POLITECNICO DI TORINO

01NWDBH - Mobile and Sensor Networks

Lab 01

Basic WI-FI scanning and Bluetooth tools

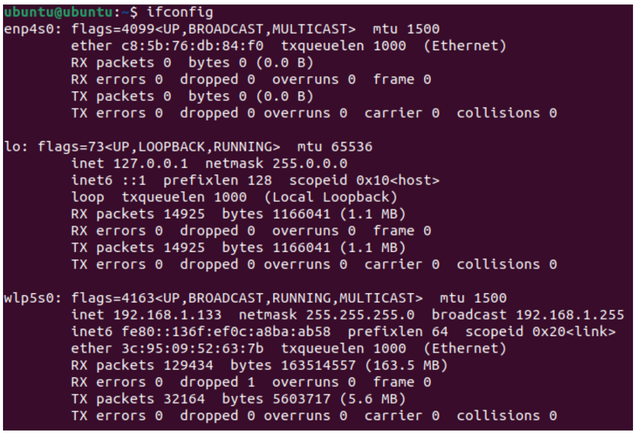
Group ID:
05

Students:

Valerio Collina	333919
Ammar Hussein	329829
Md Ismail Hossain	342704
Md. Ataur Rabby	347363

Academic year 2025/2026

1 Obtaining information about your Wi-Fi network interfaces and your AP

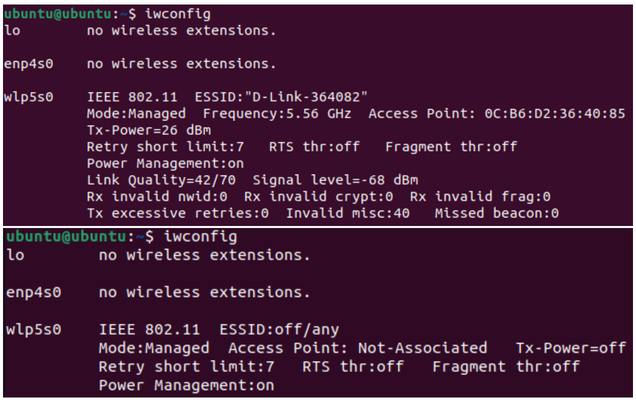


```
ubuntu@ubuntu:~$ ifconfig
enp4s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether c8:5b:76:db:84:f0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14925  bytes 1166041 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14925  bytes 1166041 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.133  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::136f:ef0c:a8ba:ab58  prefixlen 64  scopeid 0x20<link>
        ether 3c:95:09:52:63:7b  txqueuelen 1000  (Ethernet)
        RX packets 129434  bytes 163514557 (163.5 MB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 32164  bytes 5603717 (5.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1: Output of the `ifconfig` command



```
ubuntu@ubuntu:~$ iwconfig
lo        no wireless extensions.

enp4s0    no wireless extensions.

wlp5s0    IEEE 802.11  ESSID:"D-Link-364082"
          Mode:Managed  Frequency:5.56 GHz  Access Point: 0C:B6:D2:36:40:85
          Tx-Power=26 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=42/70  Signal level=-68 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:40   Missed beacon:0
```

```
ubuntu@ubuntu:~$ iwconfig
lo        no wireless extensions.

enp4s0    no wireless extensions.

wlp5s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=off
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

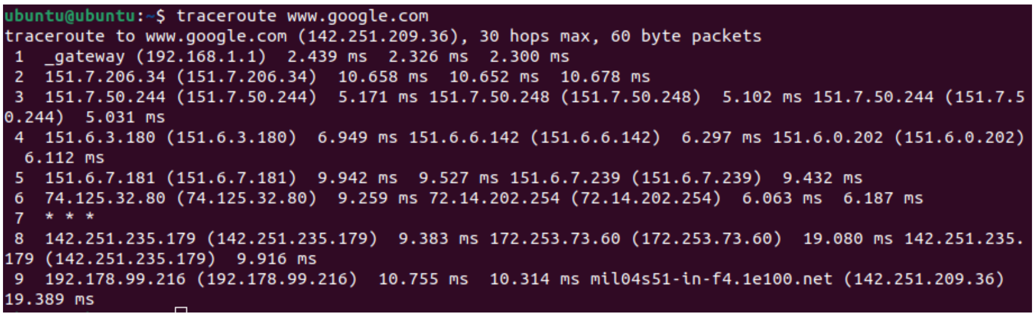
Figure 2: Output of `iwconfig` without Wi-Fi (top) and with Ethernet connection (bottom)

g,,og,rrprkgrpkgmg,gprkgor,pr

The `ifconfig` command shows all active network interfaces along with their IP and MAC addresses. The interface `wlp5s0` is the Wi-Fi card, and it had IP address `192.168.1.133` and MAC address `3c:95:09:52:63:7b`. The `iwconfig` output shows wireless-specific parameters.

When the Wi-Fi interface was disabled, the iwconfig command was executed again. This time, the output displayed only the message ”no wireless extensions”, indicating that the wireless interface was no longer active. This confirms that iwconfig provides information only when a wireless interface is enabled and connected. In contrast, ifconfig continued to display all active interfaces, including the Ethernet interface, which became active after the cable connection was established.

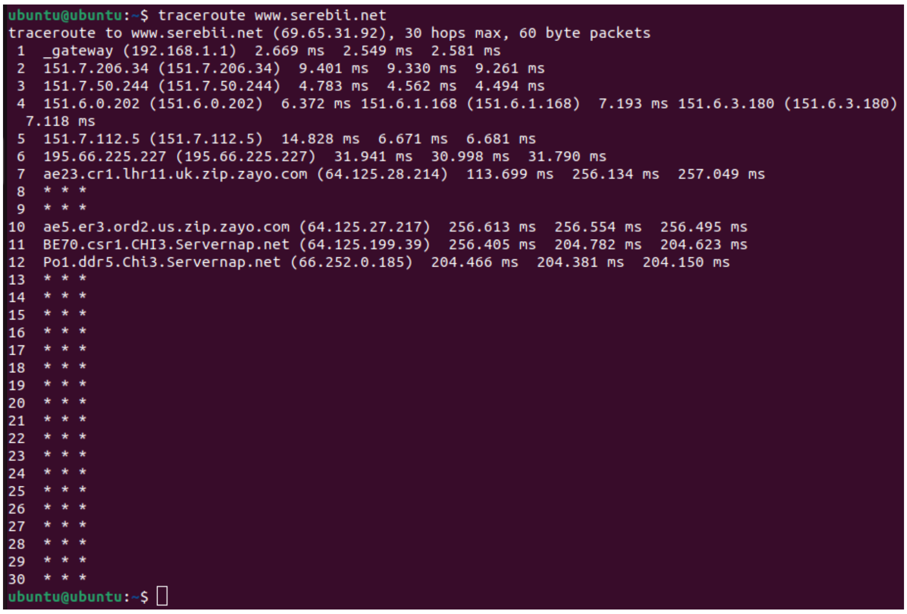
The IP address of the Access Point (AP) was not directly shown in the output of ifconfig. However, it was initially retrieved by checking the connection details from another device in the Wi-Fi settings section. The value was then confirmed by observing the first hop in the output of the traceroute command, which typically corresponds to the AP.



```
ubuntu@ubuntu:~$ traceroute www.google.com
traceroute to www.google.com (142.251.209.36), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  2.439 ms  2.326 ms  2.300 ms
 2  151.7.206.34 (151.7.206.34)  10.658 ms  10.652 ms  10.678 ms
 3  151.7.50.244 (151.7.50.244)  5.171 ms 151.7.50.248 (151.7.50.248)  5.102 ms 151.7.50.244 (151.7.5
0.244)  5.031 ms
 4  151.6.3.180 (151.6.3.180)  6.949 ms 151.6.6.142 (151.6.6.142)  6.297 ms 151.6.0.202 (151.6.0.202)
  6.112 ms
 5  151.6.7.181 (151.6.7.181)  9.942 ms  9.527 ms 151.6.7.239 (151.6.7.239)  9.432 ms
 6  74.125.32.80 (74.125.32.80)  9.259 ms 72.14.202.254 (72.14.202.254)  6.063 ms  6.187 ms
 7  * * *
 8  142.251.235.179 (142.251.235.179)  9.383 ms 172.253.73.60 (172.253.73.60)  19.080 ms 142.251.235.
179 (142.251.235.179)  9.916 ms
 9  192.178.99.216 (192.178.99.216)  10.755 ms  10.314 ms mil04s51-in-f4.1e100.net (142.251.209.36)
19.389 ms
```

Figure 3: Traceroute to Google server showing the access point as the first hop.

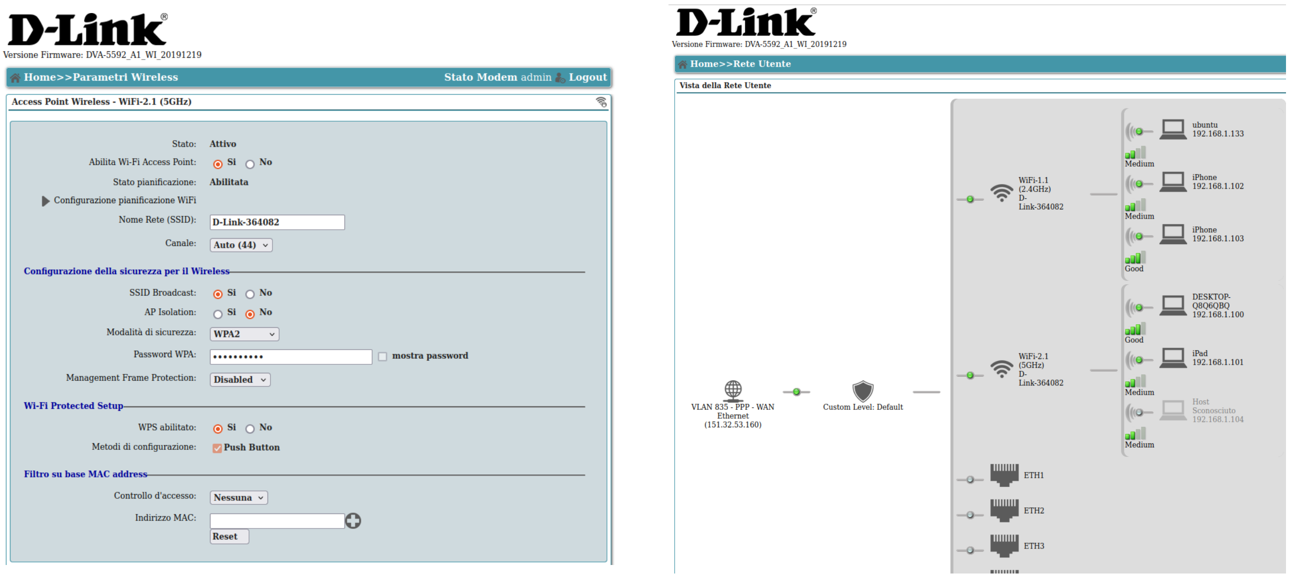
The output of the traceroute www.google.com command showed a list of IP addresses corresponding to the intermediate devices (called hops) between the local machine and the Google server. The first hop was the local router (Access Point) with IP address 192.168.1.1. After that, the output showed about 10 hops in total. Each hop represents a device on the network (like a router or a server) that forwards the data closer to the destination. For each hop, the command showed how long the data took to go and come back.



```
ubuntu@ubuntu:~$ traceroute www.serebii.net
traceroute to www.serebii.net (69.65.31.92), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  2.669 ms  2.549 ms  2.581 ms
 2  151.7.206.34 (151.7.206.34)  9.401 ms  9.330 ms  9.261 ms
 3  151.7.50.244 (151.7.50.244)  4.783 ms  4.562 ms  4.494 ms
 4  151.6.0.202 (151.6.0.202)  6.372 ms 151.6.1.168 (151.6.1.168)  7.193 ms 151.6.3.180 (151.6.3.180)
  7.118 ms
 5  151.7.112.5 (151.7.112.5)  14.828 ms  6.671 ms  6.681 ms
 6  195.66.225.227 (195.66.225.227)  31.941 ms  30.998 ms  31.790 ms
 7  ae23.cr1.lhr11.uk.zip.zayo.com (64.125.28.214)  113.699 ms  256.134 ms  257.049 ms
 8  * * *
 9  * * *
10  ae5.er3.ord2.us.zip.zayo.com (64.125.27.217)  256.613 ms  256.554 ms  256.495 ms
11  BE70.csr1.CHI3.Servernap.net (64.125.199.39)  256.405 ms  204.782 ms  204.623 ms
12  Po1.ddr5.Chi3.Servernap.net (66.252.0.185)  204.466 ms  204.381 ms  204.150 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
ubuntu@ubuntu:~$ 
```

Figure 4: Traceroute to Polito server with hidden intermediate hops due to encryption.

In the traceroute to www.serebii.net, the first hop is again the Access Point (192.168.1.1). However, from hop 13 to 30, the output shows only asterisks (*). This means that those devices on the path did not reply to the traceroute requests. This usually happens because some routers block these requests for security reasons, so the traceroute cannot show all the intermediate steps.



Versione Firmware: DVA-5592_A1_WI_20191219

Access Point Wireless - WiFi-2.1 (5GHz)

Stato: Attivo
Abilita Wi-Fi Access Point: ● Si ○ No
Stato pianificazione: Abilitata
▶ Configurazione pianificazione WiFi
Nome Rete (SSID): D-Link-364082
Canale: Auto (44)

Configurazione della sicurezza per il Wireless

SSID Broadcast: ● Si ○ No
AP Isolation: ○ Si ● No
Modalità di sicurezza: WPA2
Password WPA: •••••••••• □ mostra password
Management Frame Protection: Disabled

Wi-Fi Protected Setup

WPS abilitato: ● Si ○ No
Metodi di configurazione: ☑ Push Button

Filtro su base MAC address

Controllo d'accesso: Nessuna
Indirizzo MAC:
Reset

Versione Firmware: DVA-5592_A1_WI_20191219

Vista della Rete Utente

VLAN 835 - PPP - WAN Ethernet (151.32.53.160)
Custom Level: Default
WiFi-1.1 (2.4GHz) D-Link-364082
ubuntu 192.168.1.133
Medium
iPhone 192.168.1.102
Medium
iPhone 192.168.1.103
Good
WiFi-2.1 (5GHz) D-Link-364082
DESKTOP-Q8Q6QBQ 192.168.1.100
Good
iPad 192.168.1.101
Medium
Host Sconosciuto 192.168.1.104
Medium
ETH1
ETH2
ETH3

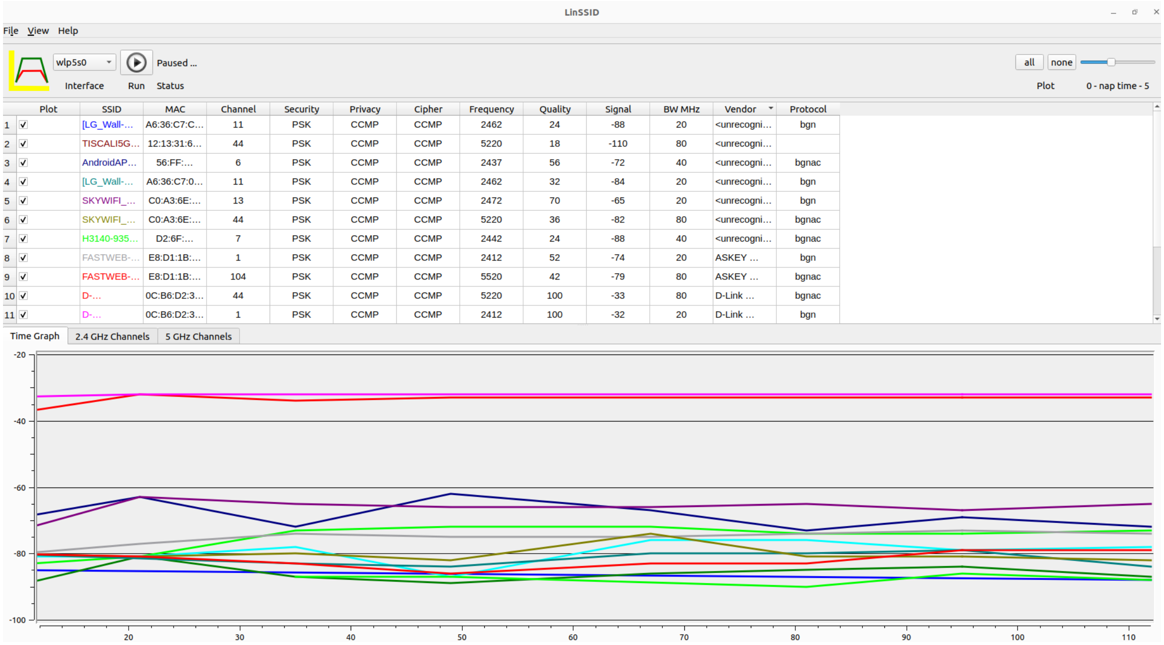
Figure 5: Various screenshots of the AP configuration page, showing different aspects of the home page and settings.

2 Wi-Fi Scanning

A Wi-Fi scan was performed using the command `sudo iw dev wlp5s0 scan`. For each of the 14 detected BSSIDs reported in Table 1, along with their corresponding SSIDs, detailed information such as signal strength, frequency, and channel was available. These data help to understand the wireless environment.

No.	BSSID	SSID
1	12:13:31:66:f1:d3	TISCALI5G-66F1D3
2	3c:a6:2f:61:fb:fa	FRITZ!Box 7530 IG-5G
3	e8:d1:1b:c1:ef:5d	FASTWEB-X3V0MV
4	0c:b6:d2:36:40:85	D-Link-364082
5	10:13:31:66:f1:cb	TISCALI-66F1CB
6	c0:4a:00:65:f1:76	TP-LINK_65F176
7	0c:b6:d2:36:40:83	D-Link-364082
8	6a:14:01:88:7b:69	DIRECT-Bc-BRAVIA
9	c0:a3:6e:b8:54:6c	SKYWIFI_CP7HG
10	a6:36:c7:c4:05:6a	[LG_Wall-Mount A/C]056a
11	3c:a6:2f:61:fb:f9	FRITZ!Box 7530 IG
12	a6:36:c7:0d:ed:3d	[LG_Wall-Mount A/C]ed3d
13	3a:0d:48:55:ab:36	Luigi S25 Ultra
14	5c:51:81:6a:1f:ff	AndroidAP1FFF

Table 1: List of Wi-Fi networks with corresponding BSS and SSID



	Plot	SSID	MAC	Channel	Security	Privacy	Cipher	Frequency	Quality	Signal	BW MHz	Vendor	Protocol
1	☑	[LG_Wall-...	A6:36:C7:C...	11	PSK	CCMP	CCMP	2462	24	-88	20	<unrecogni...	bgn
2	☑	TISCALI5G...	12:13:31:6...	44	PSK	CCMP	CCMP	5220	18	-110	80	<unrecogni...	
3	☑	AndroidAP...	56:FF:...	6	PSK	CCMP	CCMP	2437	56	-72	40	<unrecogni...	bgnac
4	☑	[LG_Wall-...	A6:36:C7:0...	11	PSK	CCMP	CCMP	2462	32	-84	20	<unrecogni...	bgn
5	☑	SKYWIFI_...	C0:A3:6E:...	13	PSK	CCMP	CCMP	2472	70	-65	20	<unrecogni...	bgn
6	☑	SKYWIFI_...	C0:A3:6E:...	44	PSK	CCMP	CCMP	5220	36	-82	80	<unrecogni...	bgnac
7	☑	H3140-935...	D2:6F:...	7	PSK	CCMP	CCMP	2442	24	-88	40	<unrecogni...	bgnac
8	☑	FASTWEB-...	E8:D1:1B:...	1	PSK	CCMP	CCMP	2412	52	-74	20	ASKEY ...	bgn
9	☑	FASTWEB-...	E8:D1:1B:...	104	PSK	CCMP	CCMP	5520	42	-79	80	ASKEY ...	bgnac
10	☑	D-...	0C:B6:D2:3...	44	PSK	CCMP	CCMP	5220	100	-33	80	D-Link ...	bgnac
11	☑	D-...	0C:B6:D2:3...	1	PSK	CCMP	CCMP	2412	100	-32	20	D-Link ...	bgn

Figure 6: Detected Wi-Fi networks displayed via `LinSSID`.

We performed four measurements in the main areas of the house: the bathroom, near the access point, the bedroom, and the balcony. An example screenshot of one of the tests inside a room is shown in Figure 6.

The collected data were processed to produce histograms displaying the channel occupancy for each measurement, as presented in Figure 7. The analysis revealed that the four most frequently used channels are 1, 6, 11, and 44, except at the farthest point from the access point, where channel 44 is replaced by channel 64.

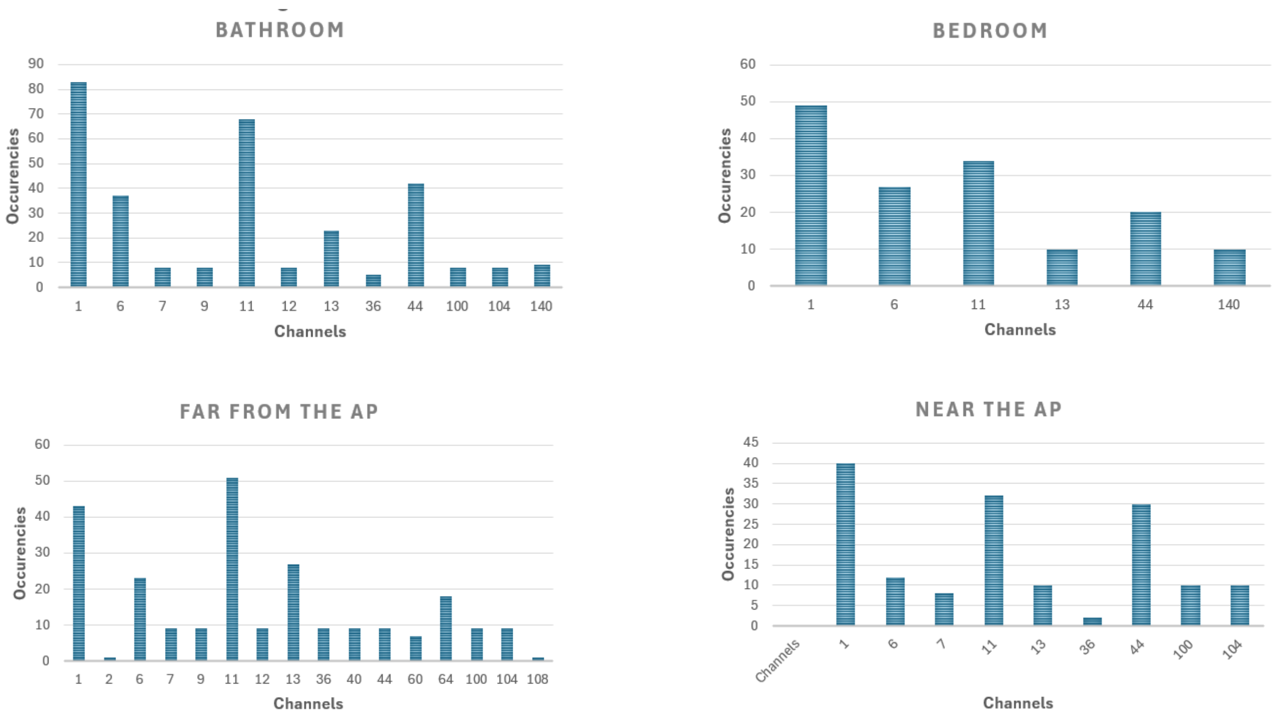


Figure 7: Distribution of Wi-Fi channels across various locations in the apartment.

Channels 1, 6, and 11 are commonly the most used because they are non-overlapping channels in the 2.4 GHz band, which helps minimize interference between networks. The presence of channels 44 and 64 in the 5 GHz band reflects the use of higher-frequency channels that generally experience less congestion but have shorter range, explaining their variation with location.

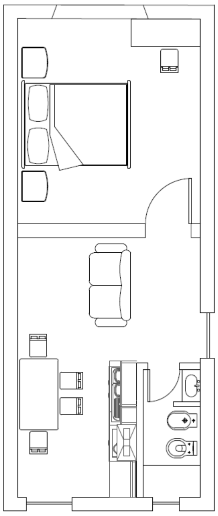


Figure 8: 2D Floor Plan of the House with Measurement Points

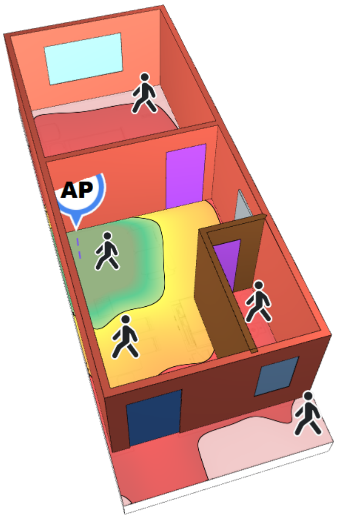


Figure 9: 3D Representation of Measurement Points and Signal Quality

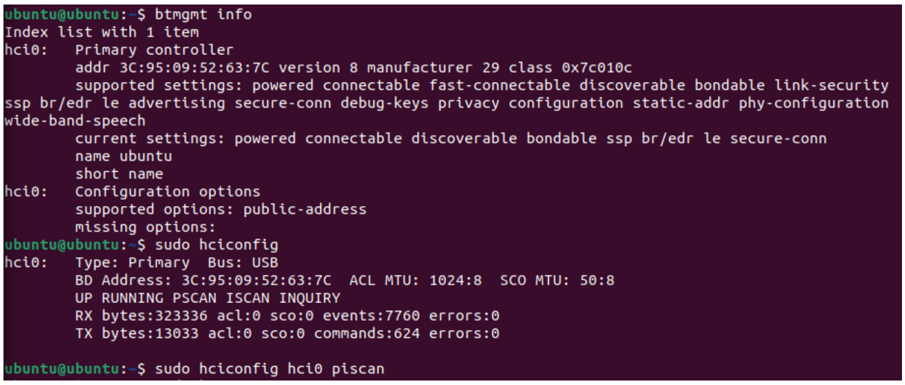
In the 3D map, all Wi-Fi scan points are shown, including an extra measurement in the kitchen to better capture signal behavior throughout the house. Using AutoCAD, we recreated the floor plan and, with Wi-Fi analysis software, generated a simulated 3D signal distribution map based on measurements from both the 5220 MHz and 2412 MHz channels of the D-Link-364082 network, with doors and windows closed (Figures 8 and 9).

Measurement Point	Signal Strength Range (dBm)	Link Quality (%)	Color on Map
Near to AP	–41 to –28 dBm	100%	Green
Kitchen	–59 to –48 dBm	73–94%	Yellow
Bathroom	–72 to –56 dBm	56–88%	Red
Bedroom	–71 to –57 dBm	58–86%	Red
Far from AP	–110 to –70 dBm	40–60%	Pink

Table 2: Wi-Fi Signal Strength and Link Quality by Measurement Point

Table 2 reports the average signal strength and link quality at each measurement point. The best link quality is near the Access Point (AP), with strong signal (-41 to -28 dBm) and 100% link quality due to proximity and fewer obstacles. The worst quality is at the farthest point, where signal drops significantly (-110 to -70 dBm) and link quality falls to 40–60%, affected by distance and walls. Intermediate rooms like the kitchen, bathroom, and bedroom show moderate values depending on distance and obstacles.

3 Basic Bluetooth tools

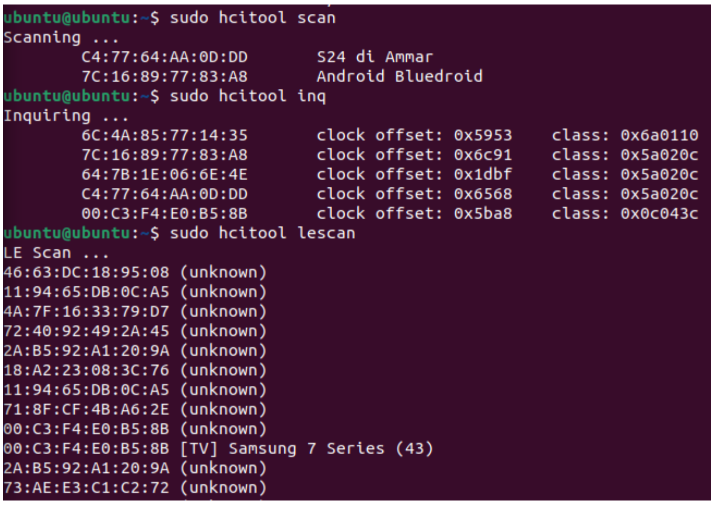


```
ubuntu@ubuntu:~$ btmgmt info
Index list with 1 item
hci0:   Primary controller
        addr 3C:95:09:52:63:7C version 8 manufacturer 29 class 0x7c010c
        supported settings: powered connectable fast-connectable discoverable bondable link-security
ssp br/edr le advertising secure-conn debug-keys privacy configuration static-addr phy-configuration
wide-band-speech
        current settings: powered connectable discoverable bondable ssp br/edr le secure-conn
        name ubuntu
        short name
hci0:   Configuration options
        supported options: public-address
        missing options:
ubuntu@ubuntu:~$ sudo hciconfig
hci0:   Type: Primary  Bus: USB
        BD Address: 3C:95:09:52:63:7C  ACL MTU: 1024:8  SCO MTU: 50:8
        UP RUNNING PSCAN ISCAN INQUIRY
        RX bytes:323336 acl:0 sco:0 events:7760 errors:0
        TX bytes:13033 acl:0 sco:0 commands:624 errors:0

ubuntu@ubuntu:~$ sudo hciconfig hci0 piscan
```

The system supports BLE, as shown by the “le” entry in **`btmgmt info`**. The interface is `hci0`, with MAC address `3C:95:09:52:63:7C`.

Figure 10: BLE support and interface info.



```
ubuntu@ubuntu:~$ sudo hcitool scan
Scanning ...
        C4:77:64:AA:0D:DD       S24 di Ammar
        7C:16:89:77:83:A8       Android Bluedroid
ubuntu@ubuntu:~$ sudo hcitool inq
Inquiring ...
        6C:4A:85:77:14:35       clock offset: 0x5953    class: 0x6a0110
        7C:16:89:77:83:A8       clock offset: 0x6c91    class: 0x5a020c
        64:7B:1E:06:6E:4E       clock offset: 0x1dbf    class: 0x5a020c
        C4:77:64:AA:0D:DD       clock offset: 0x6568    class: 0x5a020c
        00:C3:F4:E0:B5:8B       clock offset: 0x5ba8    class: 0x0c043c
ubuntu@ubuntu:~$ sudo hcitool lescan
LE Scan ...
46:63:DC:18:95:08 (unknown)
11:94:65:DB:0C:A5 (unknown)
4A:7F:16:33:79:D7 (unknown)
72:40:92:49:2A:45 (unknown)
2A:B5:92:A1:20:9A (unknown)
18:A2:23:08:3C:76 (unknown)
11:94:65:DB:0C:A5 (unknown)
71:8F:CF:4B:A6:2E (unknown)
00:C3:F4:E0:B5:8B (unknown)
00:C3:F4:E0:B5:8B [TV] Samsung 7 Series (43)
2A:B5:92:A1:20:9A (unknown)
73:AE:E3:C1:C2:72 (unknown)
```

After enabling discoverable mode with **`hciconfig hci0 piscan`**, the commands **`scan`**, **`inq`**, and **`lescan`** were executed. The first two detected classic Bluetooth devices (with **`inq`** also showing additional info), while **`lescan`** listed only BLE devices. Not all scans returned the same devices, highlighting functional differences and limitations of the outdated

Figure 11: Bluetooth scanning with hcitool.