WLAN / 802.11 (II)

I. Objectives

The objectives of this practical work are:

- Observe authentication and association processes
- Understand how information is exchanged on an 802.11 network
- Become familiar with network observation and diagnostic tools

II. Duration

This work should last one class, practical component (1h15)

III. Equipment

This Work will use:

1. 2x Cisco Access Point (AP)
2. 1x laboratory PC per work group (STA C), with Linux
3. The Wireshark application installed at STA C for capturing and analysing network traffic
4. 2x student terminals with WLAN/802.11 interface (STA A and STA B)

IV. Diagram

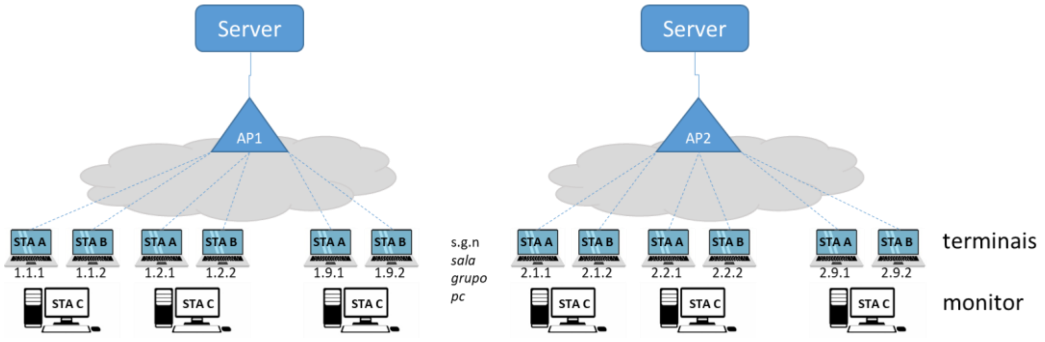


Figure 1: Network diagram for experimentation

Each AP has one SSID configured in the 2.4GHz WLAN band and has DHCPv4 server functionality, assigning IP addresses in the indicated range, as shown in the following table; one AP has open security while the other is secured:

	AP1	**AP2**
SSID	ComMoveis.33**0**.2400	ComMoveis.33**1**.2400
Channel	Channel **3** (2.422 MHz)	Channel **7** (2.442 MHz)
Security	Open	Authentication: WPAv2 Encryption: AES-CCM Password: "**Lab.Com.WiFi**"
IPv4 addressing	10.0.**1**.[100-200]/24 Server: 10.0.**1.2**/24	10.0.**2**.[100-200]/24 Server: 10.0.**2.2**/24

Table 1: WLANs configuration

1) Experimentation: Procedures

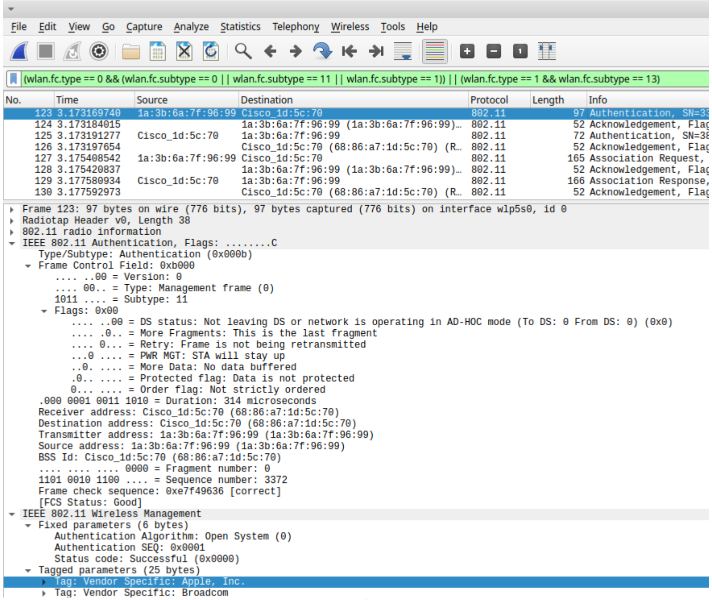
A. Authentication and Association

1) Restart capture (STA C) in Wireshark on the WLAN network interface (wlp***x***s0 interface), in channel 3 (2.422MHz)

2) Connect STA A to SSID1 ('ComMoveis.33**0**.2400') and stop the capture after it succeeded.

3) Configure a display filter for authentication, association and confirmation request frames (see fig. 2)

   - View the STA A authentication and association process in the capture and note the sequence number of these messages in the Wireshark capture.
   - Observe the Acknowledgment process.
   - Compare the body of *Authentication* and *Association* messages.



```
(wlan.fc.type == 0 && (wlan.fc.subtype == 0 || wlan.fc.subtype == 11 || wlan.fc.subtype == 1)) || (wlan.fc.type == 1 && wlan.fc.subtype == 13)
```

```
No.   Time         Source             Destination                                Protocol  Length Info
  123 3.173169740  1a:3b:6a:7f:96:99  Cisco_1d:5c:70                             802.11        97 Authentication, SN=33
  124 3.173184015                     1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…     802.11        52 Acknowledgement, Flag
  125 3.173191277  Cisco_1d:5c:70     1a:3b:6a:7f:96:99                          802.11        72 Authentication, SN=38
  126 3.173197654                     Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…     802.11        52 Acknowledgement, Flag
  127 3.175408542  1a:3b:6a:7f:96:99  Cisco_1d:5c:70                             802.11       165 Association Request,
  128 3.175420837                     1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…     802.11        52 Acknowledgement, Flag
  129 3.177580934  Cisco_1d:5c:70     1a:3b:6a:7f:96:99                          802.11       166 Association Response,
  130 3.177592973                     Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…     802.11        52 Acknowledgement, Flag
```

```
▸ Frame 123: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface wlp5s0, id 0
▸ Radiotap Header v0, Length 38
▸ 802.11 radio information
▾ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▾ Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_1d:5c:70 (68:86:a7:1d:5c:70)
    Destination address: Cisco_1d:5c:70 (68:86:a7:1d:5c:70)
    Transmitter address: 1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)
    Source address: 1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)
    BSS Id: Cisco_1d:5c:70 (68:86:a7:1d:5c:70)
    .... .... .... 0000 = Fragment number: 0
    1101 0010 1100 .... = Sequence number: 3372
    Frame check sequence: 0xe7f49636 [correct]
    [FCS Status: Good]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
  ▾ Tagged parameters (25 bytes)
    ▸ Tag: Vendor Specific: Apple, Inc.
    ▸ Tag: Vendor Specific: Broadcom
```

Figure 2

4) Change the viewing filter to add DHCP packets and observe the message exchange; note the IP address assigned to STA A.

   - Relate chronologically these messages to previous ones by comparing the sequence numbers in the capture.

B. Data transfer

5) Restart capture (STA C) in Wireshark on the WLAN network interface (wlp***x***s0 interface) and the right channel (3).

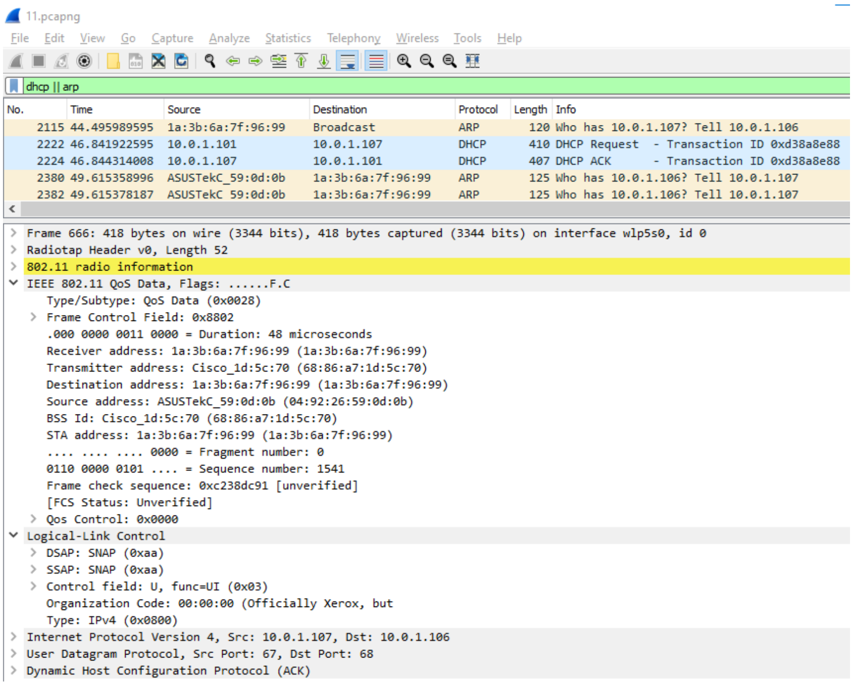
6) From STA A, ping the AccessPoint in use (10.0.**1**.2) for a few seconds (e.g. 10 seconds)

   - *Although pings were successful on your machine (STA A), Wireshark may miss and replicate some of these packets.*

7) Stop the capture and filter ICMP (*ping*) and ARP type packets in the view, analyzing the message exchanges.

   - Select one of these packages and, in the details area, note the frame and subframe type.

   - Look at the various encapsulations used until you get to the ICMP or ARP packet and explain them.


11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp || arp

```
No.     Time          Source              Destination         Protocol  Length Info
   2115 44.495989595  1a:3b:6a:7f:96:99   Broadcast           ARP          120 Who has 10.0.1.107? Tell 10.0.1.106
   2222 46.841922595  10.0.1.101          10.0.1.107          DHCP         410 DHCP Request  - Transaction ID 0xd38a8e88
   2224 46.844314008  10.0.1.107          10.0.1.101          DHCP         407 DHCP ACK      - Transaction ID 0xd38a8e88
   2380 49.615358996  ASUSTekC_59:0d:0b   1a:3b:6a:7f:96:99   ARP          125 Who has 10.0.1.106? Tell 10.0.1.107
   2382 49.615378187  ASUSTekC 59:0d:0b   1a:3b:6a:7f:96:99   ARP          125 Who has 10.0.1.106? Tell 10.0.1.107
```

```
> Frame 666: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface wlp5s0, id 0
> Radiotap Header v0, Length 52
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8802
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: 1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)
    Transmitter address: Cisco_1d:5c:70 (68:86:a7:1d:5c:70)
    Destination address: 1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)
    Source address: ASUSTekC_59:0d:0b (04:92:26:59:0d:0b)
    BSS Id: Cisco_1d:5c:70 (68:86:a7:1d:5c:70)
    STA address: 1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)
    .... .... .... 0000 = Fragment number: 0
    0110 0000 0101 .... = Sequence number: 1541
    Frame check sequence: 0xc238dc91 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
v Logical-Link Control
  > DSAP: SNAP (0xaa)
  > SSAP: SNAP (0xaa)
  > Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.0.1.107, Dst: 10.0.1.106
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (ACK)
```

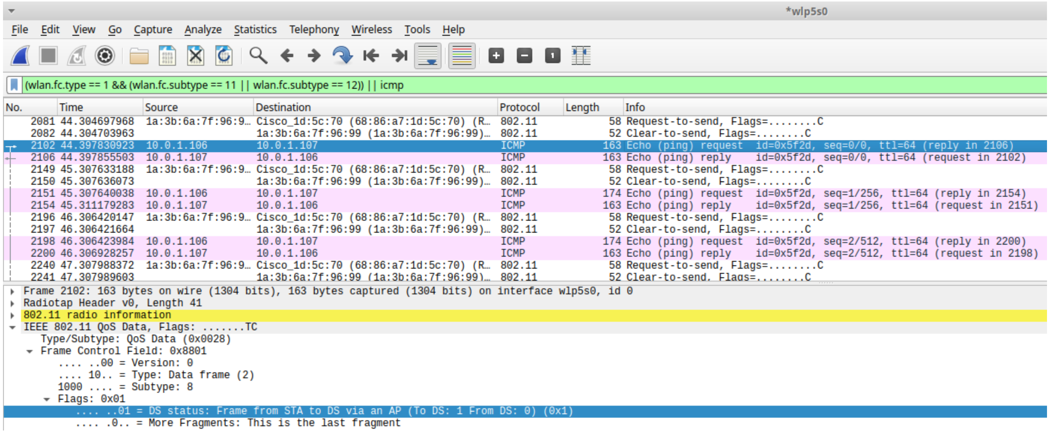
Figure 3

8) Now filter RTS, CTS and ICMP packets (*fc.type = 1 and subtype = 11 or 12*):

   - Check the packet exchange pattern between *ICMP Echo Request* requests and *ICMP Echo Reply* responses.

   - Note the type and subtype of captured frames.

   - Note the *DS status* flag of both *Echo Request* and *Reply* messages.


*wlp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(wlan.fc.type == 1 && (wlan.fc.subtype == 11 || wlan.fc.subtype == 12)) || icmp

```
No.   Time          Source              Destination                              Protocol  Length  Info
 2081 44.304697968  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
 2082 44.304703963                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
 2102 44.397830923  10.0.1.106          10.0.1.107                               ICMP         163 Echo (ping) request  id=0x5f2d, seq=0/0, ttl=64 (reply in 2106)
 2106 44.397855503  10.0.1.107          10.0.1.106                               ICMP         163 Echo (ping) reply    id=0x5f2d, seq=0/0, ttl=64 (request in 2102)
 2149 45.307633188  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
 2150 45.307636073                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
 2151 45.307640038  10.0.1.106          10.0.1.107                               ICMP         174 Echo (ping) request  id=0x5f2d, seq=1/256, ttl=64 (reply in 2154)
 2154 45.311179283  10.0.1.107          10.0.1.106                               ICMP         163 Echo (ping) reply    id=0x5f2d, seq=1/256, ttl=64 (request in 2151)
 2196 46.306420147  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
 2197 46.306421664                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
 2198 46.306423984  10.0.1.106          10.0.1.107                               ICMP         174 Echo (ping) request  id=0x5f2d, seq=2/512, ttl=64 (reply in 2200)
 2200 46.306928257  10.0.1.107          10.0.1.106                               ICMP         163 Echo (ping) reply    id=0x5f2d, seq=2/512, ttl=64 (request in 2198)
 2240 47.307988372  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
 2241 47.307989603                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
```

```
▸ Frame 2102: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface wlp5s0, id 0
▸ Radiotap Header v0, Length 41
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▾ Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
```

Figure 4

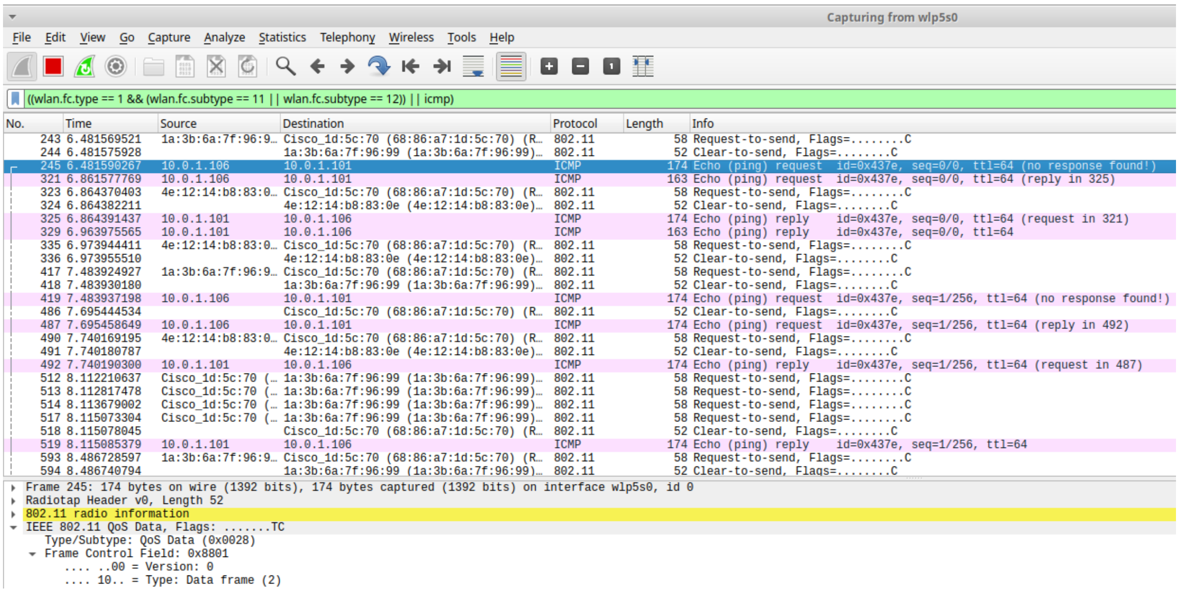
9) Restart capture (STA C) in Wireshark on the WLAN network interface (wlp***x***s0 interface) and the right channel (3).

10) Connect STA B to the SSID ('ComMoveis.33**0**.2400') of the same channel (authentication will not be requested)

    - Repeat applying a display filter to DHCP packets and note the address assigned to that station.

11) Ping from station STA A to STA B for a few seconds (e.g. 10 secs) and stop capturing

    - Filter RTS, CTS and ICMP packets
    - Why do you see the *Echo Requests* and *Echo Reply* being duplicated?


Capturing from wlp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

((wlan.fc.type == 1 && (wlan.fc.subtype == 11 || wlan.fc.subtype == 12)) || icmp)

```
No.   Time         Source              Destination                              Protocol  Length  Info
  243 6.481569521  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  244 6.481575928                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
  245 6.481590267  10.0.1.106          10.0.1.101                               ICMP         174 Echo (ping) request  id=0x437e, seq=0/0, ttl=64 (no response found!)
  321 6.861577769  10.0.1.106          10.0.1.101                               ICMP         163 Echo (ping) request  id=0x437e, seq=0/0, ttl=64 (reply in 325)
  323 6.864370403  4e:12:14:b8:83:0…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  324 6.864382211                      4e:12:14:b8:83:0e (4e:12:14:b8:83:0e)…  802.11        52 Clear-to-send, Flags=........C
  325 6.864391437  10.0.1.101          10.0.1.106                               ICMP         174 Echo (ping) reply    id=0x437e, seq=0/0, ttl=64 (request in 321)
  329 6.963975565  10.0.1.101          10.0.1.106                               ICMP         163 Echo (ping) reply    id=0x437e, seq=0/0, ttl=64
  335 6.973944411  4e:12:14:b8:83:0…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  336 6.973955510                      4e:12:14:b8:83:0e (4e:12:14:b8:83:0e)…  802.11        52 Clear-to-send, Flags=........C
  417 7.483924927  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  418 7.483930180                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
  419 7.483937198  10.0.1.106          10.0.1.101                               ICMP         174 Echo (ping) request  id=0x437e, seq=1/256, ttl=64 (no response found!)
  486 7.695444534                      Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        52 Clear-to-send, Flags=........C
  487 7.695458649  10.0.1.106          10.0.1.101                               ICMP         174 Echo (ping) request  id=0x437e, seq=1/256, ttl=64 (reply in 492)
  490 7.740169195  4e:12:14:b8:83:0…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  491 7.740180787                      4e:12:14:b8:83:0e (4e:12:14:b8:83:0e)…  802.11        52 Clear-to-send, Flags=........C
  492 7.740190300  10.0.1.101          10.0.1.106                               ICMP         174 Echo (ping) reply    id=0x437e, seq=1/256, ttl=64 (request in 487)
  512 8.112210637  Cisco_1d:5c:70 (…  1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        58 Request-to-send, Flags=........C
  513 8.112817478  Cisco_1d:5c:70 (…  1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        58 Request-to-send, Flags=........C
  514 8.113679002  Cisco_1d:5c:70 (…  1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        58 Request-to-send, Flags=........C
  517 8.115073304  Cisco_1d:5c:70 (…  1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        58 Request-to-send, Flags=........C
  518 8.115078045                      Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        52 Clear-to-send, Flags=........C
  519 8.115085379  10.0.1.101          10.0.1.106                               ICMP         174 Echo (ping) reply    id=0x437e, seq=1/256, ttl=64
  593 8.486728597  1a:3b:6a:7f:96:9…  Cisco_1d:5c:70 (68:86:a7:1d:5c:70) (R…  802.11        58 Request-to-send, Flags=........C
  594 8.486740794                      1a:3b:6a:7f:96:99 (1a:3b:6a:7f:96:99)…  802.11        52 Clear-to-send, Flags=........C
```

```
▸ Frame 245: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface wlp5s0, id 0
▸ Radiotap Header v0, Length 52
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
```

Figure 5

- Check the packet exchange pattern between ICMP Echo Request requests and ICMP Echo Reply responses; what differences do you find to the ping performed previously? Analyze based on observation of the following fields present in the 802.11 frame header:
    - *DS Status* and
    - *Receiver*, *Transmitter*, *Destination* and *Source Address*.

	Echo Req 1 STA - AP	Echo Req 2 AP - STB	Echo Rep 1 STB - AP	Echo Rep 2 AP - STA
Receiver				

Transmitter				
Destination				
Source				

C. Association with security and disassociation (STA A)

For the following procedures, AP2 and SSID 2 will be used, with the following characteristics:

AP2
ComMoveis.33**1**.2400
Channel **7** (2.442 MHz)
Authentication: **WPAv2**; Encryption: **AES-CCM**; Password: "**Lab.Com.WiFi**"
10.0.**2**.[100-200]/24 Server: 10.0.**2.2**/24

Table 2: AP2/SSID2 configuration

1) Add the key in Wireshark to be able to decrypt the contents of the packets:

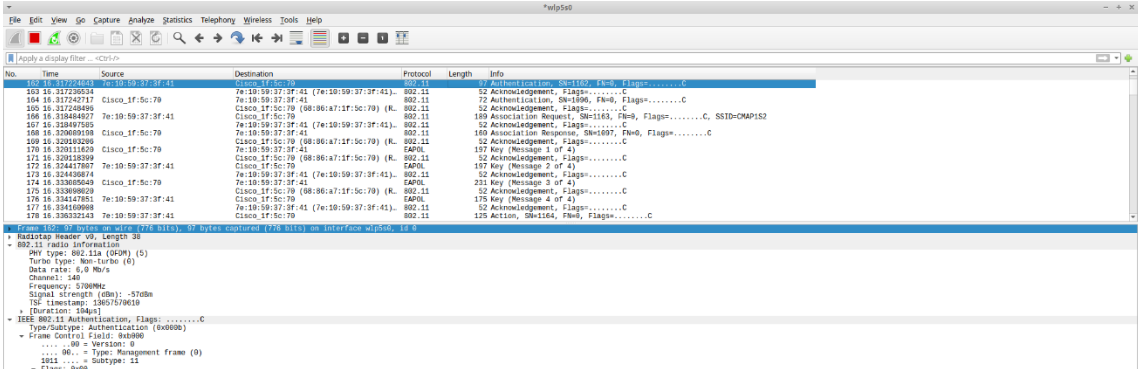
   - *Edit → Preferences → ieee802.11 → Enable decryption → edit → '+' → key-type=wpa-pwd →* ***key=Lab.Com.WiFi***

2) Change STA C to channel 7 (2.422 MHz).

3) Restart capture on the WLAN network (wlp5s0 interface).

4) Connect STA A to SSID 2 ('CMAP3.331.2400'); go back to STA C and stop the capture

   - Note the EAPoL (EAP over LAN) *4-Way Handshake* process used with WPAv2 and the parameters exchanged


*wlp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time          Source             Destination                               Protocol Length Info
162 16.317224043 7e:10:59:37:3f:41  Cisco_1f:5c:70                             802.11    97 Authentication, SN=1162, FN=0, Flags=........C
163 16.317236534                    7e:10:59:37:3f:41 (7e:10:59:37:3f:41)…    802.11    52 Acknowledgement, Flags=........C
164 16.317242717 Cisco_1f:5c:70     7e:10:59:37:3f:41                          802.11    72 Authentication, SN=1096, FN=0, Flags=........C
165 16.317248496                    Cisco_1f:5c:70 (68:86:a7:1f:5c:70) (R…    802.11    52 Acknowledgement, Flags=........C
166 16.318484927 7e:10:59:37:3f:41  Cisco_1f:5c:70                             802.11   189 Association Request, SN=1163, FN=0, Flags=........C, SSID=CMAP1S2
167 16.318497585                    7e:10:59:37:3f:41 (7e:10:59:37:3f:41)…    802.11    52 Acknowledgement, Flags=........C
168 16.320089198 Cisco_1f:5c:70     7e:10:59:37:3f:41                          802.11   160 Association Response, SN=1097, FN=0, Flags=........C
169 16.320103206                    Cisco_1f:5c:70 (68:86:a7:1f:5c:70) (R…    802.11    52 Acknowledgement, Flags=........C
170 16.320111620 Cisco_1f:5c:70     7e:10:59:37:3f:41                          EAPOL    197 Key (Message 1 of 4)
171 16.320118399                    Cisco_1f:5c:70 (68:86:a7:1f:5c:70) (R…    802.11    52 Acknowledgement, Flags=........C
172 16.324417807 7e:10:59:37:3f:41  Cisco_1f:5c:70                             EAPOL    197 Key (Message 2 of 4)
173 16.324436874                    7e:10:59:37:3f:41 (7e:10:59:37:3f:41)…    802.11    52 Acknowledgement, Flags=........C
174 16.333085049 Cisco_1f:5c:70     7e:10:59:37:3f:41                          EAPOL    231 Key (Message 3 of 4)
175 16.333098020                    Cisco_1f:5c:70 (68:86:a7:1f:5c:70) (R…    802.11    52 Acknowledgement, Flags=........C
176 16.334147851 7e:10:59:37:3f:41  Cisco_1f:5c:70                             EAPOL    175 Key (Message 4 of 4)
177 16.334160908                    7e:10:59:37:3f:41 (7e:10:59:37:3f:41)…    802.11    52 Acknowledgement, Flags=........C
178 16.336332143 7e:10:59:37:3f:41  Cisco_1f:5c:70                             802.11   125 Action, SN=1164, FN=0, Flags=........C
```

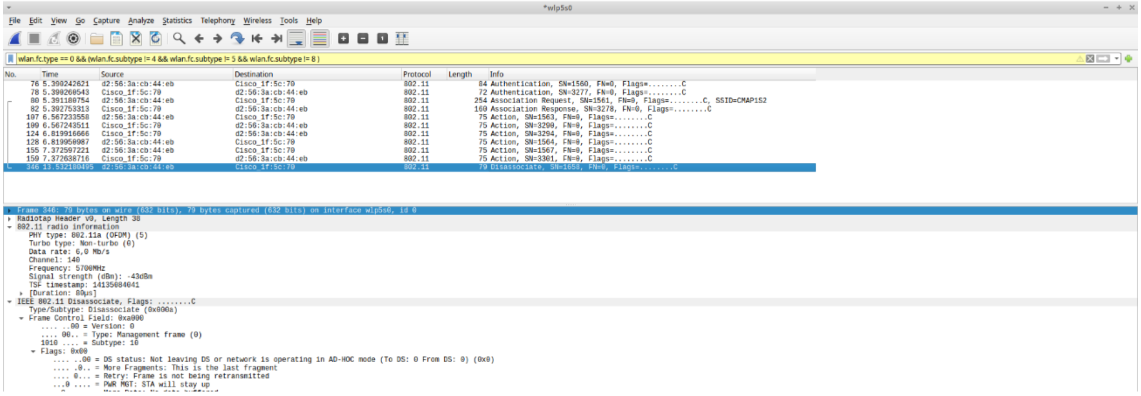
```
▸ Frame 162: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface wlp5s0, id 0
▸ Radiotap Header v0, Length 38
▾ 802.11 radio information
    PHY type: 802.11a (OFDM) (5)
    Turbo type: Non-turbo (0)
    Data rate: 6,0 Mb/s
    Channel: 140
    Frequency: 5700MHz
    Signal strength (dBm): -57dBm
    TSF timestamp: 13057570610
  ▸ [Duration: 104µs]
▾ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▾ Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
```

Figure 6

5) Restart capture on the WLAN network (wlp5s0 interface).

6) Return STA A to SSID 1 and stop capturing.

   - Note the single disassociation message.


*wlp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.fc.type == 0 && (wlan.fc.subtype != 4 && wlan.fc.subtype != 5 && wlan.fc.subtype != 8 )
```

```
No.  Time          Source             Destination        Protocol Length Info
 76 5.390242621   d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11    84 Authentication, SN=1560, FN=0, Flags=........C
 78 5.390260543   Cisco_1f:5c:70     d2:56:3a:cb:44:eb  802.11    72 Authentication, SN=3277, FN=0, Flags=........C
 80 5.391180754   d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11   254 Association Request, SN=1561, FN=0, Flags=........C, SSID=CMAP1S2
 82 5.392753313   Cisco_1f:5c:70     d2:56:3a:cb:44:eb  802.11   160 Association Response, SN=3278, FN=0, Flags=........C
107 6.567233558   d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11    75 Action, SN=1563, FN=0, Flags=........C
109 6.567243511   Cisco_1f:5c:70     d2:56:3a:cb:44:eb  802.11    75 Action, SN=3290, FN=0, Flags=........C
124 6.819916666   Cisco_1f:5c:70     d2:56:3a:cb:44:eb  802.11    75 Action, SN=3294, FN=0, Flags=........C
128 6.819950987   d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11    75 Action, SN=1564, FN=0, Flags=........C
155 7.372597221   d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11    75 Action, SN=1567, FN=0, Flags=........C
159 7.372638716   Cisco_1f:5c:70     d2:56:3a:cb:44:eb  802.11    75 Action, SN=3301, FN=0, Flags=........C
346 13.532180495  d2:56:3a:cb:44:eb  Cisco_1f:5c:70     802.11    79 Disassociate, SN=1658, FN=0, Flags=........C
```

```
▸ Frame 346: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface wlp5s0, id 0
▸ Radiotap Header v0, Length 38
▾ 802.11 radio information
    PHY type: 802.11a (OFDM) (5)
    Turbo type: Non-turbo (0)
    Data rate: 6,0 Mb/s
    Channel: 140
    Frequency: 5700MHz
    Signal strength (dBm): -43dBm
    TSF timestamp: 14135084041
  ▸ [Duration: 80µs]
▾ IEEE 802.11 Disassociate, Flags: ........C
    Type/Subtype: Disassociate (0x000a)
  ▾ Frame Control Field: 0xa000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1010 .... = Subtype: 10
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
```

Figure 7

V. Useful links

WLAN

- https://howiwifi.com/2020/07/13/802-11-frame-types-and-formats/
- https://howiwifi.com/2020/07/16/802-11-frame-exchanges/
- https://www.wifi-professionals.com/2019/01/4-way-handshake
- https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

Wireshark

https://wiki.wireshark.org/CaptureSetup/WLAN

https://www.wireshark.org/docs/dfref/w/wlan.html

VI. Wireshark usage and frame structure

Display filters

- wlan.bssid == *MAC AP*
- wlan.ra == MAC addr; wlan.sa == MAC addr
- wlan.fc.type == n (0: management; 1: control; 2: data)
- wlan.fc.subtype == n (see table below)

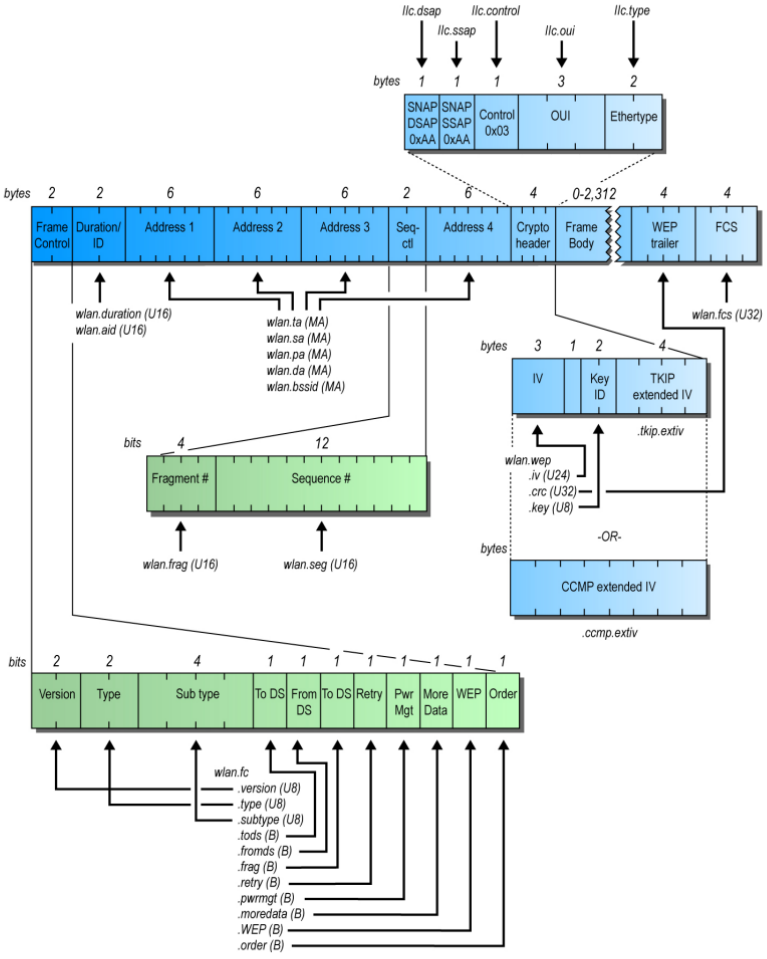


Figure 8

VII. 802.11 frames' structure and sub-types

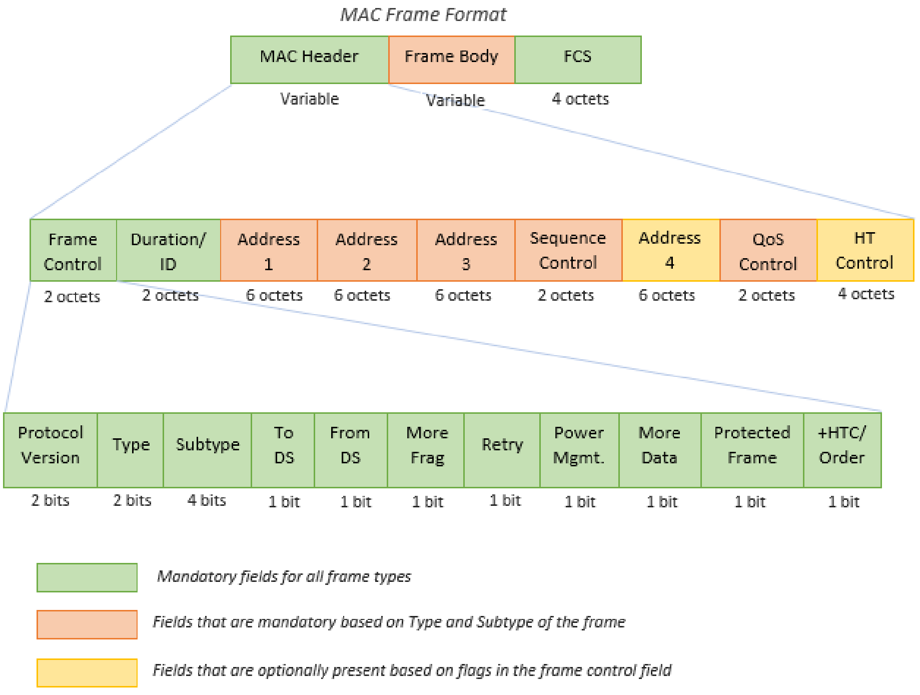


Figure 9

Type = 0 (Management)		**Type = 1** (Control)		**Type = 2** (Data)	
Association request	0000 (0)			Data	0000 (0)
Association response	0001 (1)			Data + CF-ACK	0001 (1)
Reassociation request	0010 (2)			Data + CF-Poll	0010 (2)
Reassociation response	0011 (3)			Data + CF-ACK + CF-Poll	0011 (3)
Probe request	0100 (4)	Beamforming Report Poll	0100 (4)	Null (no data)	0100 (4)
Probe response	0101 (5)	VHT/HE NDP Announcement	0101 (5)	CF-ACK (no data)	0101 (5)
Timing advertisement	0110 (6)	Control Frame Extension	0110 (6)	CF-Poll (no data)	0110 (6)
Reserved	0111 (7)	Control wrapper	0111 (7)	CF-ACK + CF-Poll (no data)	0111 (7)
Beacon	1000 (8)	Block ACK Request	1000 (8)	QoS Data	1000 (8)
		Block ACK	1001 (9)	QoS Data + CF-ACK	1001 (9)
Disassociation	1010 (10)	PS-Poll	1010 (10)	QoS Data + CF-Poll	1010 (10)
Authentication	1011 (11)	RTS	1011 (11)	QoS Data + CF-ACK + CF-Poll	1011 (11)
Deauthentication	1100 (12)	CTS	1100 (12)	QoS Null (no data)	1100 (12)
Action	1110 (13)	ACK	1101 (13)	Reserved	1101 (13)
		CF-End	1110 (14)	QoS CF-Poll (no data)	1110 (14)
		CF-END+CF-ACK	1111 (15)	QoS CF-ACK + CF-Poll (no data)	1111 (15)

Table 3

VIII. Channels and frequencies

2.4 GHz

Channel	F_0 (MHz)	Frequency Range (20 MHz)
1	2412	2401–2423
2	2417	2406–2428
3	2422	2411–2433
4	2427	2416–2438
5	2432	2421–2443
6	2437	2426–2448
7	2442	2431–2453
8	2447	2436–2458
9	2452	2441–2463
10	2457	2446–2468
11	2462	2451–2473
12	2467	2456–2478
13	2472	2461–2483
14	2484	2473–2495

Table 4

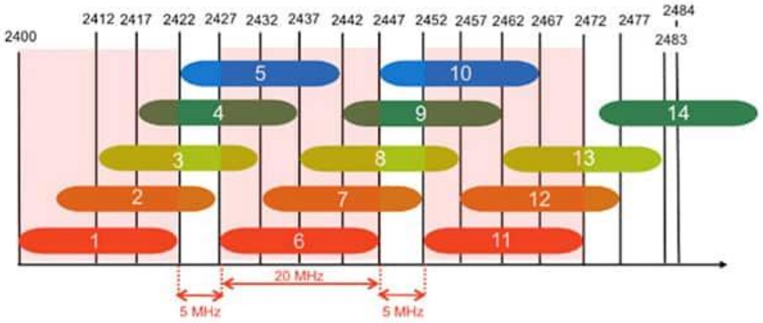


Figure 10

https://www.digikey.com/en/articles/compare-24-ghz-5-ghz-wireless-lan-industrial-applications

5GHZ

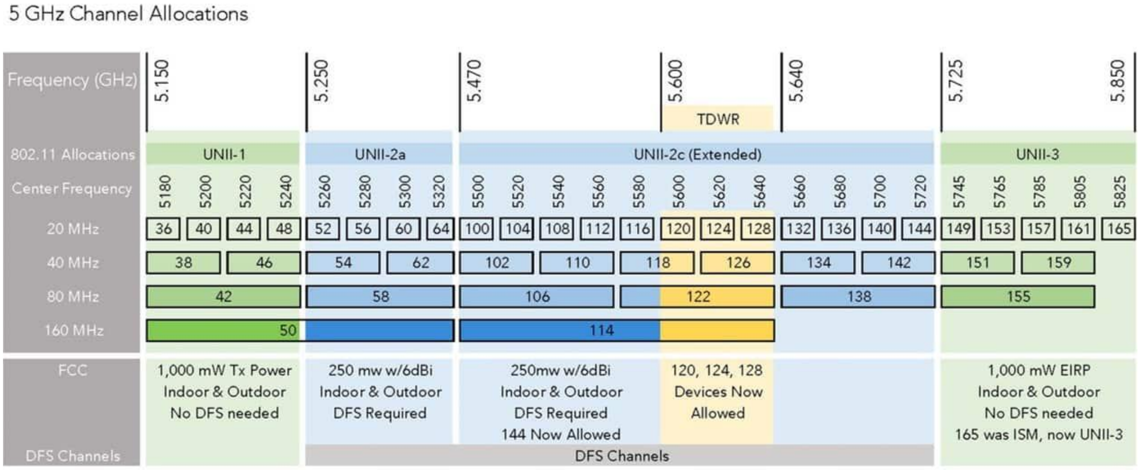


Figure 11

https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/