ALBERTO LEÓN LUENGO

MEMORIA PRÁCTICA 5: WIFI

ÍNDICE DE CONTENIDOS

1. ESCENARIO SIMPLE
    - PREGUNTA 1
    - PREGUNTA 2
    - PREGUNTA 3
    - PREGUNTA 4
    - PREGUNTA 5
    - PREGUNTA 6
    - PREGUNTA 7
    - PREGUNTA 8
    - PREGUNTA 9
    - PREGUNTA 10
    - PREGUNTA 11
    - PREGUNTA 12
    - PREGUNTA 13
    - PREGUNTA 14
    - PREGUNTA 15
    - PREGUNTA 16
    - PREGUNTA 17
    - PREGUNTA 18

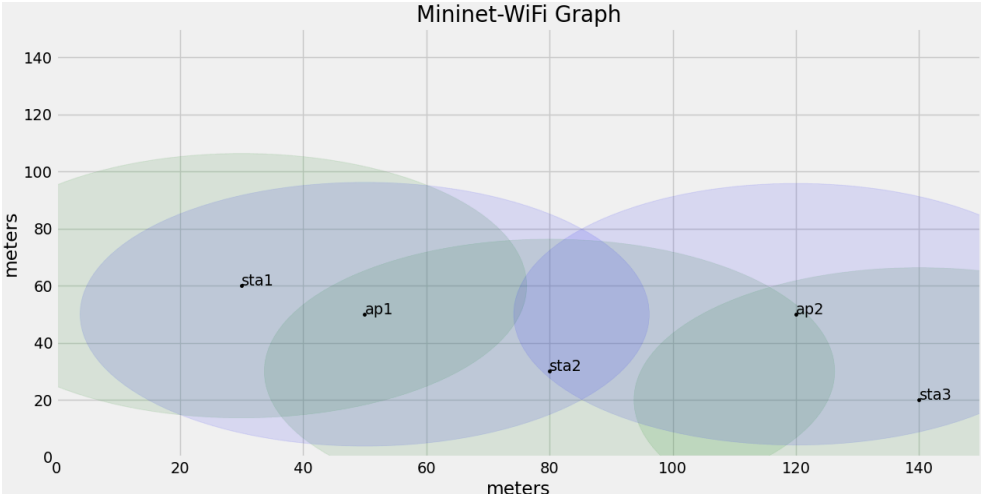
2. TRAMAS RTS/CTS
    - PREGUNTA 1
    - PREGUNTA 2
    - PREGUNTA 3
    - PREGUNTA 4
    - PREGUNTA 5
    - PREGUNTA 6

3. AUTENTICACIÓN
    - PREGUNTA 1
    - PREGUNTA 2
    - PREGUNTA 3
    - PREGUNTA 4
    - PREGUNTA 5
    - PREGUNTA 6

4. RED AD-HOC
    - PREGUNTA 1
    - PREGUNTA 2
    - PREGUNTA 3
    - PREGUNTA 4
    - PREGUNTA 5

[] 1. ESCENARIO SIMPLE

COMANDO: user@machine:~$ cd lab-wifi/ (acceder al directorio lab-wifi/)
COMANDO: user@machine:~$ sudo ./escenario_simple.py (arrancar el escenario escenario_simple.py)



PREGUNTA 1

COMANDO: mininet-wifi> net (mostrar las interfaces de red de los APs y las estaciones)

```
c0
sta1 sta1-wlan0:wifi
sta2 sta2-wlan0:wifi
sta3 sta3-wlan0:wifi
ap1 lo:  ap1-wlan1:wifi
ap2 lo:  ap2-wlan1:wifi
```

PREGUNTA 2

COMANDO: mininet-wifi> xterm sta1 (arrancar una terminal para sta1)
COMANDO: mininet-wifi> sta1 ip addr show (mostrar la configuración IP de la estación sta1)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
9: sta1-wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:00:11:11 brd ff:ff:ff:ff:ff:ff permaddr 02:00:00:00:00:00
    inet 11.211.0.1/8 brd 11.255.255.255 scope global sta1-wlan0
       valid_lft forever preferred_lft forever
    inet6 2001::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:fe00:1111/64 scope link
       valid_lft forever preferred_lft forever
```

La dirección MAC de sta1 es 00:00:00:00:11:11 y la dirección IP de sta1 es 11.211.0.1(/8).

PREGUNTA 3

COMANDO: mininet-wifi> sta1 iw dev (mostrar información de la interfaz inalámbrica de sta1)

```
phy#2
        Interface sta1-wlan0
                ifindex 9
                wdev 0x200000001
                addr 00:00:00:00:11:11
                ssid ssid1
                type managed
                channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
                txpower 14.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

COMANDO: mininet-wifi> sta1 iwconfig (mostrar información de la interfaz inalámbrica de sta1)

```
lo        no wireless extensions.

sta1-wlan0  IEEE 802.11  ESSID:"ssid1"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:11:01
          Bit Rate:1 Mb/s   Tx-Power=14 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=34/70  Signal level=-76 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:15   Missed beacon:0
```

Ambos comandos sirven para mostrar información sobre la interfaz inalámbrica de sta1, que es sta1-wlan0. Además, ésta posee un tipo de conexión managed, su ssid es ssid1 y su canal es el 1.

PREGUNTA 4

COMANDO: mininet-wifi> xterm sta2 (arrancar una terminal para sta2)

COMANDO: mininet-wifi> sta2 ip addr show (mostrar la configuración IP de la estación sta2)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
10: sta2-wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:00:11:22 brd ff:ff:ff:ff:ff:ff permaddr 02:00:00:00:01:00
    inet 11.211.0.2/8 brd 11.255.255.255 scope global sta2-wlan0
       valid_lft forever preferred_lft forever
    inet6 2001::2/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:fe00:1122/64 scope link
       valid_lft forever preferred_lft forever
```

La dirección MAC de sta2 es 00:00:00:00:11:22 y la dirección IP de sta2 es 11.211.0.2(/8).

COMANDO: mininet-wifi> sta2 iw dev (mostrar información de la interfaz inalámbrica de sta2)

```
phy#3
        Interface sta2-wlan0
                ifindex 10
                wdev 0x300000001
                addr 00:00:00:00:11:22
                ssid ssid1
                type managed
                channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
                txpower 14.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

COMANDO: mininet-wifi> sta2 iwconfig (mostrar información de la interfaz inalámbrica de sta2)

```
lo        no wireless extensions.

sta2-wlan0  IEEE 802.11  ESSID:"ssid1"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:11:01
          Bit Rate:1 Mb/s   Tx-Power=14 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=24/70  Signal level=-86 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:15   Missed beacon:0
```

Ambos comandos sirven para mostrar información sobre la interfaz inalámbrica de sta2, que es sta2-wlan0. Además, ésta posee un tipo de conexión managed, su ssid es ssid1 y su canal es el 1.

COMANDO: mininet-wifi> xterm sta3 (arrancar una terminal para sta3)

COMANDO: mininet-wifi> sta3 ip addr show (mostrar la configuración IP de la estación sta3)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
11: sta3-wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:00:11:33 brd ff:ff:ff:ff:ff:ff permaddr 02:00:00:00:02:00
    inet 11.211.0.3/8 brd 11.255.255.255 scope global sta3-wlan0
       valid_lft forever preferred_lft forever
    inet6 2001::3/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:fe00:1133/64 scope link
       valid_lft forever preferred_lft forever
```

La dirección MAC de sta3 es 00:00:00:00:11:33 y la dirección IP de sta3 es 11.211.0.3(/8).

COMANDO: mininet-wifi> sta3 iw dev (mostrar información de la interfaz inalámbrica de sta3)

```
phy#4
        Interface sta3-wlan0
                ifindex 11
                wdev 0x400000001
                addr 00:00:00:00:11:33
                ssid ssid2
                type managed
                channel 10 (2457 MHz), width: 20 MHz (no HT), center1: 2457 MHz
                txpower 14.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

COMANDO: mininet-wifi> sta3 iwconfig (mostrar información de la interfaz inalámbrica de sta3)

```
lo        no wireless extensions.

sta3-wlan0  IEEE 802.11  ESSID:"ssid2"
          Mode:Managed  Frequency:2.457 GHz  Access Point: 00:00:00:00:11:02
          Bit Rate:1 Mb/s   Tx-Power=14 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=24/70  Signal level=-86 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:15   Missed beacon:0
```

Ambos comandos sirven para mostrar información sobre la interfaz inalámbrica de sta3, que es sta3-wlan0. Además, ésta posee un tipo de conexión managed, su ssid es ssid2 y su canal es el 10.

Dispositivo	Interfaz inalámbrica	Dir. MAC	Dir. IP	Tipo de conexión	SSID	Canal
sta1	sta1-wlan0	00:00:00:00:11:11	11.211.0.1	managed	ssid1	1
sta2	sta2-wlan0	00:00:00:00:11:22	11.211.0.2	managed	ssid1	1
sta3	sta3-wlan0	00:00:00:00:11:33	11.211.0.3	managed	ssid2	10

PREGUNTA 5

COMANDO: root@machine:# wireshark (arrancar wireshark desde la terminal de sta1)

Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start

COMANDO: mininet-wifi> sta1 ping -c 3 11.211.0.2 (realizar ping de sta1 a sta2)

COMANDO: mininet-wifi> sta1 ping -c 3 11.211.0.3 (realizar ping de sta1 a sta3)

Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop

Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-01.cap (Wireshark/tcpdump/… - pcap)

COMANDO: user@machine:~$ wireshark wifi-01.cap (abrir una captura de tráfico en wireshark)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	11.211.0.1	11.211.0.2	ICMP	98	Echo (ping) request id=0x5e3f, seq=1/256, ttl=64 (reply in 2)
2	0.001818	11.211.0.2	11.211.0.1	ICMP	98	Echo (ping) reply id=0x5e3f, seq=1/256, ttl=64 (request in 1)
3	1.001211	11.211.0.1	11.211.0.2	ICMP	98	Echo (ping) request id=0x5e3f, seq=2/512, ttl=64 (reply in 4)
4	1.003316	11.211.0.2	11.211.0.1	ICMP	98	Echo (ping) reply id=0x5e3f, seq=2/512, ttl=64 (request in 3)
5	2.002777	11.211.0.1	11.211.0.2	ICMP	98	Echo (ping) request id=0x5e3f, seq=3/768, ttl=64 (reply in 6)
6	2.003986	11.211.0.2	11.211.0.1	ICMP	98	Echo (ping) reply id=0x5e3f, seq=3/768, ttl=64 (request in 5)
7	5.214914	00:00:00_00:11:11	00:00:00_00:11:22	ARP	42	Who has 11.211.0.2? Tell 11.211.0.1
8	5.215837	00:00:00_00:11:22	00:00:00_00:11:11	ARP	42	Who has 11.211.0.1? Tell 11.211.0.2
9	5.215862	00:00:00_00:11:11	00:00:00_00:11:22	ARP	42	11.211.0.1 is at 00:00:00:00:11:11
10	5.216656	00:00:00_00:11:22	00:00:00_00:11:11	ARP	42	11.211.0.2 is at 00:00:00:00:11:22
11	8.881858	00:00:00_00:11:11	Broadcast	ARP	42	Who has 11.211.0.3? Tell 11.211.0.1
12	9.886868	00:00:00_00:11:11	Broadcast	ARP	42	Who has 11.211.0.3? Tell 11.211.0.1
13	10.910866	00:00:00_00:11:11	Broadcast	ARP	42	Who has 11.211.0.3? Tell 11.211.0.1

Como se puede ver en la captura, el ping entre sta1 y sta2 funciona correctamente ya que ambas están asociadas al mismo AP, por lo que existe conectividad entre ambas. Sin embargo, el ping entre sta1 y sta3 no funciona ya que no se ha configurado una red que conecte ambos AP.

COMANDO: user@machine:~$ sudo ifconfig hwsim0 up (activar la interfaz hwsim0)

COMANDO: user@machine:~$ sudo wireshark (arrancar wireshark desde la máquina real)

IMPORTANTE: Seleccionar la interfaz hwsim0 antes de iniciar la captura.

Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start

COMANDO: root@machine:# iw dev sta1-wlan0 disconnect (desasociar estación a un SSID)

COMANDO: mininet-wifi> sta1 iw dev (mostrar información de la interfaz inalámbrica de sta1)

```
phy#2
        Interface sta1-wlan0
                ifindex 9
                wdev 0x200000001
                addr 00:00:00:00:11:11
                type managed
                txpower 20.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

En efecto, la línea ‘ssid ssid1’ ya no aparece al mostrar la información de la interfaz inalámbrica de sta1.

COMANDO: root@machine:# iw dev sta1-wlan0 connect ssid1 (asociar estación a un SSID)

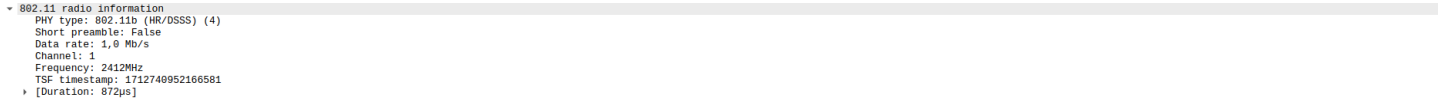
Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop

Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-02.cap (Wireshark/tcpdump/… - pcap)

COMANDO: user@machine:~$ wireshark wifi-02.cap (abrir una captura de tráfico en wireshark)

PREGUNTA 6

a)



Como se puede ver en la cabecera 802.11 radio information de este paquete, se está utilizando el canal 1, que transmite con una tasa de envío de 1 MBit/sec utilizando una frecuencia de 2412 MHz.

b)

Como se puede ver en la cabecera IEEE 802.11 Beacon frame de este paquete, los valores de los bits To Ds y From Ds que viajan en el campo Flags del campo Control Field son 0, los cuales vienen adjuntos al mensaje ‘DS status: Not leaving DS or network is operating in AD-HOC mode’. Esto quiere decir que las tramas se han enviado en modo ad-hoc y en modo infraestructura dirigido a tramas de gestión y control donde los nodos que se están comunicando proceden de una estación o de un AP.

c)

La primera dirección MAC es Receiver/Destination Address (Broadcast (ff:ff:ff:ff:ff:ff)), la cual es una dirección de Broadcast, por lo que no pertenece a ninguna máquina concreta.
La segunda dirección MAC es Transmitter/Source Address (00:00:00_00:11:01 (00:00:00:00:11:01)), la cual pertenece a ap1.
Y por último, la tercera dirección MAC es BSS Id (00:00:00_00:11:01 (00:00:00:00:11:01)), la cual, al igual que en el caso anterior, también pertenece a ap1.

d)

El número de secuencia de una trama baliza, que sirve para distinguir si una trama de datos está duplicada, es siempre 0, ya que no tiene la necesidad de identificar una trama específica en la secuencia de tramas transmitidas.

e)

El intervalo entre tramas baliza es de 0.102400 segundos, especificado en el campo Beacon Interval.

f)

El SSID que se está usando en este caso es ssid1, especificado en el primer tag (SSID parameter set) de la pestaña Tagged parameters.

g)

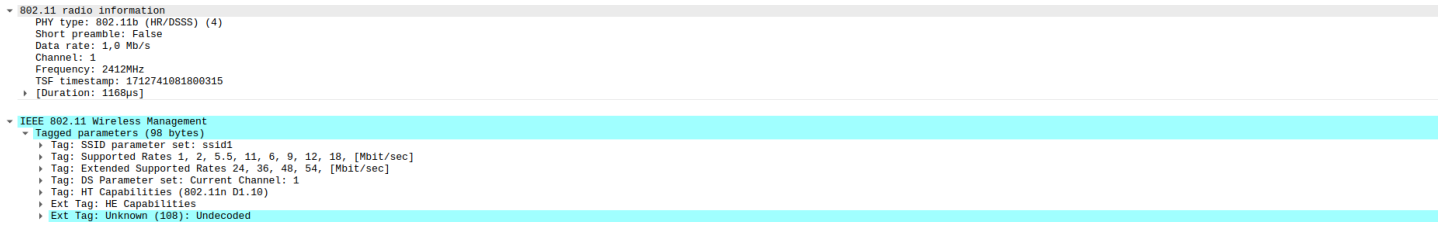
Como se puede ver en el campo Capabilities, la opción ESS capabilities es la que determina si el dispositivo que está transmitiendo es un AP o un cliente, siendo su valor 1 si transmite un AP y 0 si transmite un cliente. En este caso, el valor de este campo es 1, por tanto, quien transmite es un AP.

PREGUNTA 7

a)

La primera dirección MAC es Receiver/Destination Address (Broadcast (ff:ff:ff:ff:ff:ff)), la cual es una dirección de Broadcast, por lo que no pertenece a ninguna máquina concreta.
La segunda dirección MAC es Transmitter/Source Address (00:00:00_00:11:11 (00:00:00:00:11:11)), la cual pertenece a sta1.
Y por último, la tercera dirección MAC es BSS Id (Broadcast (ff:ff:ff:ff:ff:ff)), la cual, al igual que en la primera dirección, también es una dirección de Broadcast.

b)



Como se puede ver en la cabecera 802.11 radio information de este paquete, se está utilizando el canal 1.
Por otro lado, el SSID que se está usando en este caso es ssid1, especificado en el primer tag (SSID parameter set) de la pestaña Tagged parameters.

c)

Esta captura contiene varios mensajes Probe Request, ya que se están explorando todos los canales disponibles realizando un escaneado en cada uno de ellos.

PREGUNTA 8

a)

```
IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x0005)
  Frame Control Field: 0x5000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
    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... .... = +HTC/Order flag: Not strictly ordered
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Destination address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Transmitter address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Source address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  BSS Id: 00:00:00_00:11:01 (00:00:00:00:11:01)
  .... .... .... 0000 = Fragment number: 0
  0000 0010 1111 .... = Sequence number: 47
```

La primera dirección MAC es Receiver/Destination Address (00:00:00_00:11:11 (00:00:00:00:11:11)), la cual pertenece a sta1.
La segunda dirección MAC es Transmitter/Source Address (00:00:00_00:11:01 (00:00:00:00:11:01)), la cual pertenece a ap1.
Y por último, la tercera dirección MAC es BSS Id (00:00:00_00:11:01 (00:00:00:00:11:01)), la cual, al igual que en el caso anterior, también pertenece a ap1.

b)

```
802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1,0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    TSF timestamp: 1712741081801695
  [Duration: 824µs]
```

Como se puede ver en la cabecera 802.11 radio information de este paquete, se está utilizando el canal 1.

c)

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
      Timestamp: 1712741081801885
      Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0401
        .... .... .... ...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)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not 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
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  Tagged parameters (43 bytes)
    Tag: SSID parameter set: ssid1
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 1
    Tag: ERP Information
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Supported Operating Classes
    Tag: Extended Capabilities (8 octets)
```

Por otro lado, el SSID que se está usando en este caso es ssid1, especificado en el primer tag (SSID parameter set) de la pestaña Tagged parameters.

PREGUNTA 9

El mensaje de asentamiento hace referencia al valor del campo Receiver Address, el cual sólo lleva una única dirección (00:00:00_00:11:01 (00:00:00:00:11:01)).

PREGUNTA 10

a)

```
IEEE 802.11 Authentication, Flags: ........
    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... .... = +HTC/Order flag: Not strictly ordered
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Destination address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Transmitter address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Source address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  BSS Id: 00:00:00_00:11:01 (00:00:00:00:11:01)
  .... .... .... 0000 = Fragment number: 0
  0000 0100 1110 .... = Sequence number: 78
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

Como se puede ver en el campo IEEE 802.11 Wireless Management, el número de secuencia asociado a la fase de autenticación es 0x0001, por lo que no es una autenticación real, ya que no utiliza ningún algoritmo de autenticación.

PREGUNTA 11

a)

```
IEEE 802.11 Authentication, Flags: ........
    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... .... = +HTC/Order flag: Not strictly ordered
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Destination address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Transmitter address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Source address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  BSS Id: 00:00:00_00:11:01 (00:00:00:00:11:01)
  .... .... .... 0000 = Fragment number: 0
  0000 0011 0000 .... = Sequence number: 48
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

Como se puede ver, ap1 emplea el mismo algoritmo de autenticación que la solicitud.

b)

Como se puede ver en el campo IEEE 802.11 Wireless Management, el número de secuencia asociado a la fase de autenticación es 0x0002, cuyo mensaje de asentamiento sólo lleva una única dirección (00:00:00_00:11:11 (00:00:00:00:11:11)).

PREGUNTA 12

```
IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  Frame Control Field: 0x0000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0000 .... = Subtype: 0
    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... .... = +HTC/Order flag: Not strictly ordered
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Destination address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Transmitter address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Source address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  BSS Id: 00:00:00_00:11:01 (00:00:00:00:11:01)
  .... .... .... 0000 = Fragment number: 0
  0000 0100 1111 .... = Sequence number: 79
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
    Capabilities Information: 0x0421
        .... .... .... ...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)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Not 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
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
    Listen Interval: 0x0005
  Tagged parameters (33 bytes)
    Tag: SSID parameter set: ssid1
    Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Extended Capabilities (8 octets)
```

Como se puede ver, los valores del SSID y del Listen Interval del Association Request son ssid1 y 0x0005, respectivamente. Además, el número de secuencia de la cabecera general incrementa en uno (79) con respecto al mensaje de autenticación enviado por sta1 (78).

PREGUNTA 13

```
IEEE 802.11 Association Response, Flags: ........
    Type/Subtype: Association Response (0x0001)
  Frame Control Field: 0x1000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0001 .... = Subtype: 1
    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... .... = +HTC/Order flag: Not strictly ordered
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Destination address: 00:00:00_00:11:11 (00:00:00:00:11:11)
  Transmitter address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  Source address: 00:00:00_00:11:01 (00:00:00:00:11:01)
  BSS Id: 00:00:00_00:11:01 (00:00:00:00:11:01)
  .... .... .... 0000 = Fragment number: 0
  0000 0011 0001 .... = Sequence number: 49
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0401
        .... .... .... ...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)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not 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
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
    Status code: Successful (0x0000)
    ..00 0000 0000 0001 = Association ID: 0x0001
  Tagged parameters (31 bytes)
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Extended Capabilities (8 octets)
    Tag: BSS Max Idle Period
```

Como se puede ver, el valor del Association ID del Association Response es 0x0001.

PREGUNTA 14

COMANDO: mininet-wifi> sta1 iw dev sta1-wlan0 scan (mostrar los SSIDs que sta1 tiene disponibles)

```
BSS 00:00:00:00:11:01(on sta1-wlan0)
        last seen: 10774.587s [boottime]
        TSF: 1712673299925324 usec (19822d, 14:34:59)
        freq: 2412.0
        beacon interval: 100 TUs
        capability: ESS ShortSlotTime (0x0401)
        signal: -76.00 dBm
        last seen: 0 ms ago
        Information elements from Probe Response frame:
        SSID: ssid1
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 1
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        Supported operating classes:
                * current operating class: 81
        Extended capabilities:
                * Extended Channel Switching
                * SSID List
                * Operating Mode Notification
```

COMANDO: mininet-wifi> sta2 iw dev sta2-wlan0 scan (mostrar los SSIDs que sta1 tiene disponibles)

```
BSS 00:00:00:00:11:01(on sta2-wlan0) -- associated
        last seen: 10803.843s [boottime]
        TSF: 1712673329181155 usec (19822d, 14:35:29)
        freq: 2412.0
        beacon interval: 100 TUs
        capability: ESS ShortSlotTime (0x0401)
        signal: -86.00 dBm
        last seen: 0 ms ago
        Information elements from Probe Response frame:
        SSID: ssid1
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 1
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        Supported operating classes:
                * current operating class: 81
        Extended capabilities:
                * Extended Channel Switching
                * SSID List
                * Operating Mode Notification
BSS 00:00:00:00:11:02(on sta2-wlan0)
        last seen: 10805.235s [boottime]
        TSF: 1712673330573372 usec (19822d, 14:35:30)
        freq: 2457.0
        beacon interval: 100 TUs
        capability: ESS ShortSlotTime (0x0401)
        signal: -90.00 dBm
        last seen: 0 ms ago
        Information elements from Probe Response frame:
        SSID: ssid2
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 10
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        Supported operating classes:
                * current operating class: 81
        Extended capabilities:
                * Extended Channel Switching
                * SSID List
                * Operating Mode Notification
```

COMANDO: mininet-wifi> sta3 iw dev sta3-wlan0 scan (mostrar los SSIDs que sta1 tiene disponibles)

```
BSS 00:00:00:00:11:02(on sta3-wlan0) -- associated
        last seen: 10865.299s [boottime]
        TSF: 1712673390637246 usec (19822d, 14:36:30)
        freq: 2457.0
        beacon interval: 100 TUs
        capability: ESS ShortSlotTime (0x0401)
        signal: -86.00 dBm
        last seen: 0 ms ago
        Information elements from Probe Response frame:
        SSID: ssid2
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 10
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        Supported operating classes:
                * current operating class: 81
        Extended capabilities:
                * Extended Channel Switching
                * SSID List
                * Operating Mode Notification
```

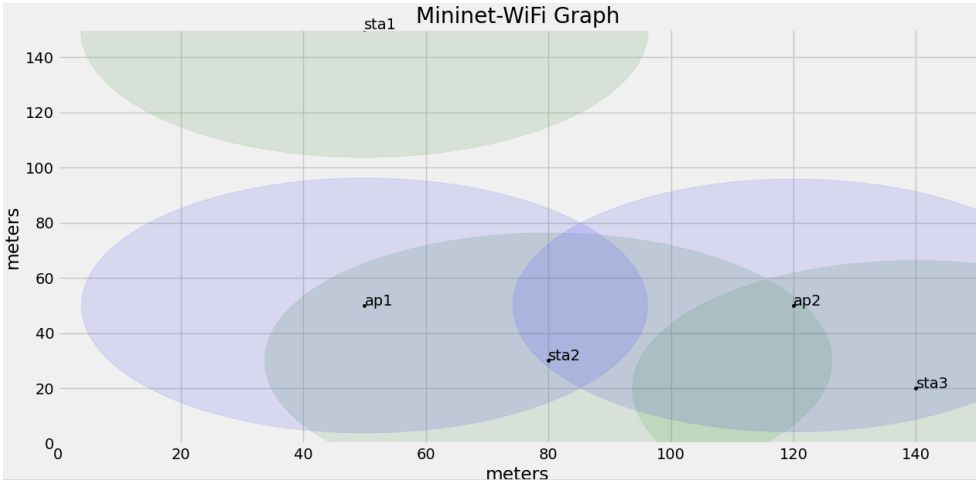
Como se puede ver en cada uno de los escaneos realizados, la potencia de señal que recibe sta1 por parte de ap1 es -76.00 dBm. Por otro lado, la potencia de señal que recibe sta2 por parte de ap1 es de -86.00 dBm, mientras que la recibida por parte de ap2 es de -90.00 dBm. Y por último, la potencia de señal que sta3 recibe de ap2 es de -86.00 dBm.

PREGUNTA 15

COMANDO: mininet-wifi> distance sta1 ap1 (mostrar la distancia desde la estación sta1 a la AP ap1)
The distance between sta1 and ap1 is 22.36 meters
COMANDO: mininet-wifi> distance sta1 ap2 (mostrar la distancia desde la estación sta1 a la AP ap2)
The distance between sta1 and ap2 is 90.55 meters
COMANDO: mininet-wifi> distance sta2 ap1 (mostrar la distancia desde la estación sta2 a la AP ap1)
The distance between sta2 and ap1 is 36.06 meters
COMANDO: mininet-wifi> distance sta2 ap2 (mostrar la distancia desde la estación sta2 a la AP ap2)
The distance between sta2 and ap2 is 44.72 meters
COMANDO: mininet-wifi> distance sta3 ap1 (mostrar la distancia desde la estación sta3 a la AP ap1)
The distance between sta3 and ap1 is 94.87 meters
COMANDO: mininet-wifi> distance sta3 ap2 (mostrar la distancia desde la estación sta3 a la AP ap2)
The distance between sta3 and ap2 is 36.06 meters
Las distancias de sta3 a ap2 y de sta1 a ap1 son demasiado grandes, ya que, como bien se observa en el apartado anterior, dichas estaciones no tienen visibilidad con los APs debido a la gran distancia entre ellas.

PREGUNTA 16

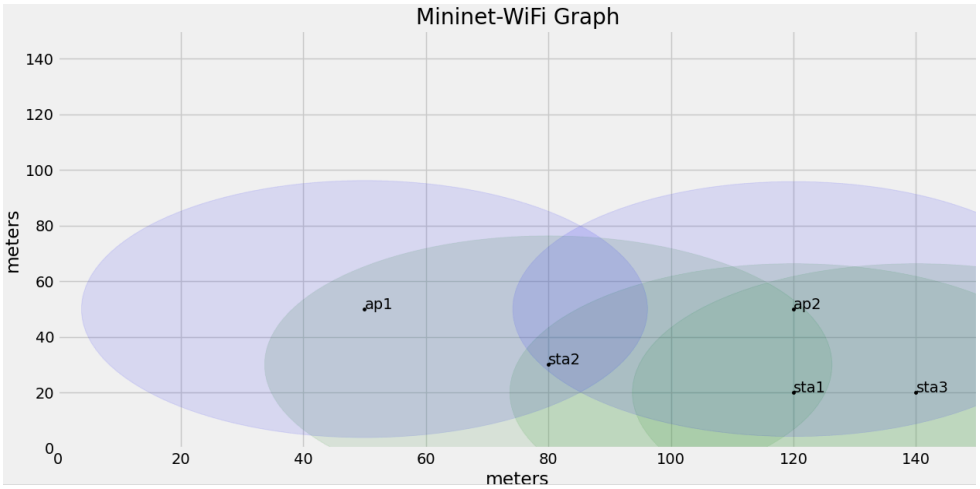
COMANDO: mininet-wifi> py sta1.setPosition('50,150,0') (mover la estación sta1 a otra posición)



COMANDO: mininet-wifi> sta1 iw dev sta1-wlan0 scan (mostrar los SSIDs que sta1 tiene disponibles)
Una vez realizado el escaneado, no se imprime nada, ya que desde la posición (50,150,0), sta1 no tiene alcance ni con ningún AP ni con ninguna estación.

PREGUNTA 17

COMANDO: mininet-wifi> py sta1.setPosition('120,20,0') (mover la estación sta1 a otra posición)



COMANDO: mininet-wifi> sta1 iw dev (mostrar información de la interfaz inalámbrica de sta1)

```
phy#2
        Interface sta1-wlan0
                ifindex 9
                wdev 0x200000001
                addr 00:00:00:00:11:11
                ssid ssid2
                type managed
                channel 10 (2457 MHz), width: 20 MHz (no HT), center1: 2457 MHz
                txpower 14.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

Como se puede ver, sta1 ha cambiado el valor de su campo ssid, pasando de ssid1 a ssid2, además del valor de su campo channel, que ha pasado de 1 a 10, por lo que ahora está asociado y puede comunicarse con sta3 en vez de con sta2 como se tenía anteriormente, ya que ambos poseen el mismo ssid.

PREGUNTA 18

COMANDO: user@machine:~$ sudo ifconfig hwsim0 up (activar la interfaz hwsim0)
COMANDO: user@machine:~$ sudo wireshark (arrancar wireshark desde la máquina real)
IMPORTANTE: Seleccionar la interfaz hwsim0 antes de iniciar la captura.
Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start
COMANDO: mininet-wifi> sta1 ping -c 3 11.211.0.3 (realizar ping de sta1 a sta3)
Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop
Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-03.cap (Wireshark/tcpdump/… - pcap)
COMANDO: user@machine:~$ wireshark wifi-03.cap (abrir una captura de tráfico en wireshark)

a)
En esta captura hay 6 mensajes ICMP echo request y 6 mensajes ICMP echo reply, los cuales se envían por pares.
El primero de los mensajes de cada par ICMP echo request tiene sus valores de To Ds y From Ds a 1 y 0, respectivamente, por lo que el primer mensaje del par ha sido enviado por una estación a través de un AP y destinado a un Ds.
Sin embargo, el segundo mensaje de cada par ICMP echo request tiene sus valores de To Ds y From Ds a 0 y 1, respectivamente, por lo que el segundo mensaje del par procede de un Ds, ha sido enviada por un AP y destinado a una estación

b)

276	12.738524	11.211.0.1	11.211.0.3	ICMP	138	Echo (ping) request id=0x5469, seq=3/768, ttl=64 (no response found!)
277	12.739044	11.211.0.1	11.211.0.3	ICMP	138	Echo (ping) request id=0x5469, seq=3/768, ttl=64 (reply in 279)
278	12.739098		00:00:00_00:11:11 (00:00:00:00:11:11) (RA)	802.11	24	Acknowledgement, Flags=........
279	12.739516	11.211.0.3	11.211.0.1	ICMP	138	Echo (ping) reply id=0x5469, seq=3/768, ttl=64 (request in 277)
280	12.739544		00:00:00_00:11:02 (00:00:00:00:11:02) (RA)	802.11	24	Acknowledgement, Flags=........
281	12.740318	11.211.0.3	11.211.0.1	ICMP	138	Echo (ping) reply id=0x5469, seq=3/768, ttl=64
282	12.740372		00:00:00_00:11:33 (00:00:00:00:11:33) (RA)	802.11	24	Acknowledgement, Flags=........
283	12.741233		00:00:00_00:11:02 (00:00:00:00:11:02) (RA)	802.11	24	Acknowledgement, Flags=........

Como se puede ver, sta1 envía un mensaje a ap1, y ap1 envía un mensaje a sta3, siendo éste el destino final.

c)
En el caso de esta captura, todos los mensajes de esta captura que no sean un Beacon Frame asienten cada uno de sus asentimientos.

[] 2. TRAMAS RTS/CTS

COMANDO: user@machine:~$ wireshark rts-cts.cap (abrir una captura de tráfico en wireshark)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1) (TA)	Objetivo_57:cc:97 (68:f9:56:57:cc:97) (RA)	802.11	76	Request-to-send, Flags=........C
2	0.000043430		Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1) (RA)	802.11	70	Clear-to-send, Flags=........C
3	0.000113351	Apple_ac:8b:b1	Objetivo_57:cc:96	802.11	138	QoS Data, SN=1992, FN=0, Flags=.p.....TC
4	0.000149767	Objetivo_57:cc:97 (68:f9:56:57:cc:97) (TA)	Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1) (RA)	802.11	88	802.11 Block Ack, Flags=........C
5	0.015765590	Apple_ac:8b:b1	Objetivo_57:cc:97	802.11	84	Null function (No data), SN=3415, FN=0, Flags=...P...TC
6	0.015777409		Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1) (RA)	802.11	70	Acknowledgement, Flags=........C
7	1.838158235	Apple_ac:8b:b1	Objetivo_57:cc:97	802.11	84	Null function (No data), SN=3416, FN=0, Flags=.......TC
8	1.838185616		Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1) (RA)	802.11	70	Acknowledgement, Flags=........C

PREGUNTA 1

La dirección MAC que tiene datos que enviar es 90:8d:6c:ac:8b:b1, y la dirección MAC de la estación que está concediendo el permiso es 68:f9:56:57:cc:97.

PREGUNTA 2

El mensaje que lleva los datos es el número 3 (QoS Data, SN=1992).

PREGUNTA 3

```
▾ Flags: 0x41
      .... ..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
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .1.. .... = Protected flag: Data is protected
      0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
Transmitter address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
Destination address: Objetivo_57:cc:96 (68:f9:56:57:cc:96)
Source address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
STA address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
.... .... .... 0000 = Fragment number: 0
0111 1100 1000 .... = Sequence number: 1992
Frame check sequence: 0xa3334e8d [unverified]
[FCS Status: Unverified]
```

El nodo que está transmitiendo es una estación, ya que en el primer flag se especifica ‘To DS: 1 From DS: 0’, por lo que dicho mensaje es enviado por una estación a través de un AP y destinada a un DS.
En este caso, los datos sí están protegidos como bien se especifica en el sexto flag con el mensaje ‘Protected flag: Data is protected’.

PREGUNTA 4

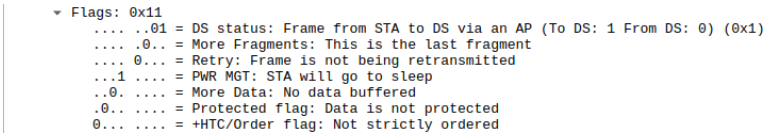
```
▾ Compressed BlockAck Response
  ▸ Block Ack Control: 0x0004
  ▸ Block Ack Starting Sequence Control (SSC): 0x7890
  ▸ Block Ack Bitmap: 0000000000000080
```

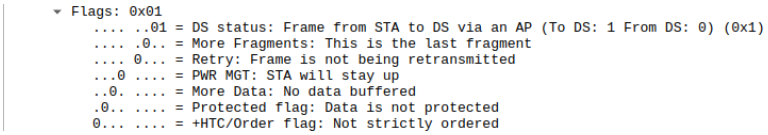
Cada bit en el campo Block Ack Bitmap representa una trama dentro de un conjunto de tramas que comienzan desde el Starting Sequence Control. En este caso, el séptimo bit (el octavo contando desde la derecha) está a 1 (00 00 00 00 00 00 00 80), lo que indica que la trama correspondiente a ese bit se ha recibido correctamente. Por tanto, el número de secuencia que se está asintiendo en este caso es 0x789 + 7 = 0x790.

PREGUNTA 5

El valor del campo Duration de los mensajes 1, 2, 3 y 4 es de 28, 28, 48 y 32 microsegundos, respectivamente, donde el valor del campo Duration de los 3 primeros mensajes se corresponde con el tiempo que se necesita para que la transmisión termine y hasta que el ACK sea completado, teniendo en cuenta siempre el mensaje anterior, ya que es el que cuenta el tiempo que llevan los mensajes anteriores.

PREGUNTA 6





Como se puede ver, los flags de los mensajes 5 y 7 son iguales, con la única diferencia del valor del flag ‘PWR GMT’, que hace referencia a la gestión de energía de una trama de control de Wi-Fi, indicando además si dicha trama es capaz de gestionar su propia energía.
El contenido de este flag en el mensaje 5 es ‘PWR GMT: STA will go to sleep’, mientras que el contenido de este mismo flag en el mensaje 7 es ‘PWR GMT: STA will stay up’.

[] 3. AUTENTICACIÓN

COMANDO: user@machine:~$ cd lab-wifi/ (acceder al directorio lab-wifi/)
COMANDO: user@machine:~$ sudo ./authentication.py (arrancar el escenario authentication.py)

PREGUNTA 1

COMANDO: mininet-wifi> dump (mostrar la configuración de red que se ha arrancado)

```
<Station sta1: sta1-wlan0:11.211.0.1 pid=10828>
<Station sta2: sta2-wlan0:11.211.0.2 pid=10830>
<OVSAP ap1: lo:127.0.0.1,ap1-wlan1:None pid=10835>
```

La dirección IP de sta1 es 11.211.0.1 y la dirección IP de sta2 es 11.211.0.2.

PREGUNTA 2

COMANDO: mininet-wifi> sta1 iwconfig (mostrar información de la interfaz inalámbrica de sta1)

```
lo        no wireless extensions.

sta1-wlan0  IEEE 802.11  ESSID:"simplewifi"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 02:00:00:00:02:00
          Bit Rate:1 Mb/s   Tx-Power=14 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-36 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:13   Missed beacon:0
```

COMANDO: mininet-wifi> sta2 iwconfig (mostrar información de la interfaz inalámbrica de sta2)

```
lo        no wireless extensions.

sta2-wlan0  IEEE 802.11  ESSID:"simplewifi"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 02:00:00:00:02:00
          Bit Rate:1 Mb/s   Tx-Power=14 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-36 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:14   Missed beacon:0
```

Como se puede ver, tanto sta1 como sta2 están asociadas al SSID ‘simplewifi’.

PREGUNTA 3

COMANDO: user@machine:~$ sudo ifconfig hwsim0 up (activar la interfaz hwsim0)
COMANDO: user@machine:~$ sudo wireshark (arrancar wireshark desde la máquina real)
IMPORTANTE: Seleccionar la interfaz hwsim0 antes de iniciar la captura.
Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start
COMANDO: root@machine:# ifconfig sta1-wlan0 down (desconectar la interfaz inalámbrica de sta1)
COMANDO: root@machine:# ifconfig sta1-wlan0 up (conectar la interfaz inalámbrica de sta1)
Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop
Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-04.cap (Wireshark/tcpdump/… - pcap)
COMANDO: user@machine:~$ wireshark wifi-04.cap (abrir una captura de tráfico en wireshark)
El algoritmo de autenticación que se está empleando es Open System.

PREGUNTA 4

```
    498 47.693961  02:00:00:00:02:00   00:00:00_00:11:01                          EAPOL       153 Key (Message 1 of 4)
    499 47.693969                      02:00:00:00:02:00 (02:00:00:00:02:00) (RA) 802.11       24 Acknowledgement, Flags=........
    500 47.694755  00:00:00_00:11:01   02:00:00:00:02:00                          EAPOL       175 Key (Message 2 of 4)
    501 47.694764                      00:00:00_00:11:01 (00:00:00:00:11:01) (RA) 802.11       24 Acknowledgement, Flags=........
    502 47.695013  02:00:00:00:02:00   00:00:00_00:11:01                          EAPOL       209 Key (Message 3 of 4)
    503 47.695018                      02:00:00:00:02:00 (02:00:00:00:02:00) (RA) 802.11       24 Acknowledgement, Flags=........
    504 47.695191  00:00:00_00:11:01   02:00:00:00:02:00                          EAPOL       153 Key (Message 4 of 4)
    505 47.695195                      00:00:00_00:11:01 (00:00:00:00:11:01) (RA) 802.11       24 Acknowledgement, Flags=........
```

```
▾ Logical-Link Control
  ▸ DSAP: SNAP (0xaa)
  ▸ SSAP: SNAP (0xaa)
  ▸ Control field: U, func=UI (0x03)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: 802.1X Authentication (0x888e)
```

Como se puede ver, el valor de la cabecera LLC del campo Type de cada uno de los 4 mensajes que intercambian información de claves es 802.1X (0x888e). Este estándar de seguridad de red se utiliza para autenticar y controlar el acceso de dispositivos a una red local antes de permitirles el acceso a la red, además de identificarles de qué forma deben procesar cada paquete.

PREGUNTA 5

Los campos ANonce y SNonce no tienen ningún valor asignado en ninguno de los cuatro mensajes.
Por otro lado, las direcciones MAC (Destination Address y Source Address) de los mensajes son 00:00:00:00:11:01 y 02:00:00:00:11:00 en el primer mensaje, 02:00:00:00:02:00 y 00:00:00:00:11:01 en el segundo mensaje, 00:00:00:00:11:01 y 02:00:00:00:02:00 en el tercer mensaje, y 02:00:00:00:02:00 y 00:00:00:00:11:01 en el cuarto mensaje.

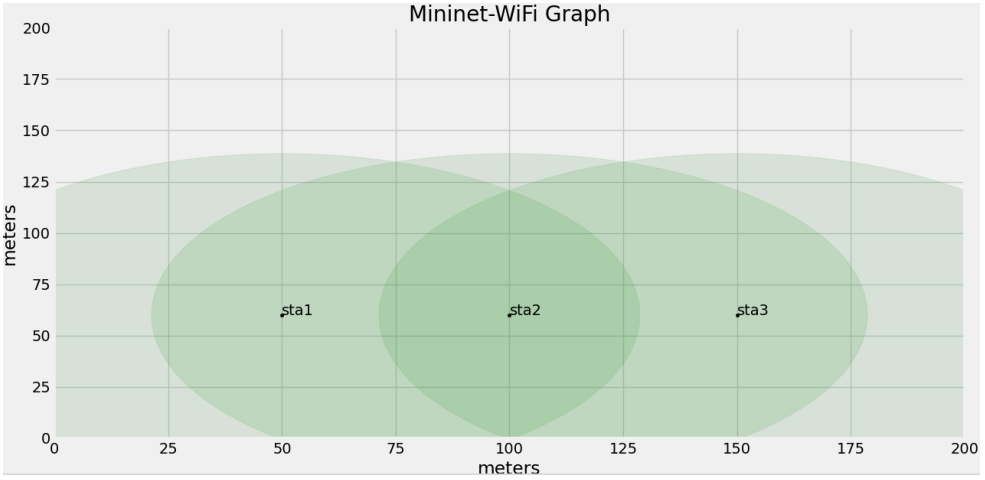
PREGUNTA 6

```
    507 47.725191 ::          ff02::16                                  ICMPv6     146 Multicast Listener Report Message v2
    508 47.725201             00:00:00_00:11:01 (00:00:00:00:11:01) (RA) 802.11      24 Acknowledgement, Flags=........
    509 47.725247 ::          ff02::16                                  ICMPv6     146 Multicast Listener Report Message v2
    510 47.805189 ::          ff02::16                                  ICMPv6     146 Multicast Listener Report Message v2
    511 47.805203             00:00:00_00:11:01 (00:00:00:00:11:01) (RA) 802.11      24 Acknowledgement, Flags=........
    512 47.805270 ::          ff02::16                                  ICMPv6     146 Multicast Listener Report Message v2
```

Como se puede ver, todos los paquetes IPv6 que han aparecido una vez realizado el descifrado son del tipo Multicast Listener Report Message v2.

[] 4. RED AD-HOC

COMANDO: user@machine:~$ cd lab-wifi/ (acceder al directorio lab-wifi/)
COMANDO: user@machine:~$ sudo ./adhoc_simple.py (arrancar el escenario adhoc_simple.py)



PREGUNTA 1

COMANDO: mininet-wifi> dump (mostrar la configuración de red que se ha arrancado)

```
<Station sta1: sta1-wlan0:11.211.0.1 pid=11496>
<Station sta2: sta2-wlan0:11.211.0.2 pid=11498>
<Station sta3: sta3-wlan0:11.211.0.3 pid=11500>
```

La dirección IP de sta1 es 11.211.0.1, la dirección IP de sta2 es 11.211.0.2 y la dirección IP de sta3 es 11.211.0.3.

COMANDO: mininet-wifi> sta1 iwconfig (mostrar información de la interfaz inalámbrica de sta1)

```
lo        no wireless extensions.

sta3-wlan0  IEEE 802.11  ESSID:"adhocNet"
          Mode:Ad-Hoc  Frequency:2.432 GHz  Cell: 02:CA:FF:EE:BA:01
          Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

COMANDO: mininet-wifi> sta2 iwconfig (mostrar información de la interfaz inalámbrica de sta2)

```
lo        no wireless extensions.

sta2-wlan0  IEEE 802.11  ESSID:"adhocNet"
          Mode:Ad-Hoc  Frequency:2.432 GHz  Cell: 02:CA:FF:EE:BA:01
          Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

COMANDO: mininet-wifi> sta3 iwconfig (mostrar información de la interfaz inalámbrica de sta3)

```
lo        no wireless extensions.

sta1-wlan0  IEEE 802.11  ESSID:"adhocNet"
          Mode:Ad-Hoc  Frequency:2.432 GHz  Cell: 02:CA:FF:EE:BA:01
          Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Como se puede ver, tanto sta1 como sta2 y sta3 están asociadas al SSID ‘adhocNet’.

PREGUNTA 2

COMANDO: user@machine:~$ sudo ifconfig hwsim0 up (activar la interfaz hwsim0)
COMANDO: user@machine:~$ sudo wireshark (arrancar wireshark desde la máquina real)
IMPORTANTE: Seleccionar la interfaz hwsim0 antes de iniciar la captura.
Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start
En este caso, todas las estaciones están enviando tramas beacon.

PREGUNTA 3

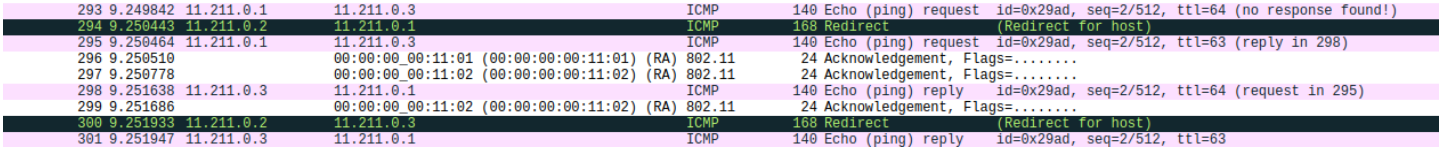
COMANDO: mininet-wifi> pingallfull (ejecutar la combinación de todos los pings posibles de esa topología)
Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop
Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-05.cap (Wireshark/tcpdump/… - pcap)
COMANDO: user@machine:~$ wireshark wifi-05.cap (abrir una captura de tráfico en wireshark)
En esta captura, todos los ping se realizan de una estación a otra, ya que todas las estaciones poseen el mismo SSID, algo que podría fallar si el número de dispositivos conectados es enorme o si la calidad de señal que se tiene es débil. Sin embargo, en ningún momento se realiza ningún ping que vaya de sta1 a sta3 debido a que la distancia que los separa es bastante grande.

PREGUNTA 4

En un escenario Adhoc, dos estaciones se comunican directamente sin pasar por un punto de acceso, cuya comunicación genera menos tráfico en la red en comparación con un escenario en modo infraestructura. Por otro lado, en un escenario en modo infraestructura, las estaciones se comunican a través de un punto de acceso y poseen un mayor número de mensajes de ping. Esto se debe a que el punto de acceso actúa como un intermediario entre las estaciones, por lo que se necesitan mensajes adicionales para establecer y mantener la conexión. Además, también se pueden enviar mensajes adicionales de control, como los mensajes de gestión, para mantener la conexión entre las estaciones y el punto de acceso.

PREGUNTA 5

COMANDO: mininet-wifi> sta2 echo 1 > /proc/sys/net/ipv4/ip_forward (activar encaminamiento en sta2)
COMANDO: mininet-wifi> sta1 ip route add 11.211.0.3 via 11.211.0.2 (configurar ruta en sta1)
COMANDO: mininet-wifi> sta3 ip route add 11.211.0.1 via 11.211.0.2 (configurar ruta en sta3)
COMANDO: mininet-wifi> staX arp -a (mostrar la caché de ARP de staX)
COMANDO: mininet-wifi> staX arp -d 11.211.0.X (borrar entrada de la caché de ARP de staX)
COMANDO: user@machine:~$ sudo wireshark (arrancar wireshark desde la máquina real)
IMPORTANTE: Seleccionar la interfaz hwsim0 antes de iniciar la captura.
Iniciar una captura de tráfico desde Wireshark: Capture ⇒ Start
COMANDO: mininet-wifi> sta1 ping -c 3 11.211.0.3 (realizar ping de sta1 a sta3)
Detener una captura de tráfico desde Wireshark: Capture ⇒ Stop
Guardar captura de tráfico desde Wireshark: File ⇒ Save As… ⇒ wifi-06.cap (Wireshark/tcpdump/… - pcap)
COMANDO: user@machine:~$ wireshark wifi-06.cap (abrir una captura de tráfico en wireshark)



Como se puede ver, sta1 envía un mensaje ICMP echo request, cuyo valor de su campo IEEE 802.11 es la dirección MAC de sta2. Por otro lado, la dirección destino que aparece en la cabecera IPv4 del mensaje es la dirección IP de sta3. De esta forma, sta2 redireccionará el mensaje a sta3 una vez lo haya recibido, siendo éste el destino final del ping. Y por último, para el mensaje ICMP echo reply se tiene el mismo escenario, con la diferencia de que su destino final es sta1 y no sta3.