



Universidade do Minho

LICENCIATURA EM CIÊNCIAS DA COMPUTAÇÃO
SISTEMAS DE COMUNICAÇÕES E REDES

Ensaio Escrito

**Nível de Ligação Lógica - Ethernet e Protocolo
ARP; Redes Sem Fios (IEEE 802.11)**

Grupo 28

Davide Santos (A102938)

Edgar Araújo (A102946)

Pedro Augusto Camargo (A102504)

Outubro 2023

Contents

1	Captura e Análise de Tramas Ethernet	3
1.1	Anote os endereços Ethernet (ou MAC) de origem e de destino da trama capturada com o pedido HTTP. Identifique a que sistemas se referem. Justifique.	3
1.2	Analisando os campos do cabeçalho da trama capturada, diga, justificando, qual o protocolo encapsulado nessa trama.	3
1.3	Quantos bytes são usados desde o início da trama até ao caractere ASCII “G” do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET (considere os bytes ocupados pela camada física e pelo FCS, indicados na Figura 1).	3
1.4	Quais são os endereços Ethernet da origem e destino? A que sistemas de rede correspondem? Justifique.	5
1.5	Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.	5
2	Protocolo ARP	6
2.1	Abra uma consola no host onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp.	6
2.1.1	Com a ajuda do manual arp (man arp), interprete sucintamente o significado de cada uma das colunas da tabela.	6
2.1.2	Indique, justificando, qual o equipamento da rede em questão que poderá apresentar a maior tabela ARP em termos de número de entradas.	7
2.1.3	Realize as operações necessárias para completar a tabela ARP identificada na alínea anterior. Indique como procedeu e apresente essa tabela completa.	7
2.2	Qual é o valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (ARP Request)? Como interpreta e justifica o endereço destino usado?	7
2.3	Qual o valor hexadecimal no campo Tipo da trama Ethernet? O que indica?	7
2.4	Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Identifique o tipo de endereços contidos na mensagem ARP.	8
2.5	Explícite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?	8
2.6	Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.	8
2.6.1	Qual o valor do campo ARP opcode? O que especifica?	8
2.6.2	Em que posição da mensagem ARP está a resposta ao pedido ARP?	8
2.6.3	Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).	9
2.7	Verifique se o ping feito ao segundo PC originou pacotes ARP e justifique a situação observada.	9
2.8	Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.	9
3	Redes Sem Fios (IEEE 802.11)	10
3.1	Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.	10
3.2	Identifique a versão da norma IEEE 802.11 que está a ser usada.	10
3.3	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.	10
3.4	Verifique qual a força do sinal (signal strength) e a qualidade expectável de receção da trama, tendo em conta a tabela apresentada em Anexo.	10
3.5	Selecione a trama beacon nr. 100+NG, sendo NG o seu número de grupo. Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?	11
3.6	Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?	12
3.7	Qual o intervalo de tempo previsto entre tramas beacon consecutivas? (nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.	13

3.8	Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explique o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).	13
3.9	Face ao endereçamento usado, indique a que sistemas são endereçadas ambas as tramas e explique qual o propósito das mesmas?	13
3.10	Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.	14
3.11	Efetue um diagrama que ilustre, com as tramas identificadas na alínea anterior, a sequência de todas as tramas trocadas no processo de autenticação e associação entre o STA e o AP.	14
3.12	Considere a trama de dados n.º 622. 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?	14
3.13	Para a trama de dados da alínea anterior, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição.	15
3.14	Observa-se que ao longo da transferência de dados são usadas tramas de controlo ACK. Tente explicar porque razão têm de existir, contrariamente ao que acontece numa rede Ethernet.	15
3.15	Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada, identificando a direccionalidade das tramas, as tramas de controlo e os sistemas envolvidos. Apresente as tramas e os sistemas devidamente identificados sob a forma de um diagrama de sequência.	15
4	Conclusao	15

1 Captura e Análise de Tramas Ethernet

Selecione a trama Ethernet que contém a mensagem HTTP GET.

```
No. Time Source Destination Protocol Length Info
309579 222.320604325 192.168.1.39 193.136.9.240 HTTP 175 GET /
ferramentas/CORE/xubuncore.html HTTP/1.1

Frame 309579: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)
on interface wlp3s0, id 0

Ethernet II, Src: CloudNet_c9:c9:03 (30:03:c8:c9:c9:03), Dst: Sagemcom_9f:a6:37
(10:d7:b0:9f:a6:37)

Internet Protocol Version 4, Src: 192.168.1.39, Dst: 193.136.9.240

Transmission Control Protocol, Src Port: 56218, Dst Port: 80, Seq: 1, Ack: 1,
Len: 109

Hypertext Transfer Protocol
```

1.1 Anote os endereços Ethernet (ou MAC) de origem e de destino da trama capturada com o pedido HTTP. Identifique a que sistemas se referem. Justifique.

Os endereços Ethernet localizam-se na camada Ethernet do modelo OSI, e são:

- Endereço de origem: 30:03:c8:c9:c9:03 (CloudNet_c9:c9:03 / O nosso computador)
O endereço de origem é o endereço do nosso computador, pois foi o computador que enviou a trama.
- Endereço de destino: 10:d7:b0:9f:a6:37 (Sagemcom_9f:a6:37 / O router)
O endereço de destino é o endereço do router, pois foi o router que recebeu a trama.

1.2 Analisando os campos do cabeçalho da trama capturada, diga, justificando, qual o protocolo encapsulado nessa trama.

O protocolo encapsulado é o IPv4, pois o campo Type da trama tem o valor 0x0800, que corresponde ao protocolo IPv4.

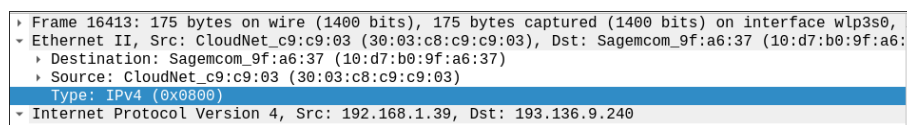


Figure 1: Campo Type da trama.

1.3 Quantos bytes são usados desde o início da trama até ao caractere ASCII “G” do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET (considere os bytes ocupados pela camada física e pelo FCS, indicados na Figura 1).

ain.

Observa-se que o caractere “G” está na posição 0x42 da trama = 66 bytes. Considerando que o preamble e o SFD ocupam 7+1 bytes no início da trama, o número de bytes usados desde o início da trama até ao caractere ASCII “G” é $66+8 = 74$ bytes.

O tamanho da trama, sem o preamble, o SFD, e o FCS é 175 bytes, com o preamble, o SFD, e o FCS é $175+7+1+4 = 187$ bytes. O tamanho do HTTP GET é $175-66=109$ bytes. Logo, a sobrecarga é de $187-109=78$ bytes. Em percentagem temos: $78/187 = 41.71\%$ de sobrecarga.

0000	10 d7 b0 9f a6 37 30 03	c8 c9 c9 03 08 00 45 0070.....E
0010	00 a1 5d d0 40 00 40 06	4f 3f c0 a8 01 27 c1 88	..]@.0?...'..
0020	09 f0 94 4e 00 50 9e 78	dd 67 99 c9 e0 8f 80 18	...N.P.x.g.....
0030	01 f6 f8 1b 00 00 01 01	08 0a 59 18 fb 48 8d 7dY..H.}
0040	db 25 47 45 54 20 2f 66	65 72 72 61 6d 65 6e 74	..%GET /f errament
0050	61 73 2f 43 4f 52 45 2f	78 75 62 75 6e 63 6f 72	as/CORE/ xubuncor
0060	65 2e 68 74 6d 6c 20 48	54 54 50 2f 31 2e 31 0d	e.html H TTP/1.1
0070	0a 48 6f 73 74 3a 20 6d	61 72 63 6f 2e 75 6d 69	..Host: m arco.umi
0080	6e 68 6f 2e 70 74 0d 0a	55 73 65 72 2d 41 67 65	nho.pt.. User-Age
0090	6e 74 3a 20 63 75 72 6c	2f 38 2e 34 2e 30 0d 0a	nt: curl /8.4.0..
00a0	41 63 63 65 70 74 3a 20	2a 2f 2a 0d 0a 0d 0a	Accept: */*....

Figure 2: Trama em formato de bytes.

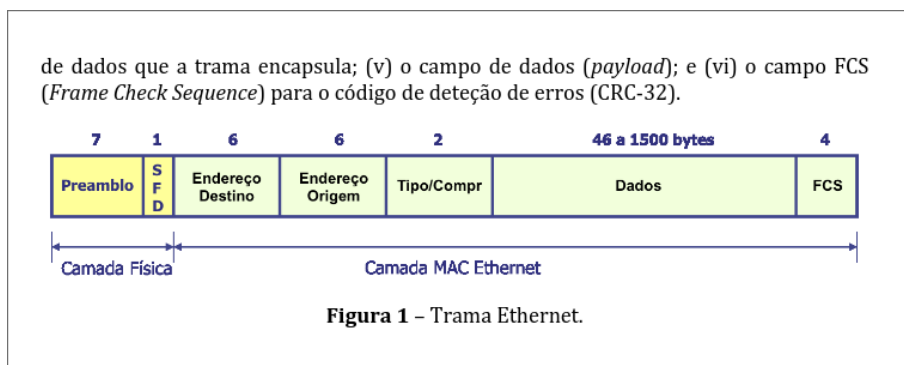


Figure 3: Tamanhos do preamblo, SFD e FCS.

A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP

```
No. Time Source Destination Protocol Length Info
16427 13.899293562 193.136.9.240 192.168.1.39 HTTP 479 HTTP/1.1 200 OK(text/html)
```

Frame 16427: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface wlp3s0

Ethernet II, Src: Sagemcom_9f:a6:37 (10:d7:b0:9f:a6:37), Dst: CloudNet_c9:c9:03 (30:03:c8:c9:c9:03)

Destination: CloudNet_c9:c9:03 (30:03:c8:c9:c9:03)

Source: Sagemcom_9f:a6:37 (10:d7:b0:9f:a6:37)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 193.136.9.240, Dst: 192.168.1.39

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 465

Identification: 0xb880 (47232)

010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 53

Protocol: TCP (6)

Header Checksum: 0xfe5e [validation disabled]

[Header checksum status: Unverified]

Source Address: 193.136.9.240

Destination Address: 192.168.1.39

Transmission Control Protocol, Src Port: 80, Dst Port: 37966, Seq: 8689, Ack: 110, Len: 413

[7 Reassembled TCP Segments (9101 bytes): #16415(1448), #16417(1448), #16419(1448), #16421(1448), #16423(1448), #16425(1448), #16427(413)]

Hypertext Transfer Protocol

Line-based text data: text/html (245 lines)

1.4 Quais são os endereços Ethernet da origem e destino? A que sistemas de rede correspondem? Justifique.

Os endereços Ethernet localizam-se na camada Ethernet do modelo OSI, e são:

- Endereço de origem: 10:d7:b0:9f:a6:37 (Sagemcom_9f:a6:37 / O router)
O endereço de origem é o endereço do router, pois foi o router que enviou a trama.
- Endereço de destino: 30:03:c8:c9:c9:03 (CloudNet_c9:c9:03 / O nosso computador)
O endereço de destino é o endereço do nosso computador, pois foi o nosso computador que recebeu a trama.

1.5 Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.

Os protocolos contidos na trama recebida são:

- Ethernet II
- IPv4
- TCP
- HTTP

2 Protocolo ARP

Selecione um host (PC, servidor) de um departamento à sua escolha. Neste host inicie a captura de tráfego com o Wireshark do CORE. A partir desse host efectue pings para dois hosts localizados na rede do outro departamento. Pare a captura de tráfego no Wireshark e localize o tráfego ARP, usando o filtro arp.

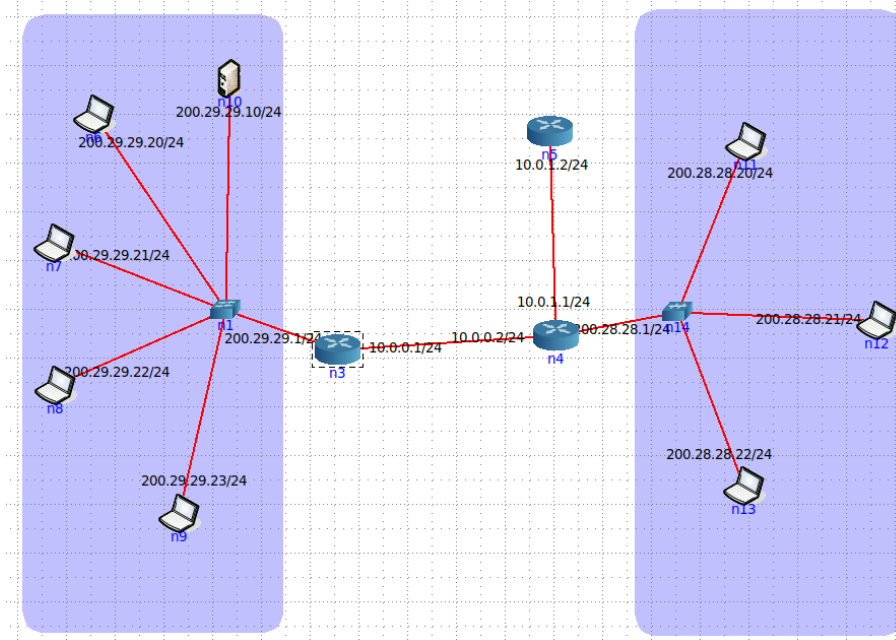


Figure 4: Rede

2.1 Abra uma consola no host onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp.

```
root@n3:/tmp/pycore.40919/n3.conf# arp
Address HWtype HWaddress Flags Mask Iface
10.0.0.2 ether 00:00:00:aa:00:0b C
```

Figure 5: Enter Caption

2.1.1 Com a ajuda do manual arp (man arp), interprete sucintamente o significado de cada uma das colunas da tabela.

Address: O endereço IP associado ao endereço MAC.

HWtype: O tipo de hardware, que é "ether" neste caso, indicando Ethernet.

HWaddress: O endereço MAC associado ao endereço IP.

Flags: As bandeiras indicam o estado da entrada na tabela. "C" significa que a entrada está completa, ou seja, o mapeamento IP-MAC é conhecido e válido.

Mask: Se estiver preenchido, indica uma máscara de sub-rede associada ao endereço IP.

Iface: A interface de rede à qual o endereço MAC está associado.

Neste caso, com base na tabela ARP, existe apenas uma entrada:

Endereço IP 10.0.0.2 está associado ao **endereço MAC 00:00:00:aa:00:0b**. A entrada na tabela ARP está marcada como completa (C) e associada à interface **eth0**.

Essa entrada significa que o endereço IP 10.0.0.2 está associado ao endereço MAC 00:00:00:aa:00:0b e que essa associação é conhecida e válida. Portanto, o sistema já possui essa informação na tabela ARP e não precisa fazer solicitações ARP adicionais para esse endereço, pois já tem o mapeamento IP-MAC correspondente.

2.1.2 Indique, justificando, qual o equipamento da rede em questão que poderá apresentar a maior tabela ARP em termos de número de entradas.

Na rede, o equipamento que provavelmente apresenta um maior número de entradas na tabela ARP será, provavelmente, o router n3, uma vez que apresenta 6 ligações, ao invés do n4 que apresenta 5 ligações.

2.1.3 Realize as operações necessárias para completar a tabela ARP identificada na alínea anterior. Indique como procedeu e apresente essa tabela completa.

Para chegar a esta tabela ARP, é necessário dar *ping* a todos os dispositivos ligados ao router n3 pelo terminal e, de seguida, é deve abrir outro terminal pelo router n3 e abrir a tabela arp, chegando a um resultado semelhante ao aqui mostrado.

```
root@n3:/tmp/pycore.40919/n3.conf# arp
```

Address	Hwtype	Hwaddress	Flags	Mask	Iface
200.29.29.23	ether	00:00:00:aa:00:04	C		eth1
200.29.29.21	ether	00:00:00:aa:00:02	C		eth1
200.29.29.22	ether	00:00:00:aa:00:03	C		eth1
200.29.29.10	ether	00:00:00:aa:00:05	C		eth1
200.29.29.20	ether	00:00:00:aa:00:01	C		eth1
10.0.0.2	ether	00:00:00:aa:00:0b	C		eth0

Figure 6: Tabela ARP do router n3

2.2 Qual é o valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (ARP Request)? Como interpreta e justifica o endereço destino usado?

No.	Time	Source	Destination	Protocol	Length	Info
12	8.694067247	fe80::200:ff:feaa:0	ff02::5	OSPF	90	Hello Packet
13	10.646947980	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
14	12.648460886	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
15	13.824304642	fe80::200:ff:feaa:4	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:04
16	14.649974950	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
17	14.848299861	fe80::7c76:5eff:fe5_	ff02::2	ICMPv6	70	Router Solicitation from 12:c1:a8:de:e7:23
18	15.360148810	fe80::200:ff:feaa:2	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:02
19	15.745008109	00:00:00:aa:00:00	Broadcast	ARP	42	Who has 200.29.29.21? Tell 200.29.29.1
20	15.715949922	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	200.29.29.21 is at 00:00:00:aa:00:02
21	15.715951489	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=1/256, ttl=64 (reply in 2..
22	15.715960769	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=1/256, ttl=64 (request in..
23	16.384052859	fe80::200:ff:feaa:5	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:05
24	16.051055118	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
25	16.736120435	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=2/512, ttl=64 (reply in 2..
26	16.736147296	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=2/512, ttl=64 (request in..
27	17.426915284	fe80::7c76:5eff:fe5_	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR..
28	17.760368250	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=3/768, ttl=64 (reply in 2..

Frame 19: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth3.1.48, id 0
Ethernet II, Src: 00:00:00:aa:00:00 (00:00:00:aa:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1. = LG bit: Locally administered address (this is NOT the factory default)
.....1. = IG bit: Group address (multicast/broadcast)
Source: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Address: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
.....0. = LG bit: Globally unique address (factory default)
.....0. = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Address Resolution Protocol (request)

Figure 7: ARP Request

O endereço de origem na trama Ethernet é 00:00:00:aa:00:00 e o endereço do destino é ff:ff:ff:ff:ff:ff. O endereço de Destino é um endereço de broadcast. Isto significa que a trama ARP está a ser enviada para todos os dispositivos na rede local para que o dispositivo de destino a reconheça.

2.3 Qual o valor hexadecimal no campo Tipo da trama Ethernet? O que indica?

Type: ARP (0x0806)

Figure 8: Enter Caption

O valor hexadecimal no campo Tipo da trama Ethernet indica o tipo de dados que a trama contém. No caso de uma trama ARP, esse valor é 0x0806, que representa o protocolo ARP, como mostra a print tirada do wireshark.

2.4 Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Identifique o tipo de endereços contidos na mensagem ARP.

É possível saber que se trata de um pedido ARP se observarmos o valor do campo "Opcode" (código de operação) na mensagem ARP. O valor 1 neste campo indica uma solicitação ARP. Os tipos de endereços contidos na mensagem ARP são o endereço IP e o endereço MAC.

2.5 Explícite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?

O host de origem faz uma pergunta à rede, perguntando "Quem possui o endereço IP X?". Nesse caso, o host deseja mapear um endereço IP para um endereço MAC correspondente.

O host de origem pergunta à rede "Quem é possui este endereço IP?". Neste caso, o host quer mapear um endereço IP para um endereço MAC.

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

No.	Time	Source	Destination	Protocol	Length	Info
12	8.694007247	fe80::200:ff:feaa:0	ff02::5	OSPF	90	Hello Packet
13	10.646947980	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
14	12.648460886	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
15	13.824304642	fe80::200:ff:feaa:4	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:04
16	14.649874958	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
17	14.848290961	fe80::7c76:5eff:fe5...	ff02::2	ICMPv6	70	Router Solicitation from 12:cl:a8:de:e7:23
18	15.369148810	fe80::200:ff:feaa:2	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:02
19	15.715908109	00:00:00:aa:00:00	Broadcast	ARP	42	Who has 200.29.29.21? Tell 200.29.29.1
20	15.715909222	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	200.29.29.21 is at 00:00:00:aa:00:02
21	15.715951409	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=1/256, ttl=64 (reply in 2...
22	15.715960769	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=1/256, ttl=64 (request in...
23	16.384052859	fe80::200:ff:feaa:5	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:05
24	16.651055118	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
25	16.736120435	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=2/512, ttl=64 (reply in 2...
26	16.736147296	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=2/512, ttl=64 (request in...
27	17.426915284	fe80::7c76:5eff:fe5...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
28	17.708368250	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=3/768, ttl=64 (reply in 2...

Frame 20: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth3.1.48, id 0
Ethernet II, Src: 00:00:00:aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Destination: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Address: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Source: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
Address: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Type: ARP (0x8006)
Address Resolution Protocol (reply)

Figure 9: Mensagem ARP a responder ao pedido ARP

A mensagem ARP em resposta ao pedido ARP está logo a seguir, como é possível ver no *printscreen*.

2.6.1 Qual o valor do campo ARP opcode? O que especifica?

O valor do campo ARP opcode é 2, como é possível ver no *printscreen* do pacote capturado pelo wireshark. Isto significa que é uma resposta ARP.

Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Type: ARP (0x8006)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
Sender IP address: 200.29.29.21
Target MAC address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
Target IP address: 200.29.29.1

Figure 10: ARP Opcode

2.6.2 Em que posição da mensagem ARP está a resposta ao pedido ARP?

A resposta ao pedido ARP está na posição após o cabeçalho ARP (28 bytes).

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

O ARP Request é enviado em **modo broadcast**, pois o host não sabe de quem é o endereço IP e precisa de perguntar a todos os dispositivos ligados quem é. A resposta ARP (ARP Reply) é enviada em **modo unicast**. Isso significa que a resposta é direcionada especificamente para o host que fez a pergunta ARP, uma vez que o dispositivo não tem necessidade de informar todos que é ele e precisa apenas de informar o host.

2.7 Verifique se o ping feito ao segundo PC originou pacotes ARP e justifique a situação observada.

O segundo ping feito também originou pacotes, como é possível ver no printscreen do wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
30	18.176560982	fe80::548c:6eff:fe3...	ff02::2	ICMPv6	70	Router Solicitation from 56:0c:6e:3a:0f:e8
31	18.181187729	fe80::200:ff:feaa:1	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:01
32	18.181565378	fe80::200:ff:feaa:3	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:03
33	18.651221769	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
34	18.724792389	fe80::200:ff:feaa:0	ff02::5	OSPF	90	Hello Packet
35	18.784172948	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=4/1924, ttl=64 (reply in ...)
36	18.784206495	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=4/1924, ttl=64 (request i...
37	18.795650234	fe80::548c:6eff:fe3...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR...
38	19.000095498	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=5/1200, ttl=64 (reply in ...)
39	19.808118267	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=5/1200, ttl=64 (request i...
40	20.651810228	200.29.29.1	224.0.0.5	OSPF	78	Hello Packet
41	20.736265108	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	Who has 200.29.29.1? Tell 200.29.29.21
42	20.736295681	00:00:00:aa:00:00	00:00:00:aa:00:02	ARP	42	200.29.29.1 is at 00:00:00:aa:00:00
43	20.832075521	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=6/1536, ttl=64 (reply in ...)
44	20.832098422	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=6/1536, ttl=64 (request i...
45	21.856329301	200.29.29.1	200.29.29.21	ICMP	98	Echo (ping) request id=0x004c, seq=7/1792, ttl=64 (reply in ...)
46	21.856362861	200.29.29.21	200.29.29.1	ICMP	98	Echo (ping) reply id=0x004c, seq=7/1792, ttl=64 (request i...

Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
▼ Ethernet II, Src: 00:00:00:aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
 ▼ Destination: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
 Address: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
 ...0. = LG bit: Globally unique address (factory default)
 ...0. = IG bit: Individual address (unicast)
 ▼ Source: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
 Address: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
 ...0. = LG bit: Globally unique address (factory default)
 ...0. = IG bit: Individual address (unicast)
 Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)

Figure 11: Enter Caption

2.8 Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.

Os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica na mensagem ARP são:

- **Tipo de Hardware:** Indica o tipo de hardware (geralmente Ethernet) e seu tamanho (6 bytes).
- **Tipo de Protocolo:** Indica o tipo de protocolo de rede (geralmente IPv4) e seu tamanho (4 bytes).

3 Redes Sem Fios (IEEE 802.11)

Acesso Rádio

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

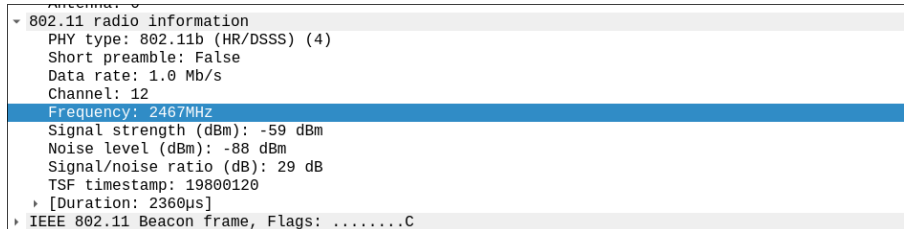


Figure 12: Frequencia e channel de operacao da rede sem fios.

A rede sem fios está a operar na frequência de 2.467 GHz, e o canal que corresponde a essa frequência é o 12.

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

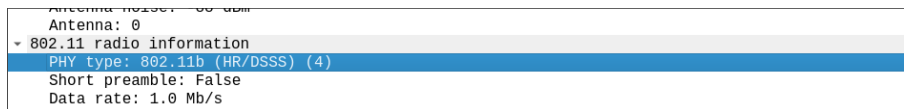


Figure 13: Versao da norma IEEE 802.11, e data rate de operacao da rede sem fios.

A versao da norma IEEE 802.11 que está a ser usada é a 802.11b.

3.3 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.

Como pode ser observado na Figura 13 o data rate de operacao da rede sem fios para a trama escolhida é de 1 Mb/s.

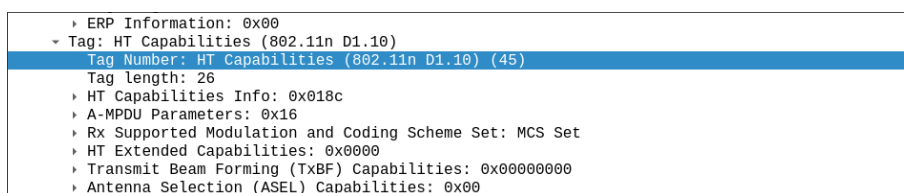


Figure 14: Capacidade de operacao da rede sem fios.

De acordo com a HT Capabilities (Figura 14) a versao 802.11n é suportada, e e de acordo com a Figura 15 o numero de Spatial Streams é de 2, logo a data rate de operacao da rede sem fios pode variar de 144.4 Mbps a 300 Mbps conforme a Figura 16.

Logo o data rate de operacao da rede sem fios para a trama escolhida não corresponde ao débito máximo a que a interface Wi-Fi pode operar.

3.4 Verifique qual a força do sinal (signal strength) e a qualidade expectável de receção da trama, tendo em conta a tabela apresentada em Anexo.

De acordo com a signal strength de -62 dBm, a qualidade expectável de receção da trama é de "reliable signal strength (the edge of what is considered accurate to support Voice over WLAN)".

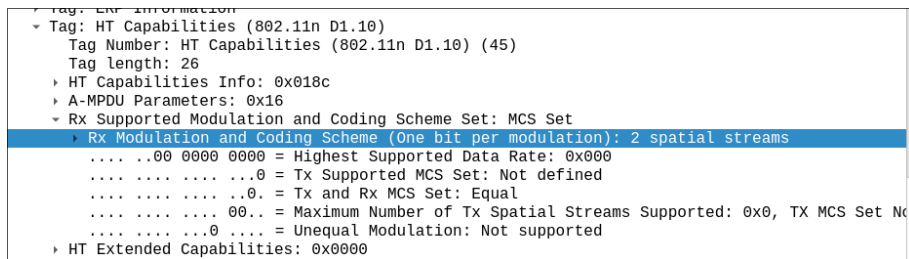


Figure 15: Numero de Spatial Streams e canais de operacao da rede sem fios.

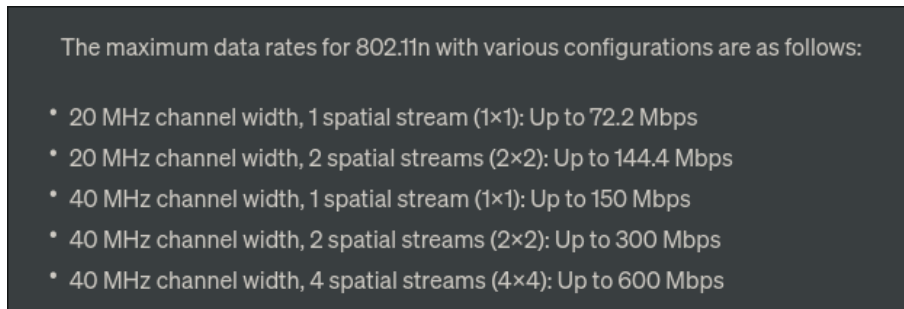


Figure 16: Data rates de operacao da rede sem fios. (GPT-3.5)

Scanning Passivo e Scanning Ativo

3.5 Selecione a trama beacon nr. 100+NG, sendo NG o seu número de grupo. Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```
No. Time Source Destination Protocol Length Info
128 4.915351 HitronTe_af:b1:98 Broadcast 802.11 296 Beacon frame,
SN=2179, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
```

Frame 128: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)

```
Radiotap Header v0, Length 25
Header revision: 0
Header pad: 0
Header length: 25
Present flags
MAC timestamp: 24715251
Flags: 0x10
Data Rate: 1.0 Mb/s
Channel frequency: 2467 [BG 12]
Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
Antenna signal: -65 dBm
Antenna noise: -88 dBm
Antenna: 0
```

```
802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 12
Frequency: 2467MHz
Signal strength (dBm): -65 dBm
Noise level (dBm): -88 dBm
Signal/noise ratio (dB): 23 dB
TSF timestamp: 24715251
```

802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 12
Frequency: 2467MHz
Signal strength (dBm): -62 dBm
Noise level (dBm): -88 dBm
Signal/noise ratio (dB): 26 dB
TSF timestamp: 20516920
Duration: 2360us

Figure 17: Signal strength da trama.

[Duration: 2360us]

```
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
.... .... 0000 = Fragment number: 0
1000 1000 0011 .... = Sequence number: 2179
Frame check sequence: 0x4646c7af [unverified]
[FCS Status: Unverified]

IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 1149675520479
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0c31
Tagged parameters (231 bytes)
Tag: SSID parameter set: "FlyingNet"
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 12
Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
Tag: Vendor Specific: Microsoft Corp.: WPS
Tag: Traffic Indication Map (TIM): DTIM 1 of 3 bitmap
Tag: ERP Information
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (1 octet)
Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
Tag: RSN Information
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
Tag: QBSS Load Element 802.11e CCA Version
Tag: Vendor Specific: Ralink Technology, Corp.

IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
```

A trama pertence ao tipo Beacon frame, e o valor dos seus identificadores de tipo e de subtipo são 0x0008 e 0x8000 respetivamente. Estes identificadores estão especificados no Frame Control Field da trama.

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

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
```

Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

A origem é o Transmitter address, e o destino é o Receiver address, e o BSS Id é o identificador da rede sem fios, que é o mesmo que o Transmitter address. A trama do tipo beacon é enviada periodicamente por um ponto de acesso (AP) ou por um nó de rede sem fios para anunciar a sua presença e disponibilidade, logo o Transmitter address é o endereço MAC do ponto de acesso (AP) ou do nó de rede sem fios, e o Receiver address é o endereço MAC de broadcast.

3.7 Qual o intervalo de tempo previsto entre tramas beacon consecutivas? (nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

```
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
```

O intervalo de tempo previsto entre tramas beacon consecutivas é de 0 microsegundos, ou seja, as tramas beacon são enviadas continuamente. Na prática, a periodicidade de tramas beacon não é verificada com precisão.

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

O filtro usado no Wireshark para obter os SSIDs dos APs que estão a operar na vizinhança da STA de captura foi o seguinte: *wlan.fc.type_subtype == 8*.

No.	Time	Source	Destination	Protocol	Length	Info
114	4.198538	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2165, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
115	4.200168	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2166, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
116	4.200945	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2167, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
117	4.302574	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2168, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
118	4.403343	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2169, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
119	4.404989	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2170, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
120	4.505605	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2171, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
121	4.507225	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2172, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
122	4.608149	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2173, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
123	4.609774	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2174, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
124	4.710559	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2175, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
125	4.712181	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2176, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
126	4.812966	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2177, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
127	4.914575	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2178, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
128	5.015351	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2179, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
129	5.116126	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2180, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
130	5.216901	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2181, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
131	5.317676	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2182, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
132	5.418451	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2183, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
133	5.519226	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2184, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
134	5.619999	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon Frame, SN=2185, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
135	5.720774	HitronTe_af:b1:98	Broadcast	802.11	295	Beacon Frame, SN=2186, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"

Figure 18: SSIDs dos APs que estão a operar na vizinhança da STA de captura.

A lista dos SSIDs dos APs que estão a operar na vizinhança da STA de captura é a seguinte:

- FlyingNet
- NOS_WIFI_Fon

3.9 Face ao endereçamento usado, indique a que sistemas são endereçadas ambas as tramas e explique qual o propósito das mesmas?

Quanto ao Probe Request, o Source Address é ea:a4:64:7b:b9:7a e o Destination Address é ff:ff:ff:ff:ff:ff. Como o Probe Request é uma mensagem enviada por um dispositivo cliente Wi-Fi para explorar a presença de redes sem fio ao seu redor, o Destination Address é um Broadcast, de forma a reconhecer todos os APs presentes ao redor. Quanto ao Probe Response, o Source Address é bc:14:01:af:b1:98 e o Destination Address é ea:a4:64:7b:b9:7a. A response tem como source o router, que manda o endereço MAC do AP que está enviando a resposta de sondagem, e tem como Destination o dispositivo que fez a request.

2467 70.147855	ea:a4:64:7b:19:7a	Broadcast	802.11	167 Probe Request, SN=2540, FN=0, Flags=.....C, SSID="ZWIRE-PT-431"
2468 70.149098	ea:a4:64:7b:19:7a	Broadcast	802.11	155 Probe Request, SN=2541, FN=0, Flags=.....C, SSID="M10card (Broadcast)"
2469 70.149792	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	411 Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2471 70.150537	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	411 Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2472 70.151237	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	411 Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2475 70.151709	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	201 Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
2477 70.152099	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	201 Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
2479 70.152578	HitronTe_af:b1:98	ea:a4:64:7b:19:7a	802.11	201 Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"

Figure 19: Probes Requests e suas respectivas Probe Responses

Processo de Associação

3.10 Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

Apple_10:6a:f5	HitronTe_af:b1:98	802.11	78 Authentication, SN=2542, FN=0, Flags=.....C
Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	Apple_10:6a:f5	802.11	39 Acknowledgement, Flags=.....C
HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=.....C
Apple_10:6a:f5	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	39 Acknowledgement, Flags=.....C
HitronTe_af:b1:98	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	175 Association Request, SN=2543, FN=0, Flags=.....C, SSID="FlyingNet"
Apple_10:6a:f5	HitronTe_af:b1:98	802.11	39 Acknowledgement, Flags=.....C
HitronTe_af:b1:98	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C
HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	Apple_10:6a:f5	802.11	39 Acknowledgement, Flags=.....C

Figure 20: Sequencia de tramas de processo de associacao

3.11 Efetue um diagrama que ilustre, com as tramas identificadas na alínea anterior, a sequência de todas as tramas trocadas no processo de autenticação e associação entre o STA e o AP.

Sequencia de tramas de processo de associacao:

- STA → AP : *Authentication Request*
- AP → STA : *Acknowledgment*
- AP → STA : *Authentication Response*
- STA → AP : *Acknowledgment*
- STA → AP : *Association Request*
- AP → STA : *Acknowledgment*
- AP → STA : *Association Response*
- STA → AP : *Acknowledgment*

Transferência de Dados

3.12 Considere a trama de dados n.º 622. 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?

Podemos observar nas Flags do Frame Control, o campo DS status, que indica se a trama é destinada ao sistema de distribuição (DS) ou se vem do sistema de distribuição. A trama possui (To DS: 0 From DS: 1), isso indica que a trama é enviada de um dispositivo cliente para o sistema de distribuição (como um AP). Ela é direcionada ao sistema de distribuição. A trama está se movendo do dispositivo cliente para o ponto de acesso, que é parte do sistema de distribuição da rede Wi-Fi. Portanto, essa trama é local à WLAN (Wireless Local Area Network) específica, ou seja, ela está sendo transmitida internamente na rede sem fio, de um dispositivo cliente para o ponto de acesso que faz parte da mesma WLAN.

3.13 Para a trama de dados da alínea anterior, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição.

- Source Address: bc:14:01:af:b1:96
- Destination Address: 64:9a:be:10:6a:f5

Como o source address é bc:14:01:af:b1:96, o MAC address do host sem fios (STA) é bc:14:01:af:b1:96. Já o MAC address correspondente ao AP é 64:9a:be:10:6a:f5, que é o destination address. O router de acesso ao sistema de distribuição é o endereço do AP que atua como gateway para a rede com fio (Sistema de Distribuição), portanto, o seu MAC address também é 64:9a:be:10:6a:f5.

3.14 Observa-se que ao longo da transferência de dados são usadas tramas de controlo ACK. Tente explicar porque razão têm de existir, contrariamente ao que acontece numa rede Ethernet.

As tramas de controlo ACK são usadas para confirmar a receção de uma trama de dados, e para indicar que a estação está pronta para receber a próxima trama de dados. Na rede Ethernet, as tramas de controlo ACK não são necessárias, pois a rede Ethernet é uma rede com fios, e por isso a probabilidade de perda de tramas de dados é menor, assim como a probabilidade de interferências.

3.15 Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada, identificando a direccionalidade das tramas, as tramas de controlo e os sistemas envolvidos. Apresente as tramas e os sistemas devidamente identificados sob a forma de um diagrama de sequência.

De forma a filtrar os pacotes RTC/CTS foi utilizado o filtro no wireshark: `wlan.fc.type_subtype == 27`, foi selecionado um dos pacotes de rtc e dps o filtro foi removido de forma a ver todos os pacotes adjacentes.

Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	HitronTe_af:b1:98 (bc:14:01:af:b1:96) (RA)	802.11	45 Request-to-send, Flags=.....C
Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39 Clear-to-send, Flags=.....C
HitronTe_af:b1:98 (bc:14:01:af:b1:96) (RA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	57 802.11 Block Ack, Flags=.....C
Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	HitronTe_af:b1:98 (bc:14:01:af:b1:96) (RA)	802.11	53 Null function (No data), SN=2498, FN=0, Flags=.....TC
Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39 Acknowledgement, Flags=.....C

Figure 21: Sequencia de tramas de RCT/CTS

- STA → AP : *Request to Send*
- AP → STA : *Clear to Send*
- STA → AP : *Null function*
- AP → STA : *Acknowledgment*

4 Conclusao

Neste relatório, exploramos com sucesso dois aspectos fundamentais de sistemas de redes: o Protocolo ARP e a tecnologia Wi-Fi IEEE 802.11. No que toca ao ARP, adquirimos uma compreensão sólida de como as tabelas de endereçamento são usadas para mapear endereços IP a endereços MAC, e como esse processo é essencial para o funcionamento de redes locais. Além disso, ao examinar a integração de novos dispositivos em redes domésticas, identificamos as complexidades envolvidas na resolução de endereços e na descoberta de dispositivos.

Em relação ao IEEE 802.11, exploramos os sistemas de Controle de Acesso ao Meio (MAC) e técnicas como o RTS/CTS (Request to Send/Clear to Send) para aprimorar a eficiência da transmissão de pacotes em redes Wi-Fi. Compreendemos que a otimização do acesso ao meio é crucial para manter o desempenho e a confiabilidade das redes sem fio, especialmente em ambientes com vários dispositivos.

Esse trabalho proporcionou-nos insights valiosos sobre a operação interna das redes, tornando-nos mais conscientes dos desafios e soluções relacionados à conectividade. À medida que continuamos a avançar no estudo de sistemas de redes, estamos confiantes de que esse conhecimento enriquecerá as nossas habilidades e contribuirá para a construção e manutenção eficazes de infraestruturas de comunicação de dados.