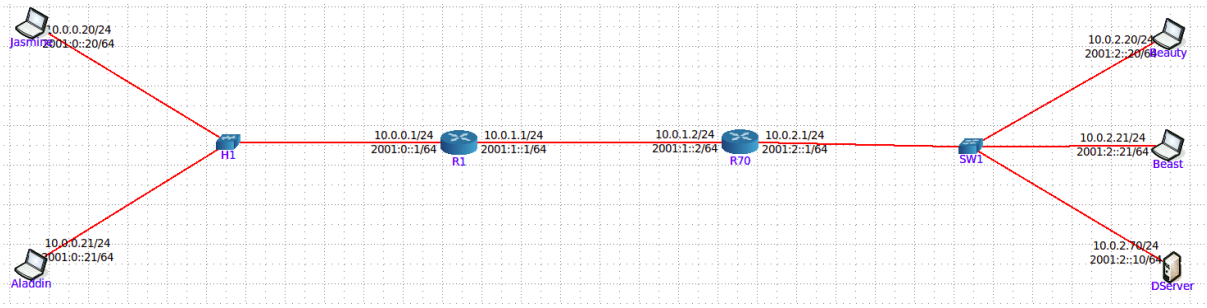
Relatório TP3

Grupo PL70 :
André Santos a106854
Daniel Parente a107363
Pedro Ferreira a107292



PARTE I - Captura e análise de Tramas Ethernet

1.1) Questão: Anote os endereços MAC de origem e MAC destino da trama capturada. Identifique a que hosts se referem. Justifique.

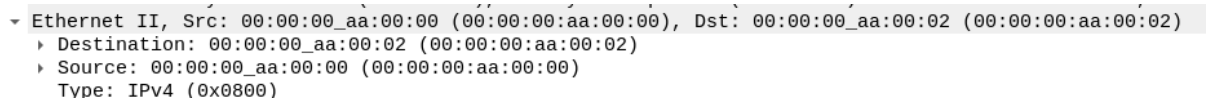
Resposta: Podemos concluir que o ***MAC 00:00:00_aa:00:00*** corresponde ao host Jasmine que corresponde à source neste caso no sentido cliente-servidor.
Podemos também ver o ***MAC 00:00:00_aa:00:02*** que corresponde ao host R1, destination no sentido cliente-servidor.

No.	Time	Source	Destination	Protocol	Length	Info
6	7.9905584…	10.0.0.20	10.0.2.70	SSH	82	Client: Encrypted packet (len=16)
9	8.0312485…	10.0.0.20	10.0.2.70	SSH	110	Client: Encrypted packet (len=44)
11	8.0313583…	10.0.2.70	10.0.0.20	SSH	110	Server: Encrypted packet (len=44)
13	8.0314363…	10.0.0.20	10.0.2.70	SSH	126	Client: Encrypted packet (len=60)
14	8.0407508…	10.0.2.70	10.0.0.20	SSH	118	Server: Encrypted packet (len=52)
16	9.8167708…	10.0.0.20	10.0.2.70	SSH	150	Client: Encrypted packet (len=84)
17	9.8357012…	10.0.2.70	10.0.0.20	SSH	94	Server: Encrypted packet (len=28)
19	9.8358667…	10.0.0.20	10.0.2.70	SSH	178	Client: Encrypted packet (len=112)
21	9.9675687…	10.0.2.70	10.0.0.20	SSH	534	Server: Encrypted packet (len=468)
23	9.9995357…	10.0.2.70	10.0.0.20	SSH	110	Server: Encrypted packet (len=44)
25	9.9997467…	10.0.0.20	10.0.2.70	SSH	1146	Client: Encrypted packet (len=1080)
27	10.001375…	10.0.2.70	10.0.0.20	SSH	174	Server: Encrypted packet (len=108)
28	10.005965…	10.0.2.70	10.0.0.20	SSH	966	Server: Encrypted packet (len=900)
31	10.043474…	10.0.2.70	10.0.0.20	SSH	118	Server: Encrypted packet (len=52)

```
▸ Frame 19: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface veth1.0.90, id 0
▾ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  ▸ Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  ▸ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Type: IPv4 (0x0800)
```

1.2) Questão: Qual o valor hexadecimal do campo Type contido no header da trama Ethernet? O que significa? Qual o campo do header IP que tem semântica idêntica?

Resposta: O valor é 0x0800 e indica que indica que o protocolo encapsulado é **IPv4**



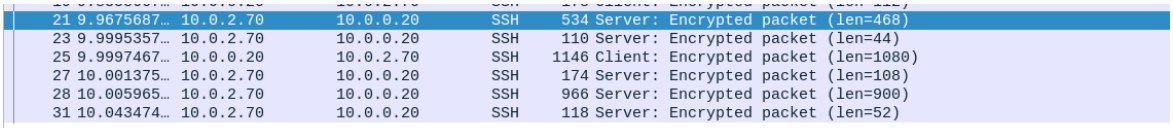
Dentro do próprio cabeçalho ***IP*** existe um campo chamado Protocol que tem exatamente a mesma semântica e objetivo: identificar qual o protocolo que está a ser encapsulado.

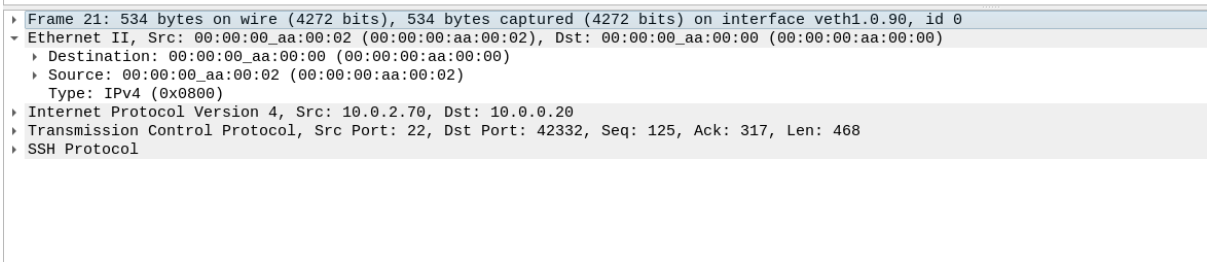
1.3) Questão: Quantos bytes são usados no encapsulamento protocolar, i.e., desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

Resposta: Tamanho da pilha protocolar: 178 bytes.
Overhead total = 20(IPv4) + 32(TCP) + 14 (Ethernet) = 66
Percentegem *Overhead* = 66/178 =37%

1.4) Questão: Qual é o endereço MAC da fonte? A que host e interface corresponde? Justifique.

Resposta: Trama Ethernet escolhida:





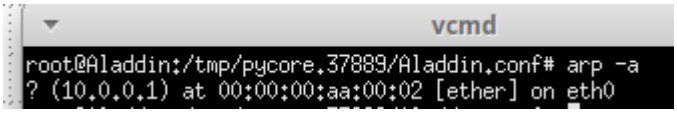
Endereço MAC da fonte: 00:00:00:aa:00:02
Host/Interface: O endereço corresponde ao R1 pois MAC são endereços camada 2 que só é usada pelo router dentro da mesma rede. Não faria assim sentido vermos os MAC do servidor que está numa outra rede.

1.5) Questão: Qual é o endereço MAC do destino? A que host e interface corresponde?

Resposta: Endereço MAC do destino: 00:00:00:aa:00:00
Host/Interface:O endereço corresponde à Jasmine.

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

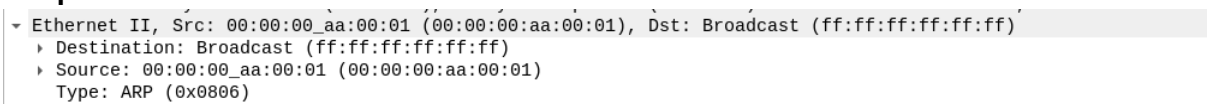
Resposta:



Após analisar a tabela ARP podemos concluir que "aprendeu" o endereço MAC correspondente ao endereço IP 10.0.0.1(R1). A tabela apresenta os seguintes campos :
Endereço IP do host cujo MAC foi resolvido -> 10.0.0.1
Endereço MAC correspondente ao IP (associado via protocolo ARP) -> 00:00:00:aa:00:02
Tipo de rede -> [ether]
Interface de rede local -> eth()

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

Resposta:



Endereço MAC origem -> 00:00:00_aa:00:01
Endereço MAC destino -> ff:ff:ff:ff:ff:ff
É usado o endereço MAC destino ff:ff:ff:ff:ff:ff pois trata-se de uma mensagem Broadcast, para todos os dispositivos na rede do endereço de origem (00:00:00_aa:00:01), pois este pretende saber o endereço MAC proprietário do endereço *IP 10.0.0.1*

2.2. b) Questão: Qual o valor hexadecimal do campo Type da trama Ethernet? O que indica?

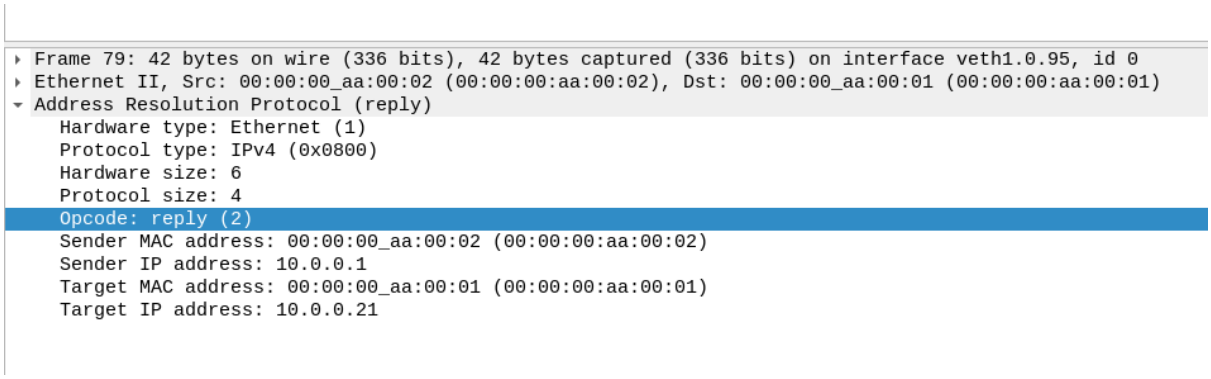
Resposta: Valor Hexadecimal do *Type :* 0x806
Indica que os dados do campo protocolar superior são um pacote ***ARP.***

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

Resposta: Podemos concluir que se trata de um pedido *ARP* analisando os campos *Opcode e Target MAC address.*
Podemos ver que o valor no campo é 1, mostrando assim que se trata de um pedido. No campo *Target MAC address* está o endereço *00:00:00:00:00:00* pois não é ainda conhecido o MAC destino. Desta forma, conseguimos ter a certeza que se trata de um pedido *ARP.*

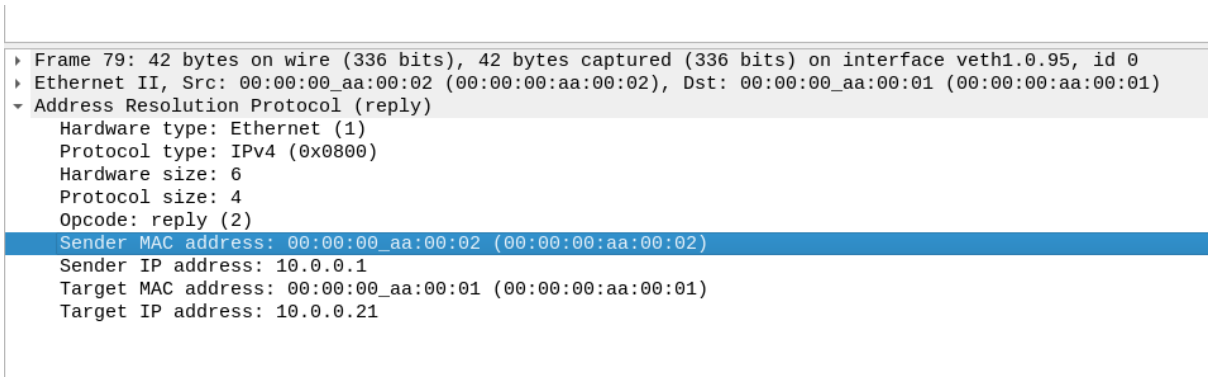
2.3. a) Questão: Qual o valor do campo ARP opcode? O que especifica?

Resposta: O valor do campo ***Opcode*** é 2, especificando assim que se trata de uma resposta *Arp.*



2.3. b) Questão: Em que campo da mensagem ARP está a resposta ao pedido ARP efetuado?

Resposta: A resposta vem no campo ***Sender MAC address***.

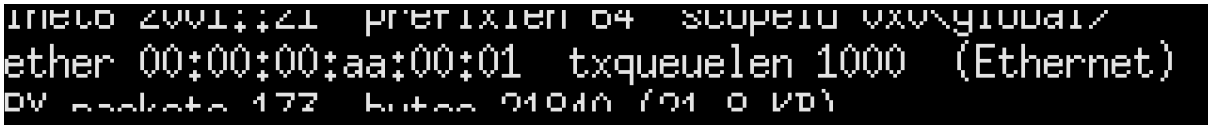


2.3. c) Questão: Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no host selecionado (Aladdin).

Resposta:

```
Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
Sender IP address: 10.0.0.1
Target MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
Target IP address: 10.0.0.21
```

Executando o comando ***ifconfig*** no host Aladdin percebemos que endereço MAC : 00:00:00:aa:00:01 pertence a ele mesmo.



De seguida executando o comando ***arp,*** vemos que o endereço MAC : 00:00:00:aa:00:02, tem como endereço lógico ***IP*** o endereço 10.0.0.1.

Finalmente, aplicando o comando ***netstat -rn*** vemos que a rota *default* corresponde a esse mesmo endereço ***IP*** 10.0.0.1 .Podemos assim concluir que o endereço MAC : 00:00:00:aa:00:02 corresponde ao router R1.

Resumindo :
Endereço MAC 00:00:00:aa:00:01 -> Aladdin
Endereço MAC 00:00:00:aa:00:02 -> R1

2.3. d) Questão: Discuta, justificando, o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

Resposta: No envio da resposta ***ARP (ARP Reply),*** o modo de comunicação usado é ***unicast,*** pois apenas o solicitador original recebe a resposta. Desta forma, é possível aumentar a segurança, reduzir o tráfego e sobrecarregamento das tabelas ***ARP***, pois caso contrário todos os dispositivos iriam receber o pedido.

2.4) Questão: Verifique se a Jasmine teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Aladdin? Qual será a razão para tal?

Resposta: A Jasmine teve acesso ao tráfego gerado pelo acesso secreto do Aladdin, pois estão ligados a um ***Hub*** que repete todo o tráfego para todas as portas.

No.	Time	Source	Destination	Protocol	Length	Info
82	93.572625…	10.0.0.21	10.0.2.70	TCP	66	47344 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=158610935…
83	93.574118…	10.0.0.21	10.0.2.70	SSHv2	108	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12)
84	93.574141…	10.0.2.70	10.0.0.21	TCP	66	22 → 47344 [ACK] Seq=1 Ack=43 Win=65152 Len=0 TSval=66900381…
85	93.589838…	10.0.2.70	10.0.0.21	SSHv2	108	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12)
86	93.589849…	10.0.0.21	10.0.2.70	TCP	66	47344 → 22 [ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=1586109…
87	93.590025…	10.0.0.21	10.0.2.70	TCP	1514	47344 → 22 [ACK] Seq=43 Ack=43 Win=64256 Len=1448 TSval=1586…
88	93.590026…	10.0.0.21	10.0.2.70	SSHv2	154	Client: Key Exchange Init
89	93.590055…	10.0.2.70	10.0.0.21	TCP	66	22 → 47344 [ACK] Seq=43 Ack=1579 Win=63616 Len=0 TSval=66900…
90	93.591546…	10.0.2.70	10.0.0.21	SSHv2	1114	Server: Key Exchange Init
91	93.592950…	10.0.0.21	10.0.2.70	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
92	93.597275…	10.0.2.70	10.0.0.21	SSHv2	1182	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypt…
93	93.636031…	10.0.0.21	10.0.2.70	TCP	66	47344 → 22 [ACK] Seq=1627 Ack=2207 Win=64128 Len=0 TSval=158…
94	94.077681…	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
95	96.068626…	10.0.0.21	10.0.2.70	SSHv2	82	Client: New Keys
96	96.078601…	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
97	96.108175…	10.0.2.70	10.0.0.21	TCP	66	22 → 47344 [ACK] Seq=2207 Ack=1643 Win=64128 Len=0 TSval=669…
98	96.108202…	10.0.0.21	10.0.2.70	SSHv2	110	Client: Encrypted packet (len=44)
99	96.108231…	10.0.2.70	10.0.0.21	TCP	66	22 → 47344 [ACK] Seq=2207 Ack=1687 Win=64128 Len=0 TSval=669…
100	96.108306…	10.0.2.70	10.0.0.21	SSHv2	110	Server: Encrypted packet (len=44)
101	96.108316…	10.0.0.21	10.0.2.70	TCP	66	47344 → 22 [ACK] Seq=1687 Ack=2251 Win=64128 Len=0 TSval=158…
102	96.108385…	10.0.0.21	10.0.2.70	SSHv2	126	Client: Encrypted packet (len=60)

2.5) Questão: De igual modo, verifique se a Beauty teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Beast? Qual será a razão para tal?

Resposta: A ***Beauty*** não teve acesso, pois estão ligados a um ***Switch*** que encaminha para a porta correta.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000…	fe80::200:ff:fe…	ff02::5	OSPF	90	Hello Packet
2	0.0174106…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
3	2.0175524…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
4	3.9326154…	fe80::2423:76ff…	ff02::2	ICMP…	70	Router Solicitation from 26:23:76:23:77:96
5	4.0177931…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
6	6.0178849…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
7	8.0182599…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
8	8.0285960…	fe80::200:ff:fe…	ff02::2	ICMP…	70	Router Solicitation from 00:00:00:aa:00:07
9	10.010156…	fe80::200:ff:fe…	ff02::5	OSPF	90	Hello Packet
10	10.018352…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
11	10.076596…	fe80::e4e6:83ff…	ff02::2	ICMP…	70	Router Solicitation from 0e:46:4c:32:ac:36
12	12.018749…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
13	13.378269…	fe80::e4e6:83ff…	ff02::fb	MDNS	203	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR…
14	14.019066…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
15	14.307531…	fe80::2423:76ff…	ff02::fb	MDNS	203	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR…
16	16.019425…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
17	18.019729…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
18	20.019882…	10.0.2.1	224.0.0.5	OSPF	78	Hello Packet
19	20.029340…	fe80::200:ff:fe…	ff02::5	OSPF	90	Hello Packet
20	20.316780…	fe80::200:ff:fe…	ff02::2	ICMP…	70	Router Solicitation from 00:00:00:aa:00:06
21	20.316848…	fe80::200:ff:fe…	ff02::2	ICMP…	70	Router Solicitation from 00:00:00:aa:bb:70

2.6) Questão: Consulte a tabela ARP do Aladdin e do Beast. Que principal diferença entre as tabelas obtidas e que impacto tem no funcionamento da rede?

Resposta:

Tabela do Aladdin :

```
root@Aladdin:/tmp/pycore.39819/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
```

Tabela do Beast :

```
root@Beast:/tmp/pycore.39819/Beast.conf# arp -a
? (10.0.2.70) at 00:00:00:aa:bb:70 [ether] on eth0
root@Beast:/tmp/pycore.39819/Beast.conf#
```

Como podemos ver, ***Aladdin*** tem conhecimento do endereço MAC do router a que está ligado, enquanto ***Beast*** tem conhecimento do endereço MAC do servidor destino.

Isto acontece pois ***Beast*** encontra-se na mesma rede que o servidor podendo assim fazer ligação direta com o mesmo, situação que não acontece com o **Aladdin.**

2.7) Questão: Esboce um diagrama em que ilustre claramente, e de forma cronológica, todo o tráfego layer 2 (tramas) entre o Aladdin e os hosts com os quais comunica, até à receção do primeiro pacote que contém dados do acesso remoto.

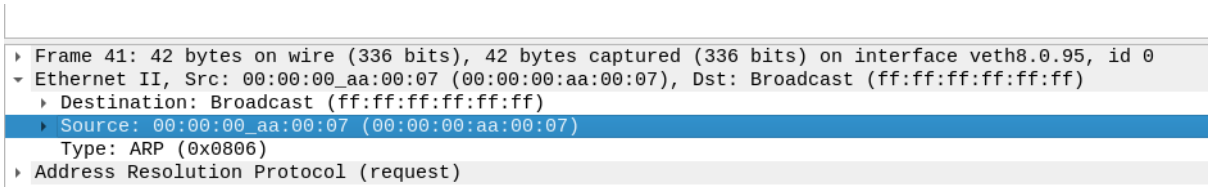
Resposta:

[Aladdin]
  |
  |--[1] ARP Request: "Quem tem 10.0.0.1?" (para Gateway R1)
  |
[H1 Switch]
  |
[Router R1]
  |
  |--[2] ARP Reply: "10.0.0.1 é 00:00:00:aa:00:02" (MAC de R1)
  |
[Aladdin]
  |
  |--[3] TCP SYN → 10.0.2.10:22 (primeira tentativa SSH)
  |
[H1] → R1 → R0 → SW1 → DServer
  |
[DServer]
  |
  |--[4] TCP SYN-ACK ← resposta do DServer
  |
[Aladdin]
  |
  |--[5] TCP ACK → estabelece conexão
  |
  |--[6] Primeiro pacote com dados SSH (criptografado)

2.8) Questão: Construa manualmente a tabela de comutação completa do switch da casa da Beauty e do Beast, (SW1) atribuindo números de porta à sua escolha.

Resposta:

Podemos ver, analisando o pedido Arp de *Beast* que o seu **MAC** é 00:00:00_aa:00:07



MAC addres	Porta
00:00:00:aa:bb:70	Fa0/1
00:00:00_aa:00:07	Fa0/2

3.1) Questão: Como proteção, a Jasmine e o Aladdin, juntamente com a Beauty e o Beast, decidiram conectar R1 e Rxy a uma rede de um ISP com endereços IP públicos, mantendo todo o endereçamento privado das suas LANs. Sabe-se que o ISP não encaminha tráfego para redes privadas, portanto, R1 e Rxy não conseguem encaminhar tráfego para endereços privados remotos, i.e., não fisicamente adjacentes.
Discuta que solução implementaria em R1 e em Rxy de modo a manter todas as funcionalidades anteriormente existentes (conectividade IP, acesso ssh ao servidor, etc.).

Resposta:

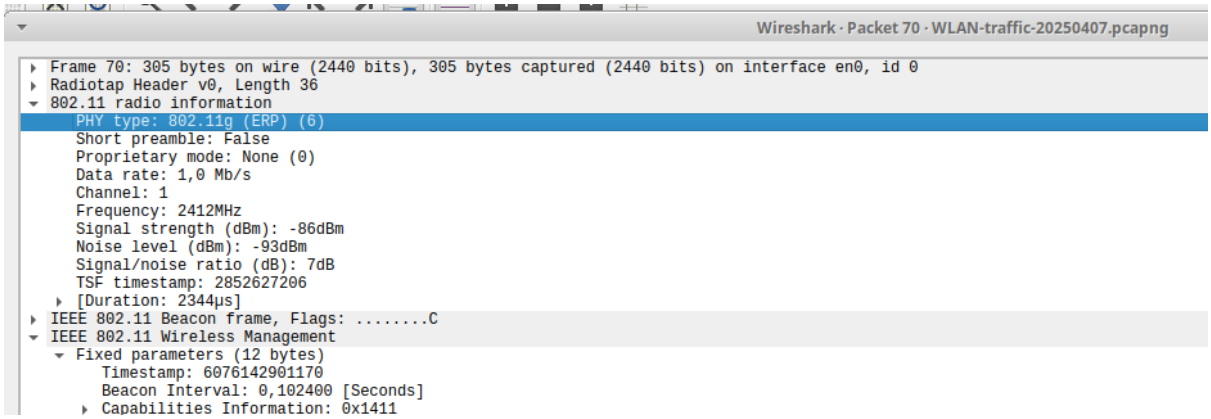
Para garantir que tudo continue a funcionar como anteriormente — incluindo o acesso SSH ao servidor e a comunicação entre dispositivos nas redes internas — é necessário configurar tradução de endereços de rede (NAT), mais concretamente NAT com sobrecarga (PAT), nos routers R1 e R70.

Como o fornecedor de serviços de Internet (ISP) apenas encaminha tráfego com endereços IP públicos, os IPs privados das LANs não são diretamente acessíveis a partir do exterior. Ao implementar PAT, os routers passam a substituir os IPs privados de origem por um IP público atribuído pelo ISP, associando cada ligação a uma porta específica. Desta forma, vários dispositivos podem partilhar o mesmo IP público sem conflitos, porque são diferenciados pelas portas.

Quando os pacotes de resposta chegam ao router, este utiliza a tabela de traduções para devolver os dados ao equipamento correto dentro da rede privada. Desta forma,é mantido o esquema de endereçamento privado nas redes locais, é permitido que o tráfego saia da rede interna usando um IP público, compatível com as regras do ISP e garante-se que todas as funcionalidades anteriores, como o acesso remoto por SSH, continuem operacionais sem alterações no funcionamento do sistema.

PARTE II

1. **Acesso Rádio**



Trama 802.11 referente ao grupo

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

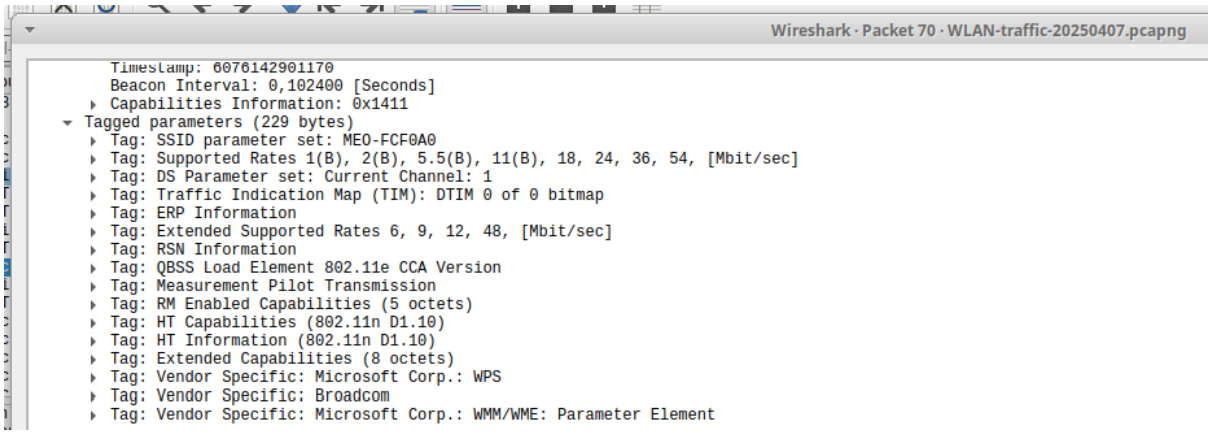
Resposta: Como se pode analisar na figura, a frequência é 2412MHz, a operar no canal 1.

1.2 Questão: Identifique a versão da norma IEEE 802.11 que está a ser usada.

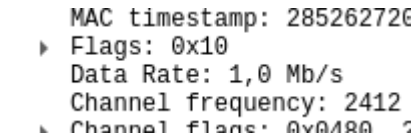
Resposta: 802.11g

1.3 Questão: 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.

Resposta:

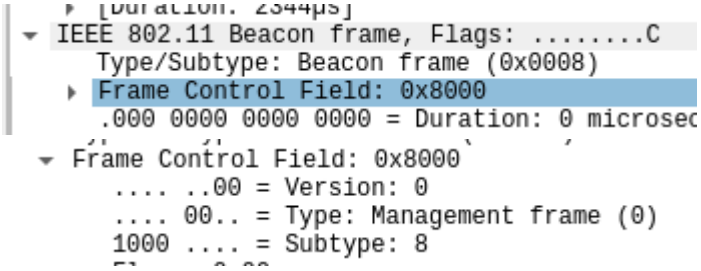


Como podemos analisar, a trama tem capacidades da norma IEEE 802.11n (que tem uma velocidade de transmissão de 600Mbps), mas foi transmitida a 1Mbp (taxa de transmissão normal das Beacon Frames - usam as taxas de transmissão mais baixas possíveis). Esta informação pode ser consultada na imagem abaixo:



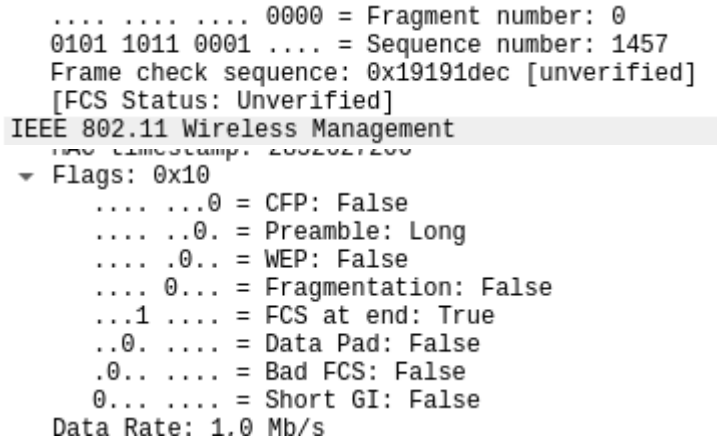
2. **Scanning Passivo e Scanning Ativo**

2.4 Questão: Selecione uma trama beacon cuja ordem (ou terminação) corresponda ao seu ID de grupo. 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)?



Resposta: Foi escolhida a mesma trama das alíneas anteriores, por ser a primeira trama que cumpre o requisito pedido. Pertence, como já vimos, às tramas do tipo 802.11g.
Identificador de tipo: 00
Identificador de subtipo: 0008
Esta parte encontra-se identificada no cabeçalho da trama, nos bits referentes ao Frame Control. O Type ocupa 2 bits (neste caso, 00 - indica que a trama é do tipo “Management”), e o Subtype ocupa 4 bits(neste caso, 1000 - indica que a trama é do subtipo “Beacon”).

2.5 Questão: 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”)



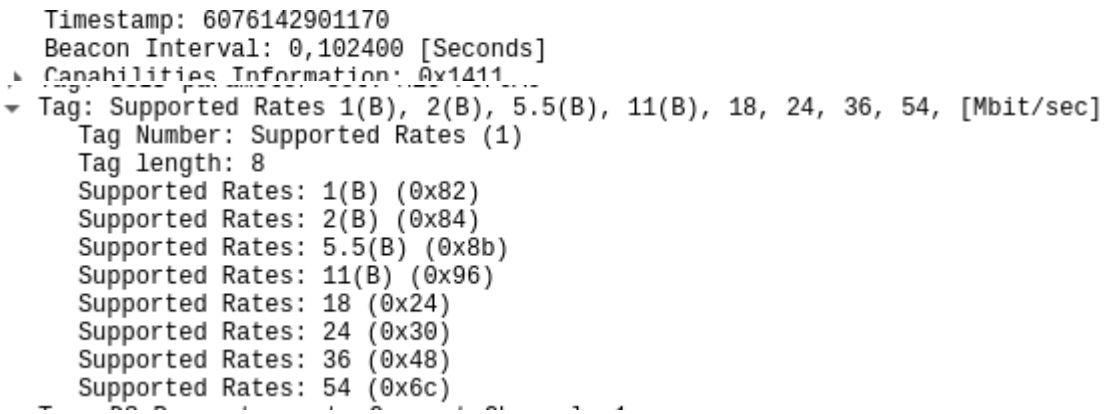
Resposta: As tramas Beacon têm um campo, FCS (Frame Check Sequence), nos últimos 4 bytes, para deteção de erros. Esta, como está marcada a “unverified”, significa que está a ser usada, mas não verificada. O bit na flag simplesmente refere-se à existência do FCS no fim da trama.

2.6 Questão: Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Resposta: A deteção de erros em redes sem fios (WI-FI, Bluetooth, entre outras) é essencial devido às características do meio de transmissão (o ar). Como este é mais propenso a alterações e/ou perturbações, a interferência dos dados torna-se mais provável do que em redes com fios. Um dos aspetos que leva a este processo é o Path Loss, ou a atenuação do sinal, produzido por obstáculos naturais, ou simplesmente pelo aumento da distância até aos APs.

Além disso, sinais de outros dispositivos ativos na zona podem colidir com o sinal que se quer transmitir, podendo causar corrupção dos dados.

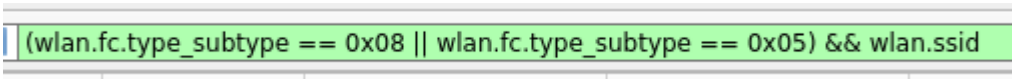
2.7 Questão: Uma trama beacon anuncia o intervalo entre beacons às várias taxas de transmissão (B) que o AP suporta, assim como várias taxas de transmissão adicionais (extended supported rates). Indique qual a periodicidade e as taxas de transmissão suportadas pelo AP da trama beacon selecionada.



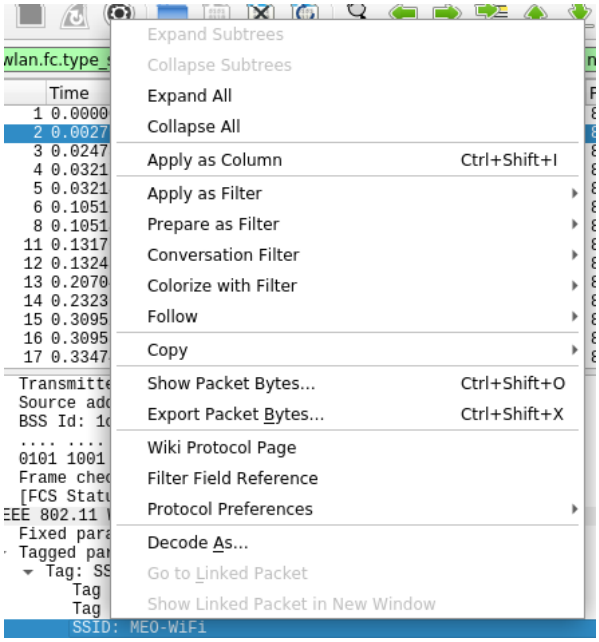
Resposta: O intervalo entre beacons transmitidos é de 0.1024 *100 = 102.4 microsegundos (valor obtido através da primeira print). Na segunda imagem, podemos observar quatro valores de taxas básicas (as marcadas com B), que são as taxas básicas que todos os dispositivos que se conectam à AP têm de suportar. As outras taxas (18, 24, 36 e 54 Mbps) não são obrigatórias, mas podem ser usadas, caso seja possível.

2.8 Questão: 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).

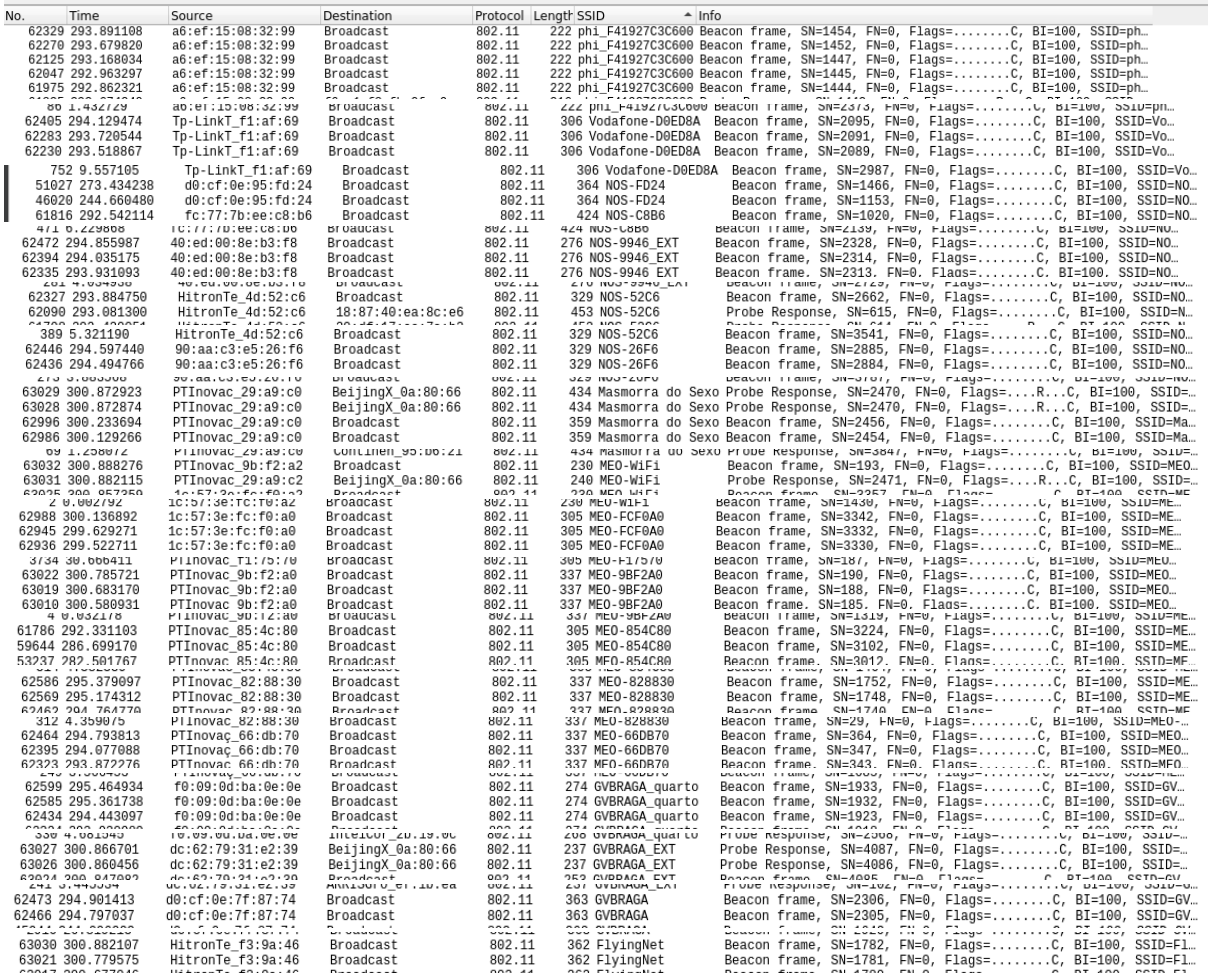
Resposta:



Foi aplicado o seguinte filtro: “wlan.fc.type_subtype == 0x08” e “wlan.fc.type_subtype == 0x05” filtram as tramas, para apenas mostrar as do tipo Beacon ou Probe Response, respetivamente, as únicas que contêm (ou podem conter) a tag SSID preenchida. O segundo filtro, “wlan.ssid”, certifica-se que são excluídas todas as tramas destes tipos que não tenham o campo SSID preenchido.



De seguida, clicou-se com o botão direito num item “SSID” de uma trama aleatória, e escolheu-se a opção “Apply as Column.” Podemos assim, listar todos os SSID que estão a operar.



Aqui estão alguns exemplos de todos os SSIDs diferentes a operar.

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

Resposta: `wlan.fc.type_subtype == 0x05 || wlan.fc.type_subtype == 0x04`
"wlan.fc.type_subtype == 0x04" -> filtra tramas probing request;
"wlan.fc.type_subtype == 0x05" -> filtra tramas probing response

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

Resposta: Foi aplicado um filtro diferente, "wlan.fc.type_subtype == 0x05 || wlan.fc.type_subtype == 0x08", para mostrar apenas as tramas que contêm o RSSI do AP. Foi adicionada uma coluna, para mostrar os valores da força do sinal (em dBm) da trama. Assim, conseguimos ver que a trama com maior RSSI é a seguinte:

No.	Time	Source	Destination	Protocol	Length	SSID	Info	Signal strength (dBm)
39127	191.415288	HitronTe_f3:9a:46	Broadcast	802.11	362	FlyingNet	Beacon frame, SN=672, FN=0, Flags=........C, BI=100, SSID=Fly…	-39dBm

2.11 Questão: Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal. Considerando os valores de sensibilidade mínima (Minimum Sensivity) e taxa de transmissão (Data Rate) que constam nas tabelas de referência (ver Anexo II), e a força do sinal recebido nas tramas do AP identificado na resposta anterior, estime o débito que a STA obterá nessa ligação.

Resposta: O valor obtido (-39 dBm) é muito superior aos requisitos de sensibilidade mínima para todas as modulações. Isso significa que a STA pode operar no maior nível de modulação suportado pelo AP (que aqui é 64–QAM 5/6).
Como aqui se assume que todos os dispositivos IEEE 802.11n utilizam um GI de 800ns, podemos inferir pela tabela do Anexo II que o débito será de 65Mbps.

3. Processo de Associação

3.12 Questão: 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.

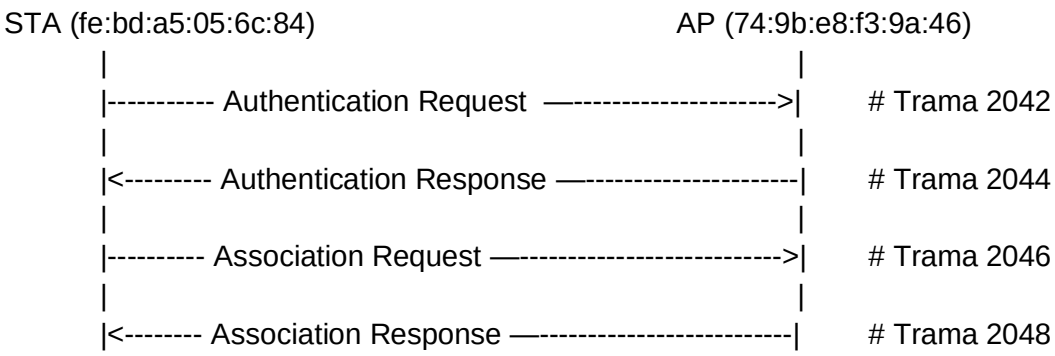
Resposta: Foi aplicado o filtro "wlan.fc.type_subtype == 0x00 || wlan.fc.type_subtype == 0x01 || wlanc.fc.type_subtype == 0x0b)", em que "0x00" corresponde às tramas Association Request, "0x01" corresponde às tramas Association Response, e "0x0b" corresponde às tramas de autenticação.

Assim, foi identificada a seguinte sequência de tramas, que representam um processo de associação entre a STA e o AP:

No.	Time	Source	Destination	Protocol	Length	Info	MAC
2042	23.707373	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	106	Authentication, SN=3343, FN=0, Flags=.…	74:9b:e8:f3:9a:46,fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46
2044	23.707398	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	70	Authentication, SN=3852, FN=0, Flags=.…	fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46,74:9b:e8:f3:9a:46
2046	23.710405	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	202	Association Request, SN=3344, FN=0, Fla…	74:9b:e8:f3:9a:46,fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46
2048	23.716772	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	210	Association Response, SN=3853, FN=0, Fl…	fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46,74:9b:e8:f3:9a:46

3.13 Questão: Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

Resposta:



4. Transferência de Dados

4.14 Questão: 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 xy, ou y caso não exista xy). 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?

Resposta: Foi aplicado o filtro “wlan.fc.type == 2 || wlan.fc.type == 1”, para filtrar as tramas de dados, e as tramas de controlo, respetivamente. Seguindo as indicações, foi escolhida a trama 1170, do tipo QoS Data.

```
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
   .... ..00 = Version: 0
   .... 10.. = Type: Data frame (2)
   1000 .... = Subtype: 8
▾ Flags: 0x41
      .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .1.. .... = Protected flag: Data is protected
      0... .... = Order flag: Not strictly ordered
```

Como podemos analisar pelas Flags, a trama foi enviada por uma STA para um AP, sendo, assim, local à WLAN (ainda não saiu para uma rede externa).

4.15 Questão: 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: Os endereços MAC são “d0:cf:0e:7f:87:74”, “de:62:79:01:e2:39” e “ff:ff:ff:ff:ff:ff”. O primeiro corresponde ao da STA (que é o que envia a trama), o segundo pertence ao AP, e o DS, neste caso, não está presente nos endereços, já que o destino é Broadcast

(endereço ff:ff:ff:ff:ff:ff), não estando a ser direcionada para um DS externo, como vimos na questão anterior.

4.16 Questão: 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 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.

Resposta: Nesta trama em específico não está a ser usado o RTS/CTS, pois não é uma característica inerente das tramas Broadcast, estando presente apenas nas comunicações fim-a-fim.

Exemplo com RTS/CTS: Trama 181 (Tramas de Dados)
Exemplo sem RTS/CTS: Trama 1170 (Tramas de Gestão)

Conclusão

Com este projeto, conseguimos entender como funcionam na prática as redes - desde a transmissão de dados em redes cabladas, até às redes sem fios. Percebemos, ao analisar as tramas Ethernet fornecidas, a importância e funcionalidade dos switches e dos hubs, e como gerem o tráfego de diferentes formas.
Os exercícios relativos ao protocolo ARP esclareceram e solidificaram o nosso conhecimento. Através da prática e da análise pelo *wireshark* foi possível compreender melhor os pedidos e respostas ARP*,* a importância da tabela ARP para o desempenho da rede e como o protocolo é fundamental para a comunicação entre dispositivos.
O NAT e o PAT também ficaram consolidados durante as atividades, permitindo uma compreensão mais clara de como esses mecanismos funcionam na tradução de endereços em redes privadas e no compartilhamento de um único endereço IP público entre múltiplos dispositivos.
Aprendemos, na segunda parte, os diferentes tipos de tramas que existem, as diferenças entre estas, e a analisar o efeito de vários fatores na qualidade da ligação, como a força do sinal ou a velocidade de transmissão.
Com tudo isso, podemos afirmar que foi uma oportunidade valiosa para aplicar os conceitos teóricos em cenários reais, e assim aprofundar o nosso conhecimento sobre a disciplina em geral.