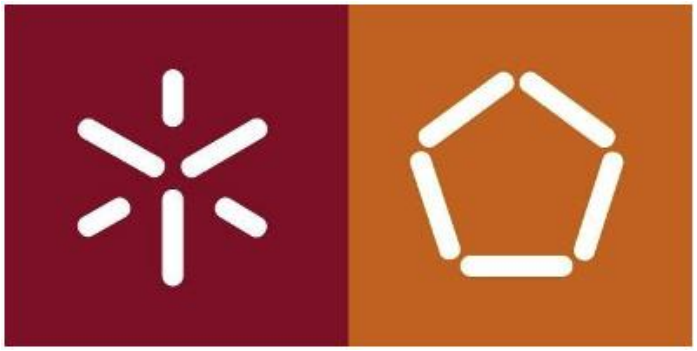
Universidade do Minho

Licenciatura em Engenharia Informática



TP3 -Nível de Ligação Lógica: Redes Ethernet, Protocolo ARP e Redes Locais sem Fios (Wi-Fi)

Trabalho realizado por:
Margarida Cunha da Silva, A104357
Maria Leonor Carvalho da Cunha, A103997
Tiago Rodrigues Barros, A104530.

Redes de Computadores

PL9 - Grupo 91
April 16, 2024

Índice

1. Parte 1

1.1. Exercício 1

Captura e análise de Tramas Ethernet

Com o aumento do preço da habitação em Braga, o Shrek e o Burro tomam a decisão economicamente sensata e decidem voltar à sua casa no Pântano. A sua rede local é constituída por um switch (n2), um router para acesso à rede (n1), assim como os portáteis do Shrek e do Burro, ligados por Ethernet a n2. O router n1 está ainda ligado a um hub (n3), que se conecta ao portátil da Fiona e ao servidor do conhecido site de notícias pantanews.com.
A caminho, o Shrek fica a saber que houve um ataque aos servidores do seu site de notícias favorito, o Pantanews, e que todos os seus dados terão sido apagados. Assim que chegam a casa, o Shrek aproveita para verificar se realmente há algum problema com o site (servidor - 10.0.1.10). Utilize o comando curl para o efeito (poderá consultar o manual do comando com man curl), apontando diretamente para o endereço do servidor. Pare a captura do Wireshark, e analise a trama que contém os primeiros dados HTTP referentes à página alojada no servidor.

1. Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique

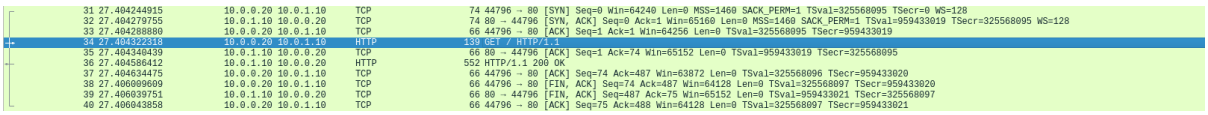


Figure 1: Pacote TCC

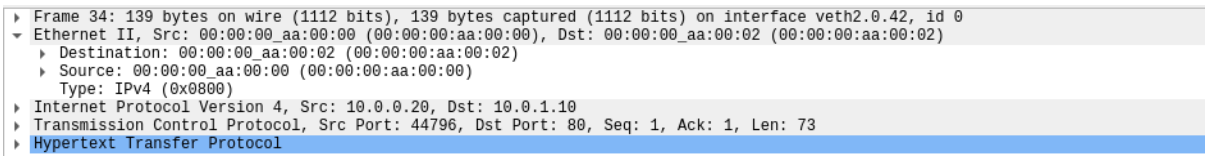


Figure 2: Trama capturada

Resposta: O endereço MAC do destino é 00:00:00:aa:00:02 e refere-se ao endereço físico do router. O endereço MAC na origem é 00:00:00:aa:00:00, este refere-se ao endereço físico da máquina que estamos a utilizar para realizar a captura.

2. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

Resposta: O endereço é 0x0800 (Figure 2) e significa que a camada superior está a utilizar o protocolo IPv4.

3. Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

Resposta: Conforme a captura de rede fornecida, a trama em questão possui um tamanho total de 139 bytes. No entanto, apenas 85 bytes são destinados aos dados do nível aplicacional, ou seja, o conteúdo da requisição HTTP.

Cálculo da sobrecarga: 85 bytes / 139 bytes ≈ 0,6115
Sobrecarga em porcentagem: 0,6115*100% = 61,15%

A análise revela que a pilha protocolar introduz uma sobrecarga significativa de 61,15% no tamanho total da trama.

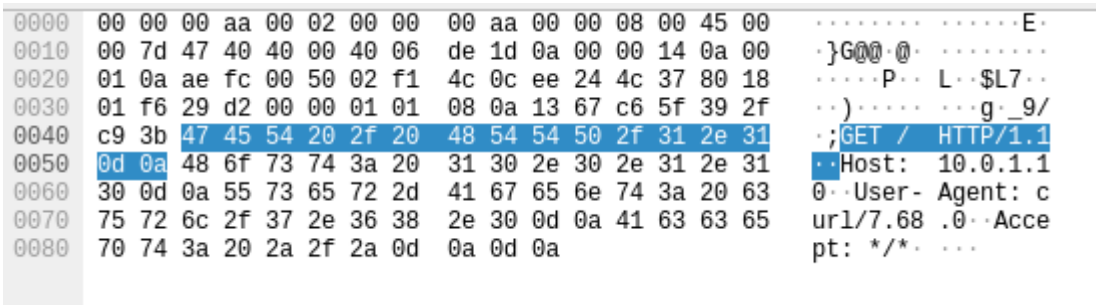


Figure 3: Valores dos bytes da trama em estudo

4. Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.

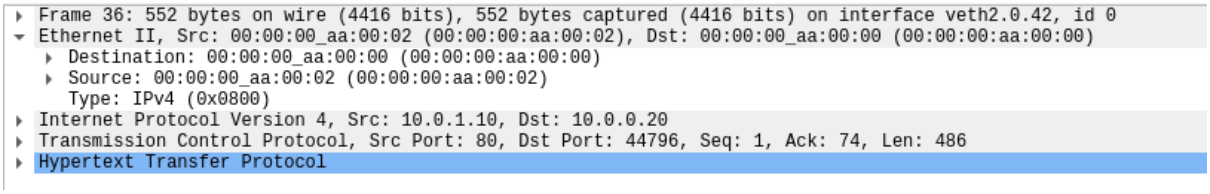


Figure 4: Resposta HTTP

Resposta: Como podemos ver na figura 4, o endereço é 00:00:00:aa:00:02 e corresponde ao endereço físico do router com que estamos a comunicar.

5. Qual é o endereço MAC do destino? A que interface corresponde?

Resposta: O endereço MAC do destino é 00:00:00:aa:00:00 e corresponde ao endereço físico da nossa máquina.

1.2. Exercício 2

Protocolo ARP e Domínios de Colisão

Deverá ter a cache ARP completamente vazia antes de iniciar esta secção: reinicie a topologia, ou utilize o comando arp -d.

Um pouco mais preocupado com a segurança dos seus dados, o Shrek repara que a Fiona sabe sempre por onde andou a navegar. Para averiguar esta situação, o Shrek experimenta de novo aceder ao site do pantanews.com (10.0.1.10) através do comando curl. Certifique-se que está a capturar tráfego com o Wireshark na interface do Shrek e na do Burro.

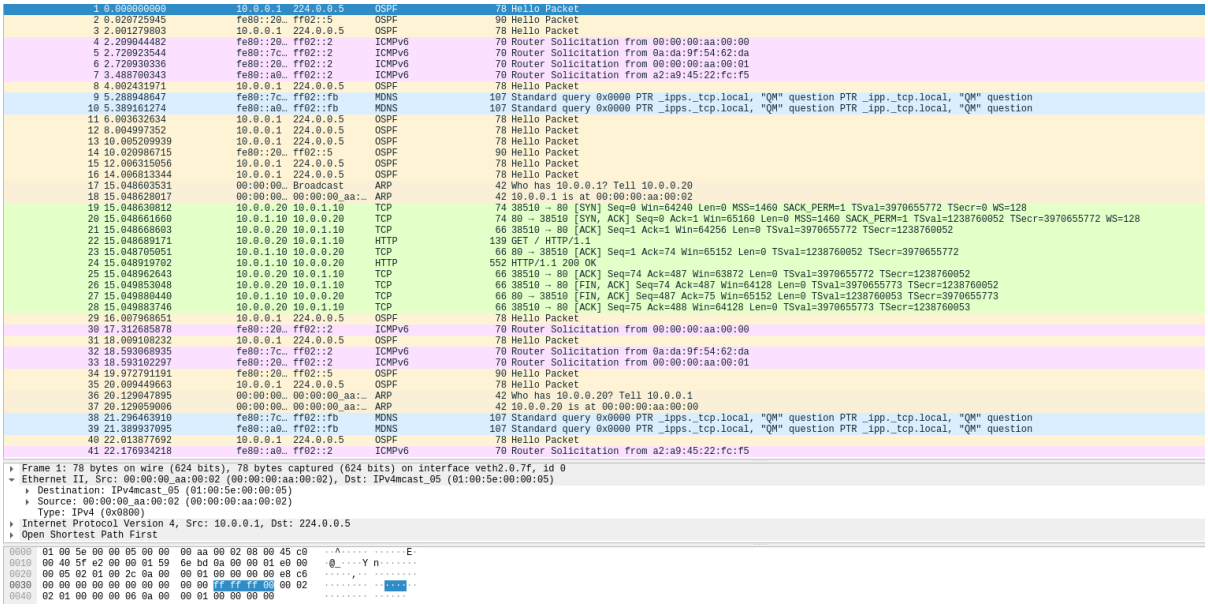


Figure 5: Captura do tráfego na interface do Shrek

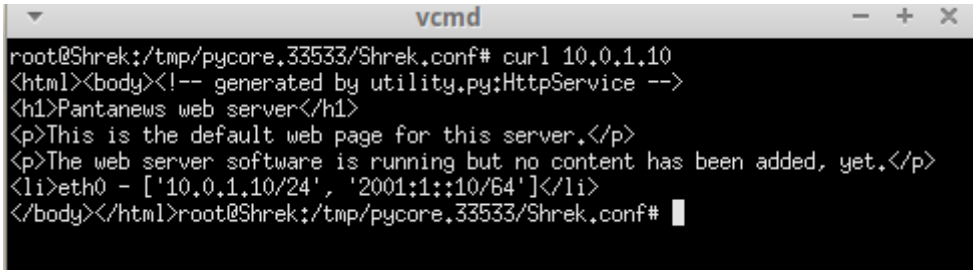
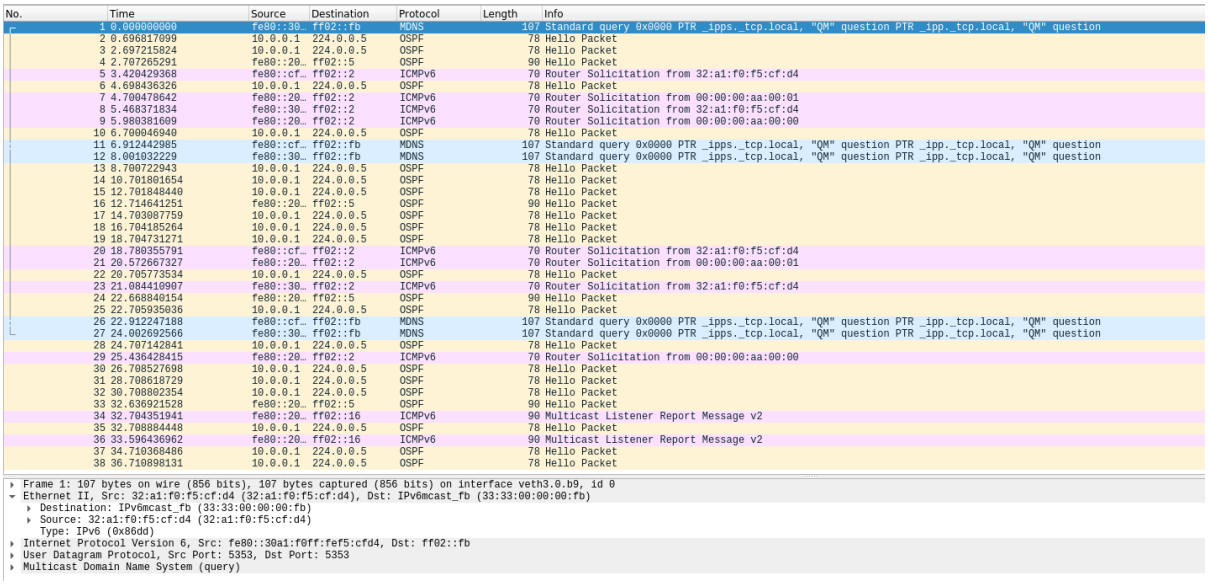


Figure 6: Aceder ao pantanews.com no Shrek através do comando curl



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::30…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
2	0.696817099	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
3	2.697215824	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
4	2.707265291	fe80::20…	ff02::5	OSPF	90	Hello Packet
5	3.420429368	fe80::cf…	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
6	4.698436326	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
7	4.700478642	fe80::20…	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:01
8	5.468371834	fe80::30…	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
9	5.980381609	fe80::20…	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
10	6.700946940	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
11	6.912442985	fe80::cf…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
12	8.001032229	fe80::30…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
13	8.700722943	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
14	10.701801654	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
15	12.701848440	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
16	12.714641251	fe80::20…	ff02::5	OSPF	90	Hello Packet
17	14.703087759	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
18	16.704185264	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
19	18.704731271	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
20	18.780355791	fe80::cf…	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
21	20.572667327	fe80::20…	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:01
22	20.705773534	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
23	21.084410907	fe80::30…	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
24	22.668840154	fe80::20…	ff02::5	OSPF	90	Hello Packet
25	22.705935036	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
26	22.912247188	fe80::cf…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
27	24.002692566	fe80::30…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
28	24.707142841	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
29	25.436428415	fe80::20…	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
30	26.708527698	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
31	28.708618729	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
32	30.708802354	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
33	32.636921528	fe80::20…	ff02::5	OSPF	90	Hello Packet
34	32.704351941	fe80::20…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
35	32.708884440	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
36	33.596436962	fe80::20…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
37	34.710368486	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
38	36.710898131	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet

```
▸ Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface veth3.0.b9, id 0
▾ Ethernet II, Src: 32:a1:f0:f5:cf:d4 (32:a1:f0:f5:cf:d4), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
  ▸ Destination: IPv6mcast_fb (33:33:00:00:00:fb)
  ▸ Source: 32:a1:f0:f5:cf:d4 (32:a1:f0:f5:cf:d4)
    Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: fe80::30a1:f0ff:fef5:cfd4, Dst: ff02::fb
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (query)
```

Figure 7: Captura do tráfego na interface do Burro

1. Observe o conteúdo da tabela ARP do Shrek com o comando arp -a. Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.

```
</body></html>root@Shrek:/tmp/pycore.33533/Shrek.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
root@Shrek:/tmp/pycore.33533/Shrek.conf#
```

Figure 8: Comando arp -a no shrek

No.	Time	Source	Destination	Protocol	Length	Info
17	15.048603531	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
18	15.048628017	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	10.0.0.1 is at 00:00:00:aa:00:02
36	20.129047895	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
37	20.129059006	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	10.0.0.20 is at 00:00:00:aa:00:00

Figure 9: tabela ARP

Resposta: A primeira coluna mostra os endereços IPs e a segunda coluna mostra os endereços MAC.

2. Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).

a. Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

Resposta: O valor hexadecimal do endereço MAC origem é 00:00:00:aa:00:00 e o endereço de destino MAC é ff:ff:ff:ff:ff:ff (Broadcast). Como o nosso dispositivo não está diretamente conectado ao dispositivo de destino, para onde enviamos a mensagem, é necessário enviar a mensagem para todos os dispositivos da rede até que o dispositivo pretendido responda ao seu endereço MAC, é por isso que o nosso endereço de destino é ff:ff:ff:ff:ff:ff.

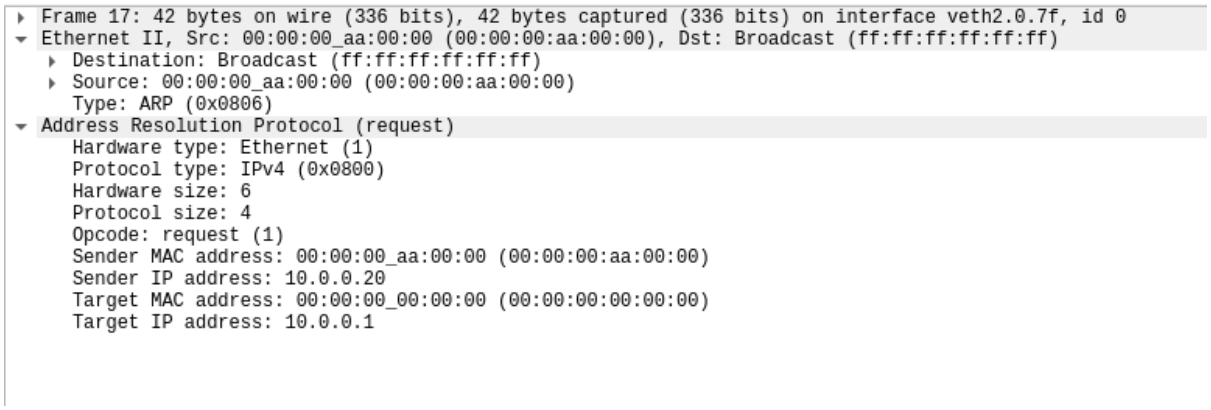


Figure 10: Trama com o pedido ARP

b. Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?

Resposta: O valor do campo tipo trama é 0x0806 e indica que a camada superior está a usar o protocolo ARP.

c. Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.

Resposta: Trata-se efetivamente de um pedido ARP pois temos a indicação que é uma "request" na figura 10.
Para além disso, na mensagem ARP estão contidos os endereços IP e MAC e o protocolo ARP permite converter um endereço IP num endereço MAC.

3. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

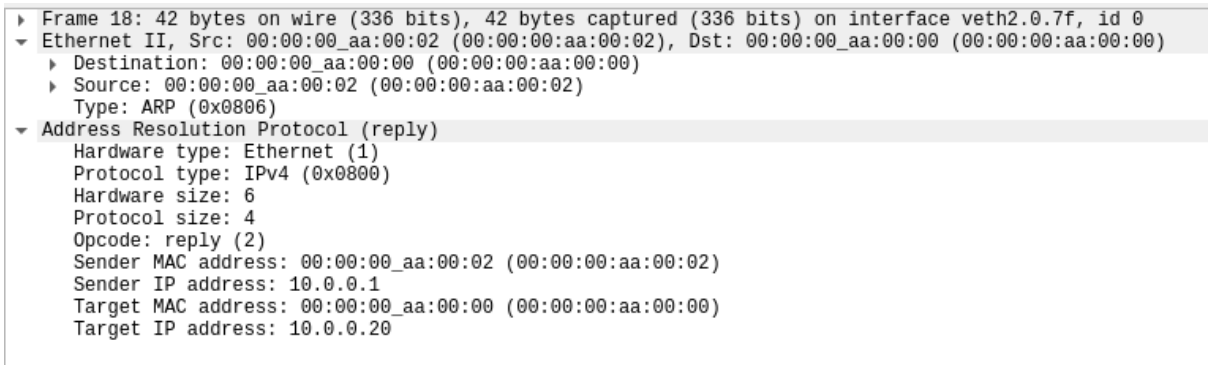


Figure 11: Mensagem ARP que é a resposta ao pedido ARP efetuado

a. Qual o valor do campo ARP opcode? O que especifica?

Resposta: O valor do campo ARP opcode é 2. Assim podemos concluir que, o IP 10.0.0.20 recebe a mensagem de "request" e está a enviar o seu endereço MAC com resposta.

b. Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?

Resposta: A resposta ao pedido encontra-se entre os bytes 15 e 42, como podemos ver na imagem abaixo.

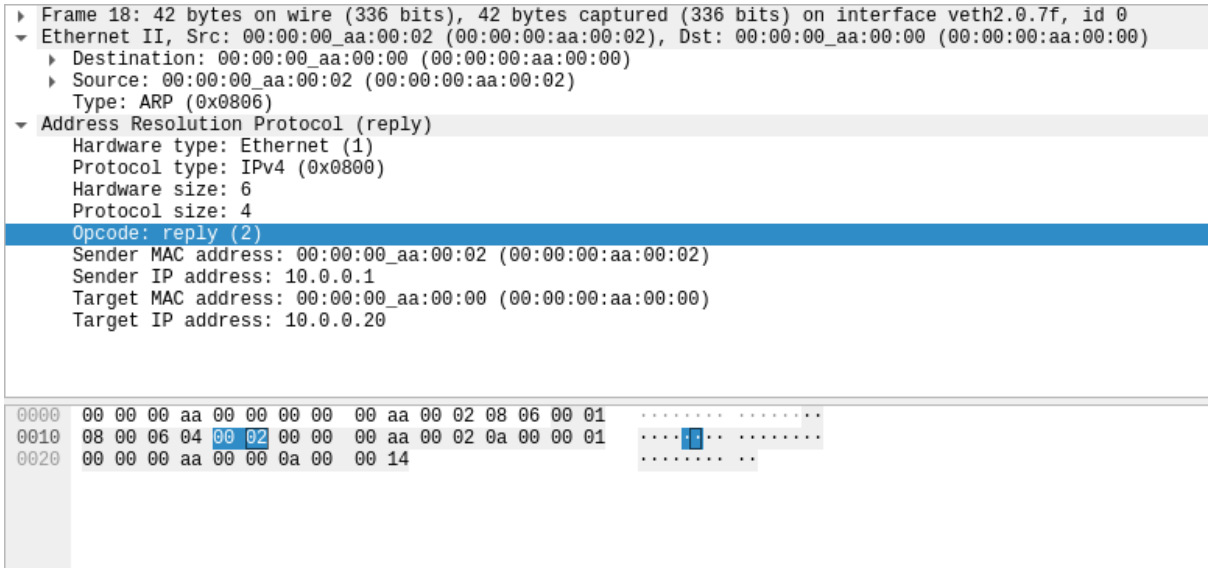


Figure 12: Trama com a resposta ARP

c. Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.

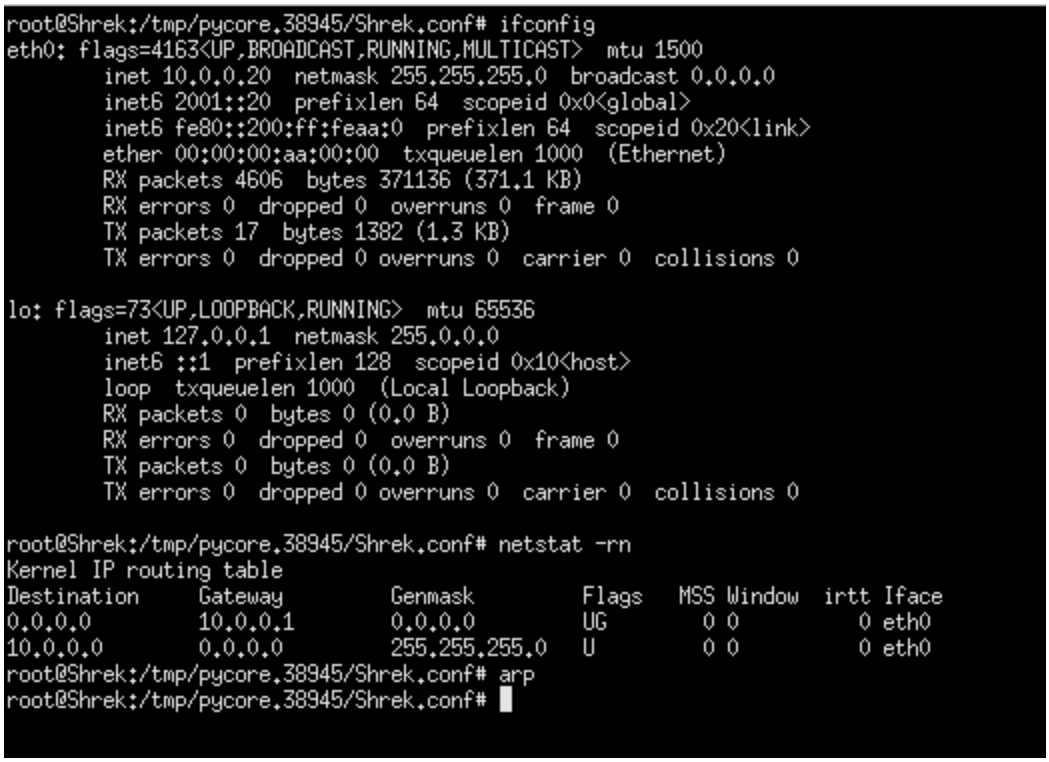


Figure 13: comandos ifconfig, netstat -rn, arp no Shrek

Resposta: Com base na figura podemos concluir que o endereço ether é 00:00:00:aa:00:00, e é o endereço MAC de origem.

d. Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

Resposta: A resposta ARP é encaminhada como unicast, ao contrário do pedido que é transmitido em broadcast. Isto garante que a resposta seja entregue diretamente ao dispositivo que solicitou, aumentando a eficiência e economizando recursos de rede. Optar por enviar a resposta como broadcast seria redundante e iria gerar tráfego desnecessário na rede, já que todos os dispositivos teriam que processar a mensagem ARP.

4. O Burro recebeu toda a informação trocada na interação anterior? Qual será a razão para tal?

Resposta: Na captura de tráfego, podemos observar que o Burro envia um pacote ARP para o RACI solicitando o endereço MAC do PC2. Isso indica que o Burro não possui o endereço MAC do PC2 em sua tabela ARP. Sem o endereço MAC do PC2, o Burro não pode enviar pacotes para ele diretamente.

5. Repita a experiência com uma captura na interface do PC da Fiona. Documente as suas observações e conclusões com base no tráfego observado/capturado.

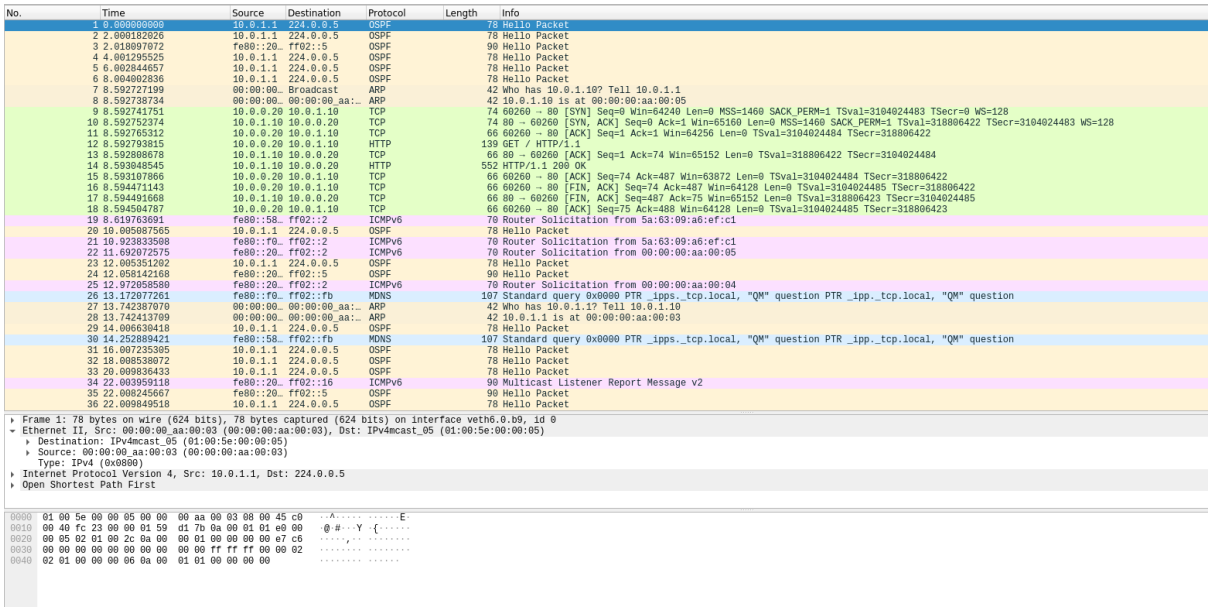
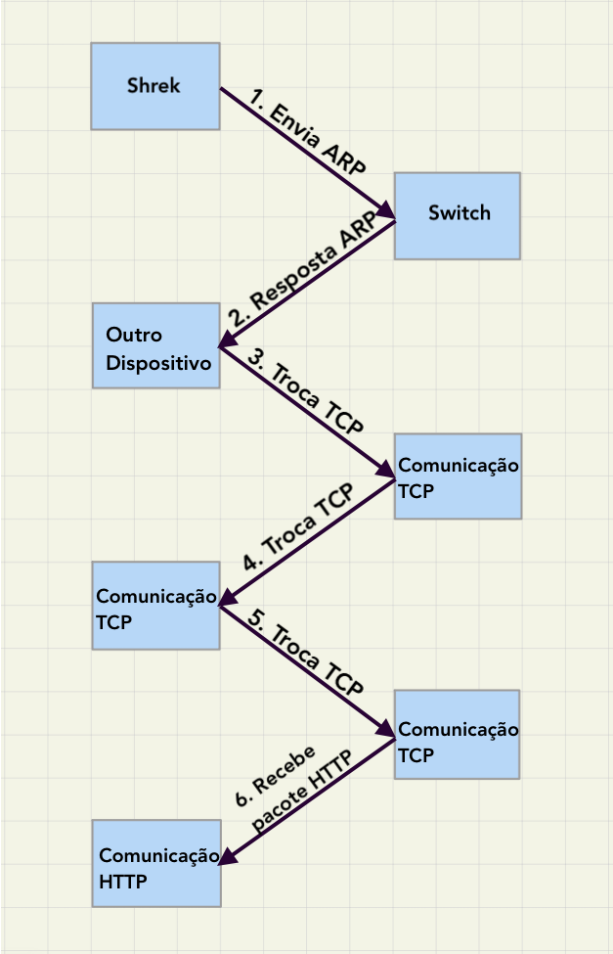


Figure 14: Captura do tráfego da interface Fiona

Resposta: A captura de tráfego da interface Fiona mostra que ela desempenha um papel ativo na rede. Ela troca pacotes OSPF com outros routers para construir e manter a topologia da rede, trocando pacotes TCP com outros hosts para transferir dados, acessando web servers e trocando mensagens ICMP com outros dispositivos para testar a conectividade e anunciar sua presença na rede.

6. Esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens trocadas entre o Shrek e os sistemas com os quais comunica, até à recepção do primeiro pacote que contém dados HTTP. Assuma que todas as tabelas ARP se encontram inicialmente vazias.

Resposta:



7. Construa manualmente a tabela de comutação do switch da casa do Shrek, atribuindo números de porta à sua escolha.

Resposta: Está associado a porta 1 do switch, o endereço MAC 00:00:00:aa:00:02. O endereço MAC 00:00:00:aa:00:00 está associado à porta 2 do switch.
A tabela abaixo, indica ao switch, tendo por base o endereço MAC de destino, por qual porta ele deve encaminhar os pacotes. Quando é recebido pelo switch um pacote com um endereço MAC 00:00:00:aa:00:02, ele encaminha-o para a porta 1, quando recebe um pacote com o endereço MAC 00:00:00:aa:00:00, ele encaminha-o para a porta 2.

MAC address	Porta
00:00:00:aa:00:02	1
00:00:00:aa:00:00	2

Tabela 1: Tabela de comutação de Switch

2. Parte 2

2.1. Exercício 1

A Fiona decide ir morar com o Shrek e o Burro, mas com a condição de deixarem de ter os cabos Ethernet espalhados pela casa. O Shrek decide então comprar equipamento Wireless e faz uma captura de tráfego para perceber melhor o seu funcionamento.
Descarregue da plataforma de ensino a captura WLAN-traffic-20240415.pcapng.zip e abra o ficheiro .pcapng no Wireshark.

Acesso Rádio
Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (radiotap header, radio information) obtida do firmware da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

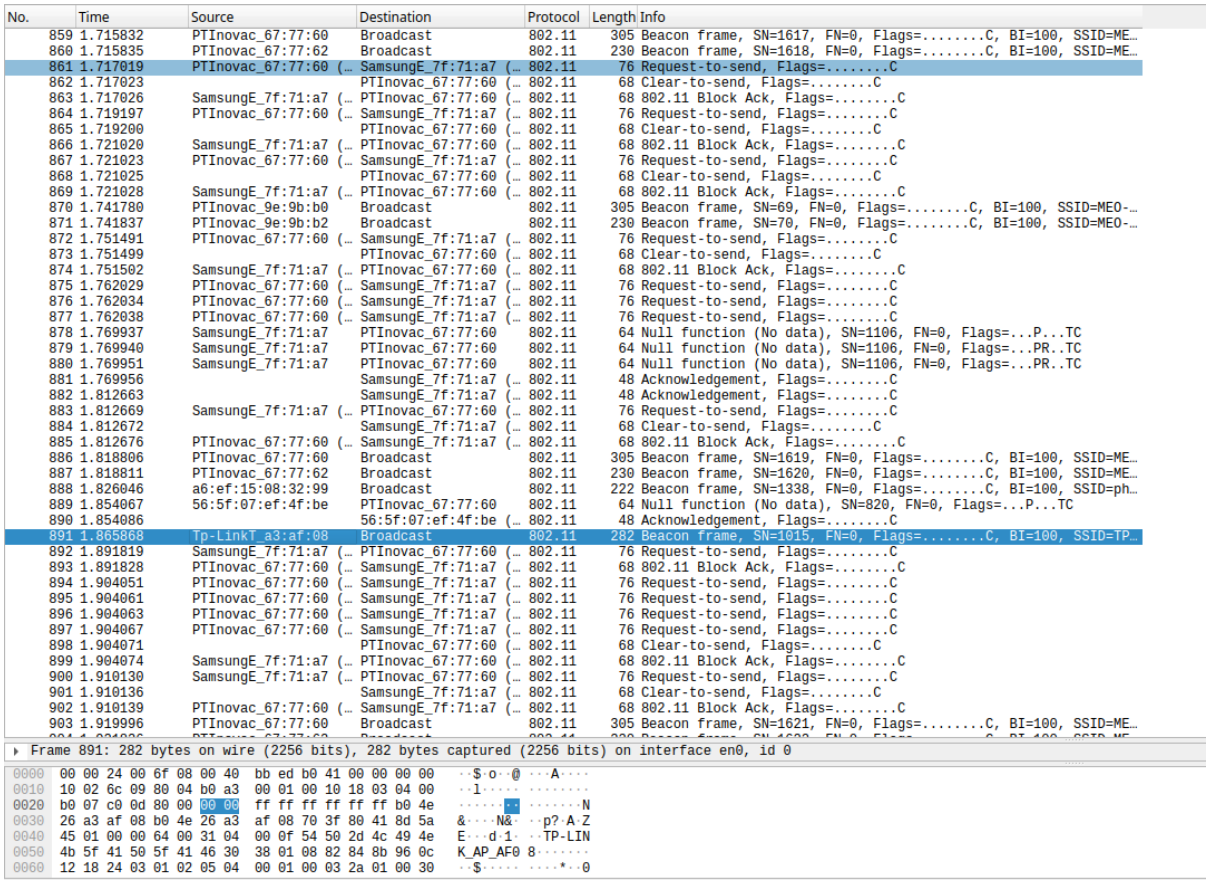


Figure 15: Trama 891 selecionada.

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

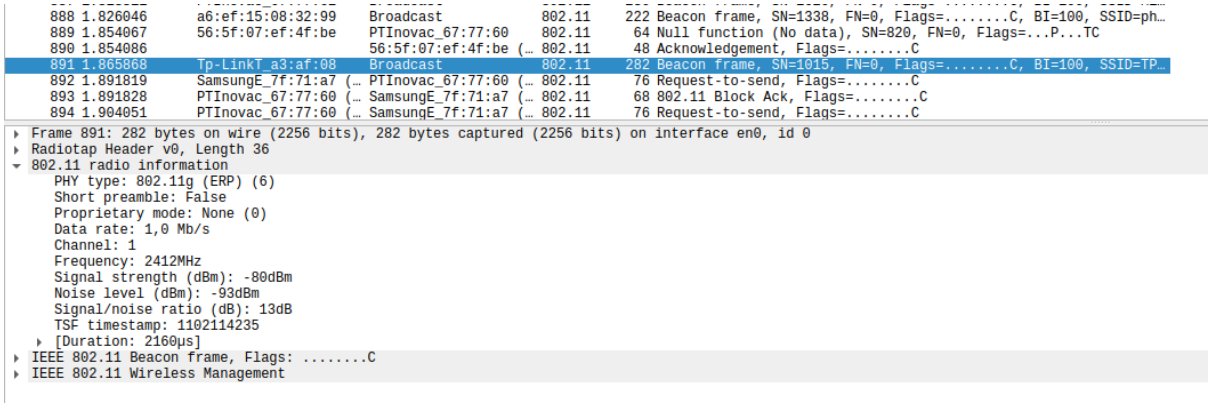


Figure 16: frequência de espetro da trama 891

Resposta: A frequência é de 2412MHz no canal 1.

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

Resposta: A versão usada é 802.11n.

3. Qual a taxa de transmissão a que foi enviada a trama escolhida? Será que essa taxa de transmissão corresponde à máxima que a interface Wi-Fi pode operar? Justifique.

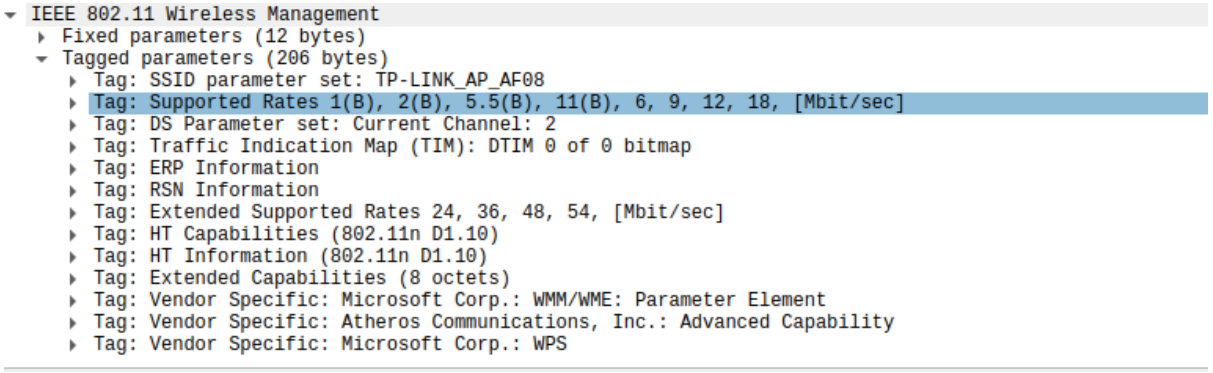


Figure 17: Débito suportado

Resposta: Como comprovamos na figura 16, o data rate é de 1,0 Mb/s. Sendo assim, o débito máximo suportado é de 11 Mb/s. O protocolo 802.11 é capaz de suportar velocidades de até 600 Mb/s, dependendo das condições da rede e das configurações utilizadas.

Como podemos observar na figura 16, o data rate da trama é de 1,0 Mb/s. No entanto, isso não significa que o utilizador final esteja a receber dados a essa velocidade. O débito máximo real depende de diversos fatores, como o protocolo de camada superior utilizado, o tipo de modulação, a taxa de erro da rede e as configurações da interface Wi-Fi.

O protocolo 802.11 possui diferentes versões, cada uma com sua taxa máxima teórica. Por exemplo, o 802.11b suporta até 11 Mb/s, enquanto o 802.11ac pode chegar a 1.750 Mb/s (em condições ideais).

É importante ressaltar que a velocidade real de uma rede Wi-Fi raramente atinge a taxa máxima teórica. Interferência de outras redes, obstáculos físicos, congestionamento da rede e configurações incorretas podem reduzir significativamente o desempenho.

2.2. Exercício 2

Scanning Passivo e Scanning Ativo

Como referido, as tramas *beacon* permitem efetuar *scanning* passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu no de TurnoGrupo (PLXX), responda às seguintes questões:

4. 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 I)?

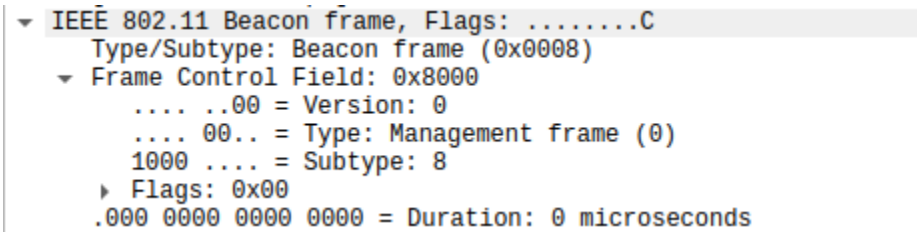


Figure 18: tipo e subtipo da trama

Resposta: A trama que selecionamos foi a 891, e como podemos ver na figura 18, esta perrtence ao tipo *Management* (0) e o seu subtipo é *Beacon* (8). Através do anexo fornecido no enunciado podemos verificar que estes pertencem ao *Frame Control*.

5. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. (Poderá ter de ativar a verificação no Wireshark, em Edit -> Preferences -> Protocols -> IPv4 -> “Validate Checksum if Possible”)

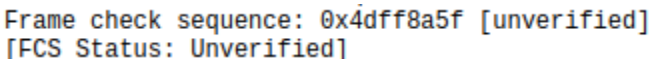


Figure 19: FCS

Resposta: Quando tentamos verificar se o método de deteção de erros está ativo, apareceu a informação que indicamos acima na figura 19. Podemos, portanto, concluir que o CRC não está ativo.

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

As tramas *beacon* são enviadas periodicamente e permitem especificar parâmetros de funcionamento para apoiar a operação e a gestão das ligações sem fios.

Resposta: É necessário usar deteção de erros em redes sem fios, pois devido a existir interferência com o meio ambiente, como, por exemplo, dispositivos eletrónicos e ruídos elétricos; existir atenuação do sinal devido a obstáculos físicos e a própria distância entre o transmissor e o recetor; erros de transmissão, como colisões, ruídos do canal e colisões; e,

por fim, mobilidade, pois é uma rede bastante usada em dispositivos móveis, como telemóveis. Todos estes motivos fazem com que exista erros em redes sem fios, daí a sua importância no seu uso.

7. Uma trama beacon anuncia o intervalo entre beacons às várias taxas de transmissão (B) que o AP suporta, assim como várias taxas de transmissão adicionais (extended supported rates). Indique qual a periodicidade e as taxas de transmissão suportadas pelo AP da trama beacon selecionada.

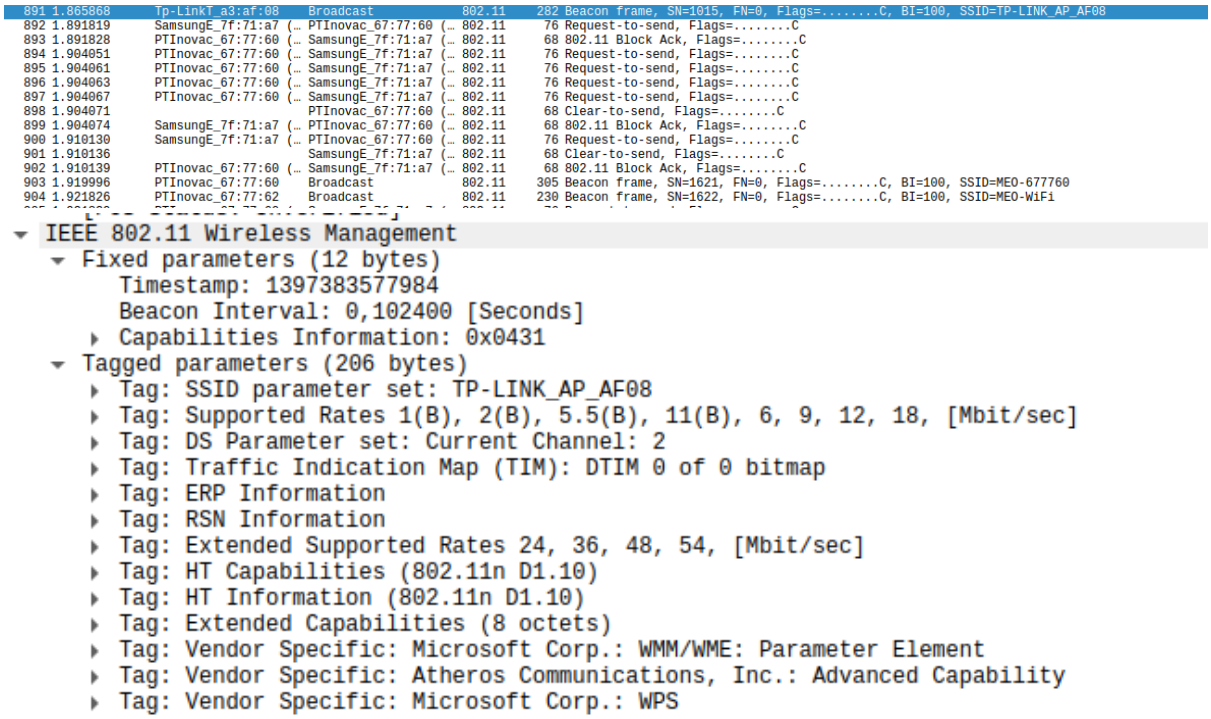


Figure 20: Débitos das tramas

Resposta: O intervalo de tempo previsto entre tramas beacon consecutivas é anunciado na trama, em Fixed parameters -> Beacon Interval que, neste caso, é 0.102400 segundos (visível na figura acima). A periodicidade como podemos ver na figura acima é 0,027979 , ((1,919996-1,865868)+(1,921826-1,919996))/2.
As taxas de transmissão suportadas são:
• 1Mb/s
• 2 Mb/s
• 5.5 Mb/s
• 11 Mb/s
• 6 Mb/s
• 9 Mb/s
• 12 Mb/s
• 18 Mb/s;

8. 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.

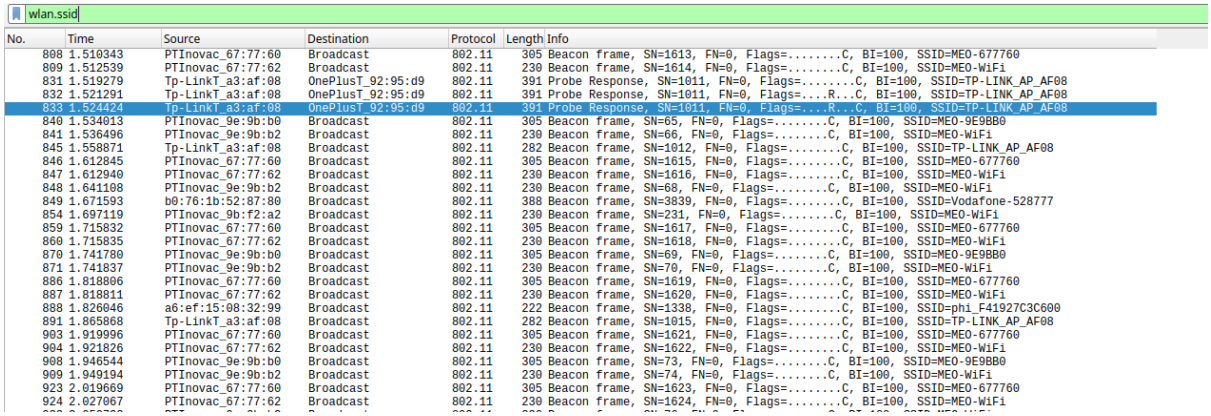


Figure 21: SSIDs a operar na vizinhança da STA

Resposta: De modo a obter os SSIDs dos APs, utilizamos o filtro wlan.ssid no wireshark que nos dá as tramas beacon capturados provenientes dos APs que conseguem comunicar com a STA. Com o uso deste filtro chegamos à conclusão que os três SSIDs são MEO, TP-LINK, Vodafone e phi.

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

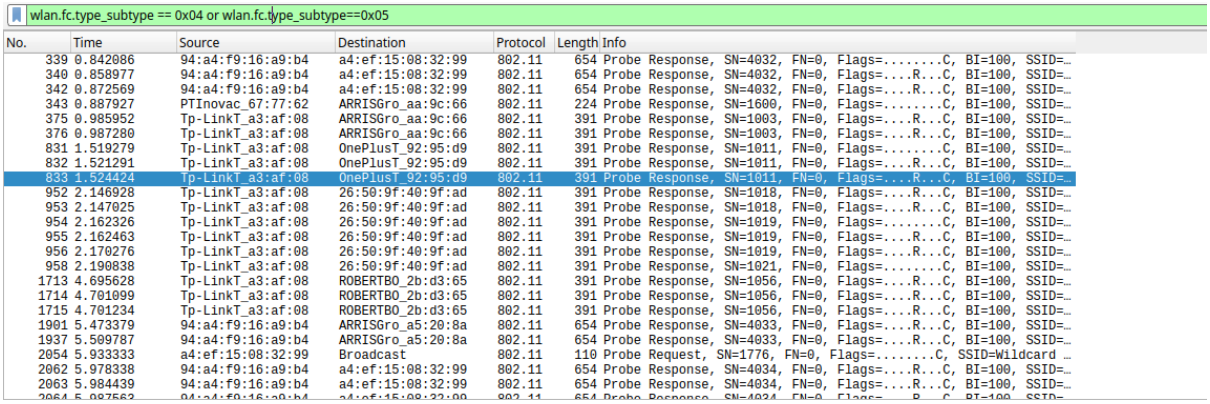


Figure 22: tráfego das tramas probing request/response

Resposta: O filtro que permite essa visualização é: wlan.fc.typesubtype == 0x04 or wlan.fc.type_subtype == 0x05. Assim testamos o subtipo das tramas, filtrando as de probing request (4) e as de probing response (5). A visualização após a aplicação do filtro, comprova a apresentação de tramas representados na figura 22.
Este filtro irá exibir todas as tramas de probe request (wlan.fc.type_subtype == 0x04) e probe response (wlan.fc.type_subtype == 0x05) capturadas na sua captura do Wireshark.

10. Assuma que a STA de captura consegue se associar a qualquer AP na vizinhança. Dadas as tramas recebidas através do scanning ativo e passivo, observe os valores da força do sinal (Signal Strength) nas meta-informações de nível físico e aponte

qual AP a STA de captura deve se associar para obter a melhor qualidade de ligação possível. Indique como chegou a esta resposta.

Resposta: Como podemos ver na figura 16, a força do sinal é -80dBm. A força do sinal não é de confiança, pelo que não é dos piores sinais mas a probabilidade da conceção ser estabelecida é reduzida, o que significa que, a probabilidade de receber tramas, nestas condições, menor.

11. Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal, utilizando-se dos valores de sensibilidade mínima (Minimum Sensivity) e taxa de transmissão (Data Rate) das tabelas referência do Anexo II, da força do sinal recebido nas tramas do AP indicado da resposta anterior, estime o débito que a STA obterá nessa ligação.

Resposta:
De acordo com a tabela de referência do Anexo II, para um MCS 3 e uma sensibilidade mínima de -81 dBm, a taxa de transmissão máxima é de 24 Mbps.
Considerando um fator de redução de 50% devido a interferências, ruído e perdas de caminho, a taxa de transmissão efetiva seria de 12 Mbps (24 Mbps * 0.5).
O débito da ligação Wi-Fi é calculado da seguinte forma:
Débito = Taxa de transmissão efetiva * Tempo de transmissão útil
Débito = 12 Mbps * (1000 bytes / 8 bits/byte) * (1 ms / 1000 ms/s) = 1500 bps

2.3. Exercício 3

Processo de Associação

Numa rede Wi-Fi estruturada, um nodo ou STA deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request da STA para o AP e a trama association response enviada pelo AP para a STA, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

12. 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.

Resposta: Para obter o conjunto completo de conexões entre a estação (STA) e o ponto de acesso (AP) em um processo de associação, foi necessário desenvolver um filtro que nos fornecesse, de maneira conveniente, um conjunto organizado dessas conexões.
Sendo assim, o filtro aplicado foi:
wlan.fc.type == 0 && (wlan.fc.type subtype == 0 or wlan.fc.type subtype == 1 or wlan.fc. type subtype == 11)
A tabela apresentada contém informações sobre os filtros e as tramas associadas a eles. Estamos, essencialmente, filtrando os quadros de gerenciamento (Management Frames) e,

dentro deles, aqueles que são do tipo "Association Request"(Solicitação de Associação), "Association Response"(Resposta de Associação) e "Authentication"(Autenticação). Essas são fases relevantes do processo de associação.
Após a aplicação do filtro, obtiveram-se as tramas seguintes:

wlan.fc.type==0 && (wlan.fc.type_subtype==0 || wlan.fc.type_subtype==1 || wlan.fc.type_subtype==11)

No.	Time	Source	Destination	Protocol	Length	Info
3228	14.890461	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81	Authentication, SN=3073, FN=0, Flags=....R...C
3624	18.716086	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81	Authentication, SN=3154, FN=0, Flags=....R...C
3625	18.716198	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81	Authentication, SN=3154, FN=0, Flags=....R...C
3626	18.719251	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81	Authentication, SN=3154, FN=0, Flags=....R...C
3627	18.728358	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81	Authentication, SN=3154, FN=0, Flags=....R...C
5177	34.292210	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81	Authentication, SN=3472, FN=0, Flags=....R...C
5178	34.292316	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81	Authentication, SN=3472, FN=0, Flags=....R...C
5179	34.295367	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81	Authentication, SN=3472, FN=0, Flags=....R...C
5180	34.301443	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81	Authentication, SN=3472, FN=0, Flags=....R...C
12855	98.374622	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	105	Authentication, SN=674, FN=0, Flags=........C
12857	98.374728	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	81	Authentication, SN=3667, FN=0, Flags=........C
12861	98.387225	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	213	Association Request, SN=675, FN=0, Flags=........C, SSID=MEO-WiFi
12863	98.387244	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	192	Association Response, SN=3670, FN=0, Flags=........C

Figure 23: Processo de associação completo - redes IEEE 802.11

Observa-se que o processo de associação consiste em duas etapas, autenticação e associação, ambas com uma solicitação e uma resposta:

- Solicitação de Autenticação - Frame 12855
- Resposta de Autenticação - Frame 12857
- Solicitação de Associação - Frame 12861
- Resposta de Associação - Frame 12863

13. Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

Resposta:

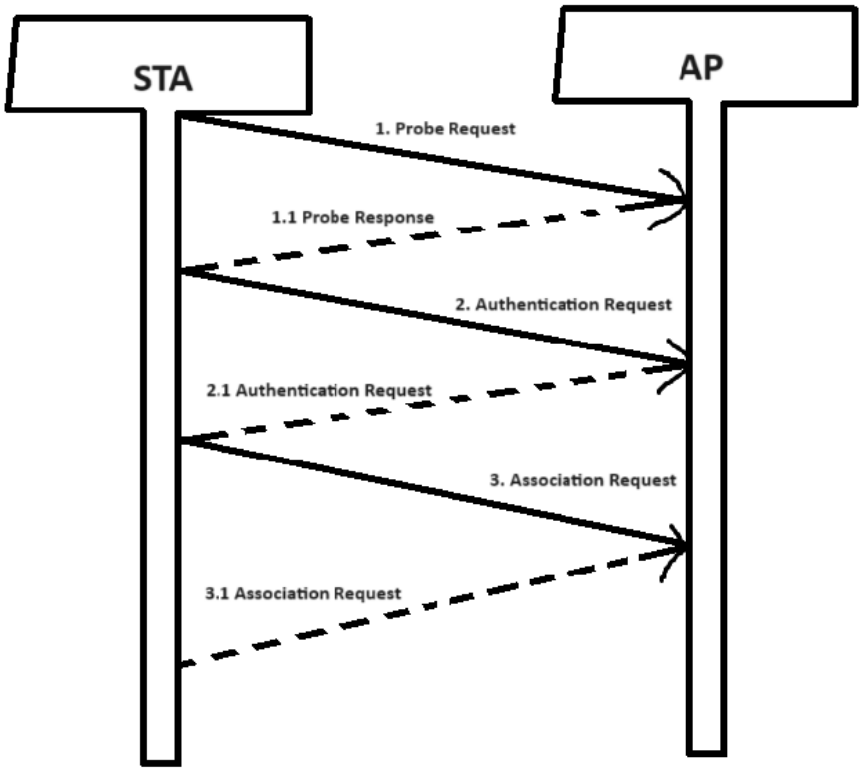


Figure 24: Processo de associação completo - diagrama - redes 802.11

2.4. Exercício 4

Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

14. Estabeleça um filtro apropriado e selecione uma trama de dados (Data ou QoS Data), cujo número de ordem inclua o seu identificador de grupo (terminação XX, ou X caso não exista XX). Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

Resposta: Analisando a flag referente ao DS status, da figura abaixo, podemos concluir que a direcionalidade desta trama pode ser observada através dos campos ”To DS: 0”e ”From DS: 1”. O primeiro indica que a trama não é direcionada ao DS e o segundo que a trama é proveniente do DS, ou seja, podemos concluir que a trama não é destinada à WLAN (Wireless Local Area Network) e é proveniente da mesma.

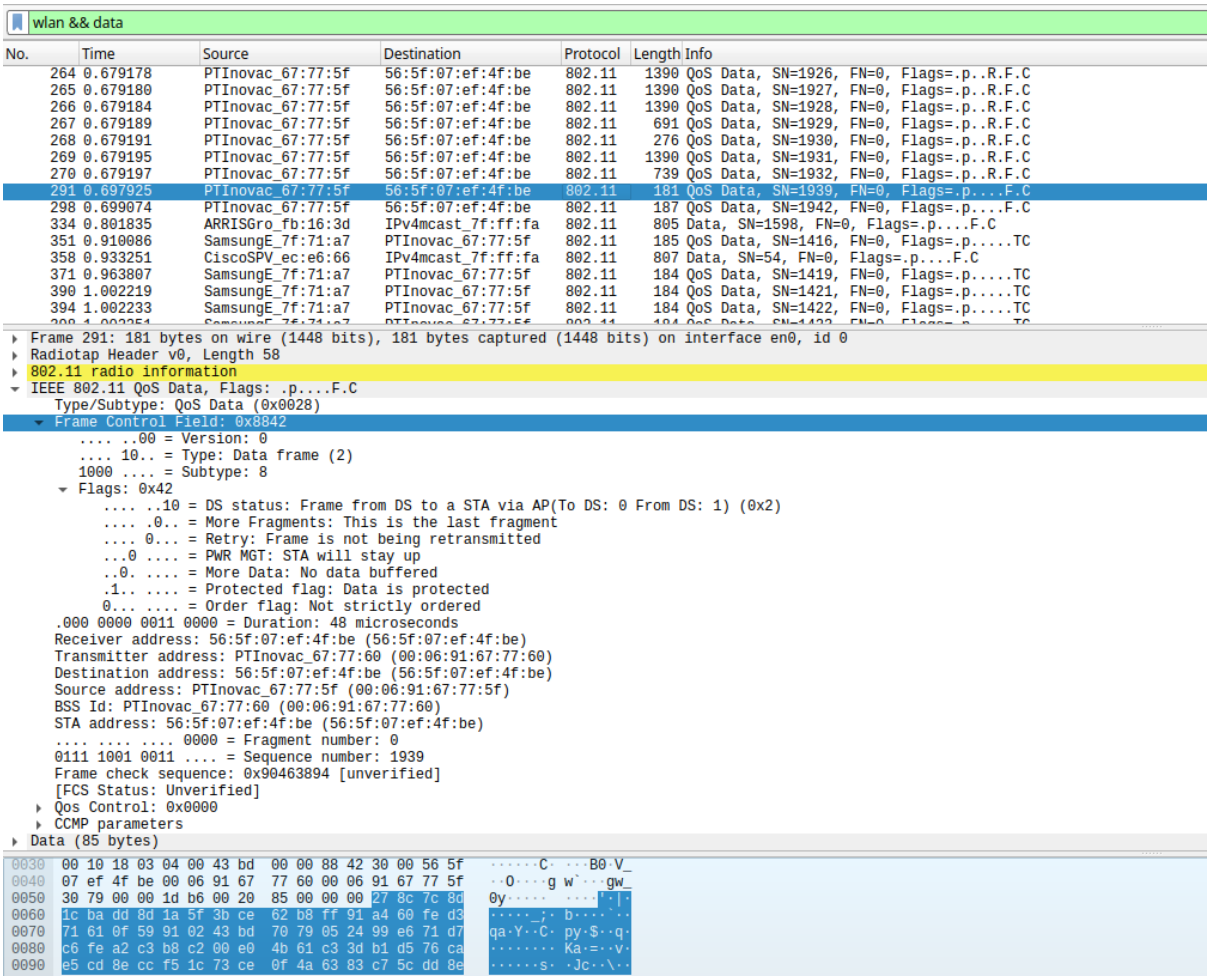


Figure 23: Trama de dados nº 291

15. Para a trama de dados selecionada, 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)?

Resposta: Com base na trama da figura abaixo concluímos assim que os endereços MAC correspondentes são:

- **STA:** 56:5f:07:ef:4f:be
- **AP:** 00:06:91:67:77:60
- **Router:** 56:5f:07:ef:4f:be

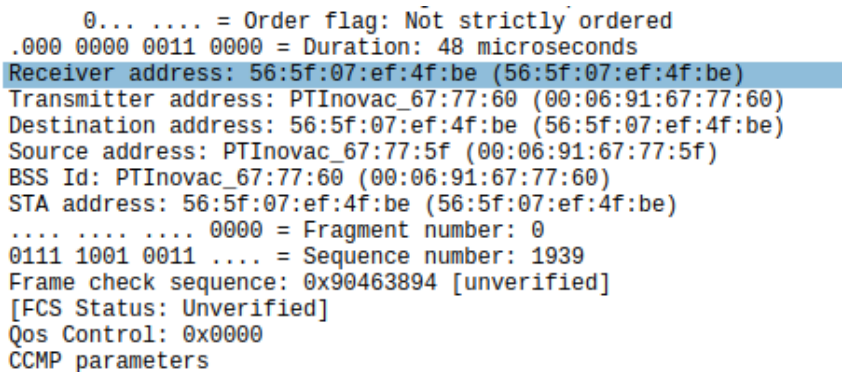


Figure 24: Totalidade da trama

16. 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 envio de dados selecionado 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 direccionalidade 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.

Reposta: De forma a encontrar transferências de dados em que é usada a opção RTC/CTS em primeiro lugar aplicamos o seguinte filtro: wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c.

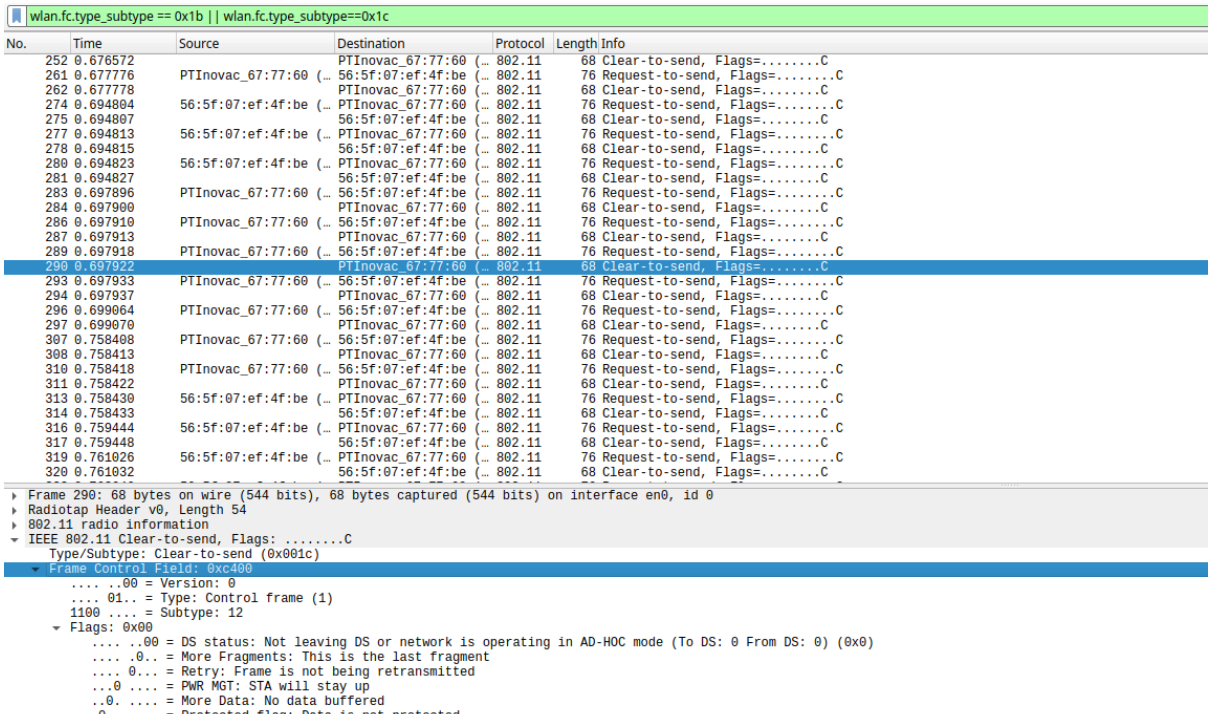


Figure 25: Filtro wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c

Conclusão

O foco principal deste trabalho é a exploração de vários aspectos relacionados às redes sem fio (Wi-Fi).

Inicialmente, abordamos o Acesso Rádio, onde investigamos a camada física das redes sem fio, incluindo elementos como canais e frequências.

Em seguida, comparamos o scanning ativo e passivo, destacando que o primeiro é realizado por meio das tramas beacon, permitindo a descoberta dos pontos de acesso disponíveis, enquanto o segundo utiliza o probe response.

No terceiro ponto, discutimos o Processo de Associação, necessário para estabelecer a conexão entre um dispositivo e um ponto de acesso. Este processo envolve um pedido de associação feito pelo dispositivo, seguido da resposta do ponto de acesso.

Por fim, examinamos o processo de Transferência de Dados, levando em consideração dois fatores: informações obtidas nas tramas e o controlo da transferência.

Além disso, aprofundamos nosso conhecimento sobre as funcionalidades da ferramenta Wireshark, o que nos permitiu utilizá-la de maneira mais eficiente.