

WLAN - Project 2

Comunicações Móveis

Carlos Costa (88755)
Diogo Correia (90327)
João Simões (88930)

Group 2

Introduction

Goal:

Test and verify the functional and performance aspects of IEEE 802.11 technology

IEEE 802.11:

IEEE 802.11 is part of the IEEE 802 set of technical standards and specifies the set of MAC and PHY protocols for implementing WLAN communication

Case studies:

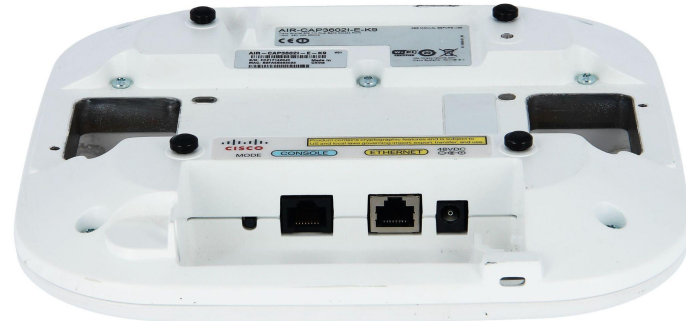
- Impact of **coverage** and **performance** configurations
- Occurrence of **roaming** between APs
- Behaviour of **ad-hoc** network
- Importance of **RTS** and **CTS** mechanism

Cisco Access Point

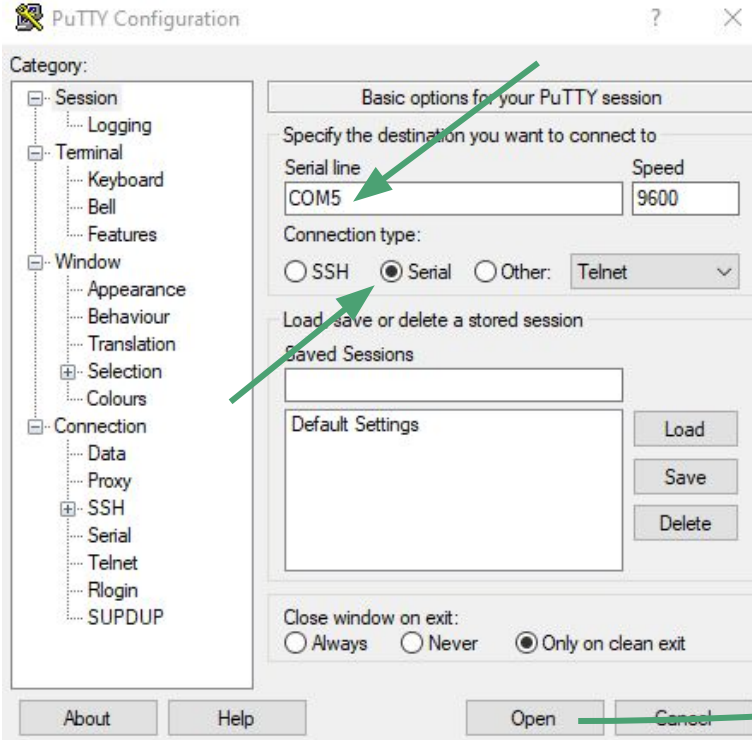
Model: AIR-CAP3602I-E-K9

IEEE standard: 802.11n

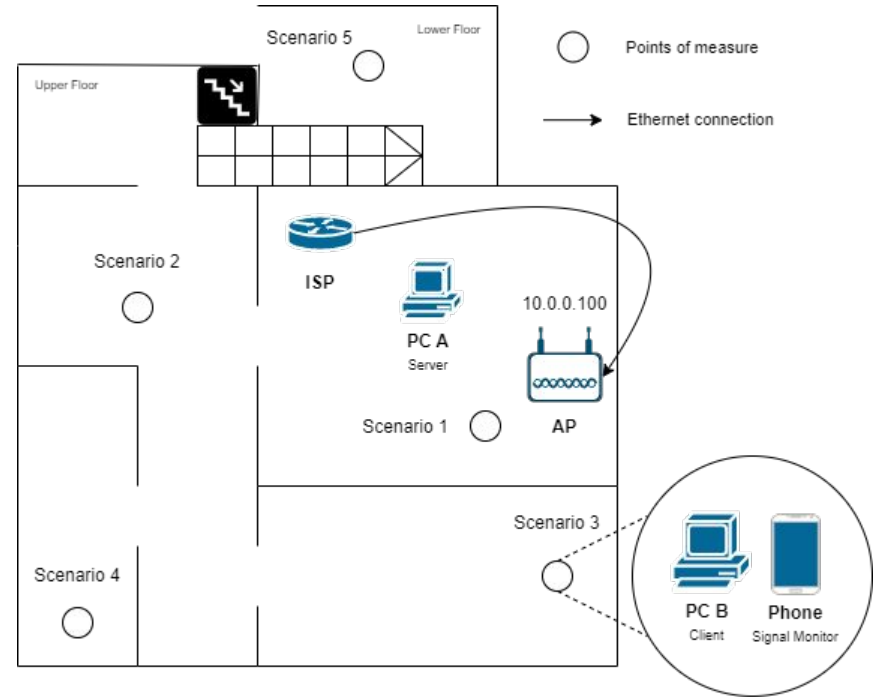
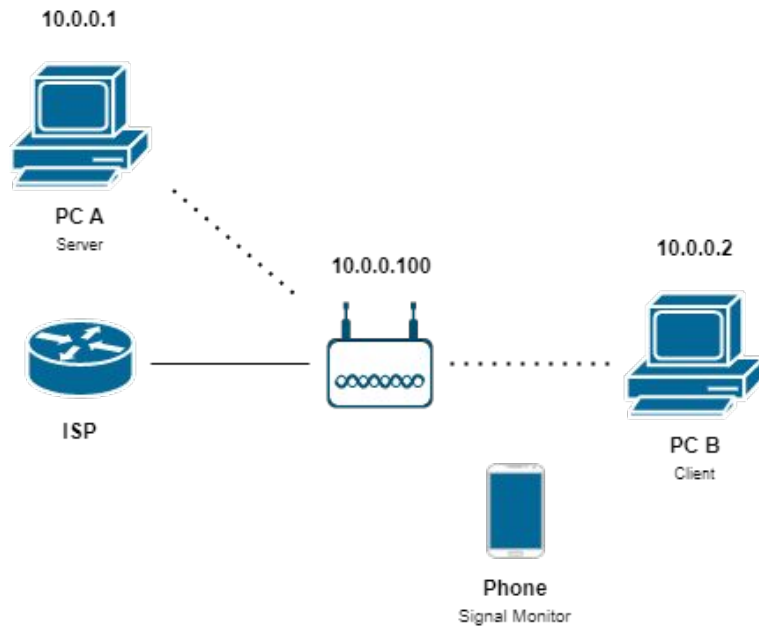
Dual Band: 2.4 GHz & 5 GHz



Access Point Configuration



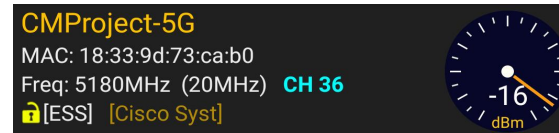
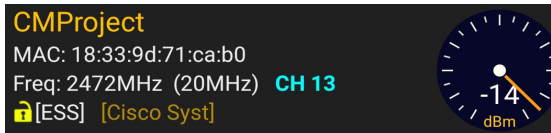
802.11 coverage and performance



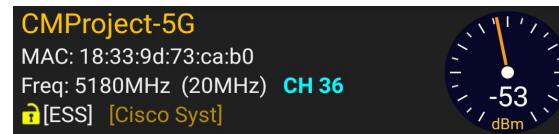
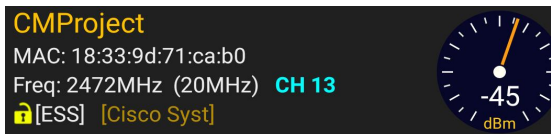
2.4GHz

5GHz

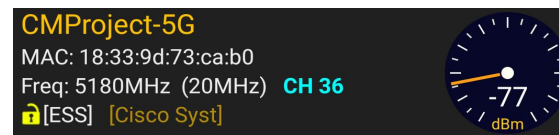
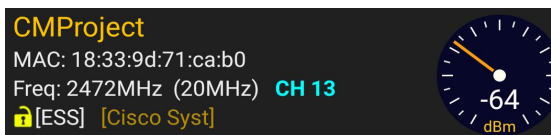
Scenario 1



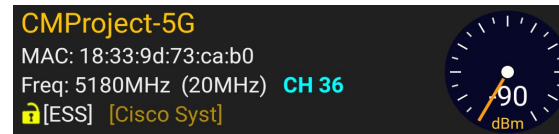
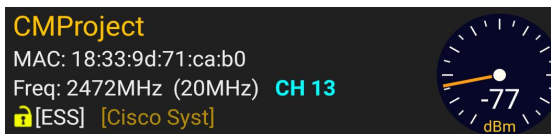
Scenario 2



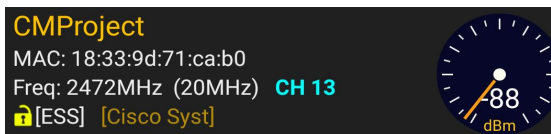
Scenario 3



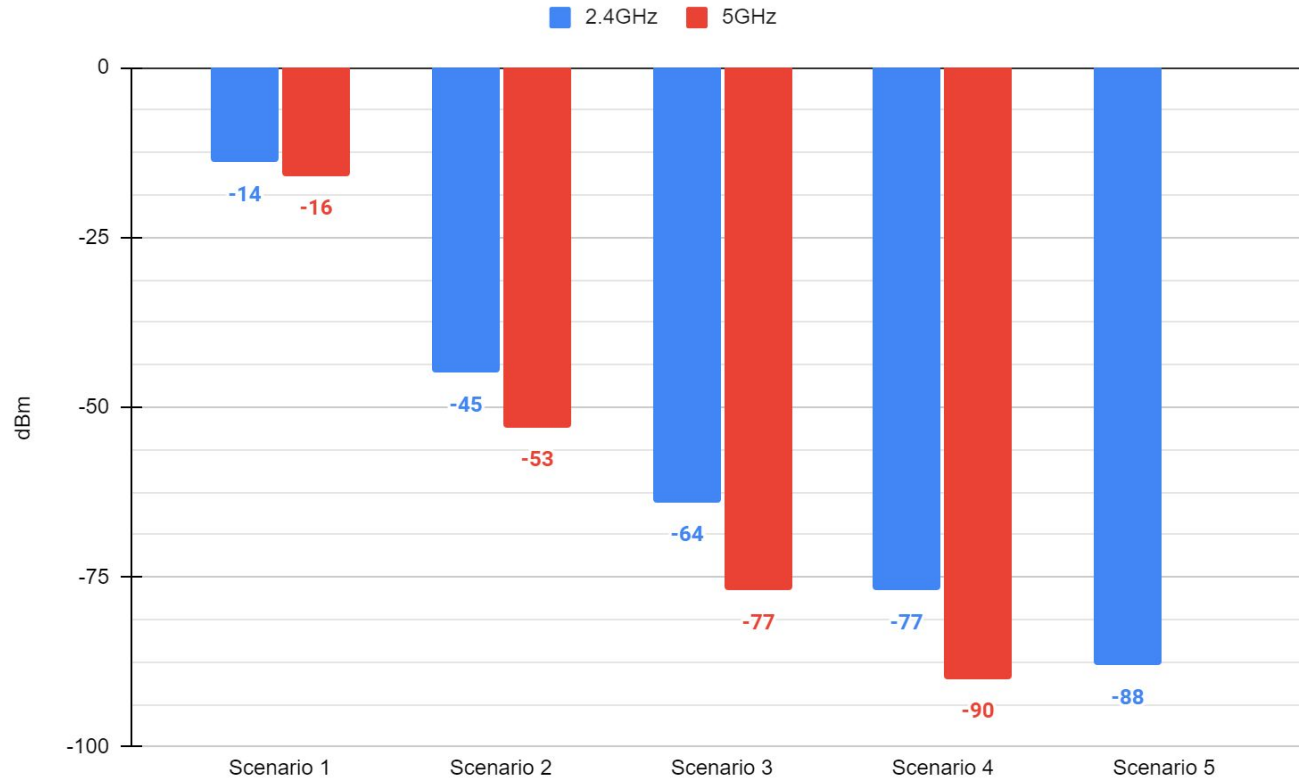
Scenario 4



Scenario 5



Signal Strength



Signal Strength

> iperf3 -c 10.0.0.2 -t 20 --logfile scenario1-test1-5g.txt

Connecting to host 10.0.1.4, port 5201

[5] local 10.0.1.5 port 63897 connected to 10.0.1.4 port 5201

[ID]	Interval		Transfer	Bandwidth
[5]	0.00-1.01	sec	4.38 MBytes	36.3 Mbits/sec
[5]	1.01-2.01	sec	4.00 MBytes	33.8 Mbits/sec
[5]	2.01-3.01	sec	3.88 MBytes	32.5 Mbits/sec
[5]	3.01-4.00	sec	4.38 MBytes	36.8 Mbits/sec
[5]	4.00-5.00	sec	4.25 MBytes	35.7 Mbits/sec
[5]	5.00-6.01	sec	4.38 MBytes	36.2 Mbits/sec
[5]	6.01-7.01	sec	4.38 MBytes	36.7 Mbits/sec
[5]	7.01-8.01	sec	4.38 MBytes	36.7 Mbits/sec
[5]	8.01-9.01	sec	4.12 MBytes	34.6 Mbits/sec
[5]	9.01-10.01	sec	4.25 MBytes	36.0 Mbits/sec
[5]	10.01-11.00	sec	4.38 MBytes	36.8 Mbits/sec
[5]	11.00-12.00	sec	4.12 MBytes	34.6 Mbits/sec
[5]	12.00-13.00	sec	4.12 MBytes	34.7 Mbits/sec
[5]	13.00-14.00	sec	4.00 MBytes	33.4 Mbits/sec
[5]	14.00-15.00	sec	4.12 MBytes	34.8 Mbits/sec
[5]	15.00-16.01	sec	4.25 MBytes	35.3 Mbits/sec
[5]	16.01-17.01	sec	4.25 MBytes	35.5 Mbits/sec
[5]	17.01-18.00	sec	4.12 MBytes	35.0 Mbits/sec
[5]	18.00-19.01	sec	4.25 MBytes	35.4 Mbits/sec
[5]	19.01-20.01	sec	4.25 MBytes	35.8 Mbits/sec

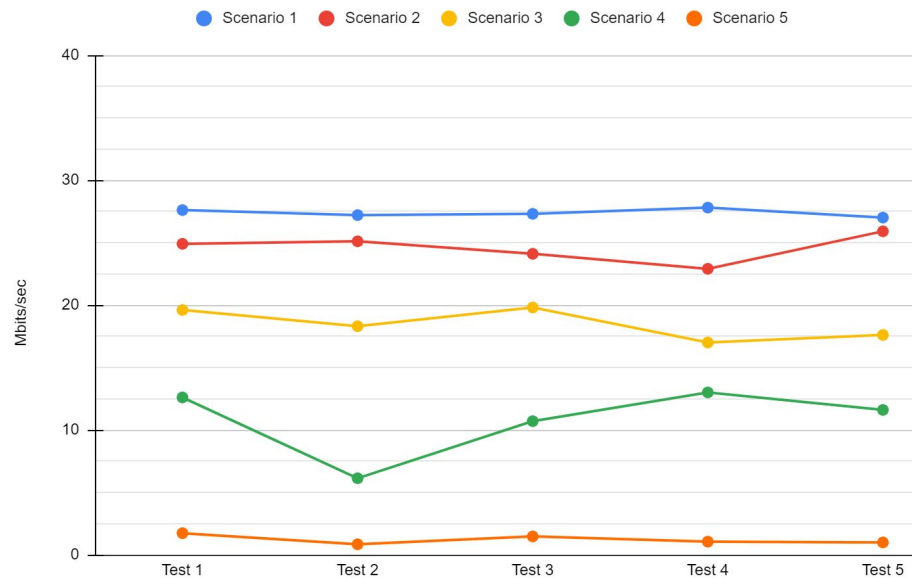
[ID]	Interval		Transfer	Bandwidth
[5]	0.00-20.01	sec	84.2 MBytes	35.3 Mbits/sec
[5]	0.00-20.01	sec	84.1 MBytes	35.2 Mbits/sec

sender
receiver

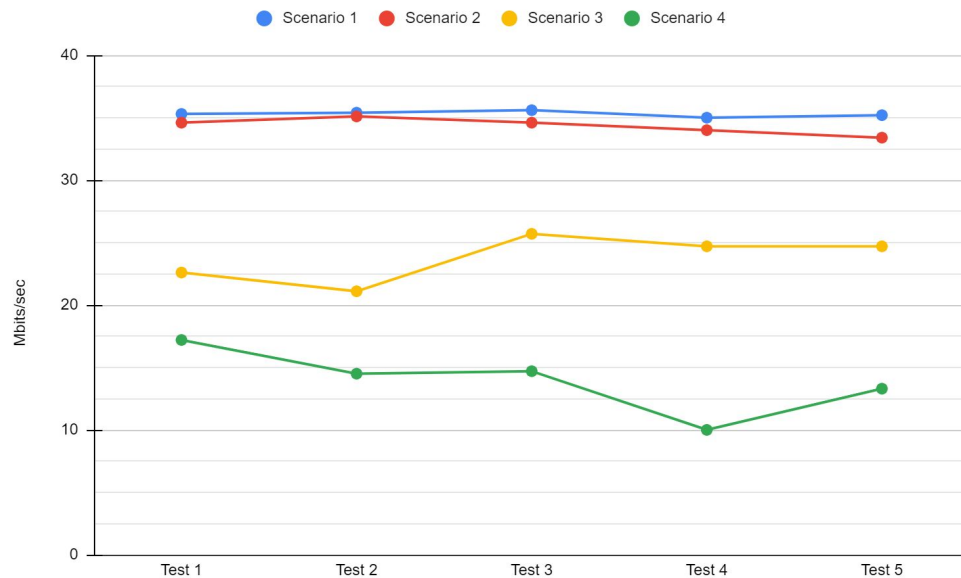
Bandwidth

iperf Done.

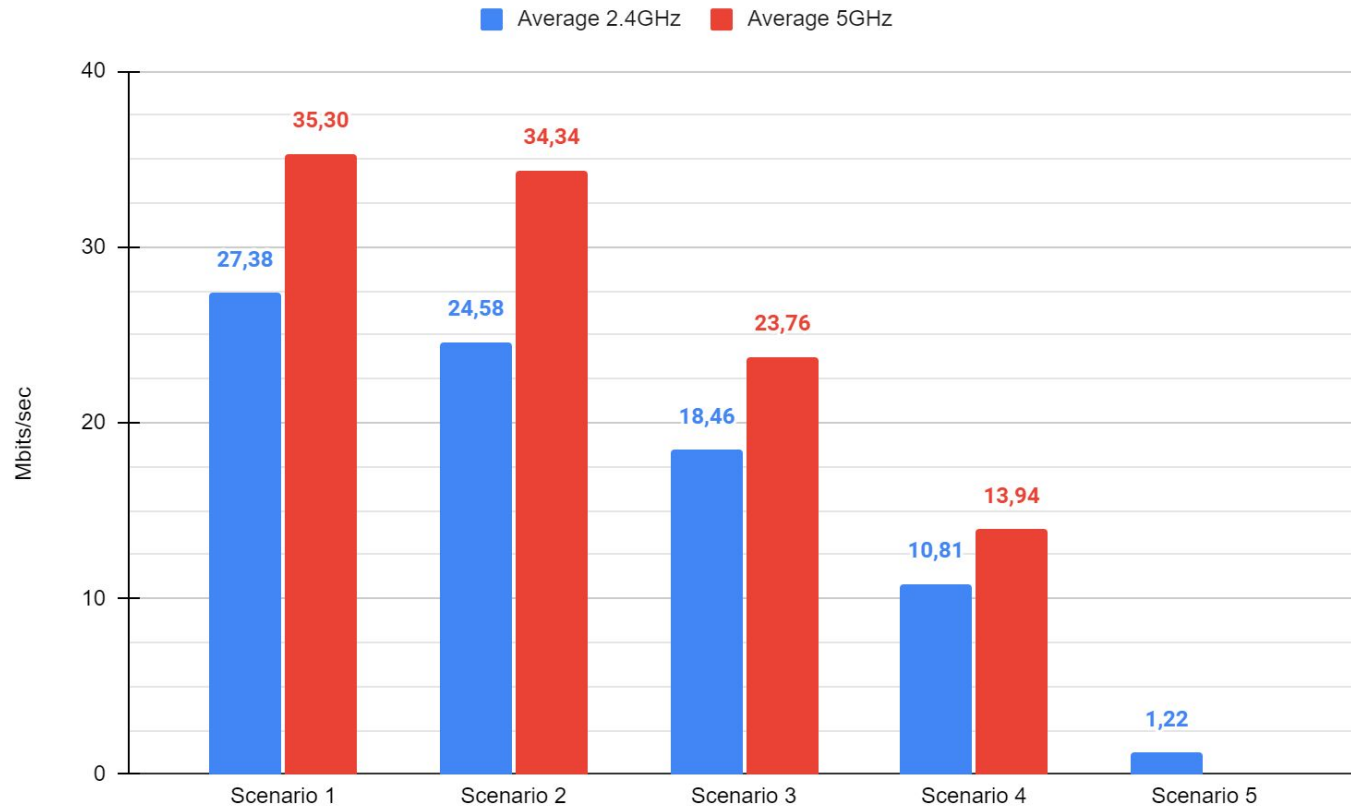
2.4GHz



5GHz

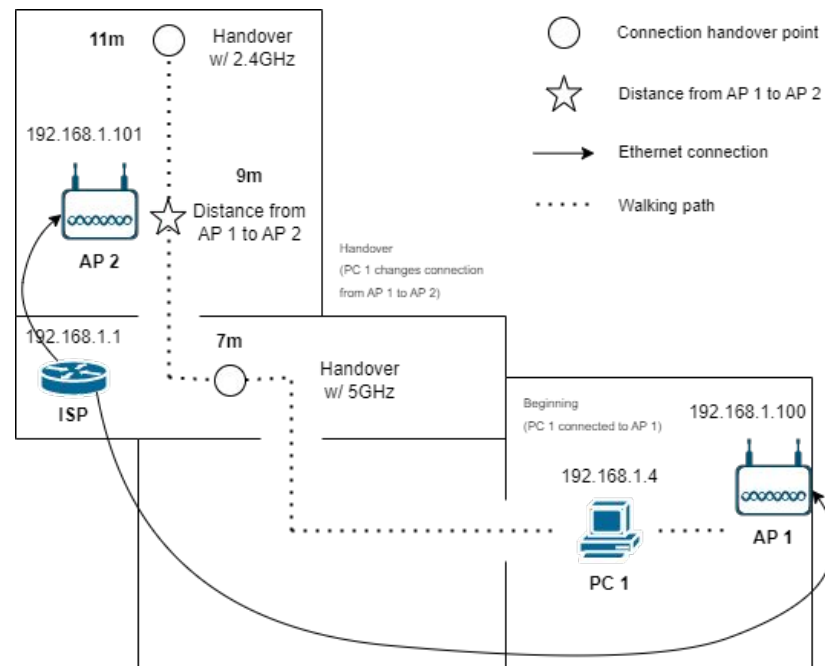
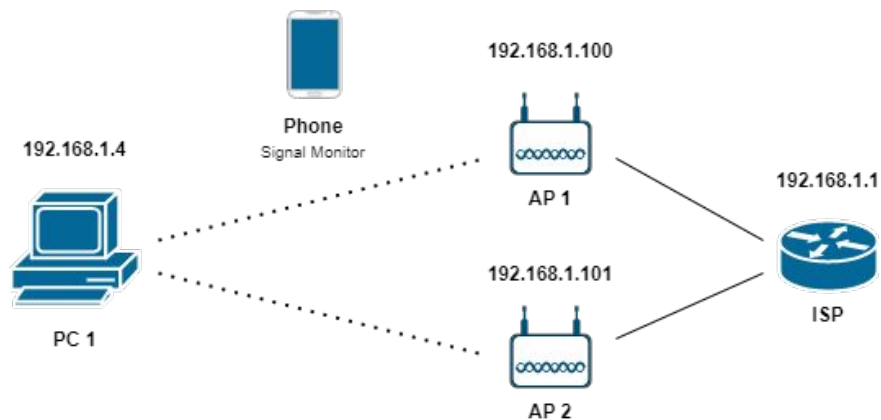


Bandwidth

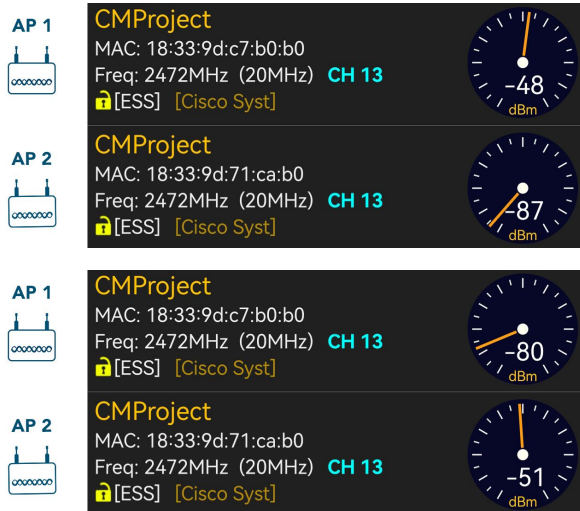


Bandwidth

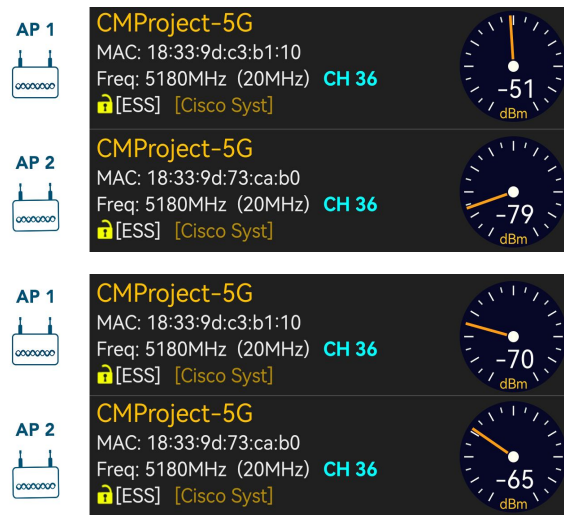
Roaming between APs



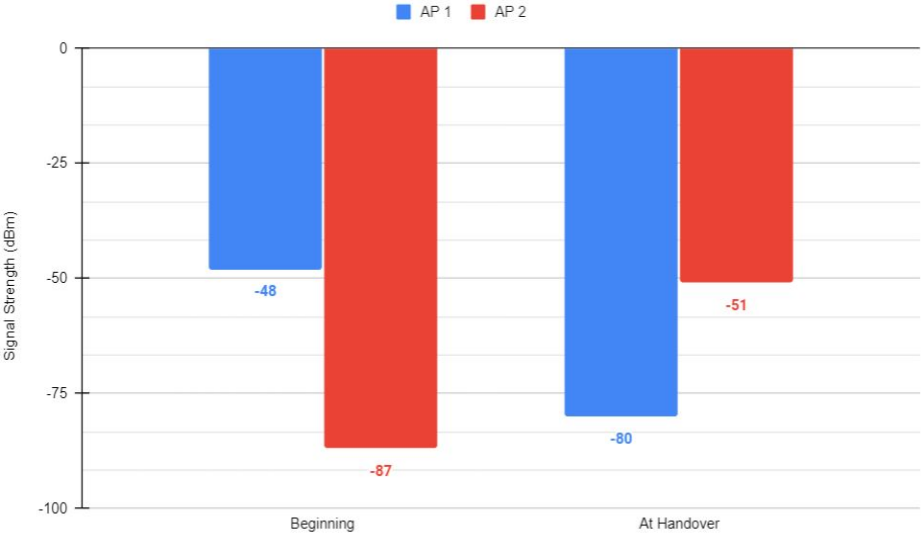
2.4GHz



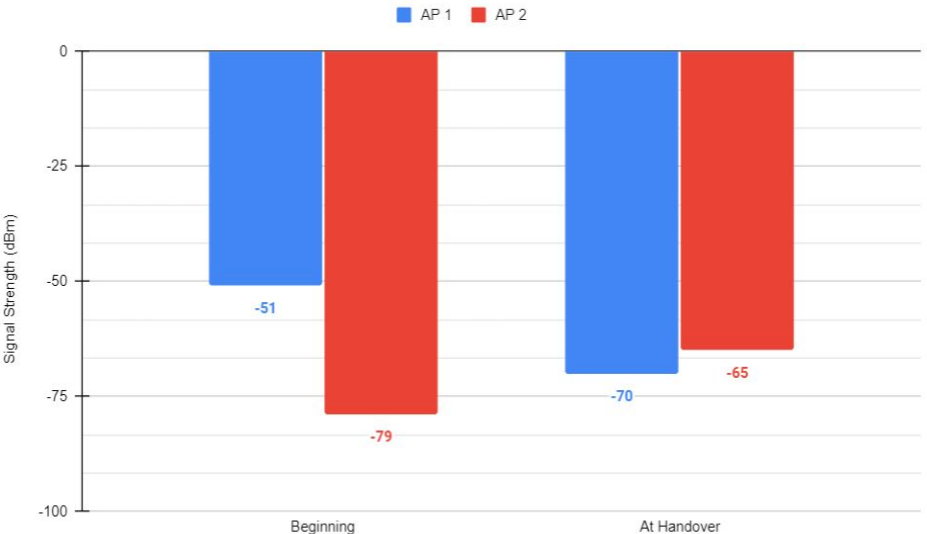
5GHz



Roaming 2.4GHz



Roaming 5GHz



Ad-hoc Network

ad hoc.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.sa == 62:e3:c3:b3:dd:83

No.	Time	Source	Destination	Protocol	Length	Info
1245	9.914745197	62:e3:c3:b3:dd:83	Broadcast	802.11	177	Probe Request, SN=1815, FN=0, Flags=.....C, SSID="AdHocNetwork"
1251	9.949265945	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	269	I, N(R)=0, N(S)=0; DSAP 0x32 Individual, SSAP NULL LSAP Command
1252	9.949273384	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	269	I, N(R)=0, N(S)=0; DSAP 0x32 Individual, SSAP NULL LSAP Command
1253	9.949280082	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	269	I, N(R)=0, N(S)=0; DSAP 0x32 Individual, SSAP NULL LSAP Command
1254	9.949287737	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	269	I, N(R)=0, N(S)=0; DSAP 0x32 Individual, SSAP NULL LSAP Command
1255	9.949294675	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	269	I, N(R)=0, N(S)=0; DSAP 0x32 Individual, SSAP NULL LSAP Command
1256	9.949302384	62:e3:c3:b3:dd:83	62:e3:c3:b3:dd:83	LLC	1069	I, N(R)=0, N(S)=0; DSAP Ungermann-Bass Individual, SSAP NULL LSAP Command

<

> Frame 1252: 269 bytes on wire (2152 bits), 269 bytes captured (2152 bits) on interface wlp1s0, id 0

> Radiotap Header v0, Length 41

▼ 802.11 radio information

- PHY type: 802.11n (HT) (7)
- MCS index: 7
- Bandwidth: 20 MHz (0)
- Short GI: True
- Number of STBC streams: 0
- Data rate: 72,2 Mb/s
- Channel: 11
- Frequency: 2462MHz
- Signal strength (dBm): -41 dBm
- TSF timestamp: 777935188

> [Duration: 65µs]

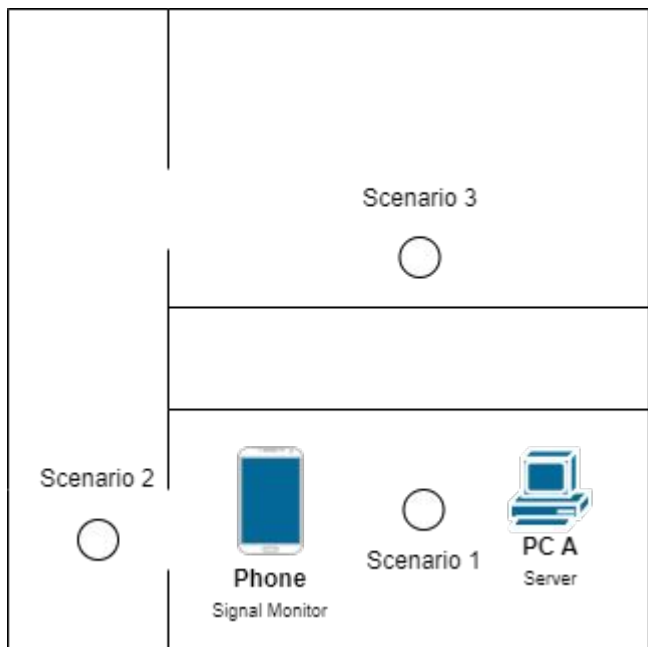
> IEEE 802.11 Data, Flags:TC

> Logical-Link Control

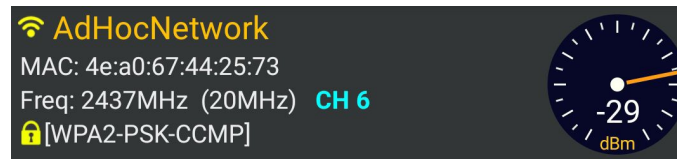
▼ Data (196 bytes)

Data: 31000000300000002f0000002e0000002d0000002c0000002b0000002a00000029000000...

[Length: 196]



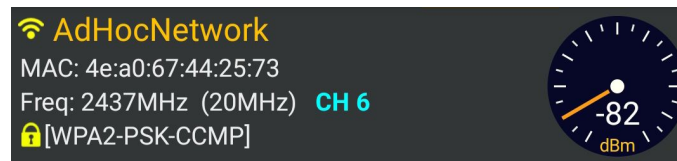
Scenario 1



Scenario 2

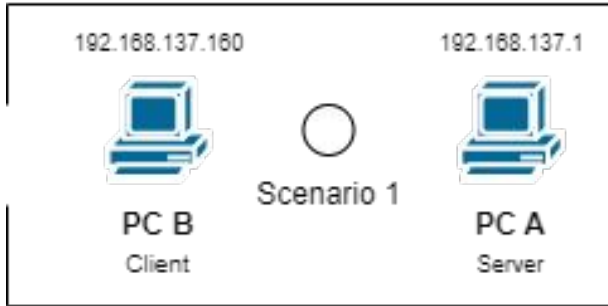


Scenario 3



Signal Strength

Ad-hoc Network

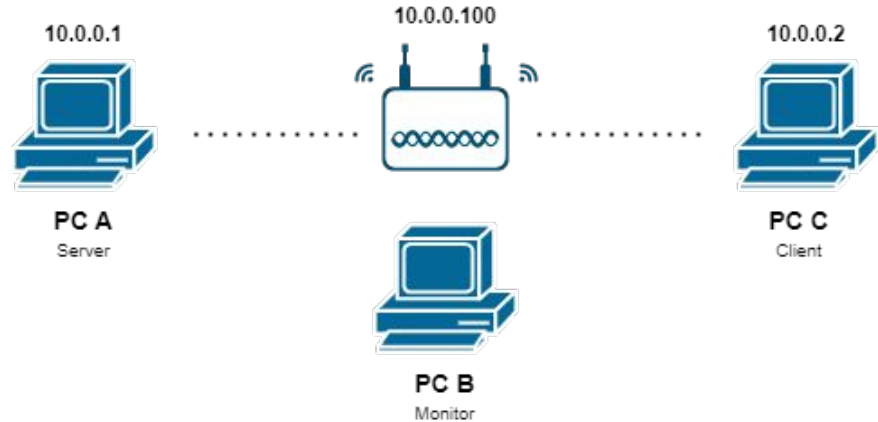


Scenario 1 Device as close as possible to the AP (< 1m)	
AP average bandwidth	Ad-hoc average bandwidth
27.38 Mbits/sec	31.64 Mbits/sec

Control Frames (not accomplished)

Why?

- Excessive amount of noise
- Need for monitor mode (Linux)
- Bugs on WiFi Jammer code



Thank you for your attention!

Questions?