# Observing IEEE 802.11

## Part 1 : Active and passive scanning

### Step : 1.1 : Obtain test equipment

Description : You need a wireless client device, such as an 802.11n- or 802.11ac-equipped laptop, and an access point. You also need a wireless protocol analyzer, such as WireShark (which is freely available) or another protocol analyzers.

I used my phone as an access point, and wireshark as protocol analyzer.

### Step: 1.2 : Configure the protocol analyzer

Description : The protocol analyzer should record 802.11 frame transmissions on all RF channels

I had some struggle doing this, as windows does not allow the *monitor mode* which is what we need to capture 802.11 frames with wireshark. As a result, I had to find a laptop with a Linux based installation on it.

First, I had to activate the *monitor mode* on the workstation, and then in Wireshark.

### Step 1.3. Position the client device within proximity, such as within the same room, to an operational access point.

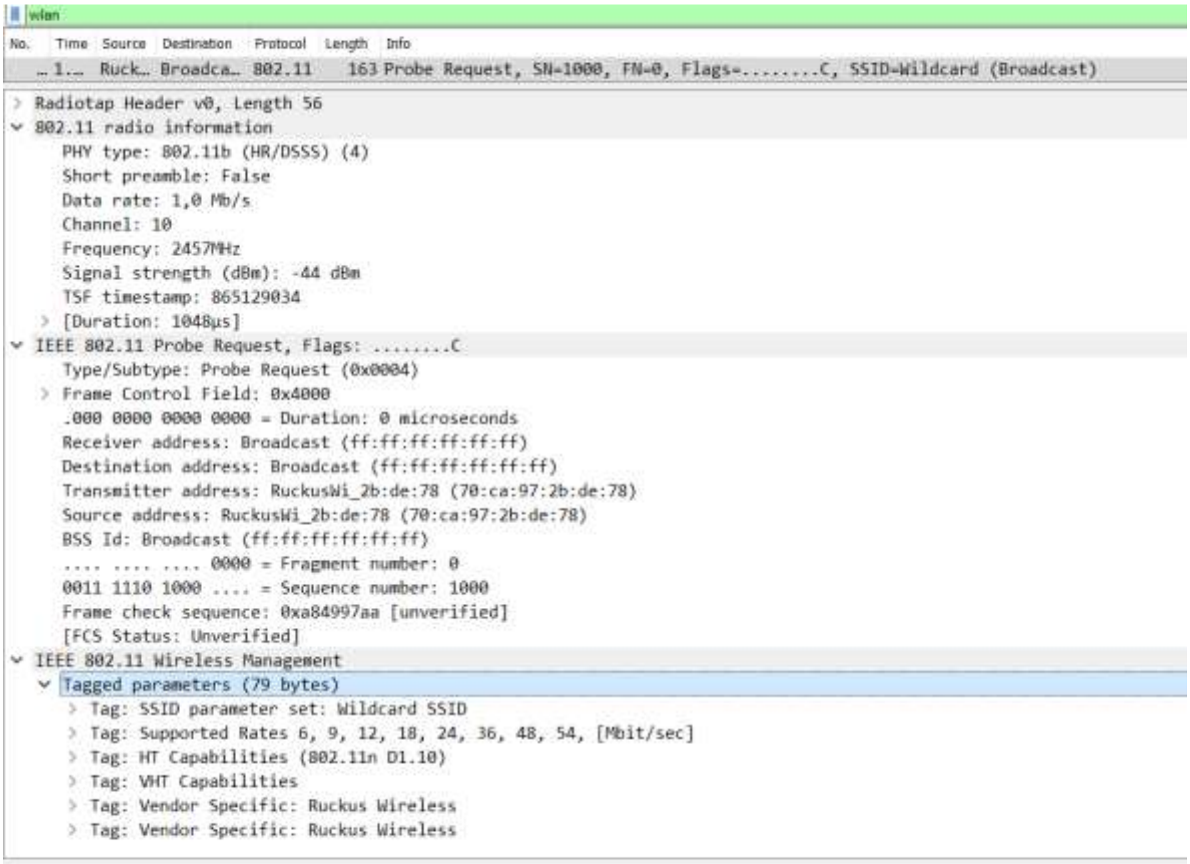
### Step 1.4. With the client device not associated to the access point, record a packet trace with the protocol analyzer (just a minute or two is enough time).

*What 802.11 probe requests do you see your client device sending on each of the channels? What probe responses do you see the access points sending? Explain your answer with the help of screenshots.*

We can observe two types of request: one that search new access point, and request to the know access points.

When the SSID is “Wildcard”, it is a broadcast request, that search for new access point. I also have a probe request to the SSID “Edouard House”, which is the name of the access point of the residence, and my computer had already been connected to it. If the AP is present, it will send a probe response.

The probe request sent to “Wildcard” SSID  (broadcast) :

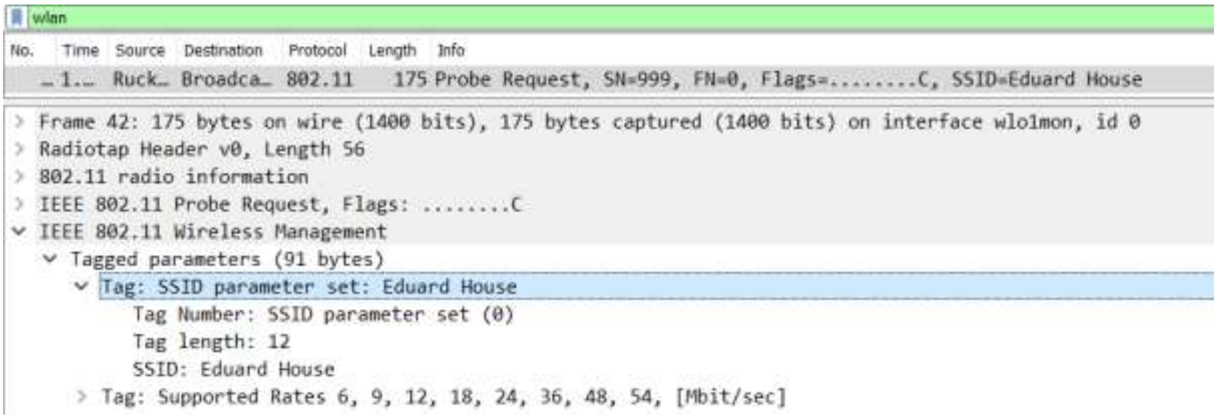


```
wlan
No.   Time  Source  Destination  Protocol  Length  Info
 … 1…  Ruck…  Broadca…  802.11    163 Probe Request, SN=1000, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

> Radiotap Header v0, Length 56
v 802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1,0 Mb/s
    Channel: 10
    Frequency: 2457MHz
    Signal strength (dBm): -44 dBm
    TSF timestamp: 865129034
  > [Duration: 1048µs]
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: RuckusWi_2b:de:78 (70:ca:97:2b:de:78)
    Source address: RuckusWi_2b:de:78 (70:ca:97:2b:de:78)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0011 1110 1000 .... = Sequence number: 1000
    Frame check sequence: 0xa84997aa [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Tagged parameters (79 bytes)
    > Tag: SSID parameter set: Wildcard SSID
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: VHT Capabilities
    > Tag: Vendor Specific: Ruckus Wireless
    > Tag: Vendor Specific: Ruckus Wireless
```

We can see some information as the channel it has been sent in (10), or the frequency.

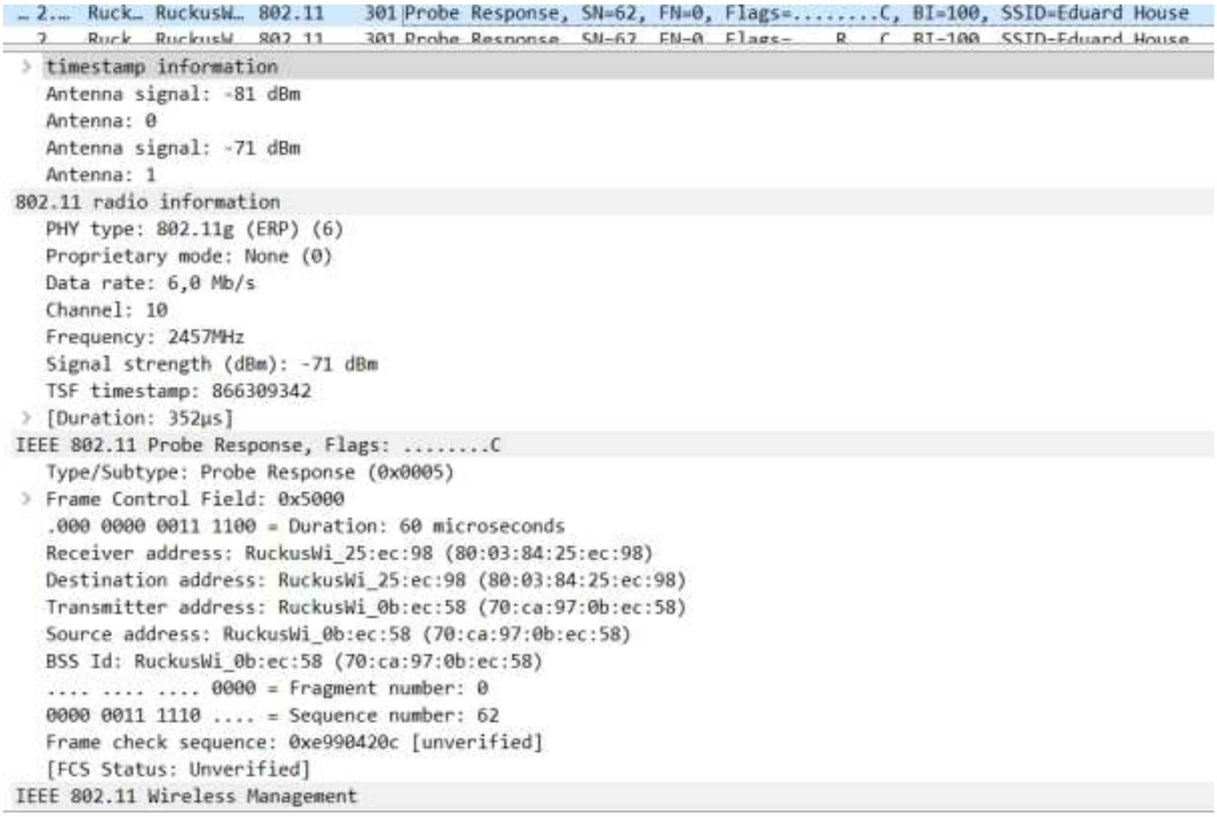
We can see that in other case the SSID is set to a known SSID :



```
wlan
No.   Time  Source  Destination  Protocol  Length  Info
 … 1…  Ruck…  Broadca…  802.11    175 Probe Request, SN=999, FN=0, Flags=........C, SSID=Eduard House

> Frame 42: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface wlo1mon, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
v IEEE 802.11 Wireless Management
  v Tagged parameters (91 bytes)
    v Tag: SSID parameter set: Eduard House
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: Eduard House
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
```

Here is a probe response from SSID Eduard House, we can see that the channel is the same :

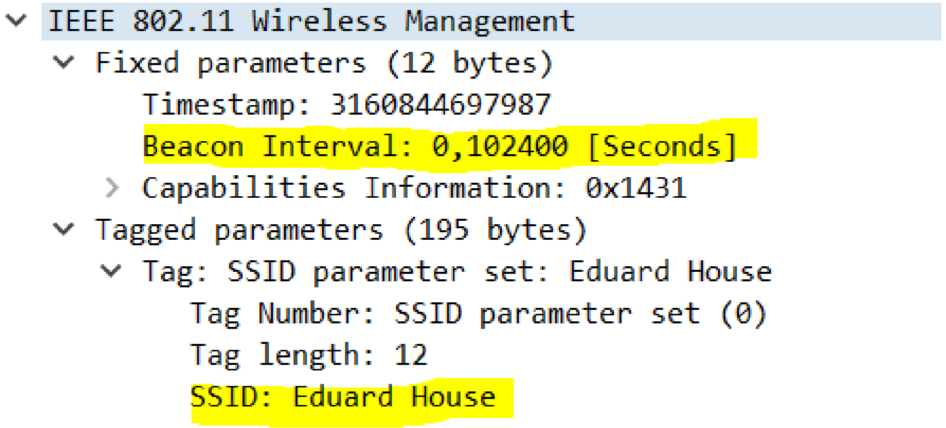


```
… 2… Ruck… RuckusW… 802.11    301 Probe Response, SN=62, FN=0, Flags=........C, BI=100, SSID=Eduard House
  2   Ruck  RuckusW   802.11    301 Probe Response  SN=62  FN=0  Flags=       R   C  BI=100  SSID=Eduard House
 > timestamp information
    Antenna signal: -81 dBm
    Antenna: 0
    Antenna signal: -71 dBm
    Antenna: 1
802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Proprietary mode: None (0)
    Data rate: 6,0 Mb/s
    Channel: 10
    Frequency: 2457MHz
    Signal strength (dBm): -71 dBm
    TSF timestamp: 866309342
 > [Duration: 352µs]
IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
 > Frame Control Field: 0x5000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: RuckusWi_25:ec:98 (80:03:84:25:ec:98)
    Destination address: RuckusWi_25:ec:98 (80:03:84:25:ec:98)
    Transmitter address: RuckusWi_0b:ec:58 (70:ca:97:0b:ec:58)
    Source address: RuckusWi_0b:ec:58 (70:ca:97:0b:ec:58)
    BSS Id: RuckusWi_0b:ec:58 (70:ca:97:0b:ec:58)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 1110 .... = Sequence number: 62
    Frame check sequence: 0xe990420c [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

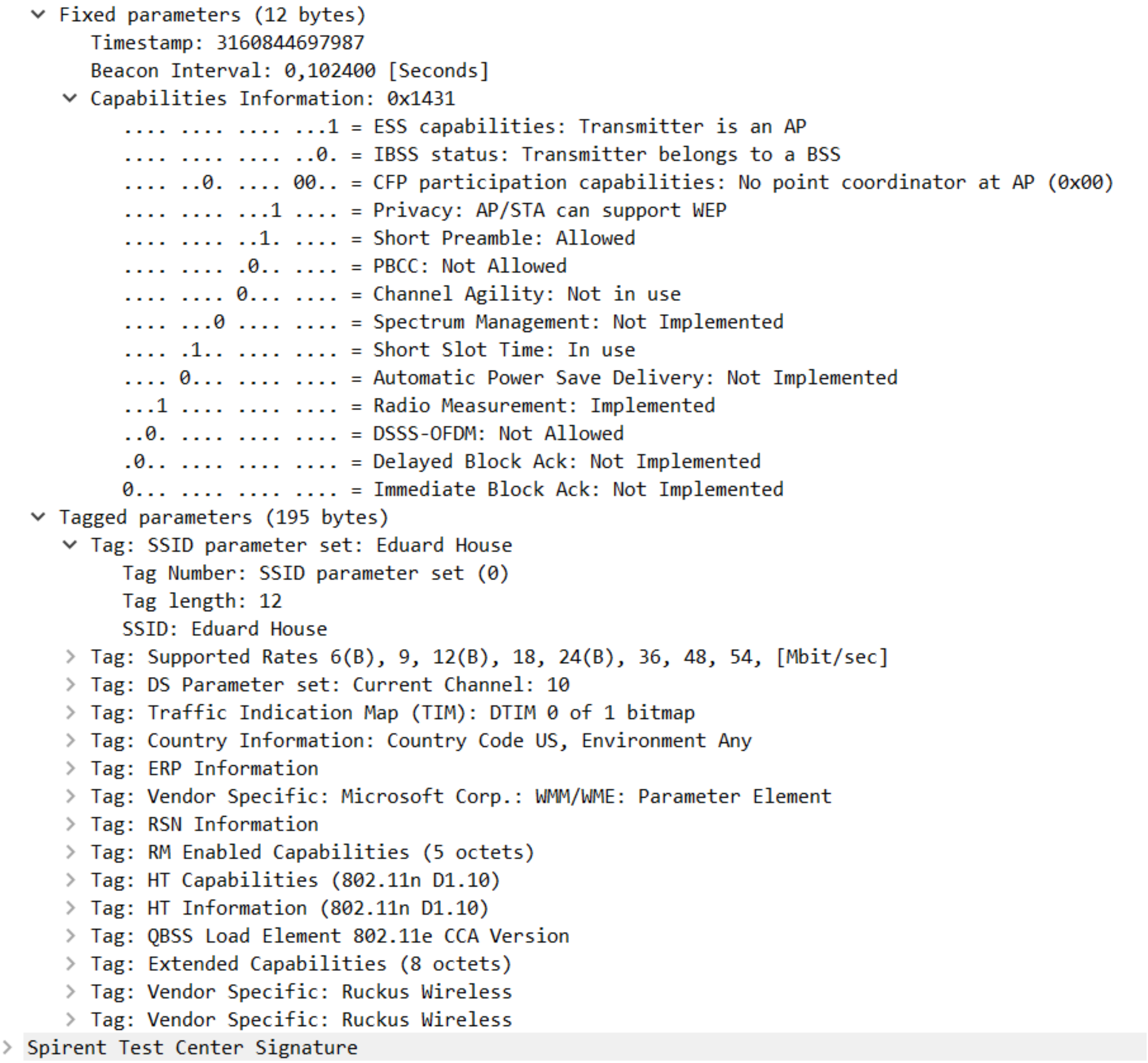
Step 1.5. Observe the packet trace and look at the details of one of the access point beacons.

*What is the time period between the beacons? Can you find the SSID in the frame body of the beacon frame? What else is included in the frame body of the beacon, and what does it tell you about the configuration of the WLAN? Explain your answer with the help of screenshots.*

The time period between the beacons is 0.1024s. We can find the SSID in the tagged parameters. We can also find the supported rate, information about the router… The fixed parameters also contain "capabilities information" : tells us if the transmitter is an AP, if the channel agility is in use, for example.



```
v IEEE 802.11 Wireless Management
    v Fixed parameters (12 bytes)
          Timestamp: 3160844697987
          Beacon Interval: 0,102400 [Seconds]
        > Capabilities Information: 0x1431
    v Tagged parameters (195 bytes)
        v Tag: SSID parameter set: Eduard House
              Tag Number: SSID parameter set (0)
              Tag length: 12
              SSID: Eduard House
```



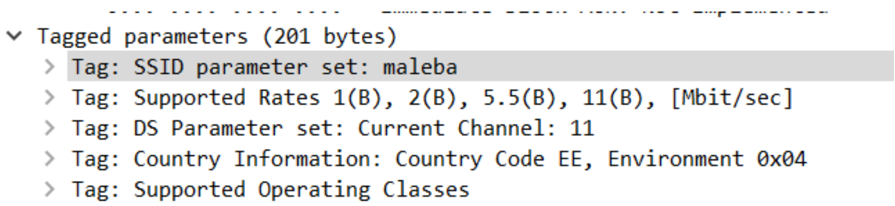
```
⌄ Fixed parameters (12 bytes)
    Timestamp: 3160844697987
    Beacon Interval: 0,102400 [Seconds]
  ⌄ Capabilities Information: 0x1431
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
      .... .... ...1 .... = Privacy: AP/STA can support WEP
      .... .... ..1. .... = Short Preamble: Allowed
      .... .... .0.. .... = PBCC: Not Allowed
      .... .... 0... .... = Channel Agility: Not in use
      .... ...0 .... .... = Spectrum Management: Not Implemented
      .... .1.. .... .... = Short Slot Time: In use
      .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
      ...1 .... .... .... = Radio Measurement: Implemented
      ..0. .... .... .... = DSSS-OFDM: Not Allowed
      .0.. .... .... .... = Delayed Block Ack: Not Implemented
      0... .... .... .... = Immediate Block Ack: Not Implemented
⌄ Tagged parameters (195 bytes)
  ⌄ Tag: SSID parameter set: Eduard House
      Tag Number: SSID parameter set (0)
      Tag length: 12
      SSID: Eduard House
  › Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  › Tag: DS Parameter set: Current Channel: 10
  › Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
  › Tag: Country Information: Country Code US, Environment Any
  › Tag: ERP Information
  › Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  › Tag: RSN Information
  › Tag: RM Enabled Capabilities (5 octets)
  › Tag: HT Capabilities (802.11n D1.10)
  › Tag: HT Information (802.11n D1.10)
  › Tag: QBSS Load Element 802.11e CCA Version
  › Tag: Extended Capabilities (8 octets)
  › Tag: Vendor Specific: Ruckus Wireless
  › Tag: Vendor Specific: Ruckus Wireless
› Spirent Test Center Signature
```

Step 1.6. Configure the access point to not broadcast the SSID in beacons (if supported by your access point), and repeat steps 4 and 5.

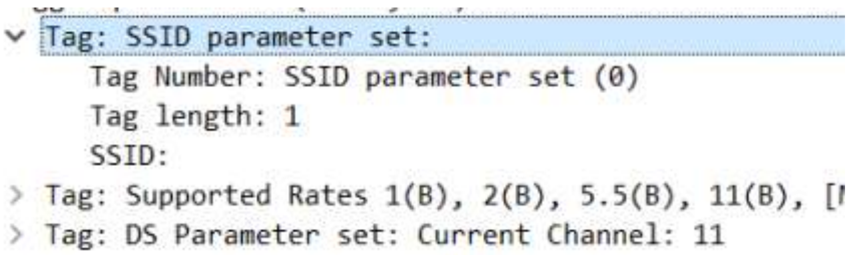
*Do you see the SSID in the beacon frame body? Explain your answer with the help of screenshots.*

After hiding the SSID, the SSID is blank in the beacon frame (null). The AP is still sending the frame, but it hide its name. I used my phone as an AP for this (SSID is maleba), which is why the channel is now 11 and the supported rates have changed.

Before hiding the SSID :



```
    .... .... .... .... = Immediate Block Ack: Not Implemented
⌄ Tagged parameters (201 bytes)
  › Tag: SSID parameter set: maleba
  › Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  › Tag: DS Parameter set: Current Channel: 11
  › Tag: Country Information: Country Code EE, Environment 0x04
  › Tag: Supported Operating Classes
```



```
Tag: SSID parameter set:
    Tag Number: SSID parameter set (0)
    Tag length: 1
    SSID:
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [
Tag: DS Parameter set: Current Channel: 11
```

Step 1.7. Turn off the access point (and any other access points that your test client device may be able to associate with) and repeat steps 4 and 5.

*What 802.11 probe requests do you see your client device sending on each of the channels now? What probe responses do you see the access points sending? Explain your answer with the help of screenshots.*

Unfortunately, I am not able to turn off all the access point because I live in a residency, so I could not do this part.

## Part 2: Observing 802.11 Frames Resulting from Typical User Traffic

Step 2.1. Start recording a packet trace with the protocol analyzer.
Step 2.2. Use typical wireless applications, such as browsing the web or sending e-mail, from the client device. After several minutes of using applications, stop the recording of the packet trace.
Step 2.3. Observe the packet trace recording and look for the transmission of 802.11 data frames that occur between the applicable client device and access point. Observe and analyze the sequence of 802.11 frames. Explain your answer with the help of screenshots.

The only way I found to capture 802.11 frames was with the monitor mode, and I could not be connected to internet as the same time, so I could not do this part.

I think I would have observed some data frame type (type value 10), as QoS data for example.