

Universidade do Minho

Licenciatura em Engenharia Informática

Redes de Computadores

Trabalho Prático 3

Grupo 101

Ana Murta (A93284)
Ana Henriques (A93268)
Leonardo Freitas (A93281)

abril, 2022

Conteúdo

1	Redes Ethernet e Protocolo ARP	4
1.1	Captura e análise de Tramas <i>Ethernet</i>	4
1.1.1	Questão 1	4
1.1.2	Questão 2	4
1.1.3	Questão 3	5
1.1.4	Questão 4	5
1.1.5	Questão 5	5
1.1.6	Questão 6	6
1.1.7	Questão 7	6
1.2	Protocolo ARP	7
1.2.1	Questão 8	7
1.2.2	Questão 9	7
1.2.3	Questão 10	8
1.2.4	Questão 11	8
1.2.5	Questão 12	9
1.2.6	Questão 13	9
1.2.7	Questão 14	10
1.3	Domínios de colisão	12
1.3.1	Questão 15	12
1.3.2	Questão 16	13
2	Conclusão	15

Listas de Figuras

1.1	Endereços MAC da mensagem HTTP GET (sublinhada)	4
1.2	<i>Bytes</i> usados desde o início da trama até ao início dos dados do nível aplicacional	5
1.3	Endereço <i>ethernet</i> da fonte	6
1.4	Conteúdo da tabela ARP do nosso computador	7
1.5	ARP <i>request</i>	8
1.6	Confirmação de que é um ARP <i>request</i>	9
1.7	Pergunta feita ao <i>host</i> de origem	9
1.8	Resposta dada à pergunta feita ao <i>host</i> de origem	9
1.9	ARP <i>request</i> - Campo <i>opcode</i>	9
1.10	ARP <i>request</i> - Campo <i>Sender MAC Address</i>	10
1.11	Diagrama geral	10
1.12	Diagrama de sequência	10
1.13	Tabela ARP	11
1.14	Tabelas ARP do Cliente, do Router e do Host	11
1.15	Tabela ARP do Cliente e Host e Tabela ARP do Router	11
1.16	Topologia LEI-RC	12
1.17	<i>Hub</i> do departamento A	12
1.18	<i>Switch</i> do departamento B	13
1.19	Capture <i>Wireshark</i> – Alladin	13
1.20	Captura <i>Wireshark</i> – Jasmine	14
1.21	Tabela de comutação do <i>switch</i> do Departamento B	14

Capítulo 1

Redes Ethernet e Protocolo ARP

O protocolo HTTPS encripta a comunicação entre dois sistemas através de um certificado digital SSL (*Secure Sockets Layer*), onde utiliza o HTTP sobre SSL, oferecendo uma ligação segura entre o cliente e o servidor. Como tal, a requisição GET é encriptada assim como os dados que circulam entre a comunicação. Por este motivo e ser mais fácil analisar a captura do *Wireshark*, recorremos ao URL <http://cbslocal.com/> em vez do proposto no enunciado.

1.1 Captura e análise de Tramas *Ethernet*

1.1.1 Questão 1

Anote os endereços MAC de origem e de destino da trama capturada

A partir da Figura 1.1, podemos retirar que:

Endereço MAC de origem - a0:51:0b:4c:e3:f7

Endereço MAC de destino - 00:d0:03:ff:94:00

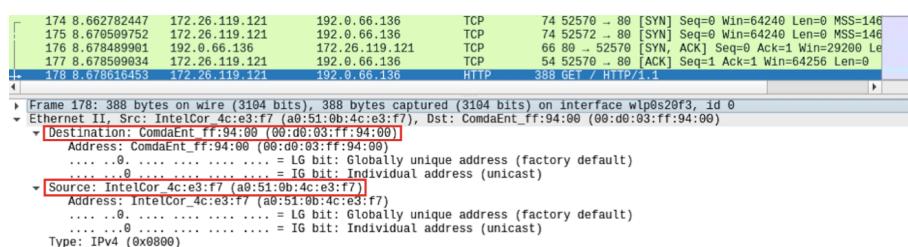


Figura 1.1: Endereços MAC da mensagem HTTP GET (sublinhada)

1.1.2 Questão 2

Identifique a que sistemas se referem. Justifique.

O endereço de origem é a interface *ethernet* do nosso computador de onde parte a trama. O endereço de destino é a interface do router da rede local que recebe a trama; neste caso, é o servidor web <http://cbslocal.com/>.

1.1.3 Questão 3

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

Como podemos ver na Figura 1.1, o valor hexadecimal do campo *Type* é 0x0800, sendo IPv4 o protocolo de camada superior usado.

1.1.4 Questão 4

Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (*Application Data Protocol*: `http-over-tls`)? Calcule e indique, em percentagem, a sobrecarga (*overhead*) introduzida pela pilha protocolar.

Na figura 1.2, retiramos que, desde o início da trama até ao início dos dados do nível aplicacional, são usados 54 bytes ($8*6+6$). No campo *TCP payload*, temos que o valor total de bytes usados no encapsulamento protocolar é 334. Logo, temos $(54/334)*100 = 16,17\%$ de *overhead*.

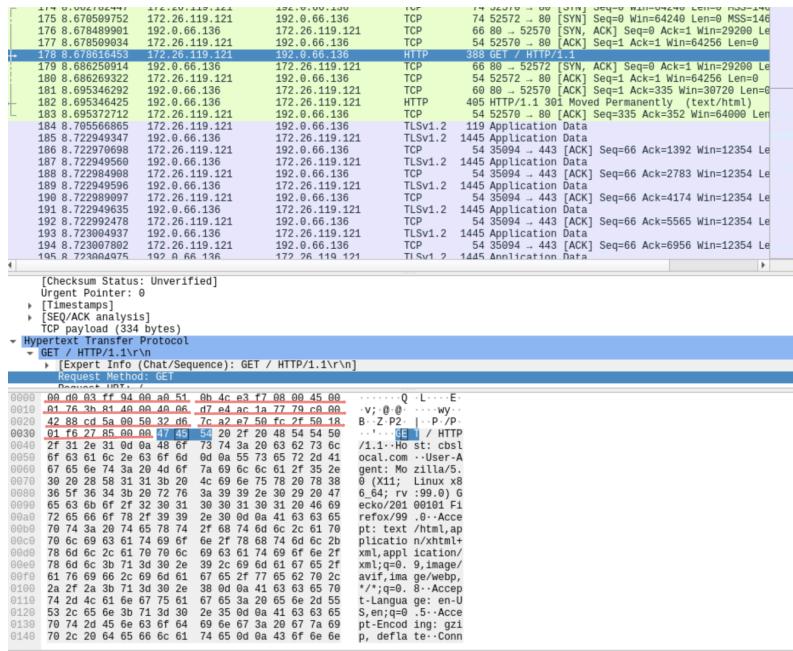


Figura 1.2: Bytes usados desde o início da trama até ao início dos dados do nível aplicacional

1.1.5 Questão 5

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

O endereço *ethernet* da fonte é 00:d0:03:ff:94:00 (Figura 1.3, sendo este o *getaway* por *default* da rede local. Como a nossa máquina não consegue alcançar endereços que não pertencem à sua rede local, como o caso do endereço do servidor, as tramas serão enviadas entre a nossa máquina e o *getaway* por *default* da rede local.

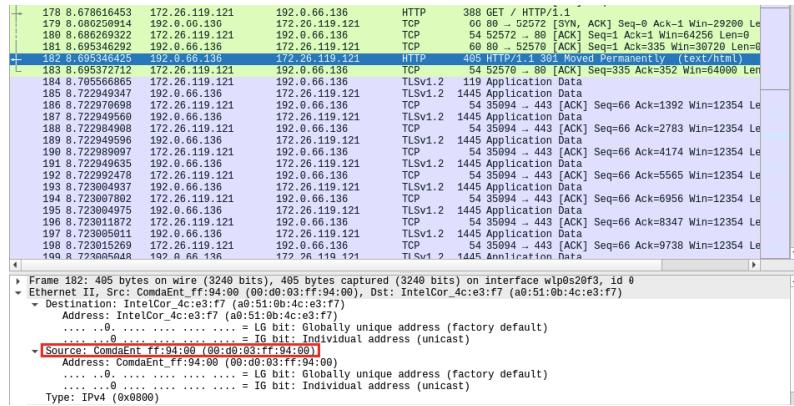


Figura 1.3: Endereço *ethernet* da fonte

1.1.6 Questão 6

Qual é o endereço MAC do destino? A que sistema corresponde?

Pela Figura 1.3, vemos que o endereço MAC de destino é a0:51:0b:4c:e3:f7, o que, comparando com os endereços da Figura 1.1, corresponde à interface *ethernet* do nosso computador.

1.1.7 Questão 7

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

Na trama recebida, são identificados os protocolos IPv4, Ethernet e TCP.

1.2 Protocolo ARP

IMPORTANTE: a resolução das seguintes perguntas foi feita num ambiente *Windows*, fora da aula prática, pelo que o endereço MAC da nossa máquina é diferente do identificado nos exercícios anteriores.

1.2.1 Questão 8

Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.

Para obter a tabela ARP do nosso computador, executou-se o comando `arp -a`, estando o resultado ilustrada na Figura 1.4.

A coluna *Internet Address* identifica vários *hosts* através dos seus endereços IP, em decimal.

A coluna *Physical Address* identifica vários *hosts* através dos seus endereços físicos (MAC), em hexadecimal.

A coluna *Type* indica se a entrada é estática ou dinâmica.

Interface	Internet Address	Physical Address	Type
192.168.1.87 --- 0x5	192.168.1.64	fc-d5-d9-aa-ea-22	dynamic
	192.168.1.254	cc-19-a8-fc-b1-bf	dynamic
	192.168.1.255	ff-ff-ff-ff-ff-ff	static
	224.0.0.22	01-00-5e-00-00-16	static
	224.0.0.251	01-00-5e-00-00-fb	static
	224.0.0.252	01-00-5e-00-00-fc	static
	239.255.255.250	01-00-5e-7f-ff-fa	static
	255.255.255.255	ff-ff-ff-ff-ff-ff	static
192.168.40.1 --- 0x6	192.168.40.255	ff-ff-ff-ff-ff-ff	static
	224.0.0.22	01-00-5e-00-00-16	static
	224.0.0.251	01-00-5e-00-00-fb	static
	224.0.0.252	01-00-5e-00-00-fc	static
	239.255.255.250	01-00-5e-7f-ff-fa	static
192.168.153.1 --- 0x12	192.168.153.255	ff-ff-ff-ff-ff-ff	static
	224.0.0.22	01-00-5e-00-00-16	static
	224.0.0.251	01-00-5e-00-00-fb	static
	224.0.0.252	01-00-5e-00-00-fc	static
	239.255.255.250	01-00-5e-7f-ff-fa	static

Figura 1.4: Conteúdo da tabela ARP do nosso computador

1.2.2 Questão 9

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?

Primeiramente, apagou-se o conteúdo da cache ARP com a execução do comando `arp -d`, tal como recomendado no enunciado.

A partir da Figura 1.5, é possível analisar a captura do *Wireshark* referente ao pedido ARP. O valor hexadecimal do endereço MAC de origem é `a0:51:0b:4c:e3:f7`, de nome `IntelCor_4c:e3:f7`, que corresponde à interface *ethernet* do nosso computador. Já o valor hexadecimal do endereço MAC de destino é `ff:ff:ff:ff:ff:ff`, sendo este o endereço de *broadcast*, que está reservado para ligações em que a trama é transmitida a todos os nós (ligação *multipoint*). Para ser possível enviar o pedido ARP, é preciso saber o endereço MAC de destino. Assim sendo, a mensagem é enviada para o endereço de *broadcast*, i.e. é enviada para todas as interfaces e, assim que alguma a receber e reconhecer o endereço de destino como o seu endereço MAC, é enviada uma resposta, que contém o endereço MAC desse *host* como endereço de origem.

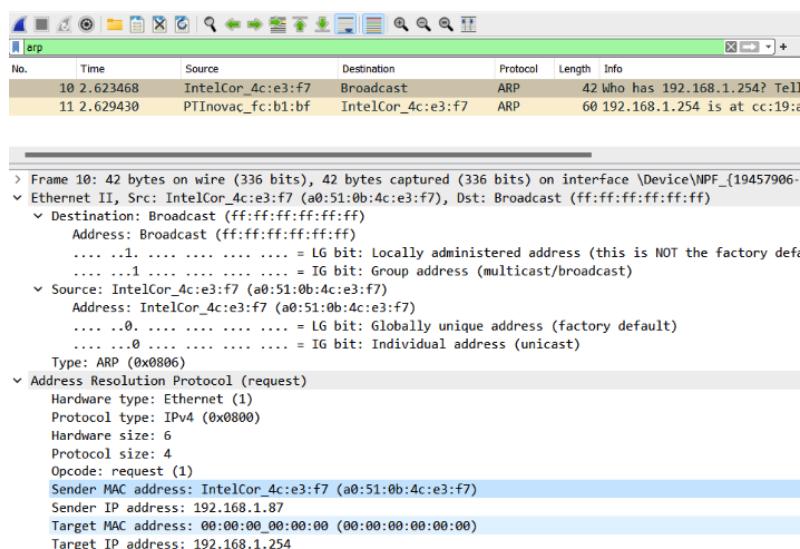


Figura 1.5: ARP request

1.2.3 Questão 10

Qual o valor hexadecimal do campo tipo da trama *Ethernet*? O que indica?

Na figura 1.5, o campo *Type* está preenchido com o valor hexadecimal `0x0806`, identificando o protocolo ARP.

1.2.4 Questão 11

Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Na figura 1.6, o campo *opcode* está preenchido com o valor `request (1)` e, por isso, estamos perante um pedido ARP. Quanto ao tipo de endereços contidos na mensagem ARP, temos dois tipos: endereços IP de origem e de destino – `192.168.1.87` e `192.168.1.254`, respectivamente – e apenas o endereço MAC de origem (da nossa máquina) – `a0:51:0b:4c:e3:f7`, já que este ainda não conhece o endereço MAC de destino `a0:51:0b:4c:e3:f7`.

```

> Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{19457906-}
> Ethernet II, Src: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7)
    Sender IP address: 192.168.1.87
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.254

```

Figura 1.6: Confirmação de que é um ARP *request*

1.2.5 Questão 12

Explicite que tipo de pedido ou pergunta é feita pelo *host* de origem.

A mensagem enviada é "Who has 192.168.1.254? Tell 192.168.1.87" – Figura 1.7. Isto significa que o *host* 192.168.1.87 quer saber quem é o *host* 192.168.1.254 e, por isso, todos os *hosts* são interrogados. Logo que encontrado o procurado, é enviada uma mensagem "192.168.1.254 is at cc:19:a8:fc:b1:bf" – Figura 1.8

```

10 2.623468 IntelCor_4c:e3:f7 Broadcast ARP 42 Who has 192.168.1.254? Tell 192.168.1.87

```

Figura 1.7: Pergunta feita ao *host* de origem

```

11 2.629430 PTInovac_fc:b1:bf IntelCor_4c:e3:f7 ARP 60 192.168.1.254 is at cc:19:a8:fc:b1:bf

```

Figura 1.8: Resposta dada à pergunta feita ao *host* de origem

1.2.6 Questão 13

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

Tal como mencionada anteriormente, a resposta ao pedido ARP efetuado é "192.168.1.254 is at cc:19:a8:fc:b1:bf", ilustrado na Figura 1.8.

Alínea a: Qual o valor do campo ARP *opcode*? O que especifica?

O valor do campo *opcode* é **reply** (2), indicando uma resposta do tipo ARP *reply* – Fig. 1.9.

```

> Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{19457906-}
> Ethernet II, Src: PTInovac_fc:b1:bf (cc:19:a8:fc:b1:bf), Dst: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PTInovac_fc:b1:bf (cc:19:a8:fc:b1:bf)
    Sender IP address: 192.168.1.254
    Target MAC address: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7)
    Target IP address: 192.168.1.87

```

Figura 1.9: ARP *request* - Campo *opcode*

Alínea b: Em que campo da mensagem ARP está a resposta ao pedido ARP?

A resposta ao pedido ARP está no campo *Sender MAC Address*, que neste caso é PTInovaçfc:b1:bf.

```
> Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{19457906-  
> Ethernet II, Src: PTInovaç_fc:b1:bf (cc:19:a8:fc:b1:bf), Dst: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7)  
✓ Address Resolution Protocol (reply)  
  Hardware type: Ethernet (1)  
  Protocol type: IPv4 (0x0800)  
  Hardware size: 6  
  Protocol size: 4  
  Opcode: reply (2)  
  Sender MAC address: PTInovaç_fc:b1:bf (cc:19:a8:fc:b1:bf)  
  Sender IP address: 192.168.1.254  
  Target MAC address: IntelCor_4c:e3:f7 (a0:51:0b:4c:e3:f7)  
  Target IP address: 192.168.1.87
```

Figura 1.10: ARP request - Campo *Sender MAC Address*

1.2.7 Questão 14

Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.

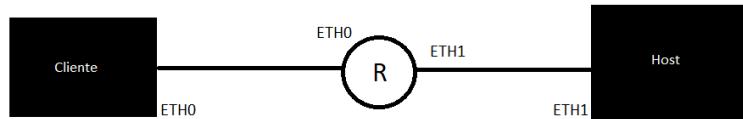


Figura 1.11: Diagrama geral

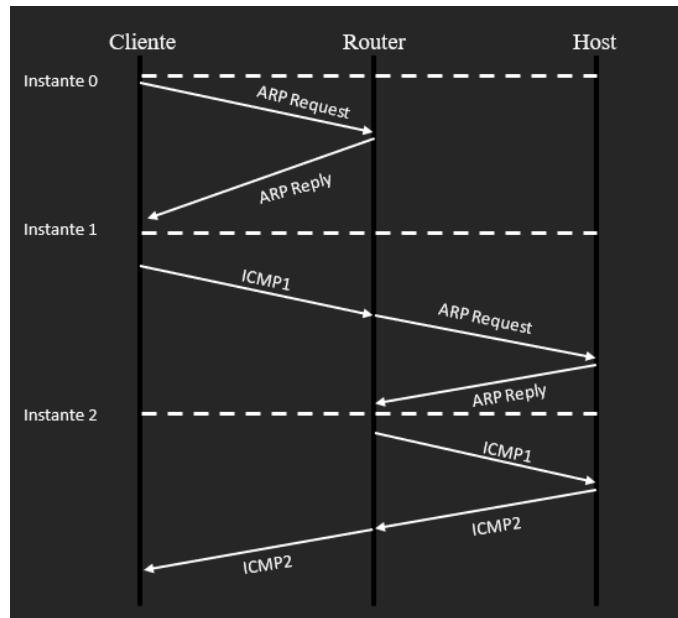


Figura 1.12: Diagrama de sequência

Tal como se pode ver na Figura 1.13, a representação da tabela ARP teve em consideração os campos identificados na pergunta 8, nomeadamente, os campos *Internet Address*, *Physical Address* e *Type*, sendo que, inicialmente as tabelas ARP dos componentes usados na comunicação estão vazias.

Internet Address	Physical Address	Type

Figura 1.13: Tabela ARP

No primeiro instante, podemos ver que a tabela ARP de Host não sofreu qualquer alteração, ao contrário das tabelas ARP do Cliente e do Router, que passaram a conhecer as estruturas uma da outra, como observável na figura 1.14.

TABELA DO CLIENTE		
Internet Address	Physical Address	Type
IP Do Router	Mac do Router	Dynamic
TABELA DO ROUTER		
Internet Address	Physical Address	Type
IP Do Cliente	Mac do Cliente	Dynamic
TABELA DO HOST		
Internet Address	Physical Address	Type

Figura 1.14: Tabelas ARP do Cliente, do Router e do Host

No último instante, como podemos ver pela Figura 1.15, a tabela ARP do Router compreende as informações do Cliente e do Host. Já as tabelas ARP do Cliente e do Host conhecem o Router separadamente, isto é, estas não se conhecem uma à outra.

TABELA DO CLIENTE E HOST		
Internet Address	Physical Address	Type
IP Do Router	Mac do Router	Dynamic
TABELA DO ROUTER		
Internet Address	Physical Address	Type
IP do Cliente	Mac do Cliente	Dynamic
IP do HOST	Mac do HOST	Dynamic

Figura 1.15: Tabela ARP do Cliente e Host e Tabela ARP do Router

1.3 Domínios de colisão

1.3.1 Questão 15

Através da opção `tcpdump` verifique e compare como flui o tráfego nas diversas interfaces do dispositivo de interligação no departamento A (LAN partilhada) e no departamento B (LAN comutada) quando se gera tráfego intra-departamento (por exemplo, fazendo ping IPaddr da Bela para Monstro, da Jasmine para o Alladin, etc.) Que conclui?

Na figura 1.16, está representada a topologia de rede com a solução de *subnetting* que construímos no âmbito do TP2, na qual se substituiu o *switch* do departamento A por um *hub*.

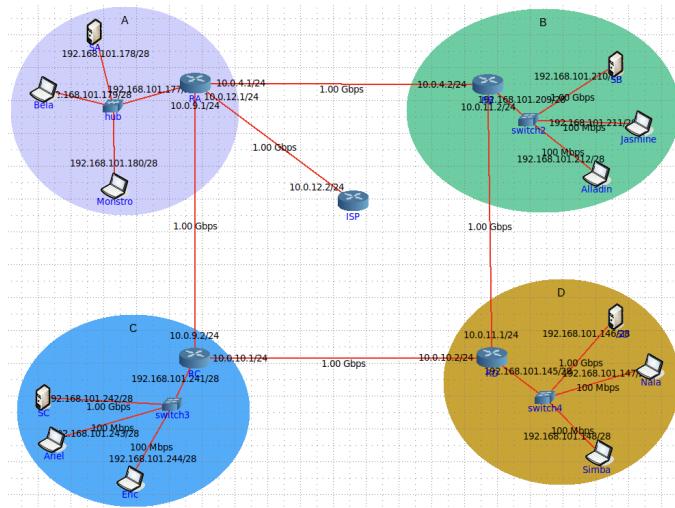


Figura 1.16: Topologia LEI-RC

Ao substituir o *switch* do departamento A por um *hub*, as interfaces de A passaram a estar ligadas ao *router* através de um *hub* – Figura 1.17. Ao executar, por exemplo, o comando `ping 192.168.101.180 -c 10` na interface Bela, i.e. ping IPaddr da Bela para Monstro e ao analisar o tráfego resultante, conclui-se que todos os *hosts* de Bela recebem esta comunicação com Monstro.

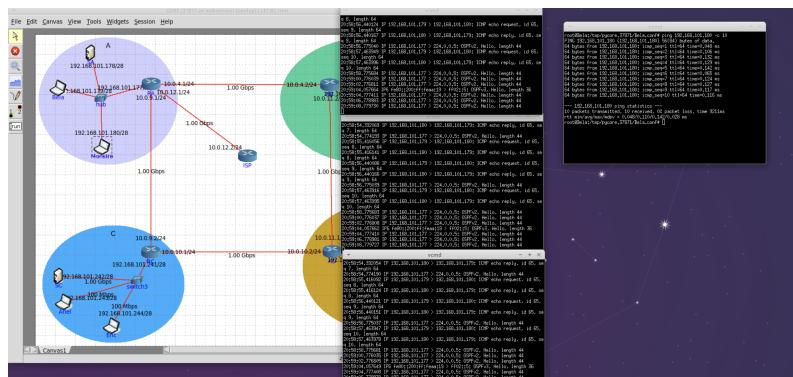


Figura 1.17: Hub do departamento A

Em contraste, as interfaces de B encontram-se ligadas a um *router* através de um *switch* – Figura 1.18. Ao executar o comando `ping 192.168.101.212 -c 10` na interface *Jasmine*, i.e. ping `IPaddr` da *Jasmine* para *Alladin* e ao analisar o tráfego resultante, verifica-se a diferença de que só os hosts envolvidos recebem esta comunicação com *Alladin*.

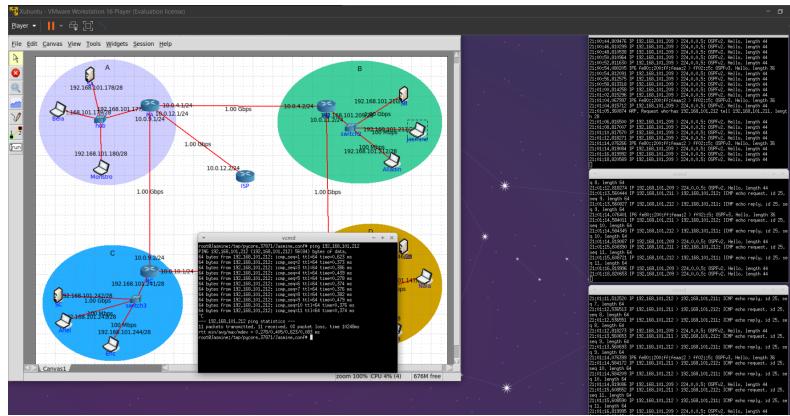


Figura 1.18: *Switch* do departamento B

1.3.2 Questão 16

Construa manualmente a tabela de comutação do *switch* do Departamento B, atribuindo números de porta à sua escolha.

MAC Alladin - 00:00:00_aa:00:01
MAC SB - 00:00:00_aa:00:15

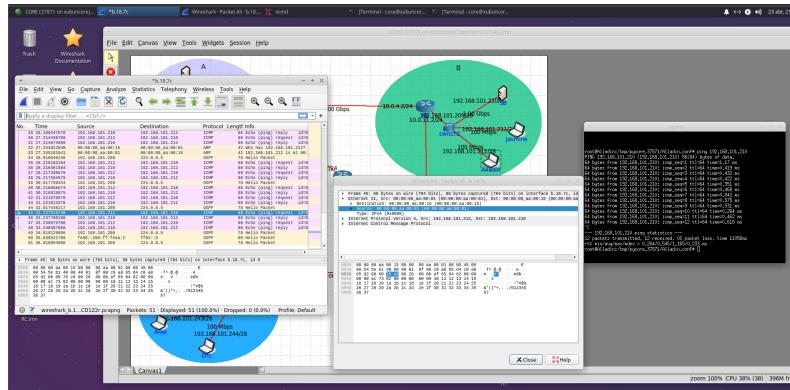


Figura 1.19: Capture *Wireshark* – Alladin

MAC Jasmine - 00:00:00_aa:00:00
MAC Router - 00:00:00_aa:00:02

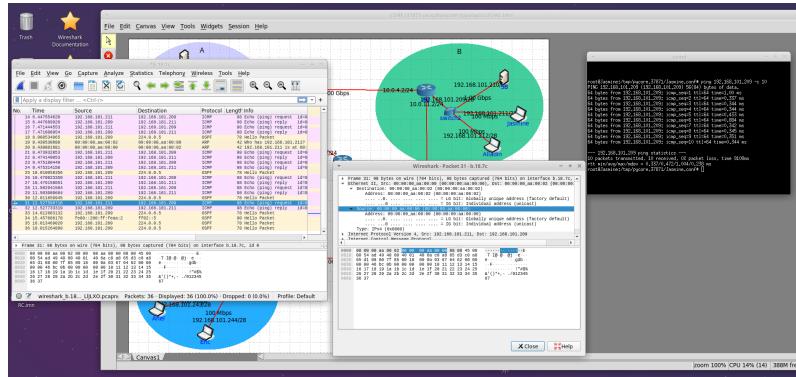


Figura 1.20: Captura Wireshark – Jasmine

Porta	Endereço MAC
1	00:00:00_aa:00:00
2	00:00:00_aa:00:01
3	00:00:00_aa:00:02
4	00:00:00_aa:00:15

Figura 1.21: Tabela de comutação do *switch* do Departamento B

Capítulo 2

Conclusão

Com a realização deste trabalho prático, foi possível solidar a matéria lecionada nas aulas teóricas relativa à camada de ligação lógica, particularmente sobre o uso da tecnologia *Ethernet* e o protocolo ARP (*Address Resolution Protocol*), bem como continuar a conhecer as ferramentas *CORE* e *Wireshark*.

O trabalho prático encontra-se dividido em três partes. Inicialmente, foi aprofundado o conhecimento relacionada com a captura e análise de tramas *Ethernet*. Nesta parte, obtivemos uma melhor percepção sobre os endereços MAC e a sua utilidade. Para além disto, também conhecemos endereços *Ethernet* e as questões protocolares.

Seguidamente, foi analisado a operação do protocolo ARP através da observação e análise do conteúdo da tabela ARP, sendo determinados alguns endereços MAC (sempre que necessários) a partir das primitivas *arp-request* e *arp-reply*.

Por último, abordou-se os domínios da colisão, verificando a diferença entre *hubs* e *switches* através da substituição de um *switch* do departamento A por um *hub*.