MEMORIA SC – PRÁCTICA 2.2

Alonso Rodríguez Iglesias – SC 2019/20 – Práctica 2.2

ÍNDICE

ÍNDICE DE FIGURAS

INTRODUCCIÓN Y DETALLES

Esta práctica trata de analizar los tiempos y funcionamiento de diversos aspectos del estándar 802.11.

Se han realizado varias capturas en las que se puede ver toda la información necesaria. En ellas he marcado regiones con cuadrados de diferentes colores, y en las respuestas hago referencia a esas regiones de colores en las figuras.

Leer el documento en texto “plano” se hace bastante pesado si escribo los colores por su nombre, por ejemplo: [Fig.X Recuadro Verde]. Por ello he decidido subrayar con un color que referencia al mismo, por ejemplo: [Fig.X] y a mi parecer agiliza mucho la lectura, aparte de que permite condensar más la información.

Las figuras se encuentran al final de cada sección, y la forma intencionada de leer este documento de forma rápida es abrir el PDF en dos ventanas separadas, una con el texto y otra con las imágenes. De esta forma la lectura es bastante cómoda. También se puede acceder a las imágenes originales en la carpeta screenshot.

Se adjuntan las capturas realizadas con Wireshark en la carpeta capture comprimidas en formato zip para ahorrar espacio.

BEACONS: INTERVALO DE BEACONING

1. Si medimos las diferencias entre los timestamps [Fig.1] dos a dos, podemos calcular el máximo, mínimo y medio:

   ```
   Máximo: 0.102387516
   Mínimo: 0.102283982
   Medio : 0.102335367
   ```

   Cálculos realizados con 7 medidas:

   ```
   1-2: 0.102326486
   2-3: 0.102366676
   3-4: 0.102387516
   4-5: 0.102309885
   5-6: 0.102342154
   6-7: 0.102330869
   7-8: 0.102283982
   ```

2. Observando el campo "Beacon Interval" [Fig.1]vemos que el valor es muy similar pero no el mismo.
   El valor medio que nosotros medimos empíricamente es:

   ```
   Beacon Interval ≈ 0.102335 ≠ 0.102400 s
   ```

   Esta discrepancia puede darse por redondeo, por errores de precisión en mi medición (quizás posteriormente sí que aumenta), o porque Wireshark lo infiere de otra manera.

   He encontrado la siguiente información:

   "Target Beacon Transmission Time Time (TBTT) is the time at which a node (AP or station when in Ad-hoc) must send a beacon. The time difference between two TBTTs is known as the beacon interval. The beacon interval is given in Time Units (TU), each TU represents 1024 microseconds. The beacon interval is typically set to 100 TUs (102400 microseconds, or 102.4 ms) and its length is two bytes."

   De esta manera, si Wireshark ve que los paquetes vienen cada 100 TUs, al tener una tolerancia de 1024μs, convierte los 100 TUs a segundos, y no redondea con los segundos de las timestamps.

   De este modo, mi hipótesis es la última de las planteadas.

BEACONS: INTERVALO DE BEACONING - FIGURAS

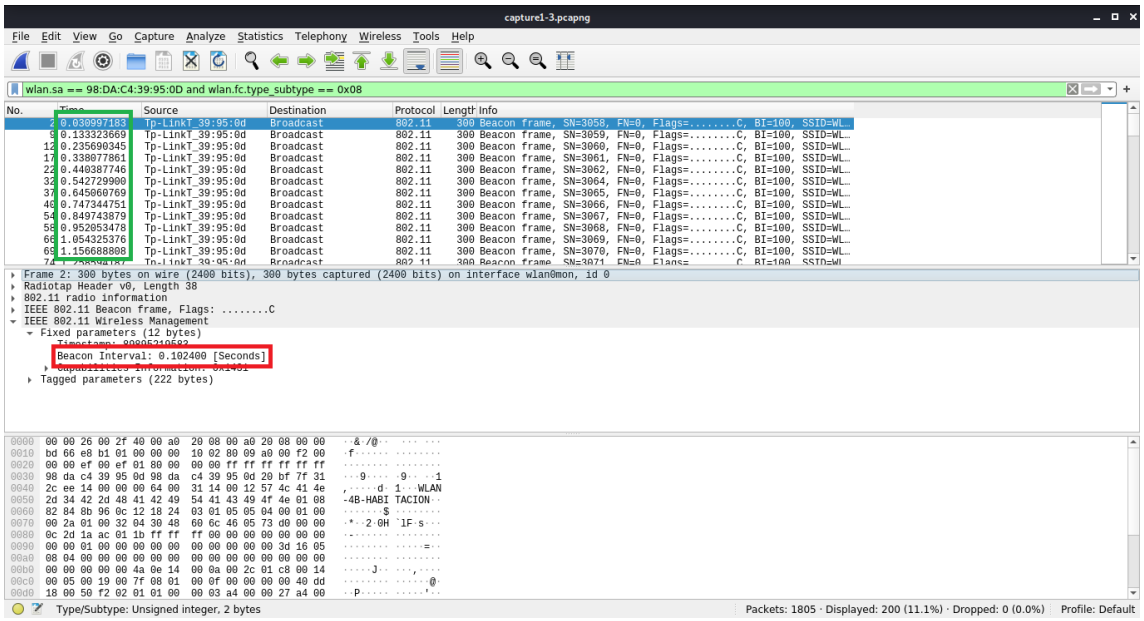
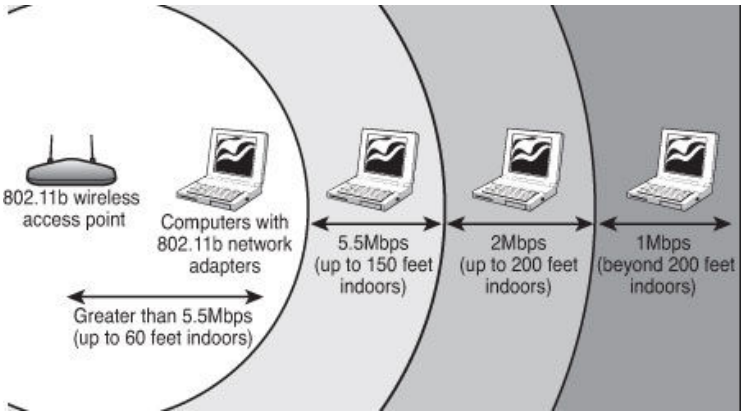


Figura 1: Análisis del Beacon Interval

BEACONS: OBTENDO DATOS SOBRE AS CAPAS PHY Y MAC

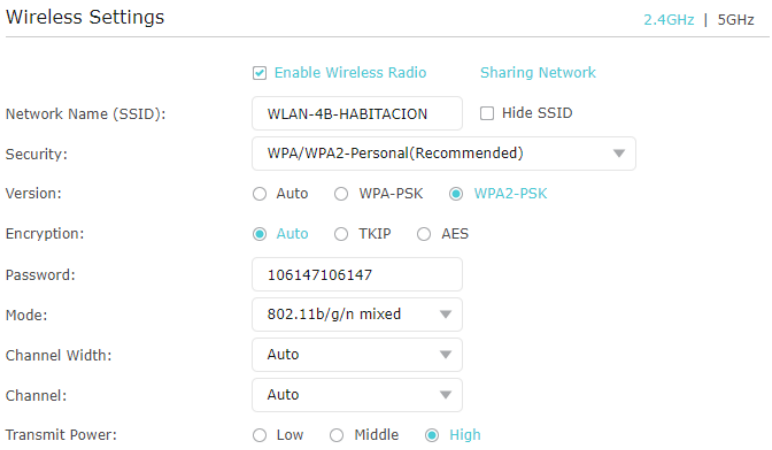
1. Se transmiten a 1Mbps [Fig.2].

   Pienso que es porque, como se puede ver en la siguiente imagen:



   nos interesa que la señal llegue lo más lejos posible, y como estamos empleando 802.11b [Fig.2] la velocidad es de 1Mbps.

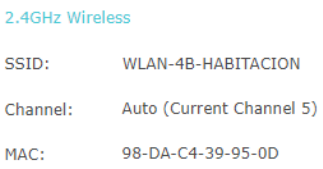
   Estaríamos empleando 802.11b por ser el más compatible de los estándares que soporta mi router para 2.4 GHz.



2. Bueno, como comentaba en el apartado anterior, ya sabemos que soporta 802.11b/g/n.

   Con respecto a encontrar esta información en Wireshark, la verdad es que no he sido capaz de encontrarla así directamente, pero si que es verdad que mirando los Tag "Supported Rates" [Fig.3] y "Extended Supported Rates" [Fig.3], podemos identificar en el primero los rates de 802.11b/g y en el segundo los rates de 802.11n en la banda de 2.4GHz, lo cual se coincide con la información que tengo de antemano sacada de la configuración de mi router.

Los paquetes se envían en los 2432MHz, es decir, el canal 5 [Fig.2], lo cual, de nuevo, se corresponde con lo que podemos observar en la configuración del router.



3. La dirección de destino es la de broadcast [Fig.3], es decir, la MAC `FF:FF:FF:FF:FF:FF`.
4. La dirección MAC es `98:DA:C4:39:95:0D`. Esto se puede ver en el campo destination [Fig.3], aunque Wireshark sustituye `98:DA:C4:` por `Tp-LinkT_`, esto es porque los primeros 24 bits de la MAC identifican al fabricante, y Wireshark tiene una lista de los mismos. También se puede consultar en "`IEEE 802.11 Beacon frame -> Transmitter address`".
5. Los más relevantes que he encontrado (y que me dicen algo) son:
    a. `WEP: False -> No estamos utilizando WEP`
    b. `Fragmentation: False -> No estamos fragmentando (lo cual es muy lógico, porque es un solo paquete de 2k.`
    c. `FCS at end: True -> Tenemos checksum al final`
    d. `[…] (OFDM): False -> No estamos usando OFDM`
    e. `2 GHz spectrum: True -> Usamos la banda de 2.4GHz`
    f. `5 GHz spectrum: False -> No usamos la de 5GHz`
    g. `Gaussian FSK: False -> No usamos FSK Gaussiano (supongo que será una variante del FSK)`
    h. `Antenna: Present -> Me llama poderosamente la atención este campo, ¿cómo no va a haber una antena presente en la comunicación? Me pregunté.`
    `Leyendo sobre esto en [http://www.radiotap.org/fields/defined] resulta que es el número de la antena utilizada.`
    i. `dBm Antenna Signal: Present -> Indica la potencia de la antena, como diferencia desde una referencia arbitraria.`
    j. `Los otros, habla de parámetros y posibilidades que contempla el estándar 802.11, pero que en este caso están prácticamente todas a False.`

BEACONS: OBTENDO DATOS SOBRE AS CAPAS PHY Y MAC – FIGURAS

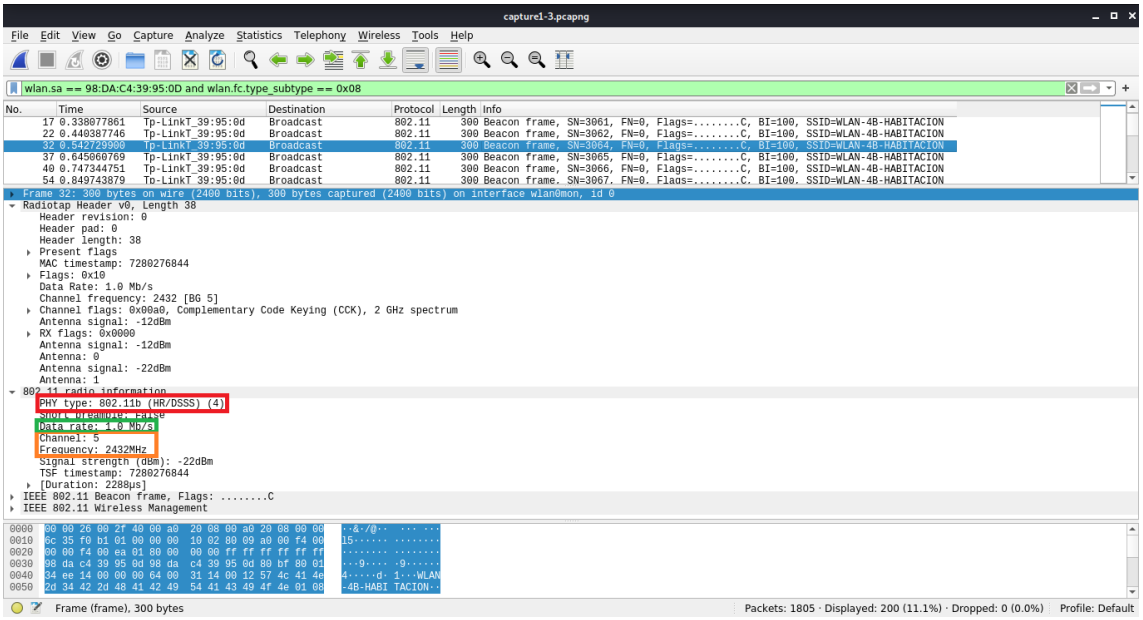


Figura 2: 802.11 radio information

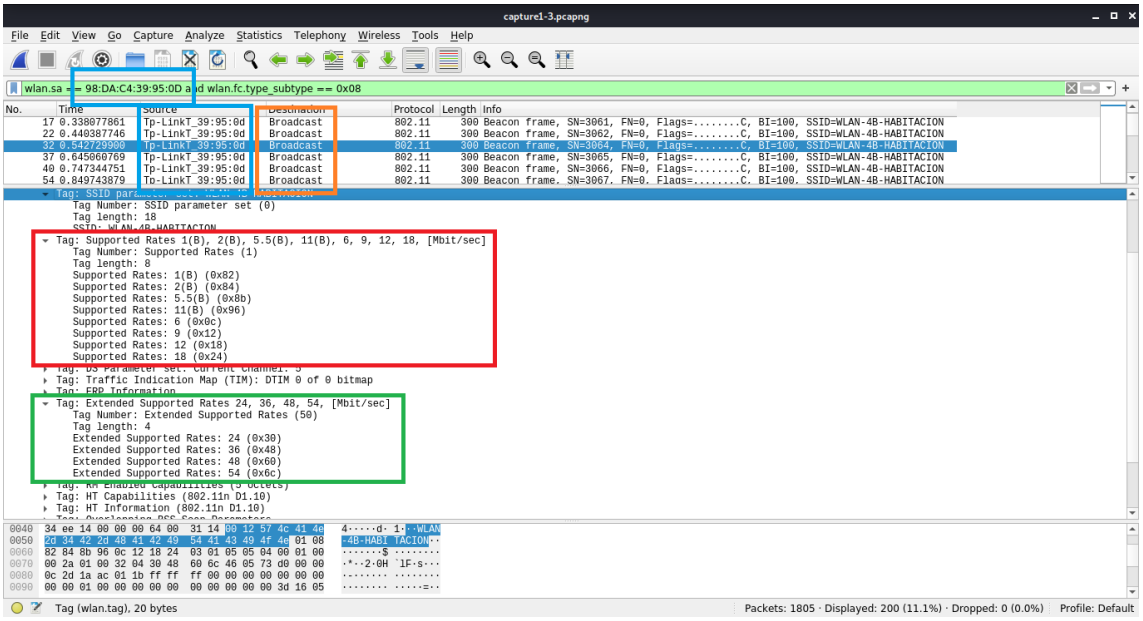


Figura 3: Supported rates y MACs Origen y Destino

BEACONS: CARACTERÍSTICAS BÁSICAS DUN AP

1. Inicialmente pensé que no había tenido interferencias, porque en todos marcaba "`IEEE 802.11 radio information -> Channel: 5`", pero parece que esa información es con respecto al canal en el que está sintonizada la antena WiFi local. Si vamos a "`IEEE 802.11 Wireless Management -> Tagged Parameters -> Tag: DS Parameter set: Current Channel: x`", veremos que x toma valores muy variados. Para mi red WiFi, efectivamente el canal es el 5, pero para otras se detectan valores como 6, 7, 4, y hasta 11.
   Por lo que sí, podemos concluir que se producen interferencias.

2. El SSID del AP monitorizado es `WLAN-4B-HABITACION` (que como su nombre indica, es la red WiFi del router que se encuentra en mi habitación). [Fig.4]

3. Como ya comenté en el apartado anterior en la cuestión 2, soporta:

   ```
    1,  2, 5.5, 11 Mbps ∈ 802.11b
    6,  9,  12, 18 Mbps ∈ 802.11g
   24, 36,  48, 54 Mbps ∈ 802.11n
   ```

   [802.11b/g Fig.3] [802.11n Fig.3]

4. Con respecto a WEP, podemos encontrar la ausencia de soporte para WEP en "`Radiotap Header v0 -> Flags -> WEP: False`".
   Con respecto a WPA(2) lo que he encontrado es en "`IEEE 802.11 Wireless Management -> Tagged Parameters -> Tag: RSN Information`", múltiples campos que hablan de la seguridad de la red. Por ejemplo "`Group Cipher Suite: […] TKIP`", "`Pairwise Cipher Suite: […] AES (CCM)`", etc. [Fig.5]

BEACONS: CARACTERÍSTICAS BÁSICAS DUN AP – FIGURAS

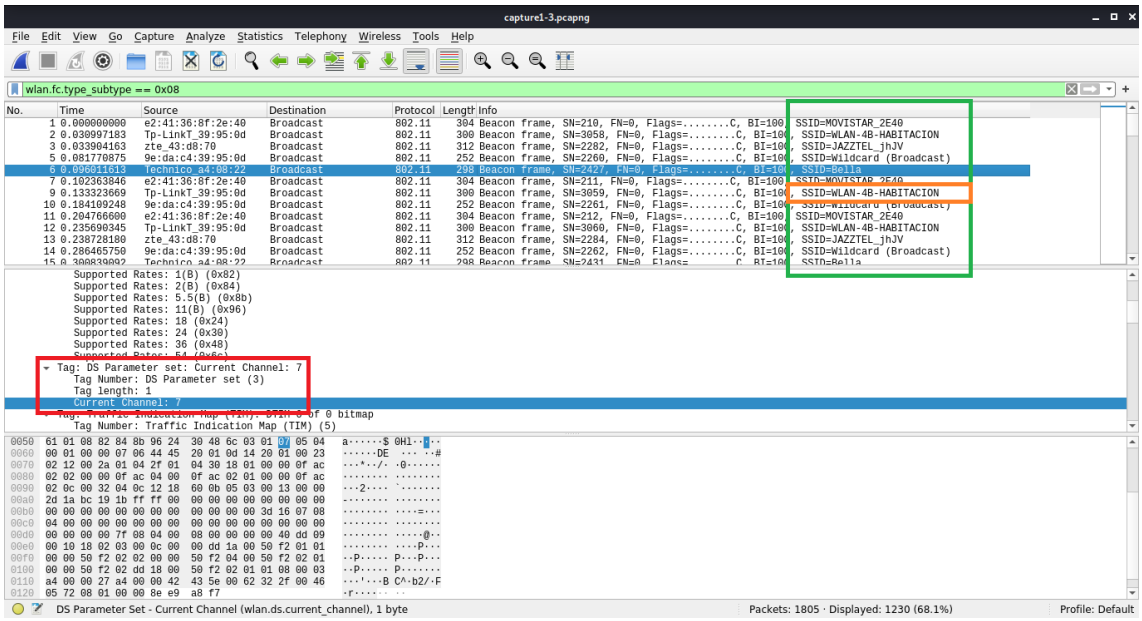


Figura 4: SSIDs de las redes vecinas, y Current Channel de una de ellas

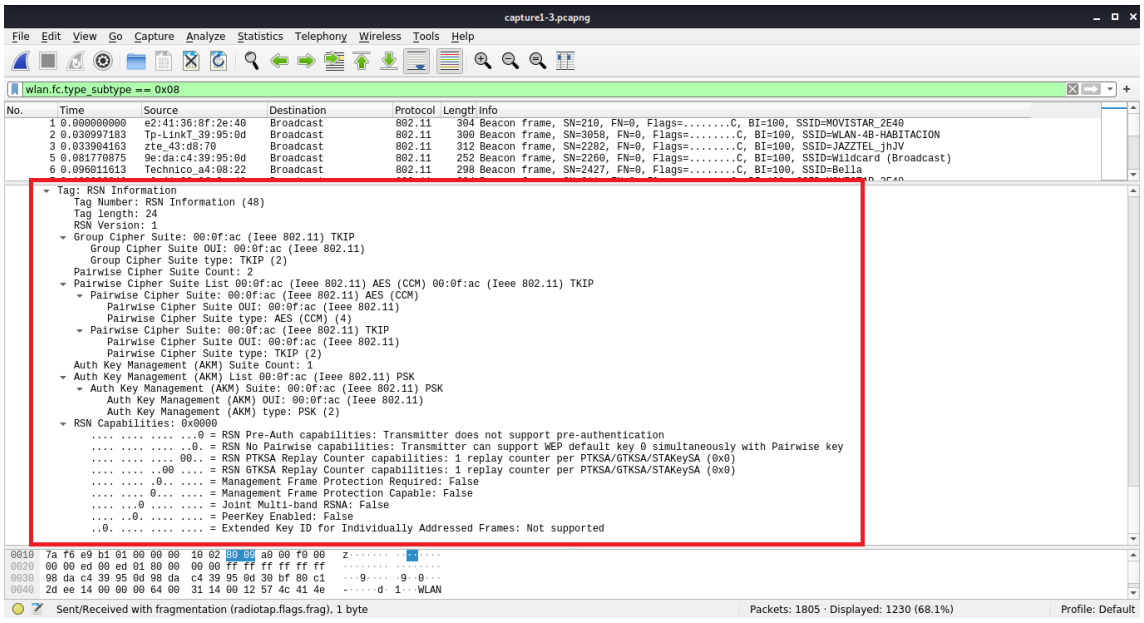


Figura 5: RSN Information del WiFi AP monitorizado

OBTENDO INFORMACIÓN DE CLIENTES: PROBE REQUESTS

1. El destino es la MAC de broadcast, por lo que se trata de un broadcast. [Fig.6]
2. Es posible identificar al emisor con su MAC. En este caso, estamos filtrando por la MAC del emisor, debido a la cantidad de redes WiFi vecinas que tengo.
   En este caso la MAC es `AC:C1:EE:51:EC:4F` [Fig.6] con `AC:C1:EE:` identificando al fabricante `Xiaomi Communications Co Ltd.` [https://hwaddress.com/oui-iab/AC-C1-EE/]

3. Soporta:

   ```
    1,  2, 5.5, 11 Mbps ∈ 802.11b
    6,  9,  12, 18 Mbps ∈ 802.11g
   24, 36,  48, 54 Mbps ∈ 802.11n
   ```

   [802.11b/g Fig.7] [802.11n Fig.7]

4. La principal diferencia es que estos probe responses son con un destino determinado, en este caso el teléfono móvil Xiaomi [Fig.8].
   También me llama la atención que se retransmiten muchas veces, puesto que después de cada envío, se retransmite el paquete tres veces más (podemos observar esto en que la flag R está activa [Fig.8]).
   Por el resto, son muy similares. También podemos encontrar los Supported rates, RSN information, etc.

OBTENDO INFORMACIÓN DE CLIENTES: PROBE REQUESTS – FIGURAS

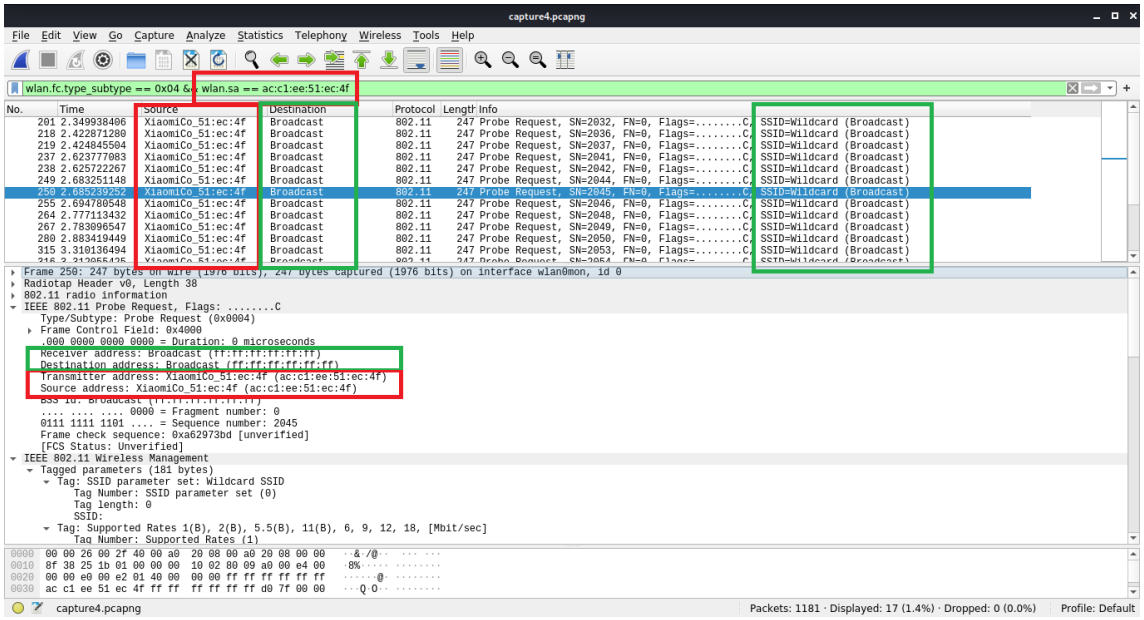


Figura 6: Filtrado de probe requests

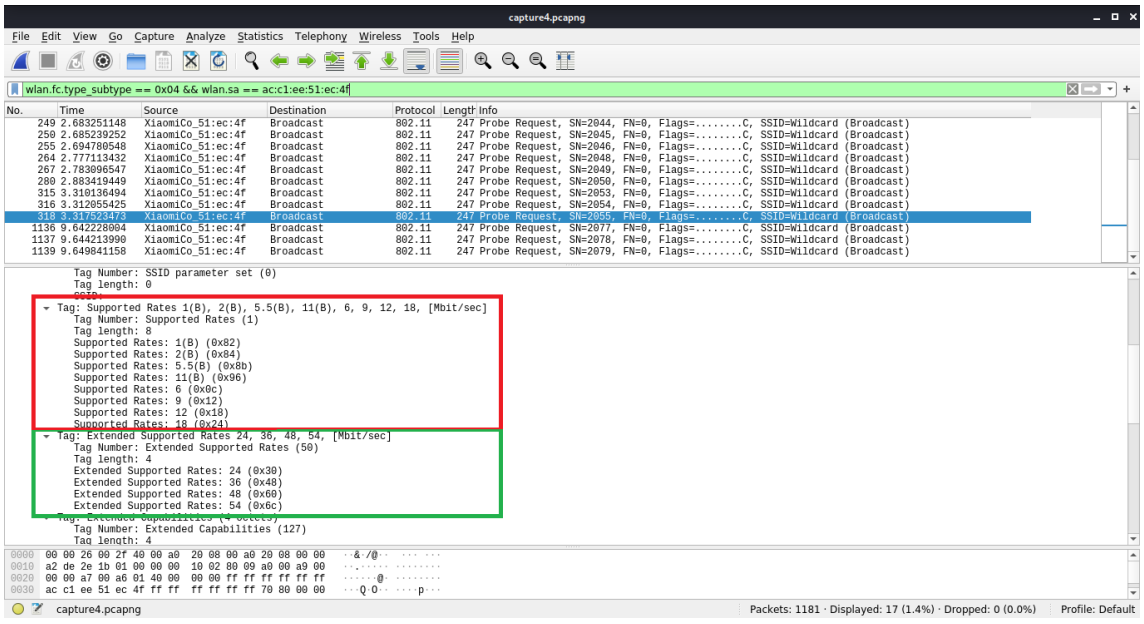


Figura 7: Supported Rates para probe request

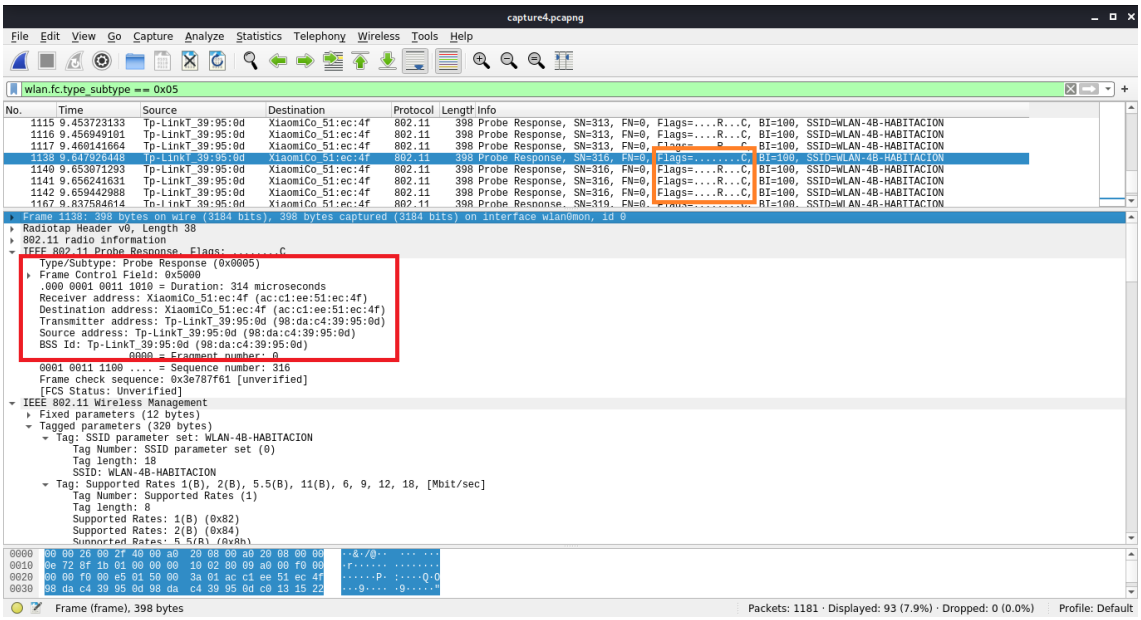


Figura 8: Diferencias entre probe reply y beacon

ACCESO AO MEDIO CON CSMA/CA: ANÁLISE TEMPORAL

1. Yo en este caso creo que no se aprecia mucho el NAV, no porque se transmita información antes, es decir, en eso se respeta, durante los x µs que se "reservan", nadie transmite nada. La historia es que después tampoco. Por qué? Porque en mi caso, directamente he tenido que activar el WiFi de 2.4GHz, ya que en mi habitación no lo utilizo para nada, y directamente lo tengo desactivado.
   Para realizar esta práctica lo he activado, y he conectado un par de móviles a la red, pero aún así no se transmite justo después del NAV, ni mucho menos.
   Así, analizando la figura 9:

   `-> Δt = t[437] – t[436] = 16.692µs < 314µs = NAV` [Fig.9]

   `-> t[438] > t[436] + NAV` [Fig.9]

   Por tanto, se cumple que durante el NAV=314µs [Fig.9] nadie envía nada. (De todos modos lo que comentaba antes, como únicamente en esta WiFi están el Xiaomi de los apartados anteriores, y este nuevo LG conectado para este apartado, pues las probabilidades de que alguien enviase algo durante el NAV ya eran bajas de por sí. De ahí que el LG ni siquiera esté transmitiendo justo después de NAV, sino que aún pasa un buen tiempo hasta que transmite algo más).

   Un detalle, por comentar más que nada como curiosidad, y es que como el LG se está conectando a internet, tenemos una MAC de receptor de señal (el router TP-Link de apartados anteriores), tenemos IP de transmisor (móvil de LG), pero además tenemos en destination address un router ZTE, que es el router que da salida a internet desde mi casa, al cual se conecta por cable el TP-Link que tengo en mi habitación. [Fig.9]

2. El valor es 0, lo cual tiene todo el sentido, puesto que NAV ya incluye el tiempo de ACK, por lo que el tiempo restante estimado tiene que ser 0. [Fig.10]

3. Tiempo de transmisión del frame 436: 16.692µs.
   Tiempo de transmisión del frame 437 [ACK]: ? No me lo indica en ningún sitio
   Tiempo de backoff: ? La verdad, no sé cómo calcularlo con los datos que tengo... pero el resultado se tiene que encontrar entre `0` y `t[438] – t[437] = 5.9ms`.

ACCESO AO MEDIO CON CSMA/CA: ANÁLISE TEMPORAL – FIGURAS

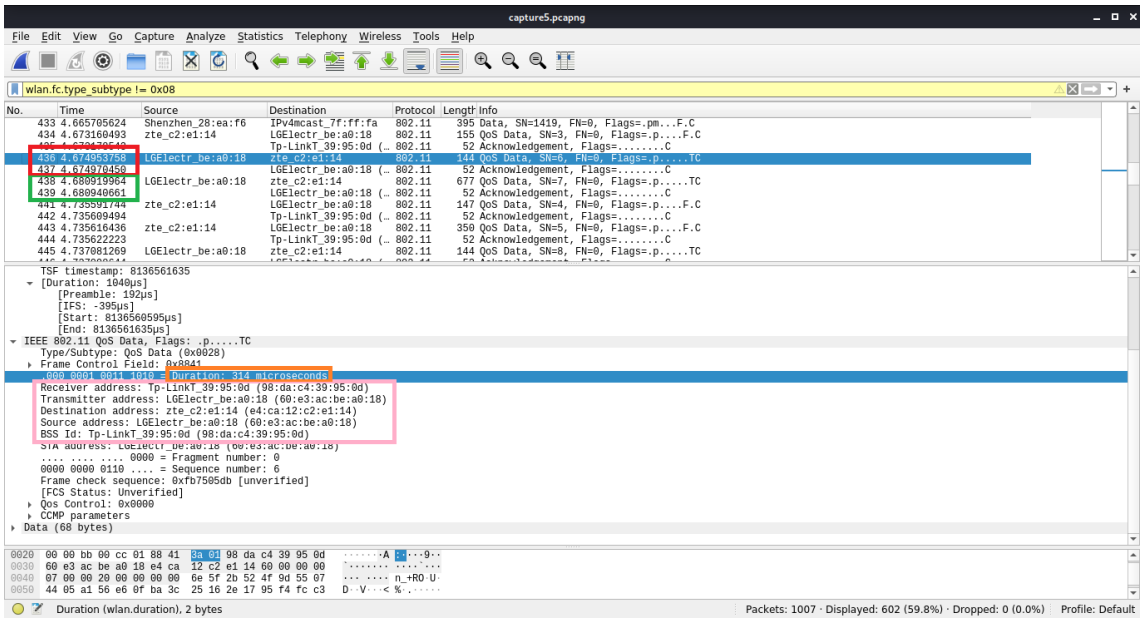


Figura 9: NAV vs Intervalo de Transmisión

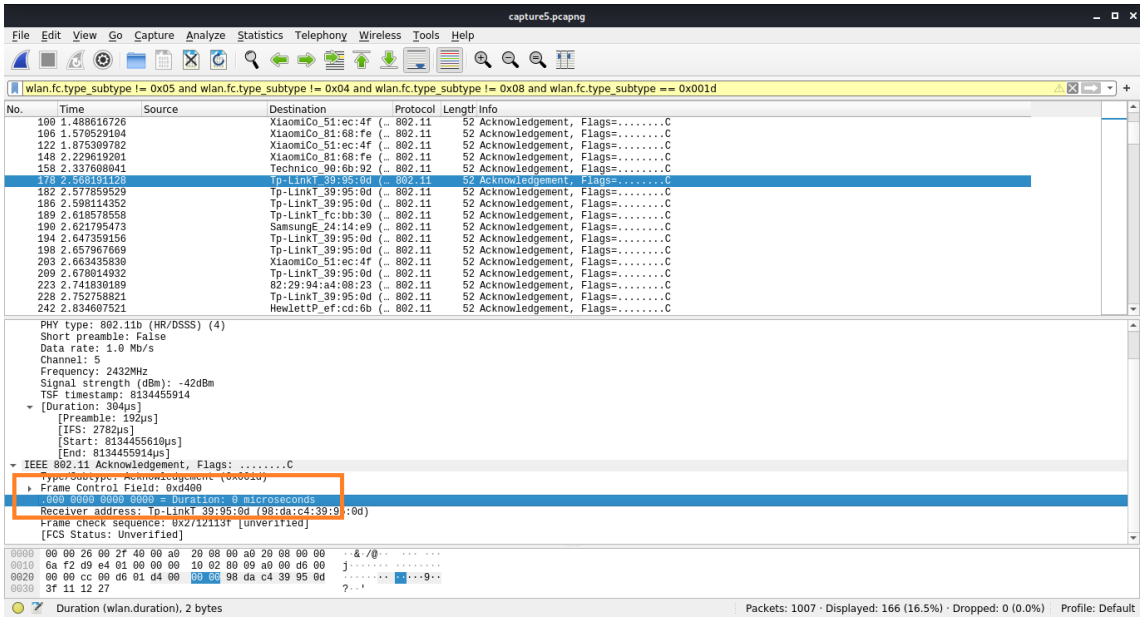


Figura 10: Valor Duration de un ACK

CONCLUSIONES

Los resultados son los esperados. La práctica me ha resultado muy interesante, y me ha servido para ver los campos de una trama, cómo realmente esa información está codificada de forma ordenada y lógica, y se corresponde con lo que se espera de ella.

El último apartado ha servido para confundirme más que otra cosa, pero la verdad es que me gustan mucho estas prácticas donde te metes en detalle en lo que estudias.

Alonso Rodriguez Iglesias. 17-Mayo-2020