**Redes de Computadores**

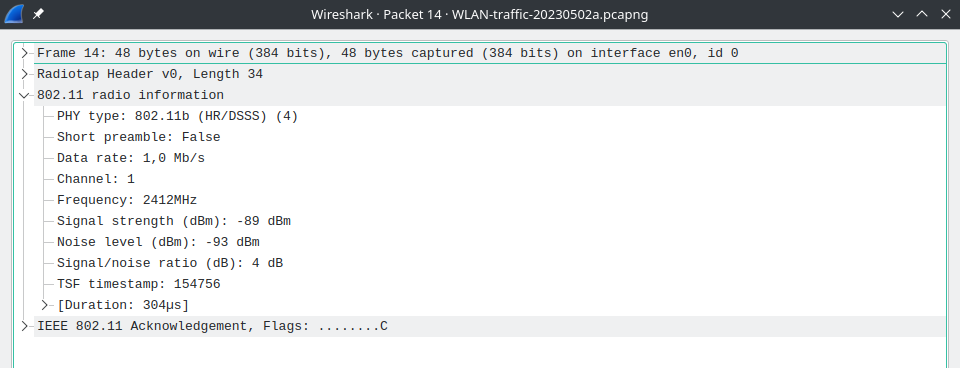
**Trabalho Prático 4**

Pedro Afonso Moreira Lopes [A100759], Gonçalo Machado Daniel Costa [A100824] e José Eduardo Silva Monteiro Santos Oliveira [A100547]

**Questões e Respostas**

**4. Acesso Rádio**

**1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.**

****

**Figura 1.** Rádio Information da trama número 14

Como se pode ver pela imagem acima, a frequência do espectro é de 2412MHz e o canal correspondente é o 1.

**2) Identifique a versão da norma IEEE 802.11 que está a ser usada.**

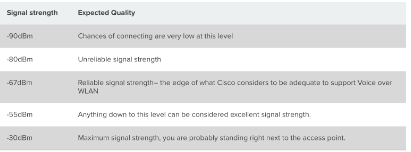
A versão da norma que está a ser usada é **802.11b (HR/DSSS),** como se pode visualizar pelo campo PHY Type na figura acima.

**3) Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface**

**Wi-Fi pode operar? Justifique.**

O débito da trama que foi enviada a trama escolhida é igual a 1.0 MB/s, o que não corresponde ao débito máximo de 11 MB/s pois este é o débito máximo deste tipo de protocolo.Este débito não é utilizado para garantir que o beacon chega a todos os hosts, utilizando assim o débito mais baixo possível.

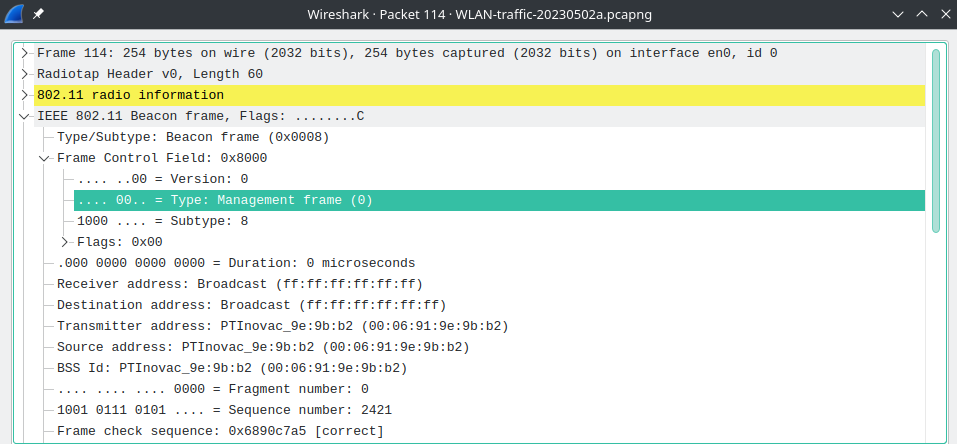
**4) Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama, sabendo que:**

****

A força do sinal, como podemos ver pela figura 1, é igual a -89 dBm, ou seja, de acordo com a tabela acima, tem uma qualidade esperada de **Unreliable Signal Strength**.

**5. Scanning Passivo e Scanning Ativo**

**5) Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?**

****

**Figura 2.** Trama beacon 114 capturada

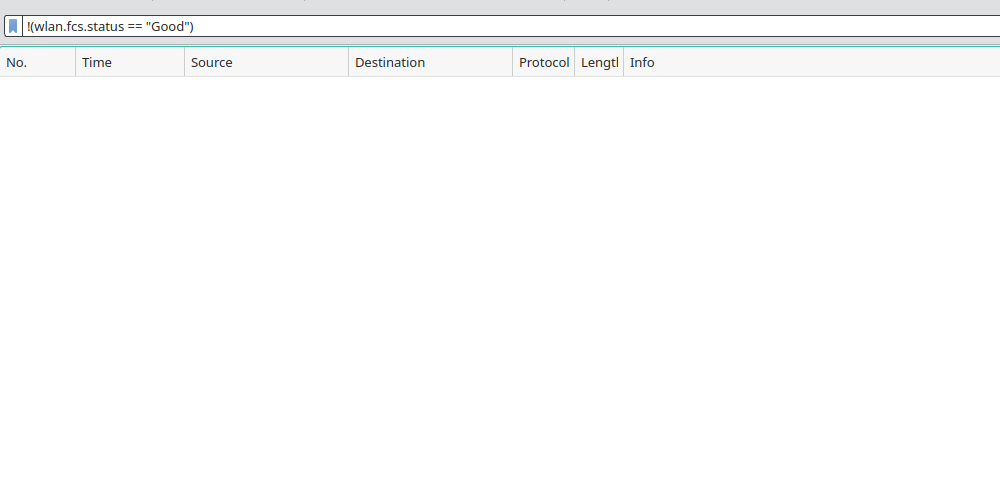
Esta trama pertence ao tipo de *Management Frame,* o seu identificador é 0 (00) e o seu subtipo é o 8 (1000). Esta informação, como se pode ver pela figura acima, encontra-se especificados nos campos *Type* e *Subtype* no cabeçalho da trama*.*

**6) Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?**

Como podemos ver pela figura 2 acima, os endereços MAC em uso são o Destination e Receiver, que ambos apresentam ser Broadcast (ff:ff:ff:ff:ff:ff), ou seja, o destino são todos os dispositivos que se encontram ligados à rede Wireless. Juntamente com estes 2, temos também os endereços Source e Transmitter, que ambos também apresentam ser também PTInovac\_9e:9b:b2 (00:06:91:9e:9b:b2).

**7) Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.**

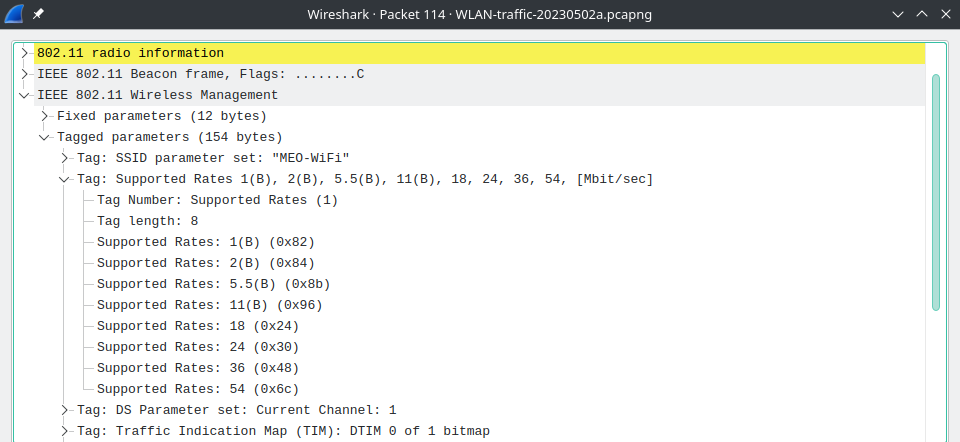
**Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.**

****

**Figura 3.** Aplicação de uma flag para verificar se o CRC está a ser usado

Como se pode ver, o método de deteção de erros (CRC) está a ser usado. Dito isto, é necessário usar deteção de erros em redes sem fios pois estas são mais suscetíveis a problemas de qualidade devido a obstáculos físicos que possam interferir com o sinal e também operam na sua maioria em ambientes compartilhados, onde pode haver colisão de envios de pacotes de dados. Sabendo isto, a detecção de erros é fulcral para detetar e corrigir estes problemas.

**8) Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.**

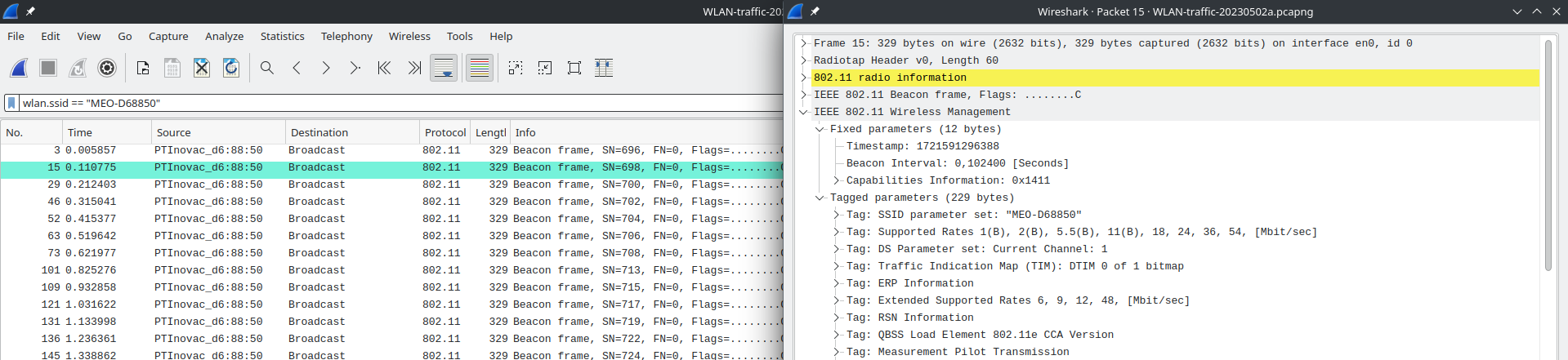
****

**Figura 4.** Débitos da trama 114

Como podemos ver pela figura acima, os débitos de base (B) são 1, 2, 5.5 e 11 e os débitos adicionais são 18, 24, 36 e 54 Mbit/seg.

**9) Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)?**

**Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.**

****

**Figura 5.** Intervalo de tempo previsto e na prática das tramas selecionadas de AP’s com SSID == “MEO-D68850”

Como podemos ver pela figura 4 acima, o tempo previsto entre tramas beacon consecutivas é de 0.102400 segundos. Contudo, isto não se verifica na prática sempre devido ao congestionamento da rede local nomeadamente na espera para a transmissão quando o meio se encontra ocupado.

**10) Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).**

**No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.**

Depois de procurar todos os SSIDs dos APs, chegamos então à conclusão que a lista é: *MEO-D68850, NOS-C876, MEO-WiFi, MEO-FCF0A0, NOS-2EC6, MEO-9E9BB0, FlyingNet, MEO-45BE30, MEO-9BF2A0, K6000 Plus, TP-LINK\_AP\_AF08, Masmorra do Sexo, Vodafone-DC61F7, GV BRAGA, MEO-D9EDE0, GRUPO GV, IA 2 5* e finalmente *Vodafone-48683C*.

Para obter esta informação, simplesmente fomos filtrando para fora todas as tramas com um certo SSID até que já não haviam tramas beacon, tendo assim chegado ao gigante filtro seguinte:

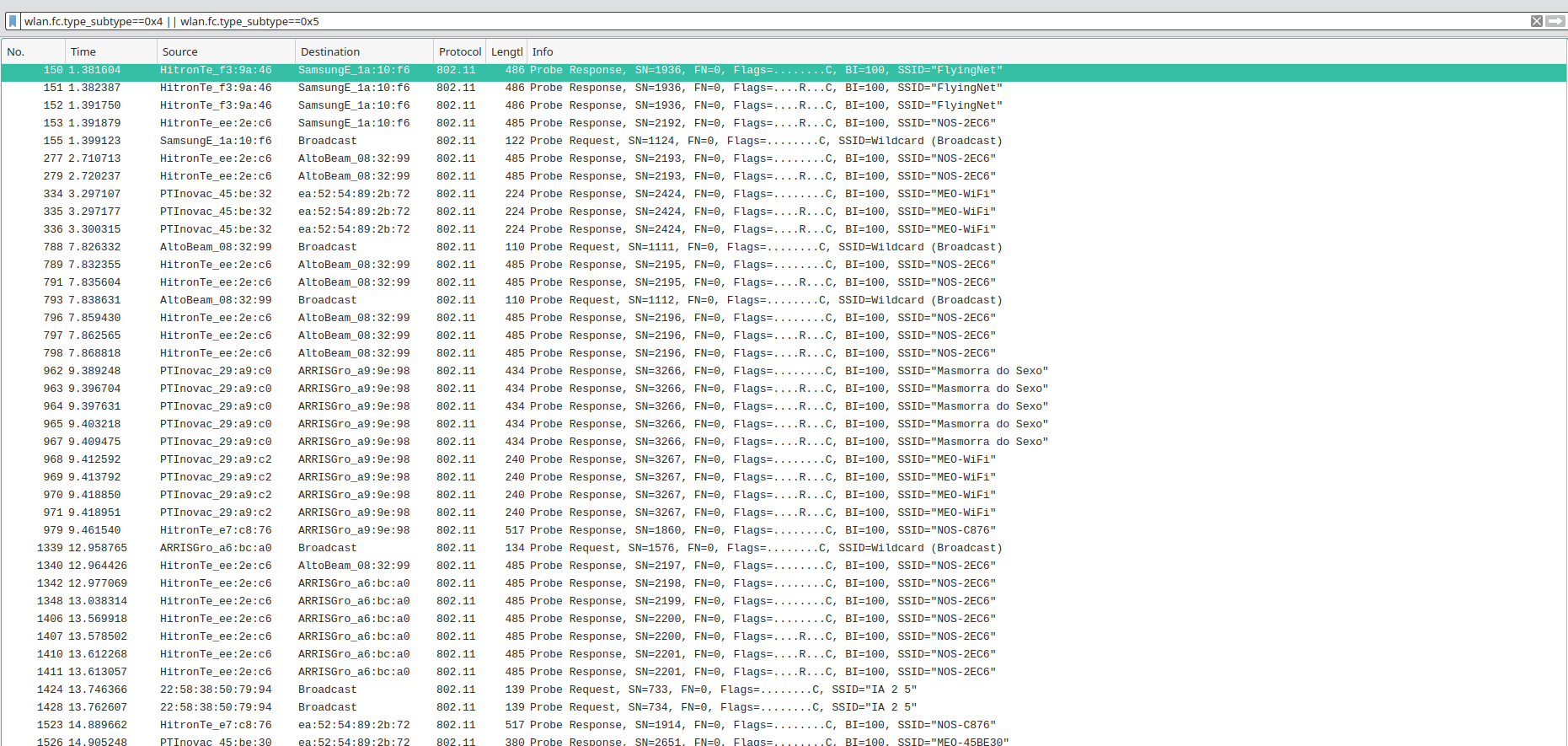
**wlan.ssid != "MEO-D68850" && wlan.ssid != "NOS-C876" && wlan.ssid != "MEO-WiFi" && wlan.ssid != "MEO-FCF0A0" && wlan.ssid != "NOS-2EC6" && wlan.ssid != "MEO-9E9BB0" && wlan.ssid != "FlyingNet" && wlan.ssid != "MEO-45BE30" && wlan.ssid != "MEO-9BF2A0" && wlan.ssid != "K6000 Plus" && wlan.ssid != "TP-LINK\_AP\_AF08" && wlan.ssid != "Masmorra do Sexo" && wlan.ssid != "Vodafone-DC61F7" && wlan.ssid != "GV BRAGA" && wlan.ssid != "MEO-D9EDE0" && wlan.ssid != "GRUPO GV" && wlan.ssid != "IA 2 5"&& wlan.ssid != "Vodafone-48683C"**

**11) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.**

Todas as tramas probing request e probing response apresentam subtipo 4 e 5. Sabendo isto, para observar estas tramas, basta aplicar o filtro:

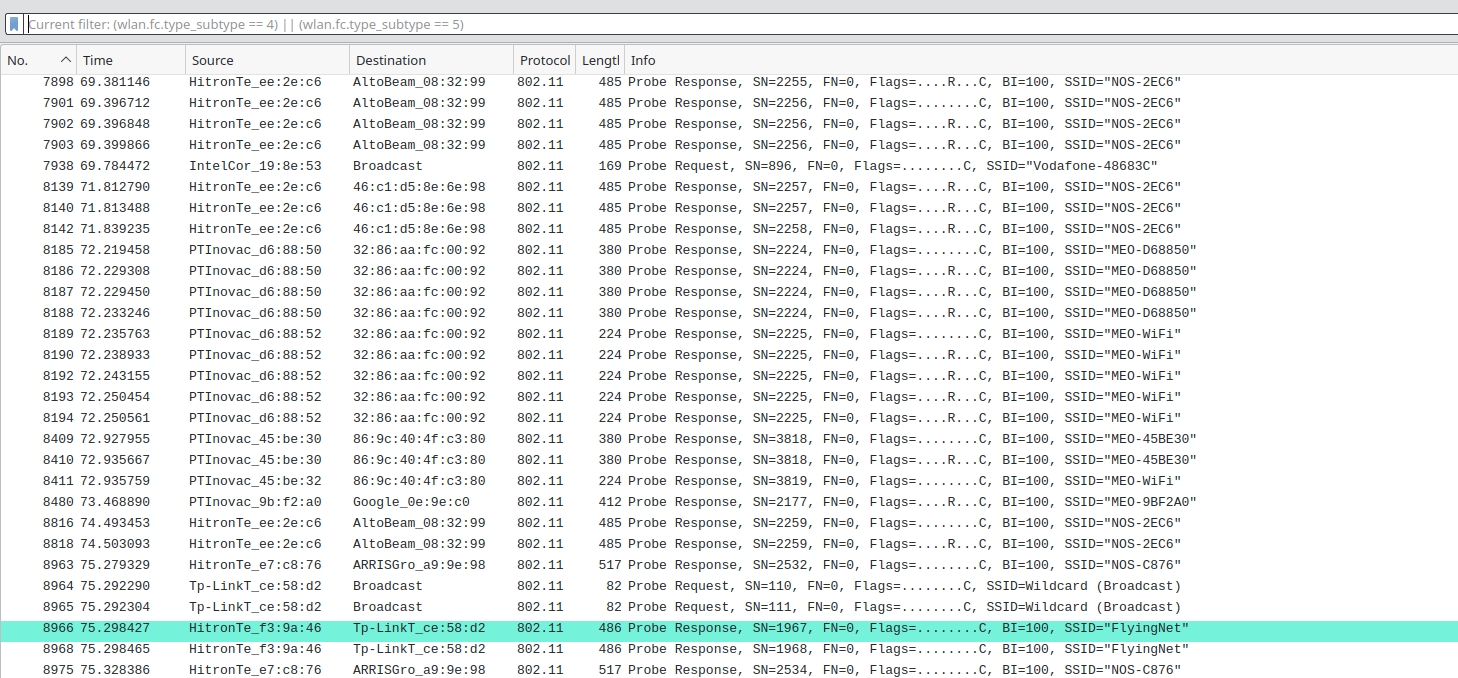
**(wlan.fc.type\_subtype == 4) || (wlan.fc.type\_subtype == 5)**

Que nos vai dar o seguinte resultado:



**Figura 6.** Filtro aplicado e resultados obtidos

**12) Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?**

****

**Figura 7.** Probing request e Probing response

Como podemos ver na figura 6 acima, como por exemplo, a trama 8965 é um probe request. Com isto, vai ser emitida uma STA HiltronTe\_f3:9a:46 para todos os dispositivos da rede, de forma a encontrar os APs que estão dentro do alcance rádio. Já a trama 8966 é um probing response, ou seja, uma resposta do Tp-LinkT\_ce:58:d2 para a STA emitida.

**6. Processo de Associação**

**13) Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA**

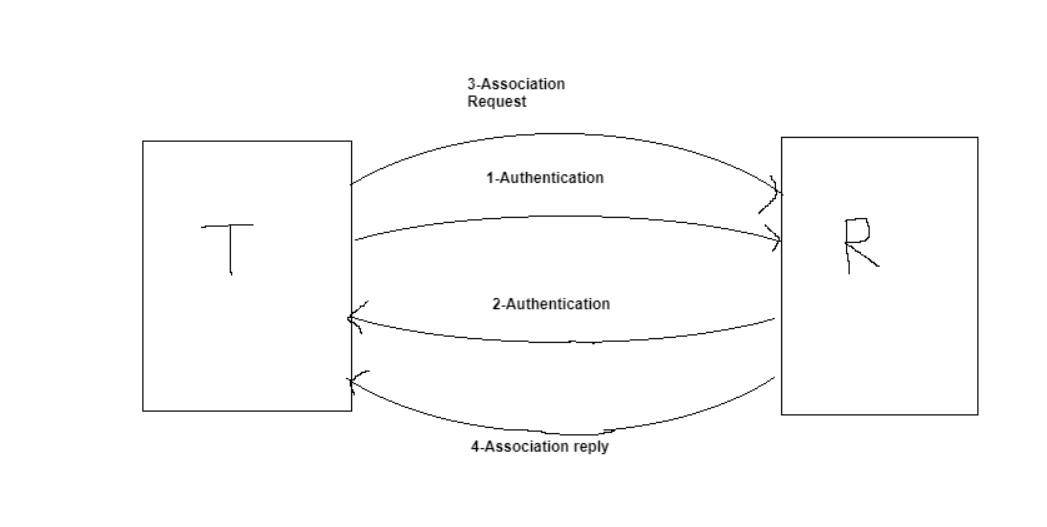
**e o AP, incluindo a fase de autenticação.**

Utilizando os filtros “wlan.fc.type\_subtype == 0x00 || wlan.fc.type\_subtype == 0x01 ||

wlan.fc.type\_subtype == 0x0B” foi possível identificar as tramas que correspondem a um processo de associação entre a STA e AP.



**14) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.**

****

**7. Transferência de Dados**

**15) Considere a trama de dados nº8503. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?**

As flags "toDS" e "fromDS" estão a 1 e 0, respetivamente. Assim, podemos concluir que as tramas vão do STA para o router de acesso, assim verificando a direcionalidade desta trama. Para além disso, com esses mesmos valores, podemos também deduzir que é local à WLAN.

**16) Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?**

STA - 80:c5:f2:0f:0e:9b(source address)

AP - 74:9b:e8:f3:9a:46(receiver adress)

DS - 33:33:00:00:00:16(destination address)

**17) Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?**

As flags "toDS" e "fromDS" estão a 0 e 1, respetivamente. Assim, podemos concluir que as tramas vão do STA para o router de acesso para o STA.

STA - 80:c5:f2:0f:0e:9b(destination address)

AP - 74:9b:e8:f3:9a:46(transmitter adress)

DS - 33:33:00:00:00:16(source address)

**18) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)**

O subtipo de tramas de controlo transmitidas na transferência de dados é a "QoS Data"(0x28). Normalmente este subtipo é utilizado para gerir e manusear a transmissão de tipos específicos de dados e para garantir que os diferentes serviços recebem os recursos necessários para o seu bom funcionamento, de acordo com os seus requisitos e prioridades.

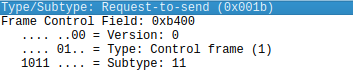
**19) O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direcionalidade das tramas e os sistemas envolvidos.**

**Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.**

O filtro "wlan.fc.type\_subtype == 0x1B" permite-nos listar as tramas que usam RTS/CTS. Por exemplo, a trama nº7.



Podemos verificar que é RTS.

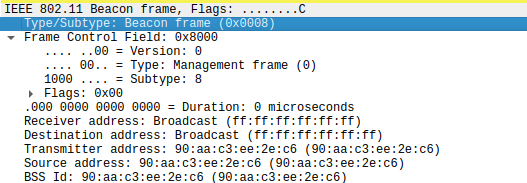


Como os valores das flags "toDS" e "fromDS" são ambas 0 podemos concluir que estamos numa network AH-HOC, ou seja, não há infraestruturas centralizadas, logo a ligação entre dispositivos é direta.

Como a ligação entre dispositivos é direta, o receiver address corresponde ao destino (ce:90:6f:21:42:3a) e o transmitter address corresponde à origem(PTInovac\_d6:88:50).



Agora, uma tabela cuja opção RTS/CTS não foi utilizada.



**Conclusão**

Com a conclusão do TP4, acreditamos ter concluído este trabalho com sucesso, respondendo a todas as questões pedidas, e com isso aprender sobre vários aspectos do protocolo IEEE 802.11, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo. Tivemos também as nossas devidas dificuldades mas com ajuda do excelente senhor professor Pedro António conseguimos eventualmente superá-las.