802.11 Fundamental

Beacon, Probe, Authentication, Association

MUM Myanmar 2019

ALAGAS NETWORK
www.mikrotik.sg

AlagasNetwork

ABOUT ME

I am Soragan Ong

I am MikroTik Certified Trainer

I work for Alagas Network

WHO IS ALAGAS NETWORK?

- MikroTik Value Added Distributor based in Singapore
- Distributing MikroTik since 2010
- 2Gbps in Singapore in 2014, second in the world after Japan
- MikroTik Training Centre Since 2016

802.11

WHAT IS 802.11?

- Family specification of Wireless LAN
- Developed by IEEE
- Origins in 1985 by FCC

802.11ad

802.11aj

802.11j

802.11ah

802.11n

802.11a

802.11-1997

802.11g

802.11af

802.11b

802.11y

802.11ay

802.11p

802.11ac

ESTABLISHING WIRELESS CONNECTION

- Beacons

  Networks to advertise presence

- Probes

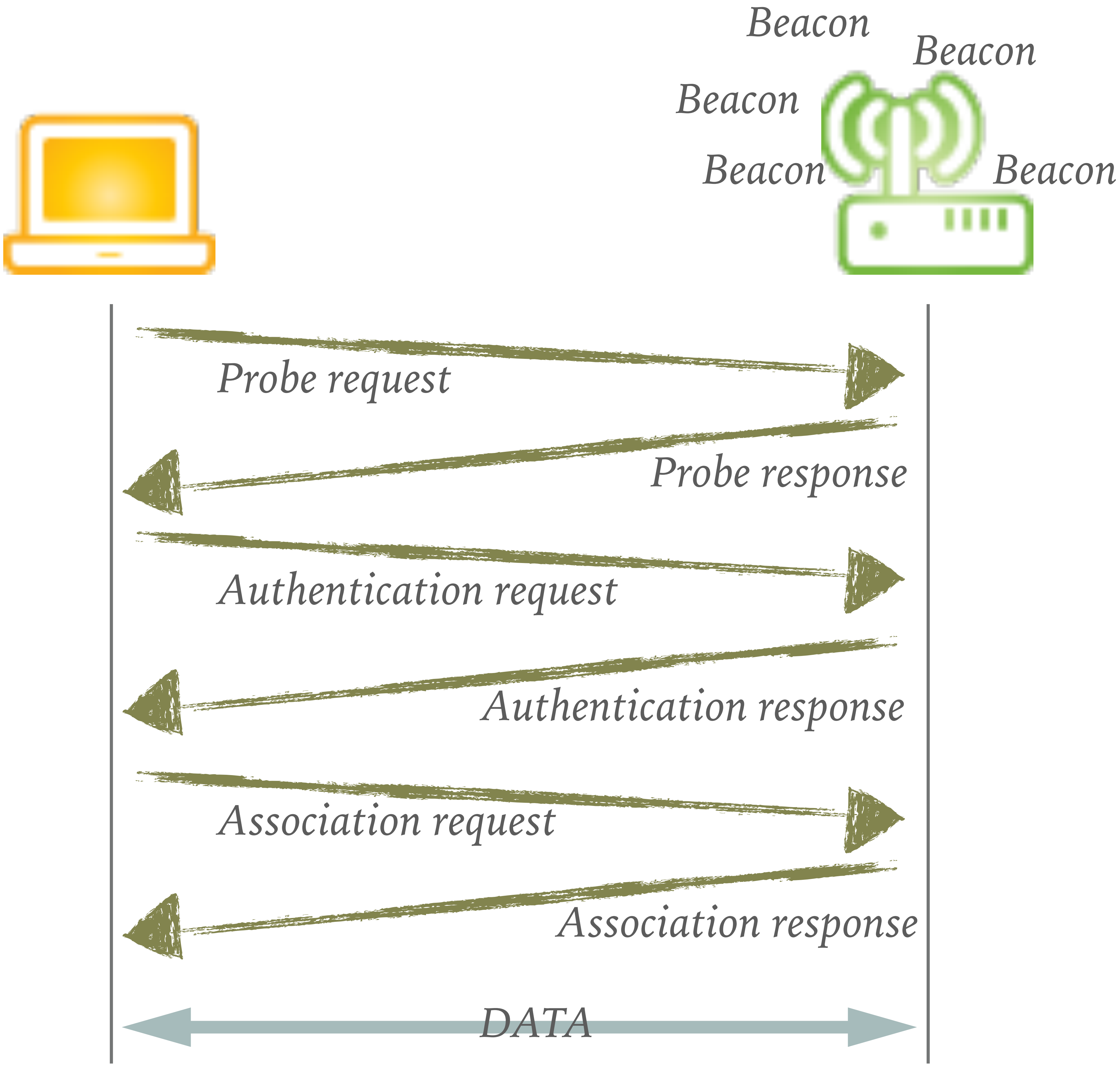
  Clients to find networks

- Authentication

  Verify that the client is allowed to join network

- Association

  Established data link between Access Point and Station



Beacon

Beacon

Beacon

Beacon

Beacon

Probe request

Probe response

Authentication request

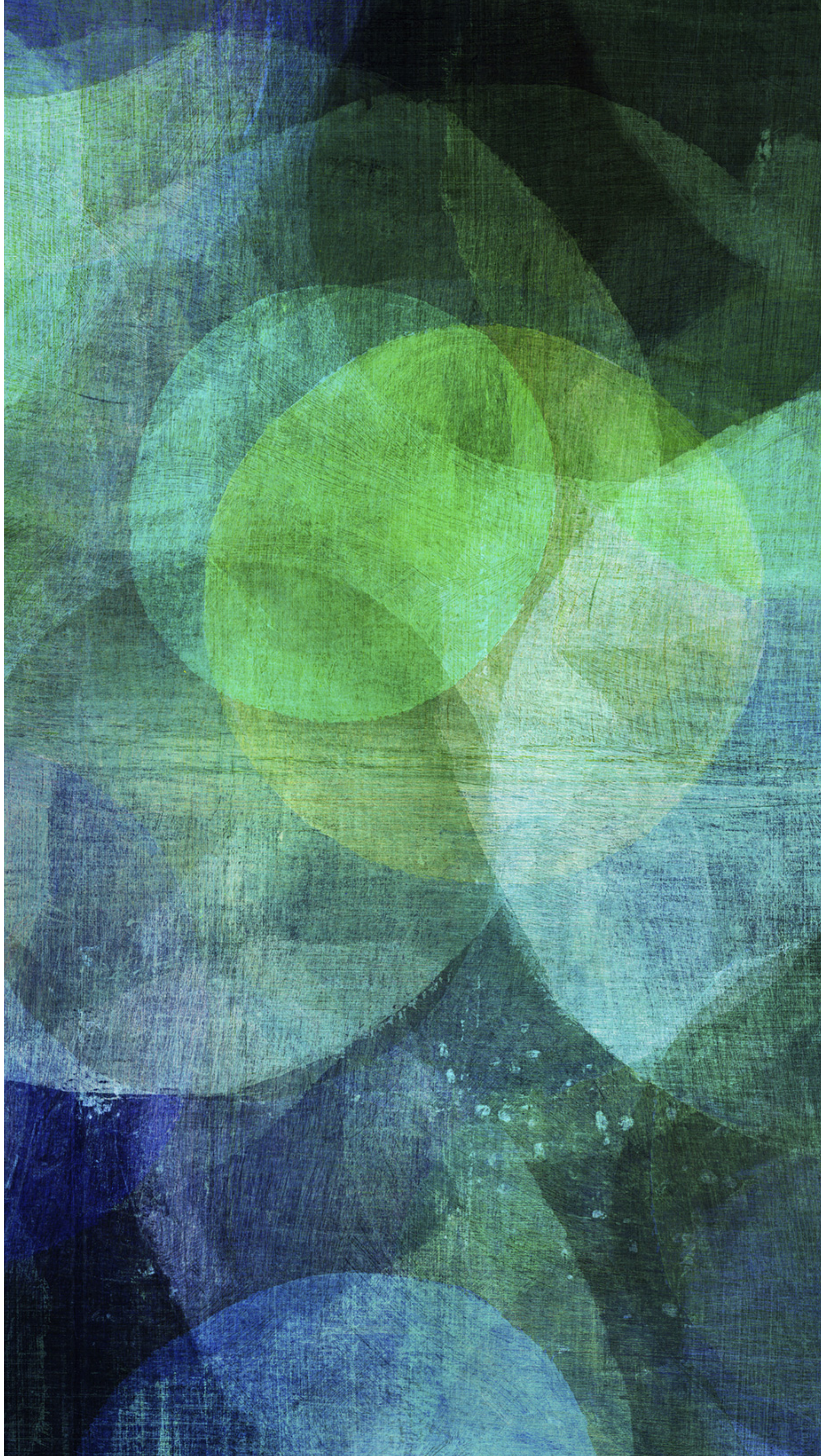
Authentication response

Association request

Association response

DATA

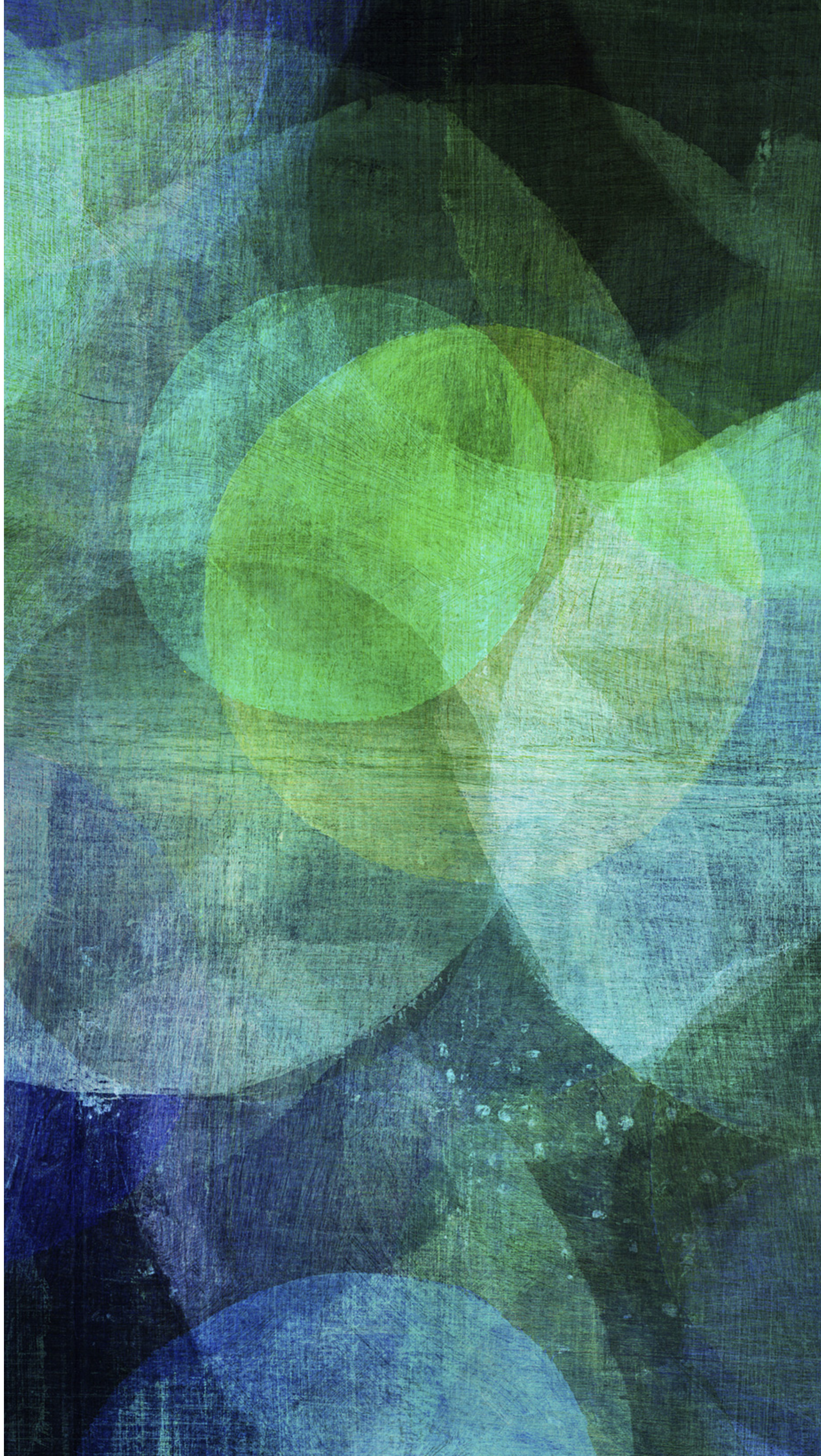
BEACONS



BEACONS

- Broadcast regularly, typically every 100ms
- Frames contain: SSID, BSSID
- Supported Rates, Parameters (Channel, Security, etc)

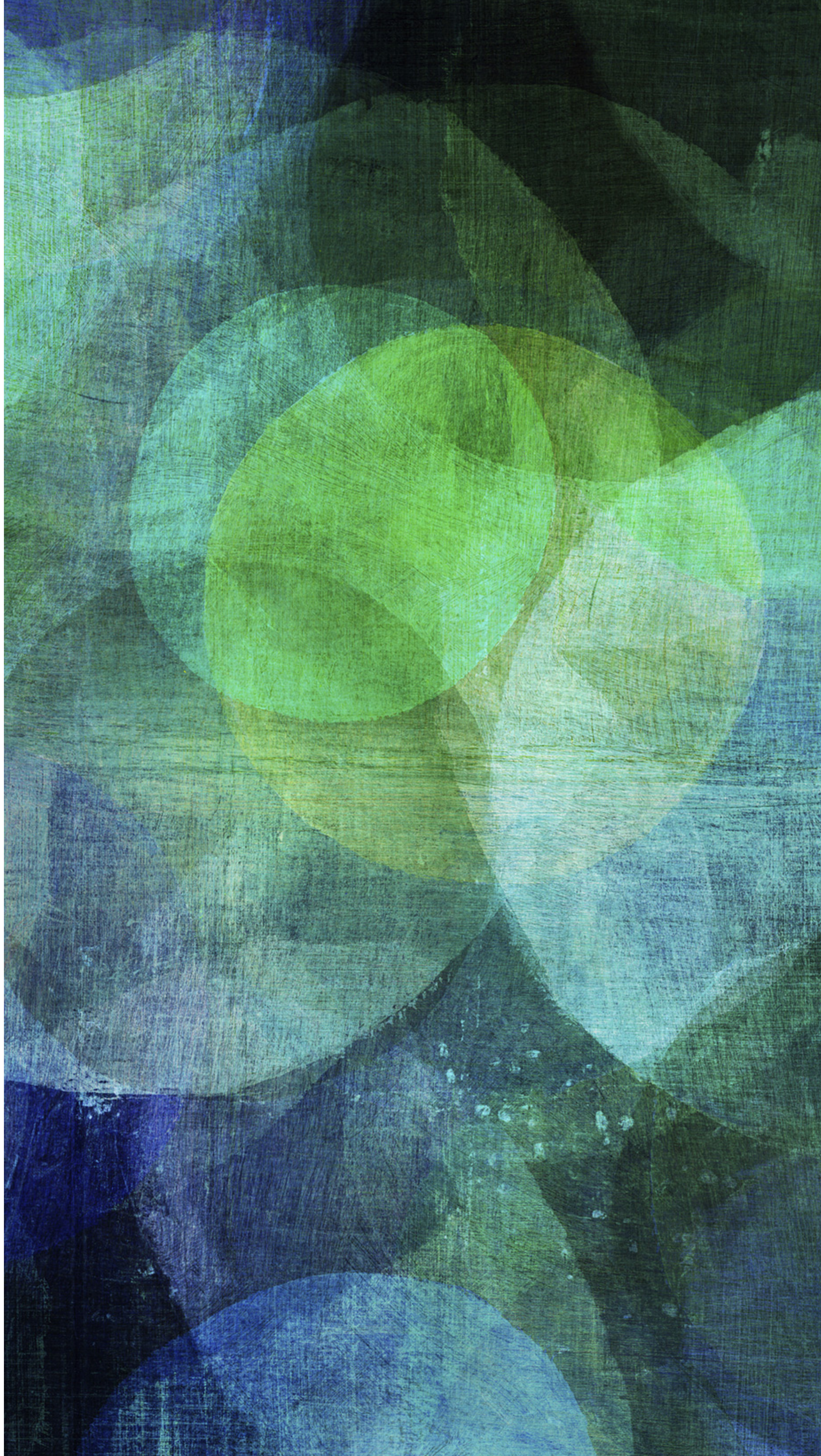
PROBES



PROBES

- Search for specific network
- Multiple Channel
- Contain network name (SSID) and bit rates

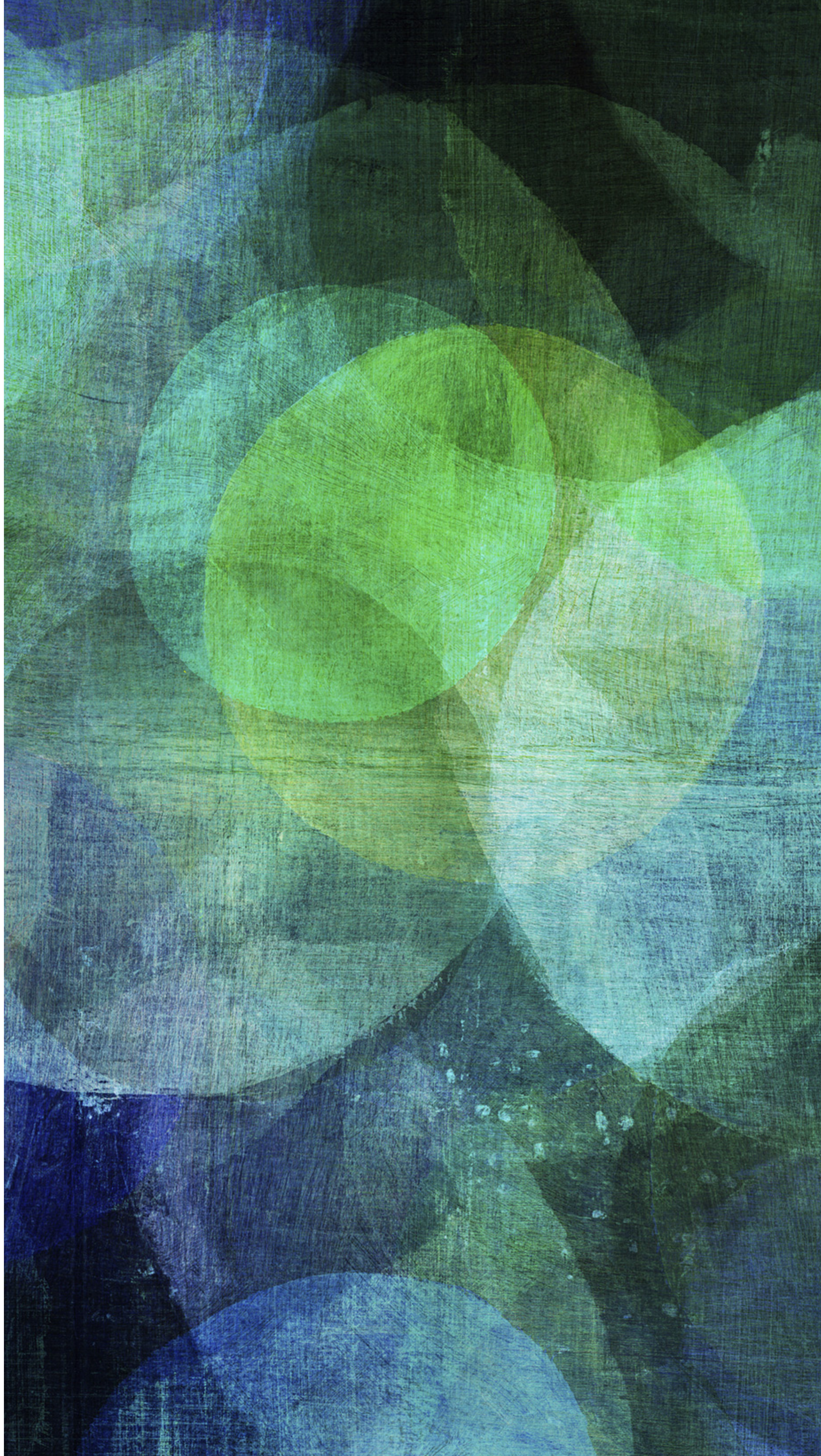
AUTHENTICATION



AUTHENTICATION

- Verify client has access to join the network
- If key is used
  - Authentication Request with Cleartext Challenge
  - Authentication Request with Encrypted Challenge

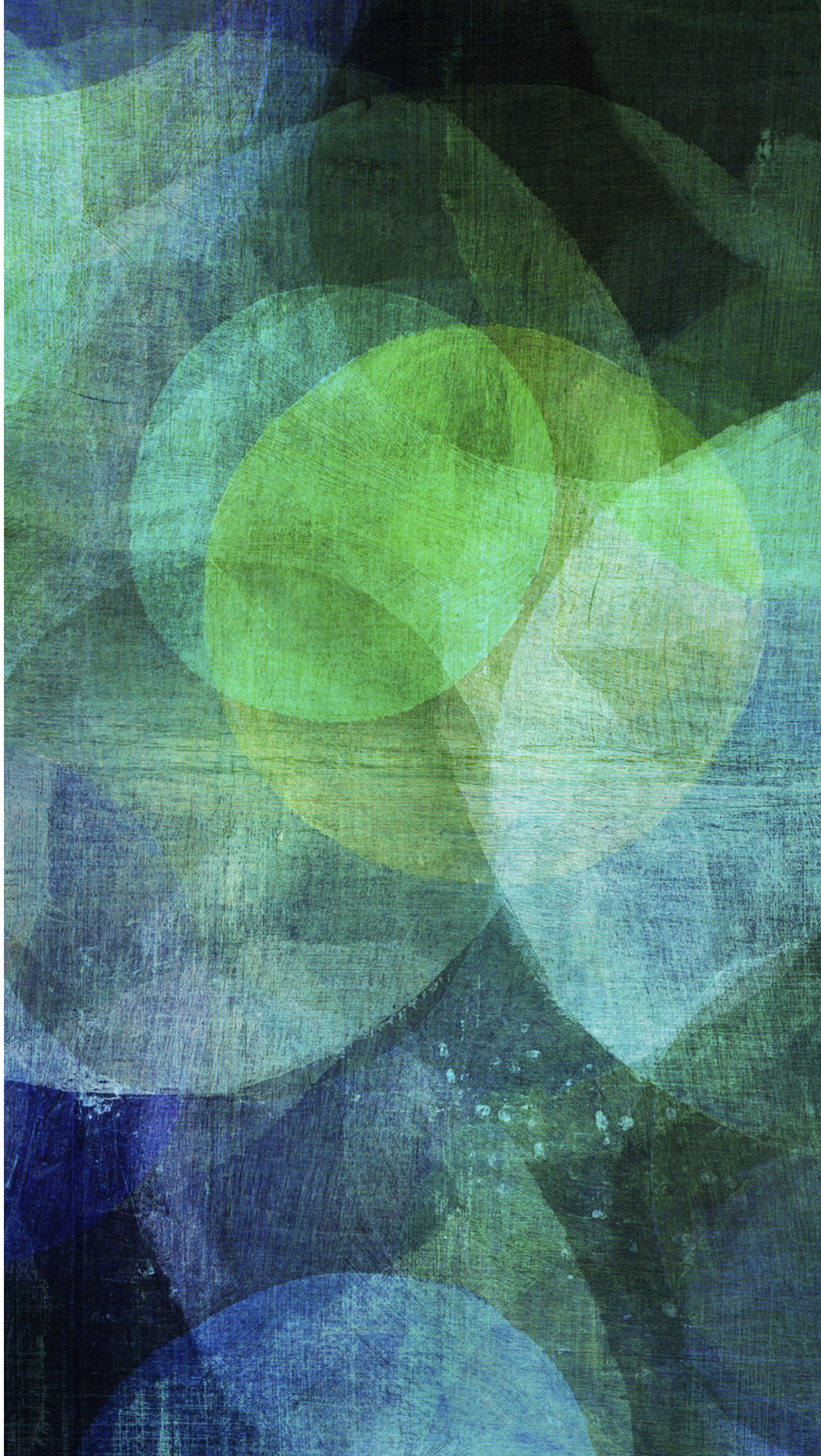
ASSOCIATION

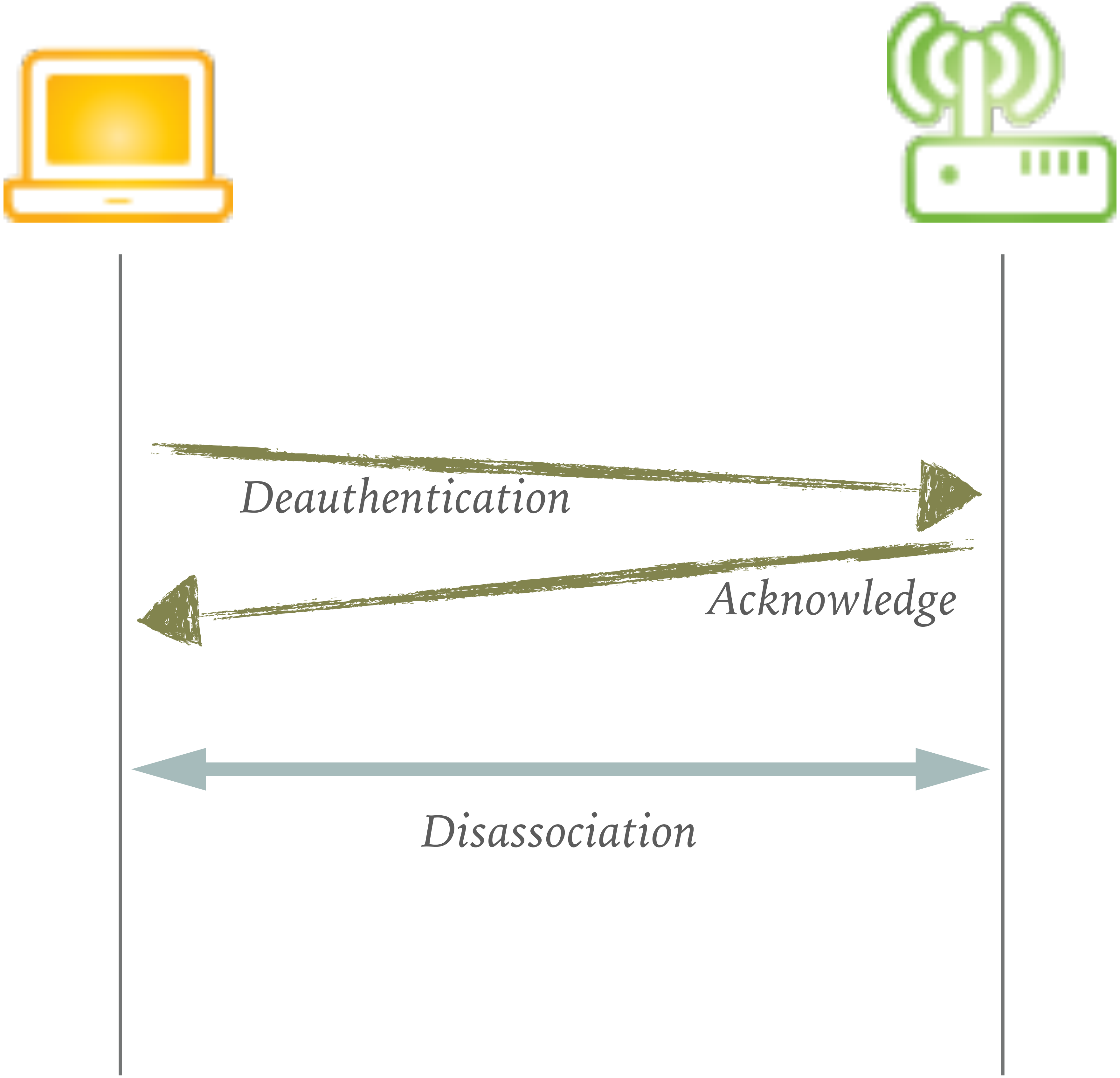


ASSOCIATION

- After client is authenticated
- Officially join the wireless network
- Data

LEAVING NETWORK

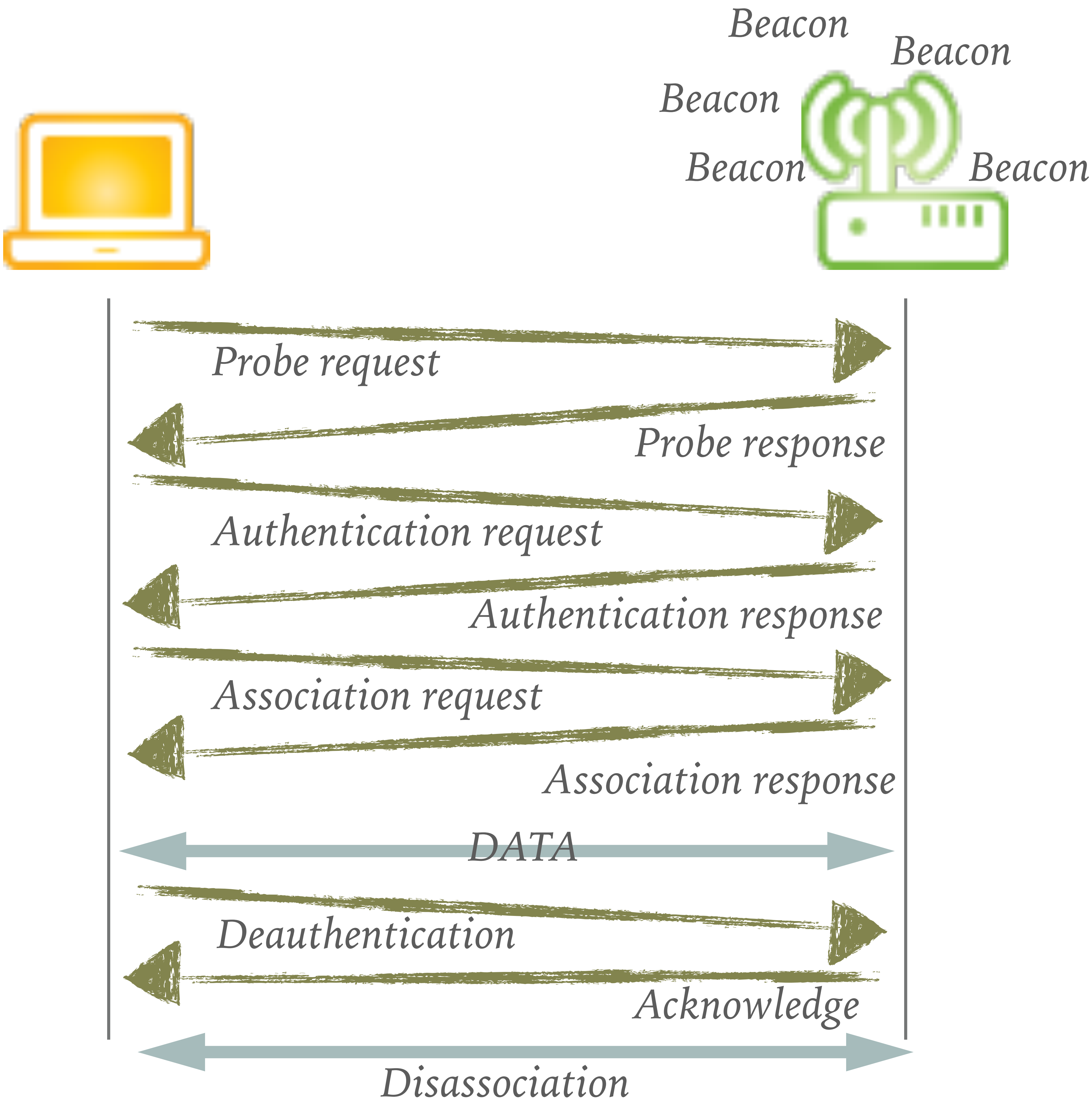




Deauthentication

Acknowledge

Disassociation


Beacon
Beacon
Beacon
Beacon
Beacon
Probe request
Probe response
Authentication request
Authentication response
Association request
Association response
DATA
Deauthentication
Acknowledge
Disassociation

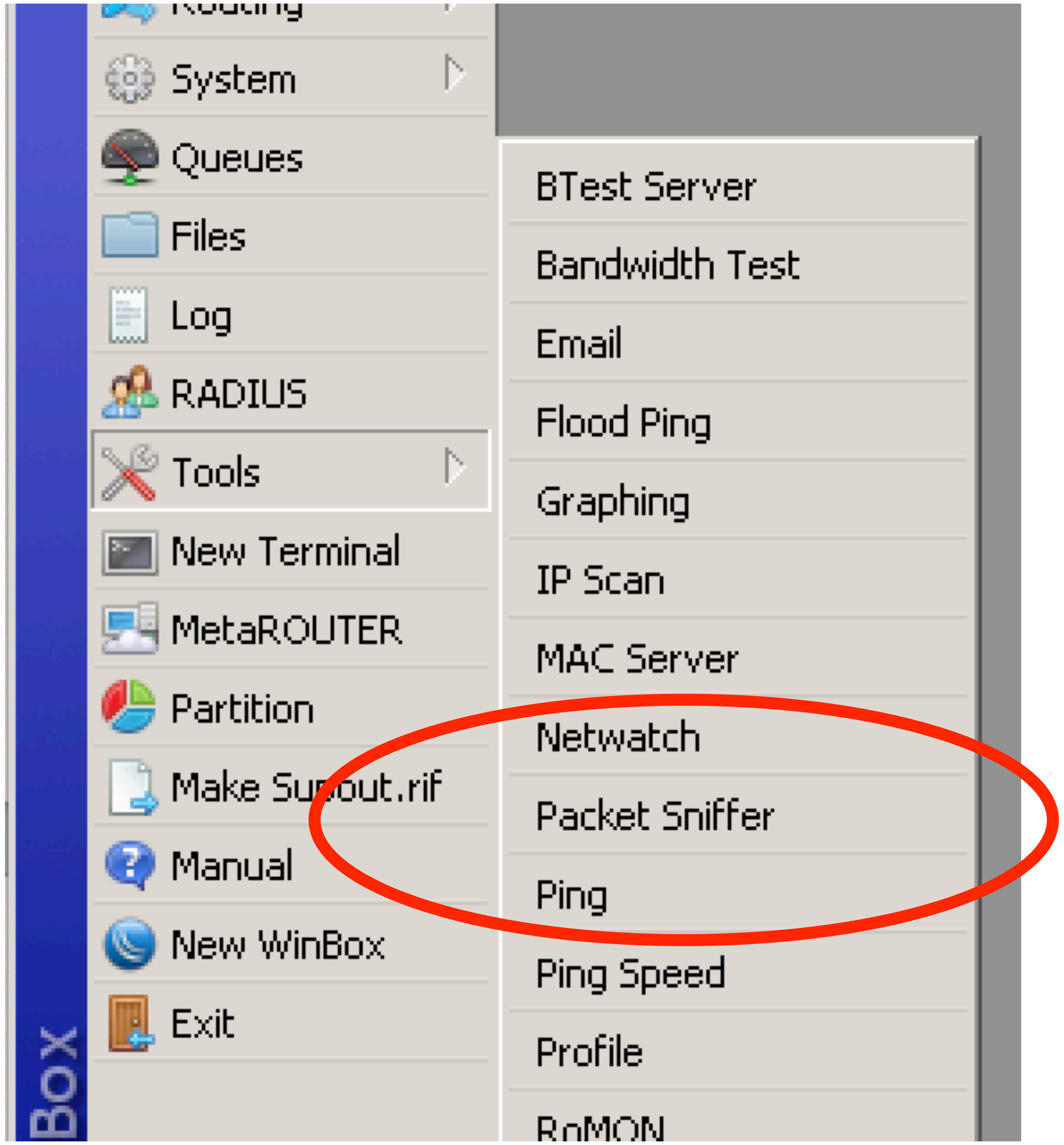
DEMO

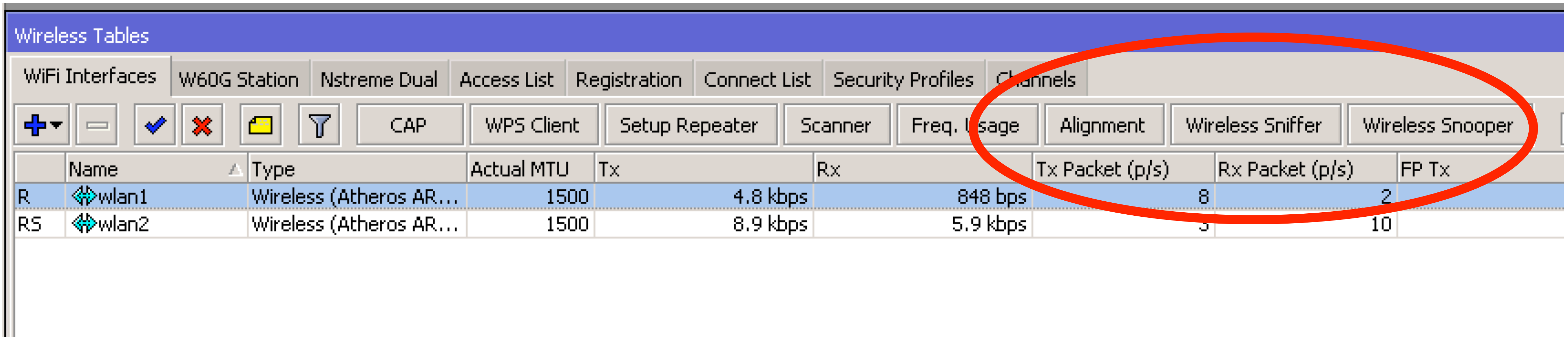
Let’s do it together!
Let’s attacked together!
Let’s fix together!

TOOLS FOR DEMO

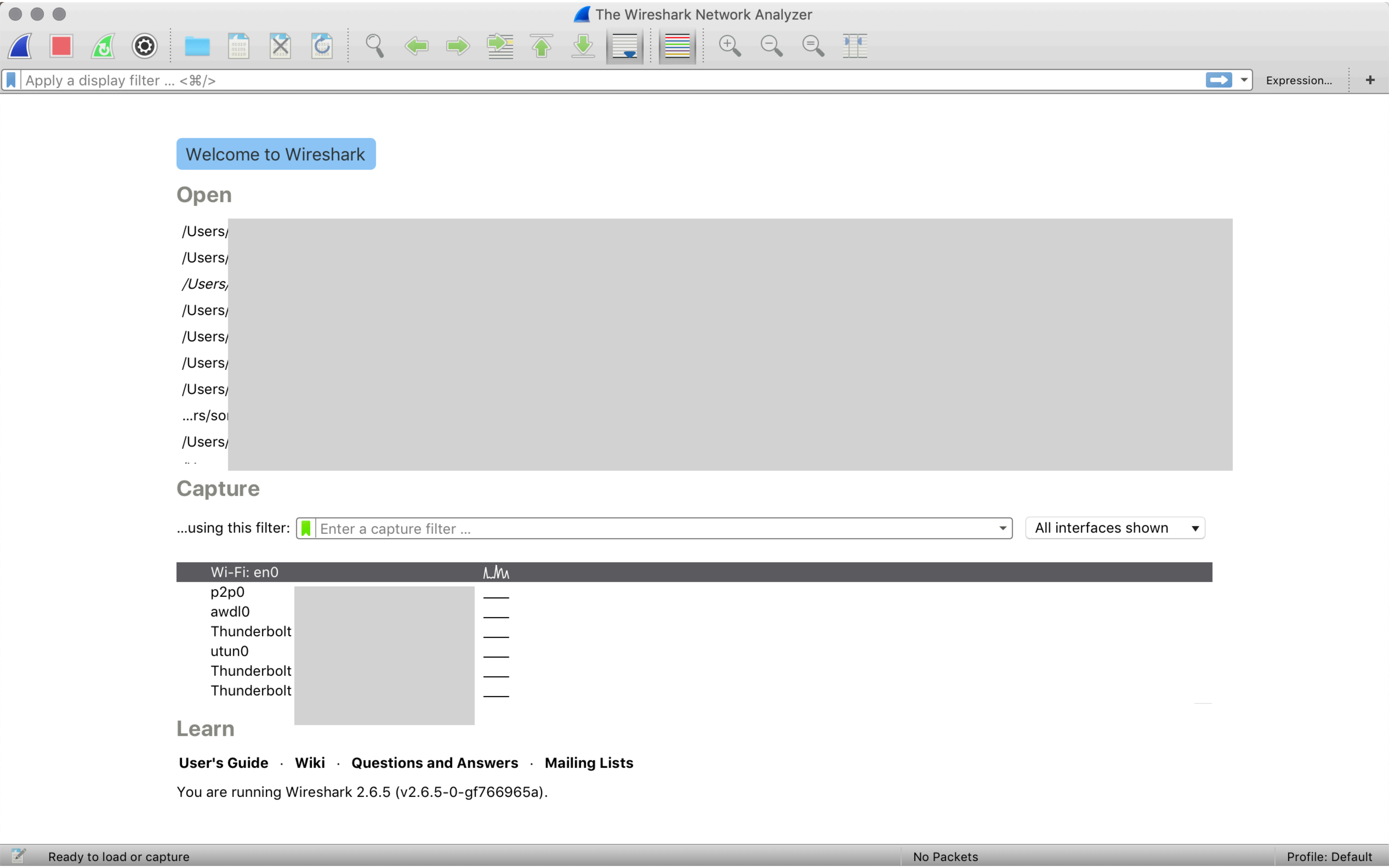
- Sniffer (Built-in)
- Wireshark (Free Download)
- An easily obtained attack device (US$9-12)

Sniffer Tool





	Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
R	wlan1	Wireless (Atheros AR...	1500	4.8 kbps	848 bps	8	2	
RS	wlan2	Wireless (Atheros AR...	1500	8.9 kbps	5.9 kbps	3	10	



Apply a display filter … <⌘/>

Welcome to Wireshark

Open

/Users/[redacted]
/Users/
/Users/
/Users/
/Users/
/Users/
/Users/
…rs/so
/Users/

Capture

…using this filter: Enter a capture filter …

All interfaces shown

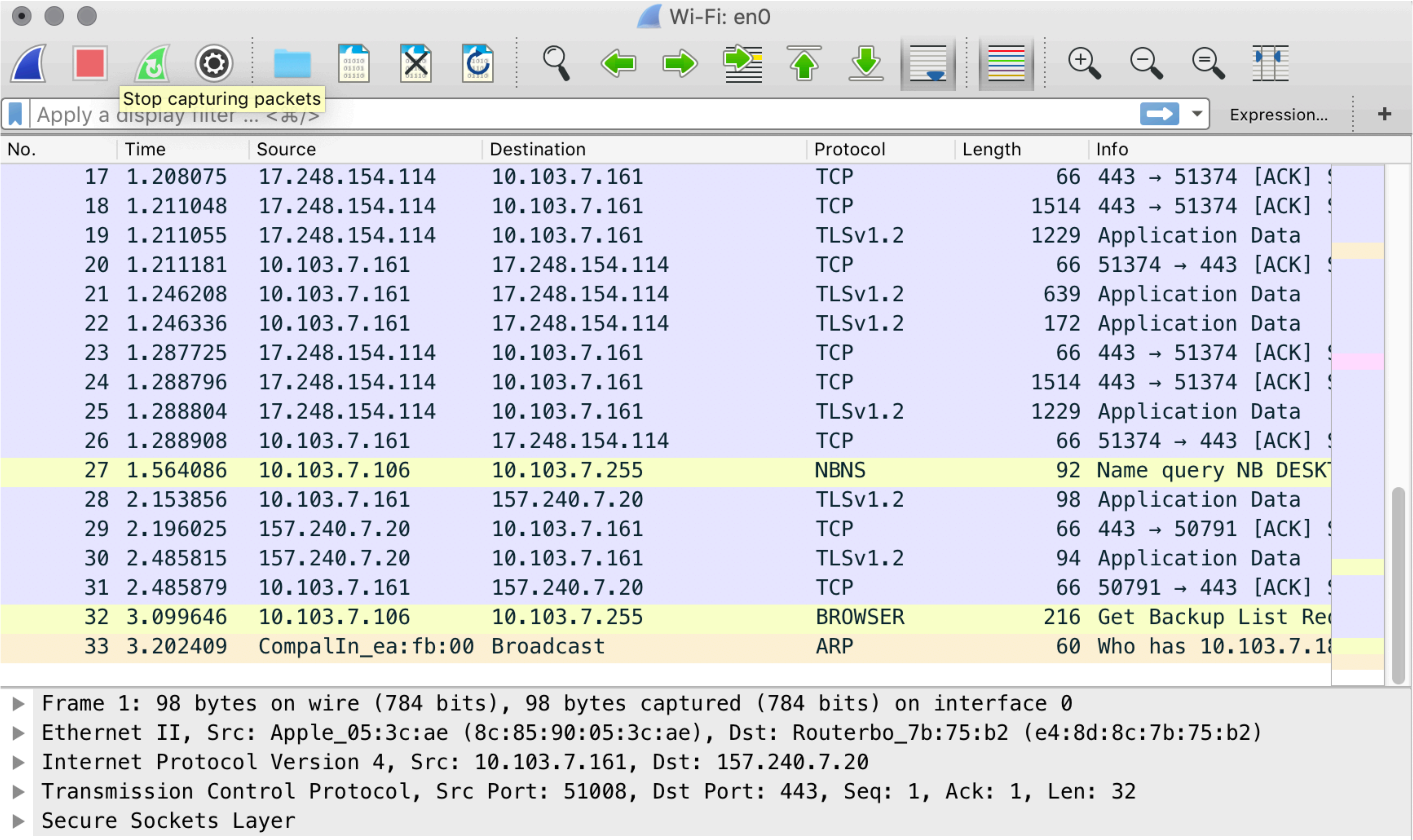
Wi-Fi: en0
p2p0 [redacted]
awdl0
Thunderbolt
utun0
Thunderbolt
Thunderbolt

Learn

User's Guide · **Wiki** · **Questions and Answers** · **Mailing Lists**

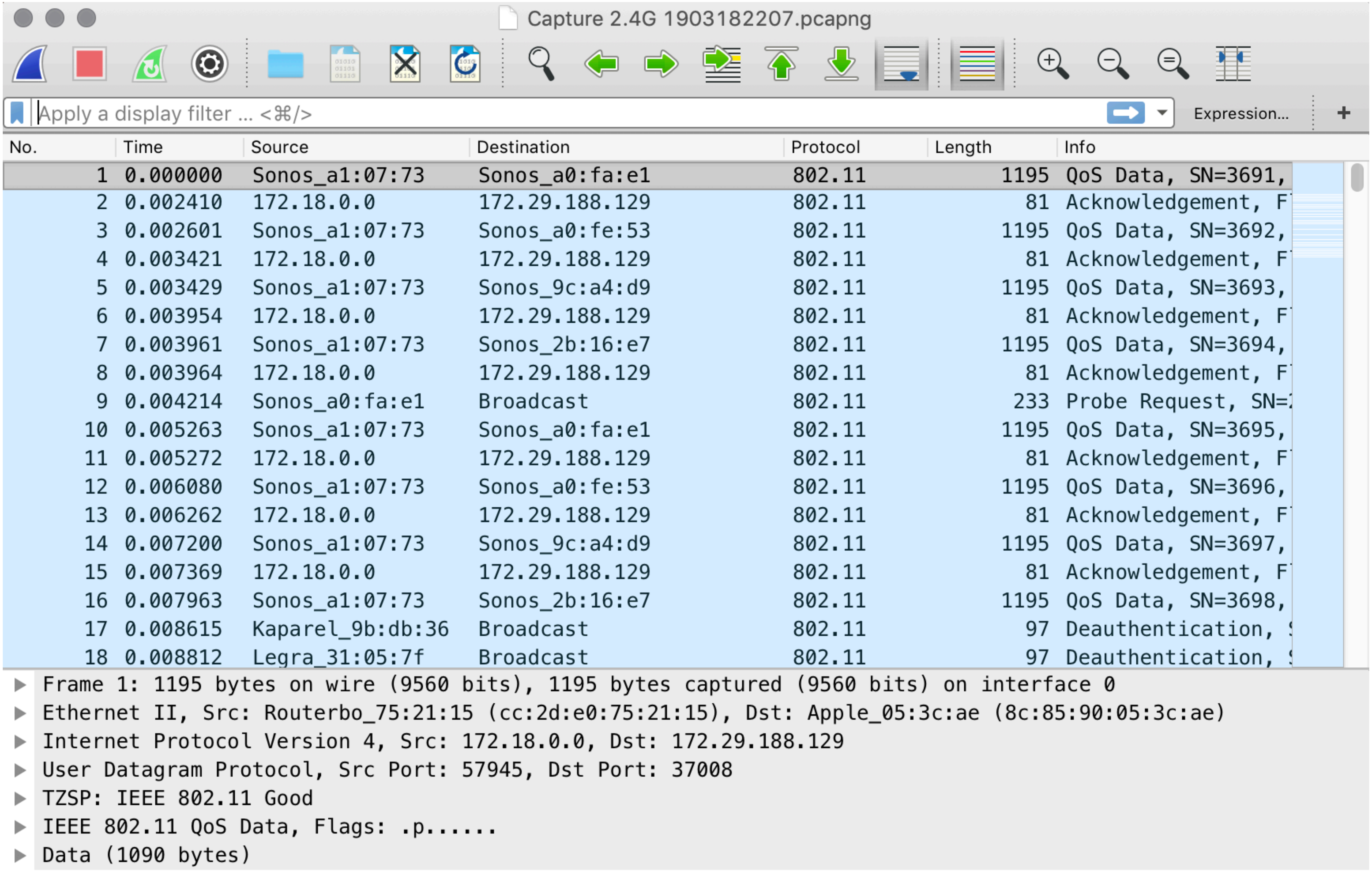
You are running Wireshark 2.6.5 (v2.6.5-0-gf766965a).

Ready to load or capture   No Packets   Profile: Default



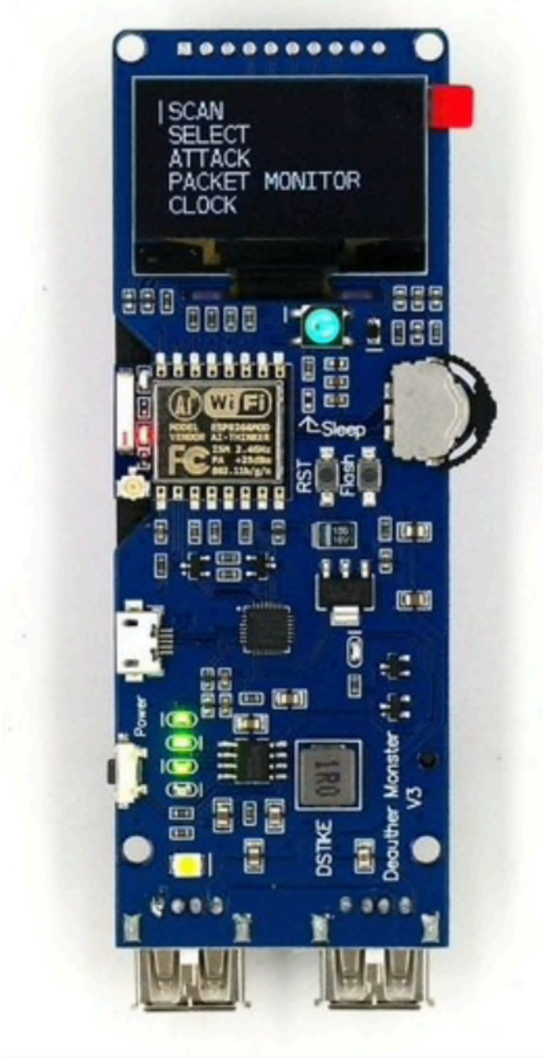
No.	Time	Source	Destination	Protocol	Length	Info
17	1.208075	17.248.154.114	10.103.7.161	TCP	66	443 → 51374 [ACK]
18	1.211048	17.248.154.114	10.103.7.161	TCP	1514	443 → 51374 [ACK]
19	1.211055	17.248.154.114	10.103.7.161	TLSv1.2	1229	Application Data
20	1.211181	10.103.7.161	17.248.154.114	TCP	66	51374 → 443 [ACK]
21	1.246208	10.103.7.161	17.248.154.114	TLSv1.2	639	Application Data
22	1.246336	10.103.7.161	17.248.154.114	TLSv1.2	172	Application Data
23	1.287725	17.248.154.114	10.103.7.161	TCP	66	443 → 51374 [ACK]
24	1.288796	17.248.154.114	10.103.7.161	TCP	1514	443 → 51374 [ACK]
25	1.288804	17.248.154.114	10.103.7.161	TLSv1.2	1229	Application Data
26	1.288908	10.103.7.161	17.248.154.114	TCP	66	51374 → 443 [ACK]
27	1.564086	10.103.7.106	10.103.7.255	NBNS	92	Name query NB DESK
28	2.153856	10.103.7.161	157.240.7.20	TLSv1.2	98	Application Data
29	2.196025	157.240.7.20	10.103.7.161	TCP	66	443 → 50791 [ACK]
30	2.485815	157.240.7.20	10.103.7.161	TLSv1.2	94	Application Data
31	2.485879	10.103.7.161	157.240.7.20	TCP	66	50791 → 443 [ACK]
32	3.099646	10.103.7.106	10.103.7.255	BROWSER	216	Get Backup List Re
33	3.202409	CompalIn_ea:fb:00	Broadcast	ARP	60	Who has 10.103.7.1

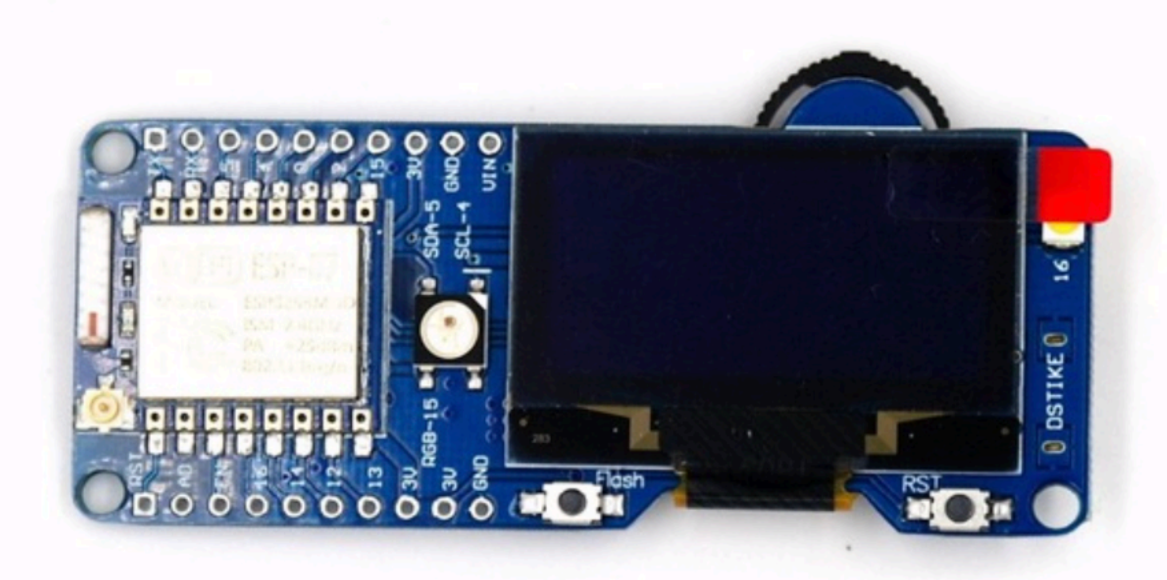
```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Apple_05:3c:ae (8c:85:90:05:3c:ae), Dst: Routerbo_7b:75:b2 (e4:8d:8c:7b:75:b2)
▶ Internet Protocol Version 4, Src: 10.103.7.161, Dst: 157.240.7.20
▶ Transmission Control Protocol, Src Port: 51008, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
▶ Secure Sockets Layer
```

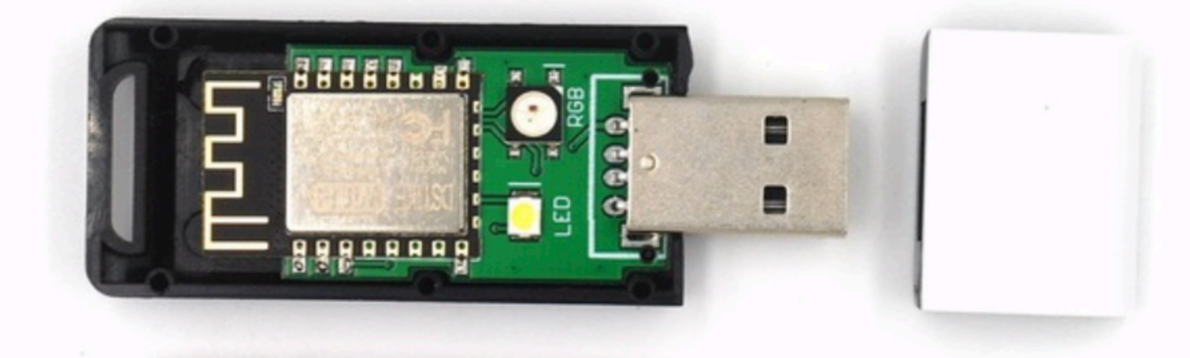


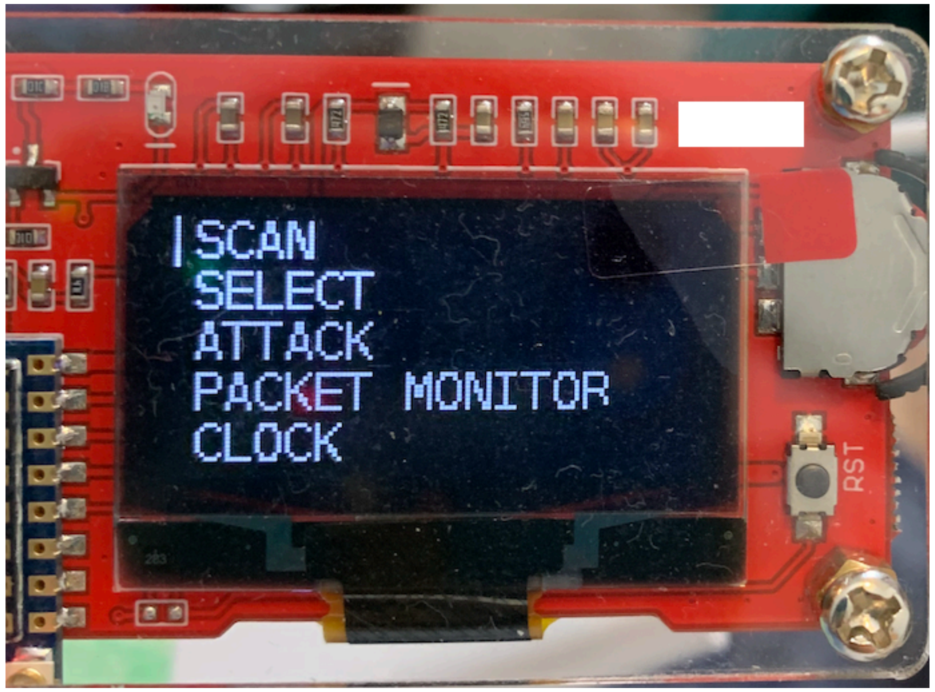
```
No.  Time      Source             Destination      Protocol  Length  Info
   1 0.000000  Sonos_a1:07:73     Sonos_a0:fa:e1   802.11      1195  QoS Data, SN=3691,
   2 0.002410  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
   3 0.002601  Sonos_a1:07:73     Sonos_a0:fe:53   802.11      1195  QoS Data, SN=3692,
   4 0.003421  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
   5 0.003429  Sonos_a1:07:73     Sonos_9c:a4:d9   802.11      1195  QoS Data, SN=3693,
   6 0.003954  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
   7 0.003961  Sonos_a1:07:73     Sonos_2b:16:e7   802.11      1195  QoS Data, SN=3694,
   8 0.003964  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
   9 0.004214  Sonos_a0:fa:e1     Broadcast        802.11       233  Probe Request, SN=
  10 0.005263  Sonos_a1:07:73     Sonos_a0:fa:e1   802.11      1195  QoS Data, SN=3695,
  11 0.005272  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
  12 0.006080  Sonos_a1:07:73     Sonos_a0:fe:53   802.11      1195  QoS Data, SN=3696,
  13 0.006262  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
  14 0.007200  Sonos_a1:07:73     Sonos_9c:a4:d9   802.11      1195  QoS Data, SN=3697,
  15 0.007369  172.18.0.0         172.29.188.129   802.11        81  Acknowledgement, F
  16 0.007963  Sonos_a1:07:73     Sonos_2b:16:e7   802.11      1195  QoS Data, SN=3698,
  17 0.008615  Kaparel_9b:db:36   Broadcast        802.11        97  Deauthentication,
  18 0.008812  Legra_31:05:7f     Broadcast        802.11        97  Deauthentication,
```

```
▶ Frame 1: 1195 bytes on wire (9560 bits), 1195 bytes captured (9560 bits) on interface 0
▶ Ethernet II, Src: Routerbo_75:21:15 (cc:2d:e0:75:21:15), Dst: Apple_05:3c:ae (8c:85:90:05:3c:ae)
▶ Internet Protocol Version 4, Src: 172.18.0.0, Dst: 172.29.188.129
▶ User Datagram Protocol, Src Port: 57945, Dst Port: 37008
▶ TZSP: IEEE 802.11 Good
▶ IEEE 802.11 QoS Data, Flags: .p......
▶ Data (1090 bytes)
```


SCAN
SELECT
ATTACK
PACKET MONITOR
CLOCK
Sleep
RST
Flash
Power
1R0
DSTIKE
Deauther Monster
V3


ESP-07
3V
GND
VIN
SDA-5
SCL-4
RGB-15
RST
Flash
RST
16
DSTIKE


RGB
LED


SCAN
SELECT
ATTACK
PACKET MONITOR
CLOCK
RST

LET’S DO IT

1. Access Point (SSID: IthinkIamSECURED)
2. Connect to the AP
3. Everything work just fine
4. Until…….

STEPS

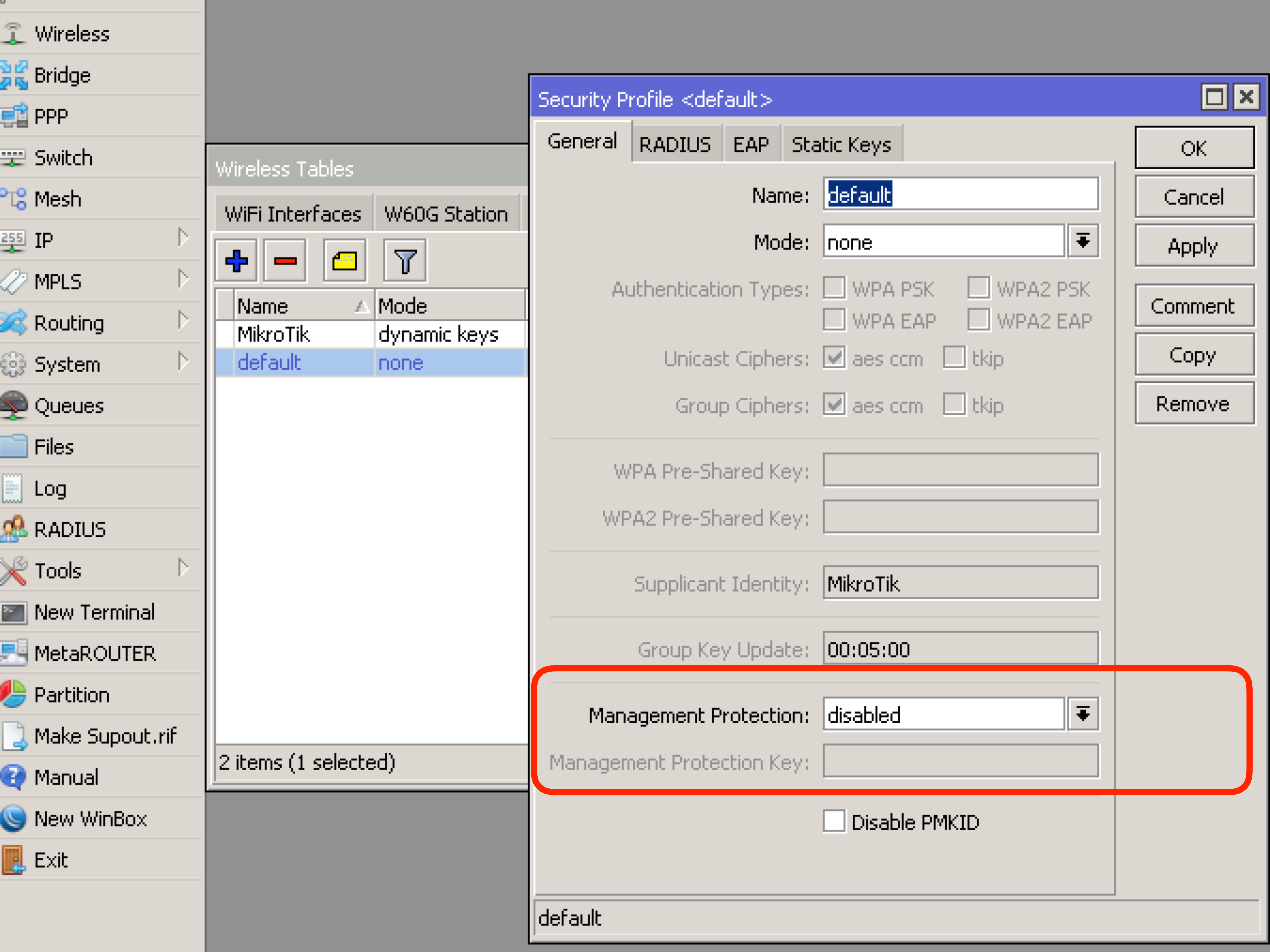
1. Access Point (SSID: IthinkIamSECURED)
2. Connect to the AP
3. Everything is working perfectly
4. Until…….

Question?

HOW TO PROTECT?

PROTECTED MANAGEMENT FRAMES 802.11W

- Prevent :
  - Eavesdropping
  - Forging
- Unicast
- Multicast
- PROBLEM: Not all wireless device support



Name	Mode
MikroTik	dynamic keys
default	none

2 items (1 selected)

Security Profile <default>

Name: default

Mode: none

Authentication Types: □ WPA PSK □ WPA2 PSK □ WPA EAP □ WPA2 EAP

Unicast Ciphers: ☑ aes ccm □ tkip

Group Ciphers: ☑ aes ccm □ tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity: MikroTik

Group Key Update: 00:05:00

Management Protection: disabled

Management Protection Key:

□ Disable PMKID

default

Question?

- 📱 *Approach me :)*
- ✉ *soragan.ong@alagasnetwork.com*
- f *soragan.ong*
- *@sguox*