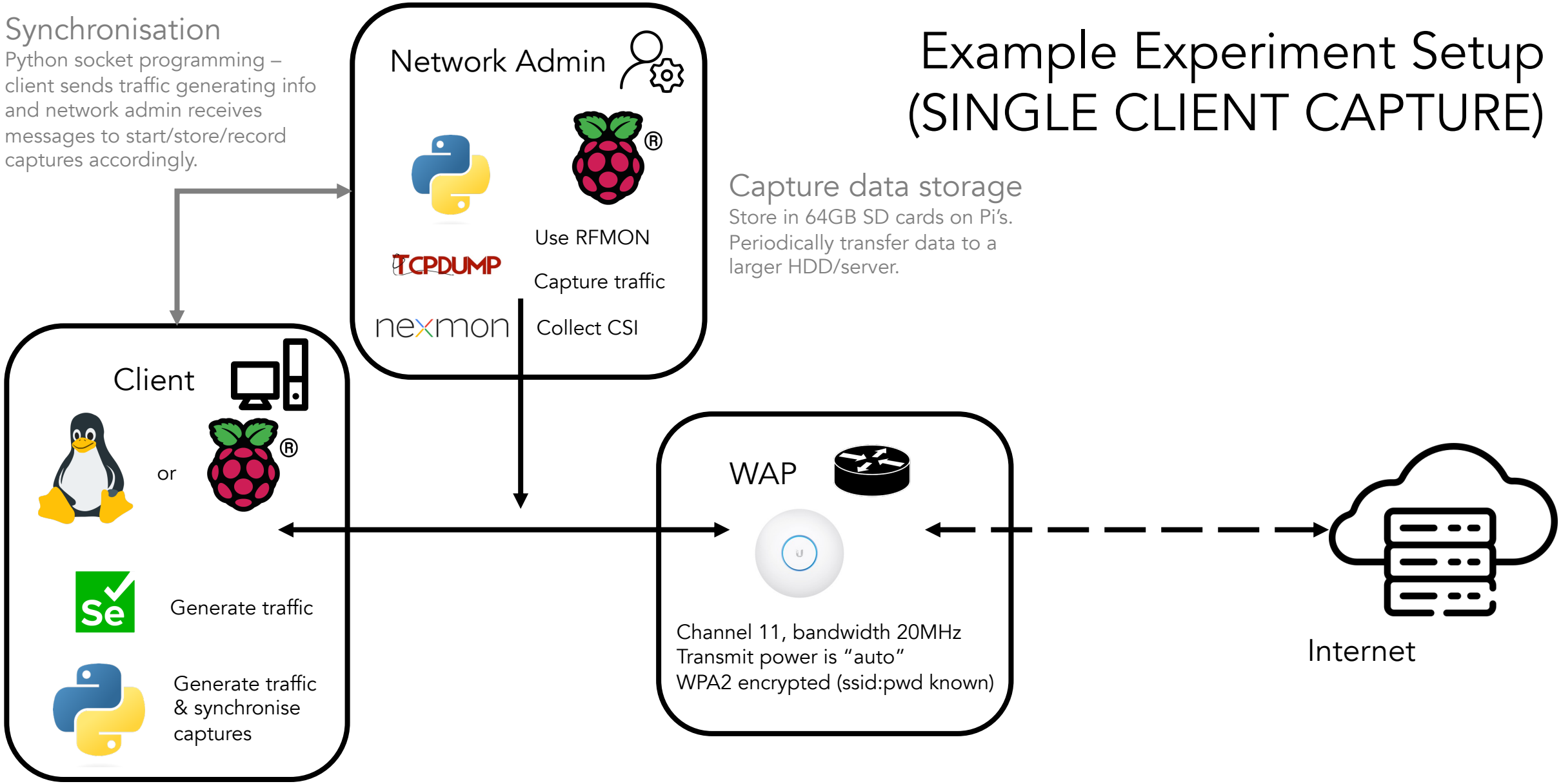
Independent Variable	Values
Traffic	3 different YouTube videos
Device	Custom built PC, Rpi-4
Location (distance)	0.5m, 2m, 5m
Location (is through wall)	Yes, No

Currently taking 100 captures for each independent variable combination.
RED denotes captures for this have not been finished yet.

Example Experiment Setup (SINGLE CLIENT CAPTURE)

Synchronisation

Python socket programming – client sends traffic generating info and network admin receives messages to start/store/record captures accordingly.

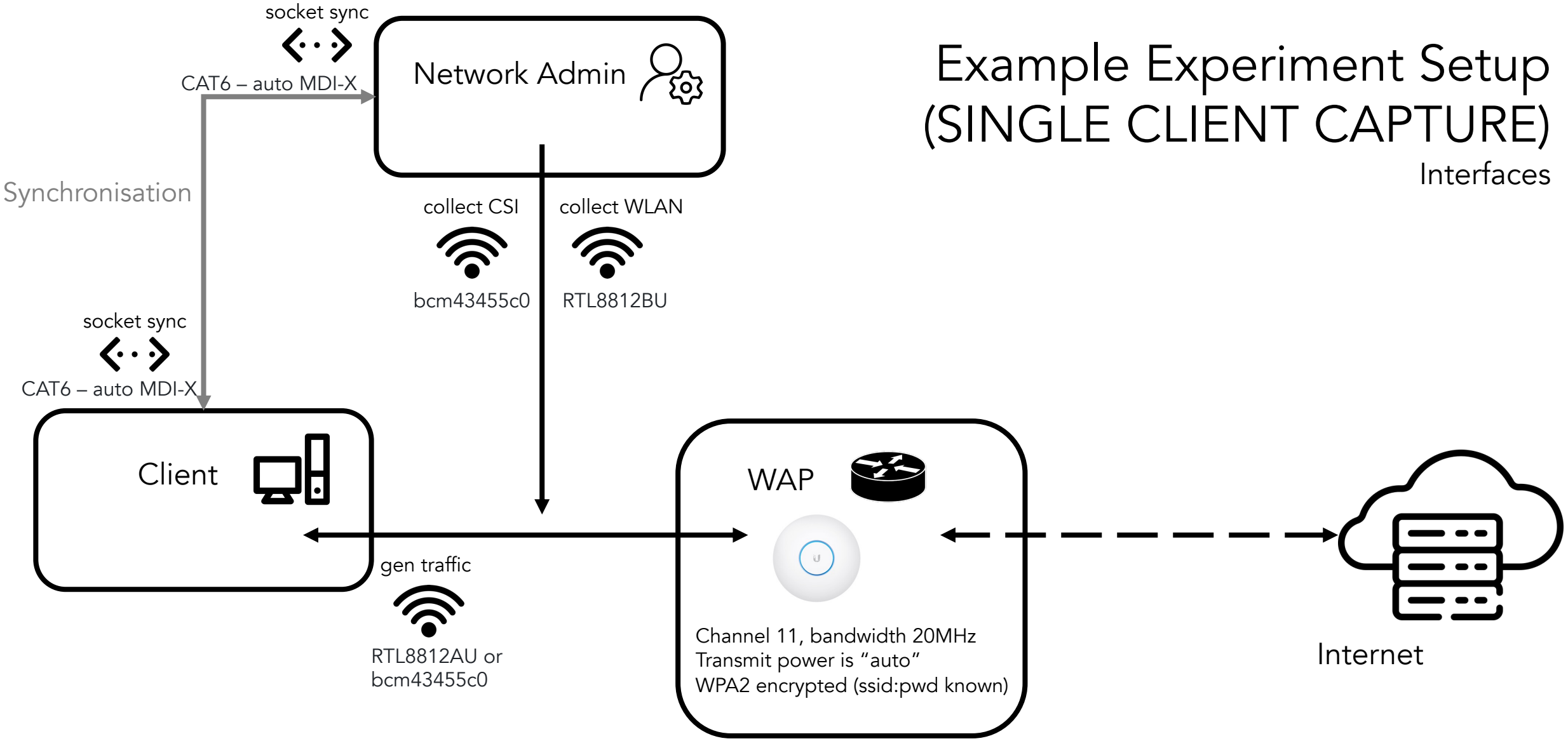


Capture data storage

Store in 64GB SD cards on Pi's. Periodically transfer data to a larger HDD/server.

Example Experiment Setup (SINGLE CLIENT CAPTURE)

Interfaces



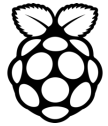
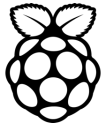
Client Items

Experiment Items Explanation

Item	Usage	Reason
 or 	Hardware	Client A: 2-core CPU custom built PC. It is using a Linux OS Client B: RPi4
 or 	OS	Client A: Ubuntu Client B: Raspberry Pi OS NOTE: Both use 64bit versions
	Generate traffic	Browsing automation framework on Python (and others). Works with Chrome, FireFox, etc. drivers. Can stream videos.
	Use nmcli	nmcli is the NetworkManager client. It allows a user to connect, disconnect, reconnect, and manage network settings (e.g. default channel, gateway).

Network Admin Items

Experiment Items Explanation

Item	Usage	Reason
	Hardware	Lightweight and versatile. Pi 4 is preinstalled with WiFi chip supported by Nexmon CSI and we use a USB RTL8812bu WNIC.
	OS	32bit ARM version works with Nexmon CSI *AND* RTL8812bu WNIC WiFi adapter. I've written install instructions in 0_setup – this is the only setup I have gotten working with Nexmon and another RFMON WiFi adaptor.
TCPDUMP	Capture in-air packets	Listening and capturing all WiFi frames in air with TCPdump.
nexmon	Collect CSI	To collect the CSI of the client's in-air packets

Experiment Development

Synchronisation

Python socket programming – client sends traffic generating info and network admin receives messages to start/store/record captures accordingly.

Network Admin

Use RFMON

Capture traffic

Collect CSI

Capture data storage

Store in 64GB SD cards on Pi's. Periodically transfer data to a larger HDD/server.

Client

or

Generate traffic

Generate traffic & synchronise captures

Need to prevent ads on YouTube. Experimenting with using adblocker ext.

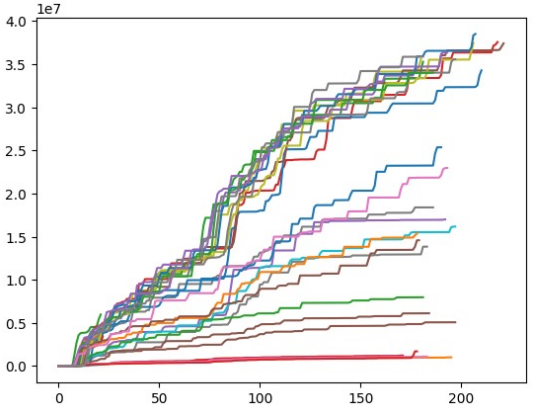
WAP

Channel 11, bandwidth 20MHz
Transmit power is "auto"
WPA2 encrypted (ssid:pwd known)

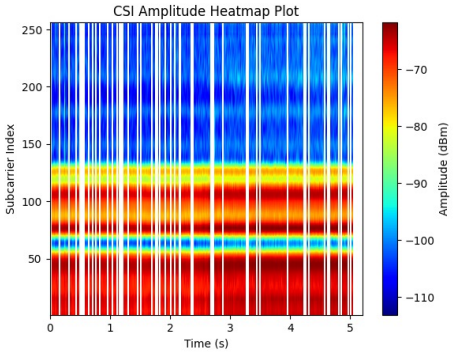
Internet

Proposed Data Analysis

Type	Feature	Filter
WLAN	• Number of packets • Number of bytes • NOTE: these metrics are consistently the best for traffic classification but we can try others • Min packet size • Max packet size • Ave packet size • Var packet size • Group by packet number (groups of *p* packets) • Group by timestamp (in time bins of size *t*)	• Incoming MAC addr is client • Outgoing MAC addr is client • Both • All streams included • Top *n* streams included • Streams with total transferred bytes above *k*
CSI	• Each subcarrier's amplitude • Each subcarrier's phase • NOTE: there are bandwidth * 3.2 subcarriers	• Incoming MAC addr is client • Outgoing MAC addr is client • Both



Example WLAN capture.
Shows cumulative packet sizes across time (seconds) for 35 captures of the same YT video



Example CSI from GitHub.
Shows amplitude of all subcarriers (256 for a 80MHz bandwidth) across time for a single capture