## Configuración del puente WDS

**MAC WIFI1:** 00:1F:C6:82:22:40

**IP WIFI1:** 192.168.1.1

**Wireless:** SSID halo canal 10

**MAC PC1:** 00:1b:21:82:71:1e

**IP PC1(eth1)**: 192.168.1.119

**MAC WIFI2:** 00:1F:C6:51:33:F4

**IP WIFI1:** 192.168.1.2

**Wireless:** SSID halo canal 10

**MAC PC2:** 00:1b:21:82:71:36

**IP PC2(eth1)**: 192.168.1.101

Ejercicio 1

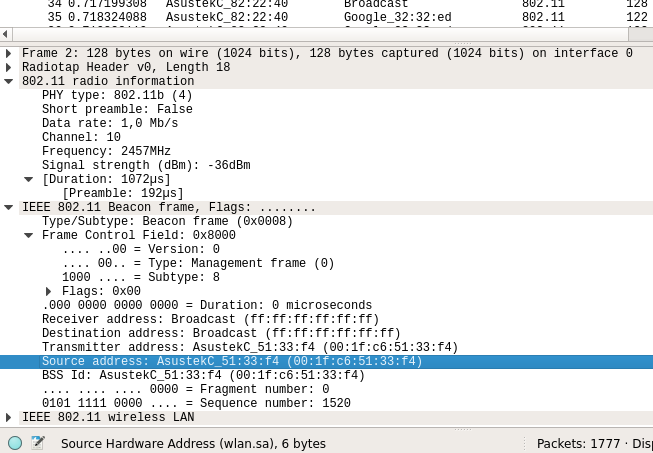
¿Por qué crees que ha sido necesario configurar las direcciones MAC entre ambos puntos de acceso?

Ha sido necesario, para que ambos se conozcan mutuamente, para poder funcionar en modo puente. Sino tuviéramos que configurar en ambos la MAC, cualquiera podría dar uso de nuestra red inalámbrica, solo conociendo la MAC del dispositivo

Ejercicio 2

1. Observad la lista de tramas capturadas. Comprobad que la mayoría de ellas pertenecen a la red de nuestro SSID.
2. Seleccionad una trama cualquiera de tipo “Beacon” y examinad el apartado “802.11

Beacon Frame” de la trama ¿Podemos saber el origen de la trama?

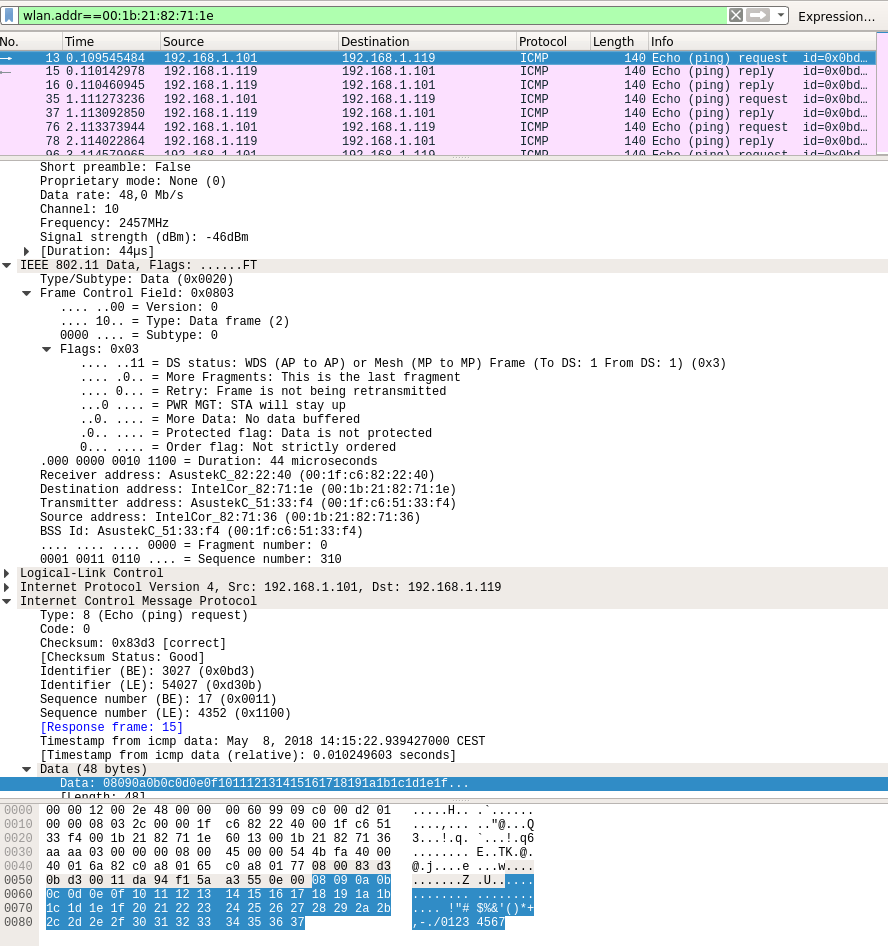


1. Filtrad aquellas cuyo origen o destino sea uno de nuestros PCs (filtro IEEE 802.11,

campo “wlan.addr==MAC\_PC\_ETH”) y examinad alguna de ellas. ¿Están cifrados

los datos que transportan?

No, se puede leer claramente los datos del mensaje.



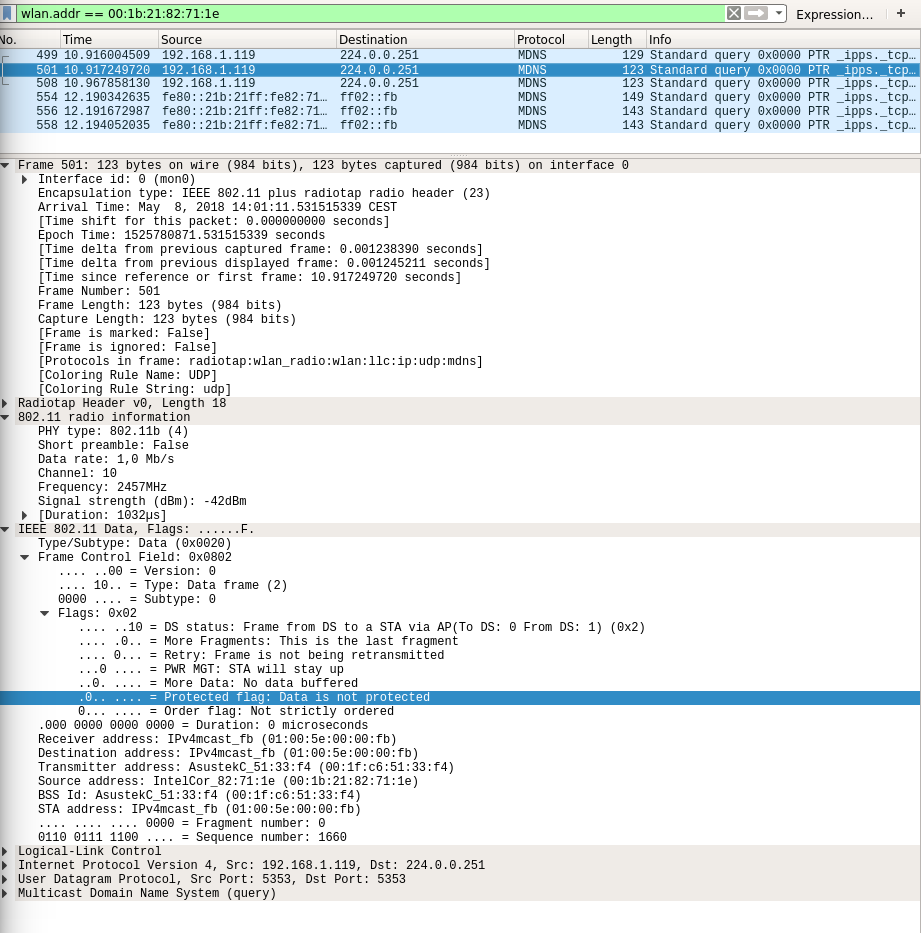
1. Filtrad por ICMP (escribiendo “ICMP” directamente en la caja de texto del filtro).

¿Cuál es la dirección MAC del origen de la trama? ¿Cuál es la dirección MAC del

transmisor de la trama?

Como no está cifrado, nos aparece claramente el protocolo ICMP, que es utilizado para comunicarse entre PC, pero si estamos cifrado no aparece dicho campo.

La manera de saber que MAC es, y si está cifrado, hacemos uso de “ wlan.addr==MAC\_PC\_ETH”,nos devolvera tramas del tipo ICMP

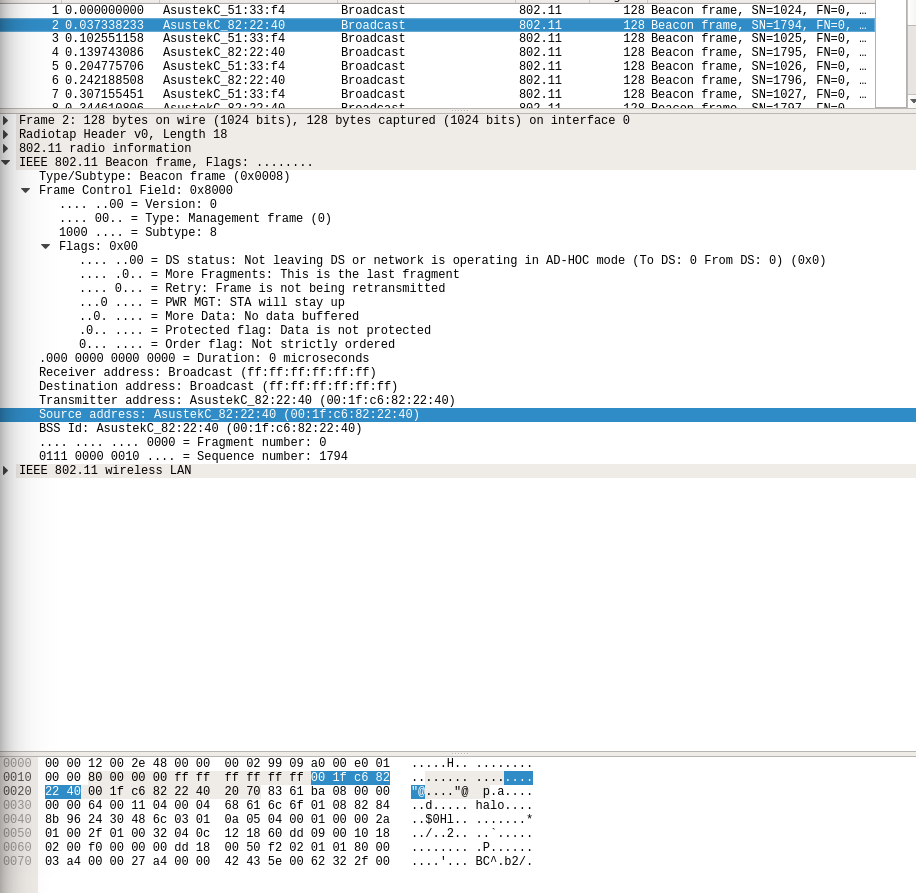


Ejercicio 3

1. Seleccionad una cualquiera de las de tipo “Beacon” y examinad el apartado “802.11

Beacon Frame” de la trama ¿Podemos saber quién la envía? ¿Están cifradas este

tipo de tramas?

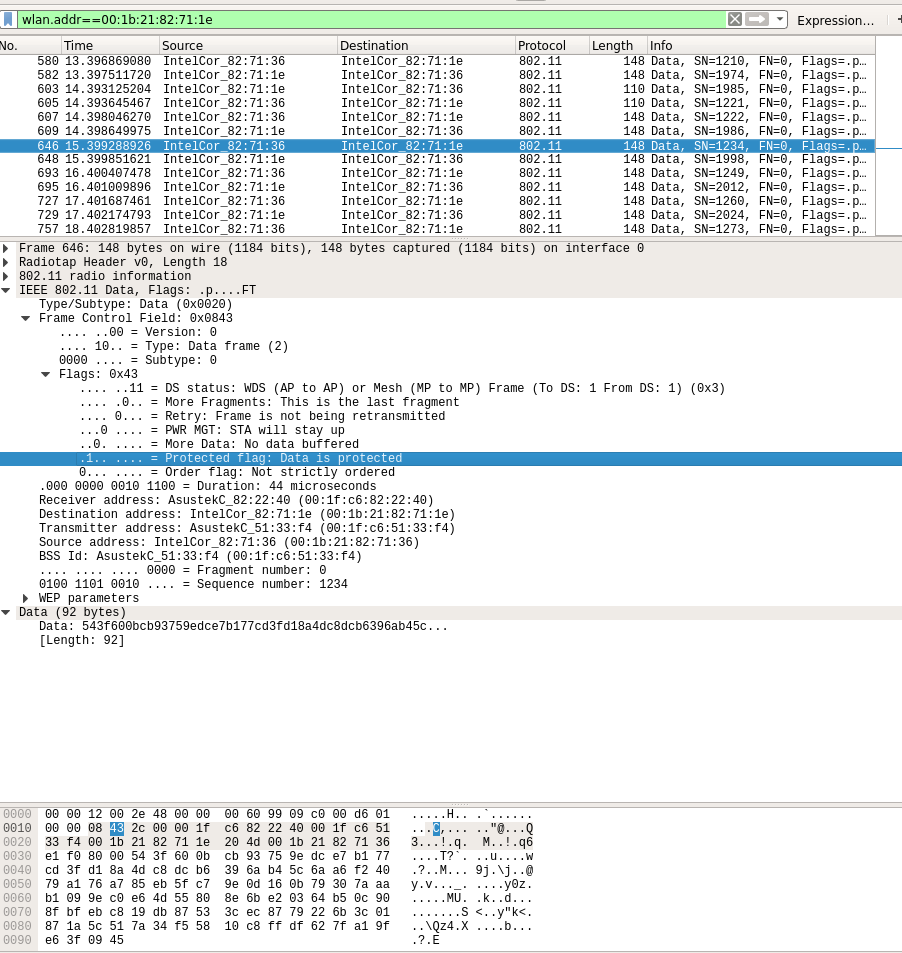


No están cifradas se puede leer perfectamente el nombre del SSID halo, porque no lleva datos críticos al ser un datagrama de baliza.

1. Filtrad aquellas cuyo origen o destino sea uno de nuestros PCs (filtro IEEE 802.11,

campo “wlan.addr==MAC\_PC\_ETH”) y examinad alguna de ellas. ¿Cuántas tra-

más habéis encontrado? ¿Qué datos contienen dichas tramas?



1. ¿Qué tramas estan cifradas? ¿Qué tramas no lo están? ¿Qué partes de la trama

están cifradas? ¿Se filtra toda la trama?

Tramas cifradas, son las de ICMP, en cambio as de Baliza no (Beacon frame).

Las partes cifradas son el protocolo, ya que en vez de ICMP como antes aparece solo 802.11 y el campo de datos, porque ya no aparecen al final números, sino caracteres extraños.

Pero no se filtra todas las tramas, las macs de origen o de destino como vemos no está cifrado.

**Ejercicio 4**

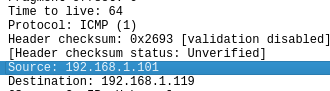
Observad de nuevo la lista de tramas capturadas. Volved a filtrar por ICMP. ¿Podéis

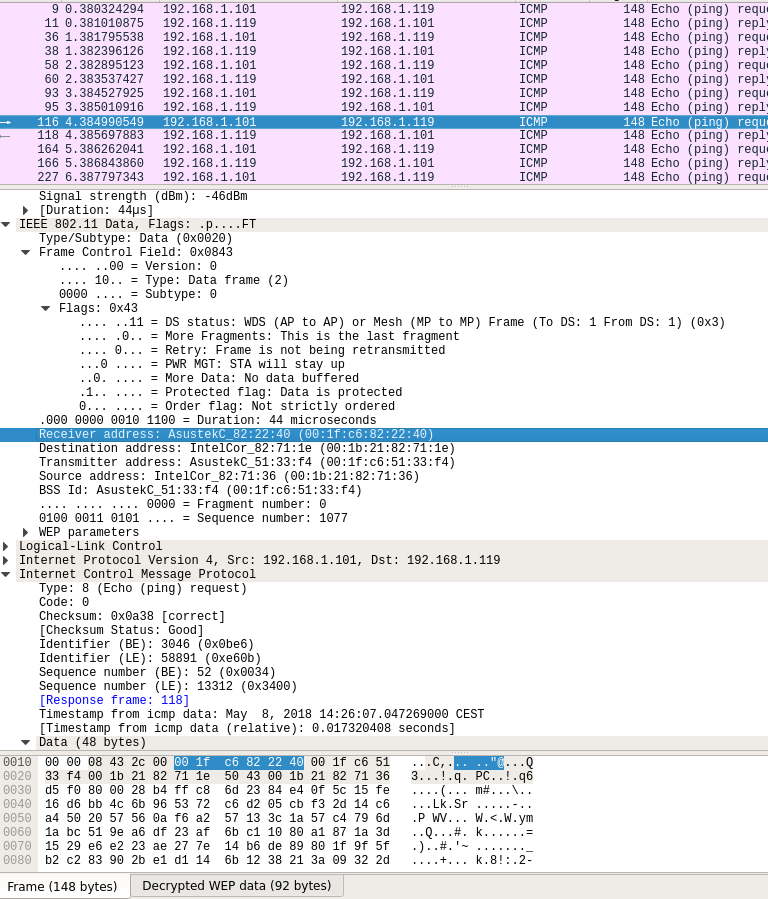
ver el contenido ahora?

NO, están cifrados los datos y wireshark no lo puede mostrar. SI ponemos el descifrado con la key si se puede ver todo, i se puede ver los ICMP

Examinad las cabeceras IP e ICMP de las tramas que contienen los pings. Comprueba que las direcciones IP que figuran son las esperadas ¿Cuál es el tiempo de vida (TTL) de estos paquetes?

TTL = 64





Examinad las cabeceras MAC de las tramas que contienen los ping ¿Cuántas direc-

ciones MAC se emplean en las comunicaciones a través del puente WDS? ¿Para que se usa cada una de ellas?

Son 4

