**IEEE 802.11 con Wireshark**

**1A. (Para Wireshark\_802\_11 y Wireshark\_802\_11LOCAL) ¿Cuántas APs están en la cobertura de la estación desde la que se realizó la captura? (Localiza las tramas Beacon) ¿Cuáles son los identificadores de las tres estaciones desde las que se están recibiendo más tramas de este tipo? ¿Cada cuánto tiempo envían una trama Beacon? ¿Qué tipo de trama es? (valor del campo tipo).**

*Comando usado: wlan.fc.type\_subtype==8*

El valor del campo tipo para todas las tramas es 0, ya que son tramas de gestión.

Tiempo de intervalo de envío de tramas igual para todas las estaciones.

A screenshot of a computer

Description automatically generated

d3:95:ca:bb:f0:f5 / LinksysG\_67:22:94 / Cisco-Li\_f7:1d:51 / Cisco-Li\_f5:ba:bb / 00:ac:20:67:22:94 / 00:86:bc:d2:22:94

|  |  |  |
| --- | --- | --- |
| ***N*** | ***AP*** | ***Tiempo Envío (segundos)*** |
| 1 | Cisco-Li\_f7:1d:51 | 0.102400 |
| 2 | Cisco-Li\_f5:ba:bb | 0.102400 |
| 3 | LinksysG\_67:22:94 | 0.102400 |

A screenshot of a computer

Description automatically generated

*802.11*

Hay 33 APs

Mas repetidas: 00:1e: 7a:a9:50:a5 / 00:1e:7a:a9:50:a4 / 00:1e:7a:a9:50:a2

A screenshot of a computer

Description automatically generated

*802.11 Local*

**1B. (Para Wireshark\_802\_11) Muestra con una captura de pantalla la estructura y contenido de los campos de una trama Beacon.**

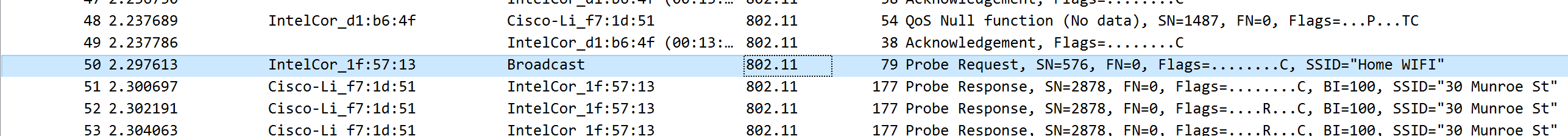
A diagram of a data flow

Description automatically generated with medium confidence

**2A. (Para Wireshark\_802\_11 y Wireshark\_802\_11LOCAL) ¿En la captura, hay alguna estación que realice un escaneo activo? ¿Hay APs que respondan? ¿Qué tipos de tramas son? (Consulta e indica el valor del campo tipo).**

*Wireshark\_802\_11*

Tramas 50 y 51, donde InterCor manda un mensaje BroadCast de tipo Probe Request y le responde AP Cisco-Li… con una trama de tipo Probe Request.



Las tramas que realizan un escaneo activo son IntelCor\_1f: 57:13 y IntelCor\_d1: b6:4f, y los puntos de acceso que responde es Cisco-Li\_f7:1d:51.

*Wireshark\_802\_11\_LOCAL*

Tenemos hasta 8 estaciones que realizan escaneos activos.

A group of black and white text

Description automatically generated

*Se adjuntan algunas de ellas*

**2B. (Para Wireshark\_802\_11 y Wireshark\_802\_11LOCAL) Localiza en la captura alguna trama de petición activo y la respuesta correspondiente. Muestra con una captura de pantalla la estructura y contenido de ambas tramas.**

*Tramas 50 y 51 en por ejemplo Wireshark\_802\_11*

A screenshot of a computer

Description automatically generated

*Probe Request*

A screenshot of a computer

Description automatically generated

*Probe Response*

**3A. Localiza en la captura Wireshark\_802\_11 alguna petición de asociación. ¿Qué información incluye? Localiza en la captura alguna respuesta de asociación. ¿Qué información incluye? ¿Qué tipos de tramas son? (valor del campo tipo).**

A screenshot of a computer

Description automatically generated

*Filtramos con wlan.fc.type\_subtype==0x0000*

A screenshot of a computer program

Description automatically generated

*Ejemplo de contenido de la trama*

**3B. Localiza en la captura Wireshark\_802\_11 alguna trama de petición de asociación y la respuesta correspondiente. Muestra con una captura de pantalla la estructura y contenido de ambas tramas.**

A screenshot of a computer

Description automatically generated

*Filtramos por wlan.fc.type\_subtype==0x0000 || wlan.fc.type\_subtype==0x0001*

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

*Trama Association Request Trama Association Response*

**A diagram of a computer connected to a wireless network

Description automatically generated4 ¿Cuál de estos dos escenarios correspondería con un escaneado pasivo y con uno activo? ¿Por qué?**

El escenario A representa un **escaneo pasivo**. Los puntos de acceso se ponen en contacto con la estación enviándole tramas Beacon. La estación elige un punto de acceso para mandar peticiones de conexión con Association Request y la AP responde con un Association Response.

A diagram of a computer connected to a wireless network

Description automatically generated

El escenario B representa un **escaneo activo**. En este caso es la estación quién manda tramas Probe Request buscando APs cercanos, quienes reciben la trama y le envían de vuelta a la estación una trama Probe Response para confirma que existe. Tras ello, es la estación la que nuevamente el elige una AP y empieza a enviarle peticiones.

**5A. ¿Cuántas tramas de datos diferentes observas en la captura Wireshark\_802\_11LOCAL? ¿Qué estaciones participan de esta comunicación? ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?**

Encontramos tramas Data, QoS Data y Null Function. Entre las estaciones que participan se encuentran Cisco, Apple, ASUS e Intel, donde se producen entre ellas comunicaciones directas.

**5B Localiza en la captura Wireshark\_802\_11 alguna trama de datos y la confirmación correspondiente. Muestra la estructura y contenido de ambas tramas.**



A screenshot of a computer

Description automatically generated

*Trama QoS*

A screenshot of a computer code

Description automatically generated

*Trama ACK de confirmación*

**5C. Localiza en la captura Wireshark\_802\_11LOCAL alguna trama de datos NULL Muestra la estructura y contenido de esta trama. ¿Qué la diferencia de las tramas de datos normales? ¿Para qué sirve?**

A screenshot of a computer

Description automatically generatedNo contiene el campo Data, ya que no contiene datos. La utilidad principal que tiene este tipo de tramas son varias, como para el mantenimiento de la conexión, permitiendo mantener activa la conexión entre un dispositivo cliente y un AP. Enviar información sobre el estado del dispositivo, como el consumo, o para sincronizar dispositivos como cuando queremos hacer un *login* a un servidor.

**6. Encuentra la trama que contenga el segmento TCP SYN de la primera sesión TCP (que descarga alice.txt). Muestra su contenido.**

**6A. ¿Cuáles son las tres direcciones MAC de esta trama? ¿Cuál es la dirección MAC correspondiente al host inalámbrico desde el que se hace la petición? (representación hexadecimal) ¿Cuál la del punto de acceso? ¿y la del (primer) router?**

A screenshot of a computer

Description automatically generated

*A screenshot of a computer

Description automatically generatedFiltramos por http y la primera trama será la que buscamos*

Si observamos la trama podemos ver que en el campo DS status tenemos un valor de 01, donde el To DS es un 1 y el From DS es un 0. Por lo tanto, mirando las diapositivas podemos darnos cuenta de que estamos en el caso 3 de los mecanismos de direccionamiento.



**A table with different languages

Description automatically generatedAP receptor**: 00:16:b6:f7:1d:51

**Origen**: 00:13:02:d1:b6:4f

**Destino**: 00:16:b6:f4:eb:a8

**6B. ¿Cuál es la dirección IP del host inalámbrico que envía este segmento? ¿y la dirección IP destino? ¿con que se corresponde esta dirección IP destino? (host, punto de acceso, router, o cualquier otro dispositivo de la red). Razona tu respuesta.**



La IP del host que envía la petición es 192.168.1.109, y la IP destino es 128.119.245.12. La dirección IP corresponde con la página web de la universidad de Massachusetts.

**7. Localiza las tramas RTS y CTS en la captura Wireshark\_802\_11. ¿Es posible que sólo haya tramas RTS? ¿Y CTS? ¿Por qué?**



Solo tenemos una trama que es CTS.

Puede haber solo tramas RTS o CTS. Por ejemplo, un punto de acceso puede enviar tramas RTS, pero no haber tramas CTS debido a que no hay nadie a quién haya podido conectarse. Y en el caso de CTS, se puede enviar una trama de este tipo para decir que la estación está disponible para recibir información, pero que durante el tiempo que dura la captura no se ha querido enviar nada.

**8. Localiza las tramas RTS y CTS capturadas en el fichero Wireshark\_802\_11\_RTS\_CTS.pcap. ¿Qué información contienen estas tramas? ¿Para qué sirve el valor NAV? Identifica su valor en la trama.**

**RTS**: Es una trama de control que indica la intención de transmitir y solicita permiso para hacerlo, ayudando a evitar colisiones en el canal al reservar tiempo para transmitir y notifica a otros dispositivos cercanos que deben esperar antes de intentar transmitir. Contiene la dirección del receptor y del transmisor y el NAV, que es el tiempo mencionado previamente que se solicita para reservar el canal y transmitir sin colisiones.

**CTS**: Trama que confirma que el canal está libre y que el dispositivo que envió la trama RTS puede proceder con la transmisión. Contiene la dirección del receptor y el NAV, menor que el del RTS.

**NAV**: El NAV es un vector de asignación de red, es el tiempo que se necesita utilizar el canal según el tamaño de la trama, en el RTS se manda al dispositivo al que se le quiere mandar información, y en el CTS se difunde por los demás dispositivos para que sepan que en ese tiempo el canal va a estar ocupado y hasta que no se acabe ese tiempo no intenten transmitir.