



Redes de Computadores
(3º ano LEI)

Trabalho Prático 3

Relatório de Desenvolvimento

Grupo 4

a93241 Francisco Reis Izquierdo
a89526 Duarte Augusto Rodrigues Lucas
a96277 Diogo Miguel Serra Silva

23 de Abril de 2022

Conteúdo

1	Introdução	3
2	Captura e análise de Tramas Ethernet	3
2.1	Pergunta 1	4
2.2	Resposta 1	4
2.3	Pergunta 2	4
2.4	Resposta 2	4
2.5	Pergunta 3	5
2.6	Resposta 3	5
2.7	Pergunta 4	5
2.8	Resposta 4	6
2.9	Pergunta 5	7
2.10	Resposta 5	7
2.11	Pergunta 6	8
2.12	Resposta 6	8
2.13	Pergunta 7	8
2.14	Resposta 7	8
3	Protocolo ARP	8
3.1	Pergunta 8	8
3.2	Resposta 8	8
3.3	Pergunta 9	9
3.4	Resposta 9	9
3.5	Pergunta 10	9
3.6	Resposta 10	9
3.7	Pergunta 11	9
3.8	Resposta 11	9
3.9	Pergunta 12	10
3.10	Resposta 12	10
3.11	Pergunta 13	10
3.11.1	Pergunta a	10
3.11.2	Resposta a	10
3.11.3	Pergunta b	10
3.11.4	Resposta b	10
3.12	Pergunta 14	11
3.13	Resposta 14	11
4	Domínios de colisão	11
4.1	Pergunta 15	11
4.2	Resposta 15	11
4.3	Pergunta 16	12
4.4	Resposta 16	13
5	Conclusão	14

Listings

Lista de Figuras

1	Endereços MAC da caputa do pacote TCP - SYN/ACK	4
2	Endereço MAC	5
3	Tamanho do pacote	6
4	Tamanho do cabeçalho IP	6
5	Tamanho do cabeçalho TCP	7
6	Trama que contém o primeiro byte da resposta HTTP	7
7	Tabela ARP do nosso computador.	8
8	Pedido ARP.	9
9	ARP reply.	10
10	Diagrama ARP e ICMP.	11
11	Comandos executados no departamento A e no departamento B .	12
12	Topologia	13
13	Comando ifconfig	14
14	Tabela de comutação do switch	14

1 Introdução

Para este terceiro trabalho prático, no âmbito da disciplina de Redes de Computadores, o grupo de trabalho realizou uma manipulação e estudo aprofundado sobre deteção e correção de erros, endereços MAC, ARP (*Address Resolution Protocol*) e *Ethernet*.

2 Captura e análise de Tramas Ethernet

A captura de tráfego deverá ser efetuada usando a aplicação Wireshark instalada na máquina nativa. Uma vez que as salas de aula atuais não disponibilizam uma ligação com fios a uma rede Ethernet, a captura será realizada na rede Eduroam. Este facto não impacta na realização do trabalho porque, por defeito, o Wireshark disponibiliza o tráfego capturado ao utilizador como sendo (pseudo) Ethernet.

Assegure-se que a cache do seu browser está vazia.

Ative o Wireshark na sua máquina nativa.

No seu browser, aceda ao URL <https://elearning.uminho.pt>.

Pare a captura do Wireshark., e proceda da seguinte forma: Localize o estabelecimento da conexão entre o cliente e o servidor HTTP (sequência de tramas com as TCP flags TCP SYN, SYN- ACK, ACK ativas). Após a fase de estabelecimento seguro da conexão, obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à trama que transporta os primeiros dados aplicativos enviados do cliente para o servidor (Application Data). Identifique também o número de ordem da trama com a resposta proveniente do servidor que contém os dados correspondentes ao acesso web realizado pelo cliente (browser).

Note que os dados aplicativos são enviados de forma segura usando o protocolo TLS (Transport Layer Security), mapeados para um segmento TCP, transportado num datagrama IP que, por sua vez, é encapsulado no campo de dados da trama Ethernet. Expand a informação do nível da ligação de dados e observe o conteúdo da trama Ethernet (cabeçalho e dados (payload)). Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem de acesso ao servidor (HTTP GET encriptada).

Sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada. Para imprimir um pacote, use File->Print, escolha Selected packet only e Packet summary line, ou Universidade do Minho LEI, Redes de Computadores, 2021/2022 use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o mínimo detalhe necessário para responder à pergunta.

2.1 Pergunta 1

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

2.2 Resposta 1

Endereço MAC de origem → 90:9c:4a:c8:c4

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

No.	Time	Source	Destination	Protocol	Length	Info
34	2.690727	193.137.9.150	172.26.98.228	TLSv1	111	Encrypted Handshake Message
35	2.690809	172.26.98.228	193.137.9.150	TCP	66	63111 → 443 [ACK] Seq=644 Ack=6171 Win=131088 Len=0 TSval=382118888 TSecr=3668352159
36	2.691297	172.26.98.228	193.137.16.65	DNS	82	Standard query 0x213a A gevent.ocsp.sectigo.com
37	2.693551	193.137.16.65	172.26.98.228	DNS	488	Standard query response 0x213a A gevent.ocsp.sectigo.com CNAME ocsp.sectigo.com CNAME ocsp.comodoca
38	2.695276	172.26.98.228	104.18.32.68	TCP	78	63112 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=793801619 TSecr=0 SACK_PERM=1
39	2.701708	104.18.32.68	172.26.98.228	TCP	66	80 → 63112 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 WS=1024
40	2.701868	172.26.98.228	104.18.32.68	TCP	54	63112 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
41	2.702281	172.26.98.228	104.18.32.68	OCSP	509	Request
42	2.709277	104.18.32.68	172.26.98.228	TCP	60	80 → 63112 [ACK] Seq=1 Ack=456 Win=68608 Len=0
43	2.808271	104.18.32.68	172.26.98.228	OCSP	1249	Response
44	2.808433	172.26.98.228	104.18.32.68	TCP	54	63112 → 80 [ACK] Seq=456 Ack=1196 Win=268928 Len=0
45	2.812377	172.26.98.228	193.137.9.150	TLSv1	569	Application Data
46	2.831622	193.137.9.150	172.26.98.228	TCP	66	443 → 63111 [ACK] Seq=6171 Ack=1147 Win=262144 Len=0 TSval=3668352159 TSecr=382118938
47	2.837022	172.26.98.228	210.50.215.103	TCP	54	63100 → 80 [ACK] Seq=1 Ack=1 Win=2848 Len=0

Frame 46: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface em0, id 0
Ethernet II, Src: Apple_C8:B:C4 (90:9c:4a:c8:c4), Dst: ComdAnt_ff:94:00 (00:d0:03:ff:94:00)
Destination: ComdAnt_ff:94:00 (00:d0:03:ff:94:00)
Source: Apple_C8:B:C4 (90:9c:4a:c8:c4)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.98.228, Dst: 193.137.9.150
Transmission Control Protocol, Src Port: 443, Dst Port: 6171, Seq: 644, Ack: 6171, Len: 503
Transport Layer Security

Figura 1: Endereços MAC da capta do pacote TCP - SYN/ACK

2.3 Pergunta 2

Identifique a que sistemas se referem. Justifique.

2.4 Resposta 2

Através do comando *ip link* conseguimos verificar e visualizar o endereço MAC do computador, neste caso tivemos que recorrer a um modo diferente visto que o sistema do computador na qual está ser realizado esta parte do trabalho é MACOS, sendo necessário recorrer às definições do computador. Deste modo, concluímos que a origem refere-se ao nosso computador e o destino é relativo ao servidor *elarning.uminho.pt*.

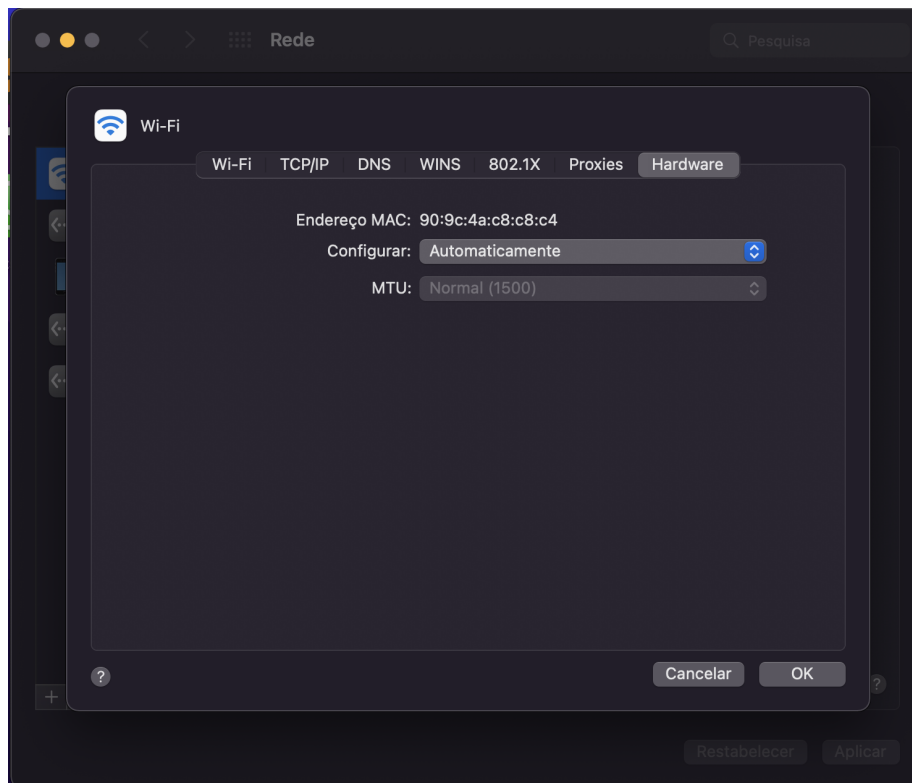


Figura 2: Endereço MAC

2.5 Pergunta 3

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

2.6 Resposta 3

Através da figura 1 podemos observar que o valor do campo *Type* é 0x0800, representando o protocolo de camada superior utilizado, neste caso IPv4.

2.7 Pergunta 4

Quanto 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.

2.8 Resposta 4

A partir da figura 3 é possível concluir que o tamanho do pacote é de 569 bytes, possível observar nas figuras 4 e 5, por sua vez, que o tamanho do cabeçalho IP tem um total de 20 bytes, o cabeçalho TPC tem um total de 32 bytes, o tamanho do cabeçalho ethernet é de $\rightarrow 569 - (503 + 20 + 32) = 14$. Concluimos deste modo temos que o número de bytes utilizado para o encapsulamento protocolar é de 52 bytes. Por fim, $(14 + 32 + 20) / 569 = 11,6\%$ de overhead.

```
▼ Frame 45: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface en0, id 0
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 26, 2022 14:07:11.658351000 WEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1650978431.658351000 seconds
    [Time delta from previous captured frame: 0.003944000 seconds]
    [Time delta from previous displayed frame: 0.003944000 seconds]
    [Time since reference or first frame: 2.812377000 seconds]
    Frame Number: 45
    Frame Length: 569 bytes (4552 bits)
    Capture Length: 569 bytes (4552 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ttl]
```

Figura 3: Tamanho do pacote

```
> Frame 45: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface en0, id 0
> Ethernet II, Src: Apple_c8:c8:c4 (90:9c:4a:c8:c8:c4), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
▼ Internet Protocol Version 4, Src: 172.26.98.228, Dst: 193.137.9.150
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 555
    Identification: 0x0000 (0)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x5eaf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.26.98.228
```

Figura 4: Tamanho do cabeçalho IP

```

> Internet Protocol version 4, Src: 172.26.98.228, Dst: 193.137.9.150
> Transmission Control Protocol, Src Port: 63111, Dst Port: 443, Seq: 644, Ack: 6171, Len: 503
  Source Port: 63111
  Destination Port: 443
  [Stream index: 4]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 503]
  Sequence Number: 644 (relative sequence number)
  Sequence Number (raw): 403194729
  [Next Sequence Number: 1147 (relative sequence number)]
  Acknowledgment Number: 6171 (relative ack number)
  Acknowledgment number (raw): 38807638
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
  Window: 2048
  [Calculated window size: 131072]
  [Window size scaling factor: 64]
  Checksum: 0xdeb0 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (503 bytes)

```

Figura 5: Tamanho do cabeçalho TCP

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

No.	Time	Source	Destination	Protocol	Length	Info
37	2.693551	193.137.16.65	172.26.98.228	DNS	488	Standard query response 0x213a A geant.ocsp.sectigo.com
38	2.695276	172.26.98.228	104.18.32.68	TCP	78	63112 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=793001619 TSecr=0 SACK_PERM=1
39	2.703700	104.18.32.68	172.26.98.228	TCP	66	80 → 63112 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 WS=1024
40	2.701668	172.26.98.228	104.18.32.68	TCP	54	63112 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
41	2.702281	172.26.98.228	104.18.32.68	OCSP	509	Request
42	2.709277	104.18.32.68	172.26.98.228	TCP	68	80 → 63112 [ACK] Seq=1 Ack=456 Win=68688 Len=0
43	2.080271	104.18.32.68	172.26.98.228	OCSP	1249	Response
44	2.080433	172.26.98.228	104.18.32.68	TCP	54	63112 → 80 [ACK] Seq=456 Ack=1196 Win=260928 Len=0
45	2.012377	172.26.98.228	193.137.9.150	TLSv1.	569	Application Data
46	2.031622	193.137.9.150	172.26.98.228	TCP	66	443 → 63111 [ACK] Seq=6171 Ack=1147 Win=262144 Len=0 TSval=3660352159 TSecr=382110930
47	2.037022	172.26.98.228	216.58.215.163	TCP	54	63100 → 80 [ACK] Seq=1 Ack=1 Min=2048 Len=0
48	2.052916	216.58.215.163	172.26.98.228	TCP	66	[TCP ACKed unseen segment] 80 → 63100 [ACK] Seq=1 Ack=2 Win=265 Len=0 TSval=3406439926 TSecr=27567
49	2.097763	193.137.9.150	172.26.98.228	TLSv1.	922	Application Data
50	2.097764	193.137.9.150	172.26.98.228	TLSv1.	1252	Application Data
51	2.097766	193.137.9.150	172.26.98.228	TCP	1304	443 → 63111 [ACK] Seq=8213 Ack=1147 Win=262144 Len=1238 TSval=3660352159 TSecr=382110930 [TCP segm
52	2.097941	172.26.98.228	193.137.9.150	TCP	66	63111 → 443 [ACK] Seq=1147 Ack=9451 Win=127744 Len=0 TSval=382111015 TSecr=3660352159
53	2.098518	193.137.9.150	172.26.98.228	TLSv1.	841	Application Data
54	2.098519	193.137.9.150	172.26.98.228	TCP	1304	443 → 63111 [ACK] Seq=10226 Ack=1147 Win=262144 Len=1238 TSval=3660352159 TSecr=382110930 [TCP segm
55	2.098520	193.137.9.150	172.26.98.228	TLSv1.	841	Application Data

Figura 6: Trama que contém o primeiro byte da resposta HTTP

2.9 Pergunta 5

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

2.10 Resposta 5

O endereço *Ethernet* da fonte é 90:9c:4a:c8:c8:c4, o seu sistema pertence à interface *Ethernet* do computador.

2.11 Pergunta 6

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

2.12 Resposta 6

O endereço MAC do destino é 00:d0:03:ff:94:00, e o seu sistema é o router a qual o computador está associado.

2.13 Pergunta 7

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

2.14 Resposta 7

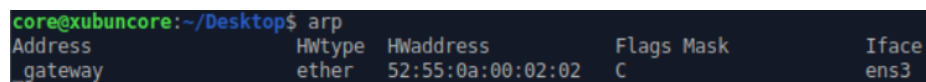
Os vários protocolos contidos na trama são:

- *Ethernet*
- IPv4
- TCP

3 Protocolo ARP

3.1 Pergunta 8

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



Address	HWtype	HWaddress	Flags	Mask	Iface
gateway	ether	52:55:0a:00:02:02	C		ens3

Figura 7: Tabela ARP do nosso computador.

3.2 Resposta 8

A coluna *Address* nomeia os endereços, neste caso temos apenas o gateway da rede local. A coluna *HWtype* explicita o tipo de protocolo usado, e a coluna *HWaddress* o endereço MAC. A coluna *Flags* mostra-nos o tipo de registo que está a ser colocado em memória. Na nossa tabela este valor é C, o que significa que o registo foi obtido dinamicamente pelo protocolo ARP. A coluna *Mask* corresponde à máscara de subrede. A última coluna, *Iface* dá-nos a interface da rede, no nosso caso ens3.

3.3 Pergunta 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?

3.4 Resposta 9

O endereço MAC origem é 00:00:00:aa:00:00 e o endereço destino é ff:ff:ff:ff:ff:ff (endereço de *broadcast*. O endereço destino é o de *broadcast* porque a máquina que envia o ARP request precisa de conhecer qual o endereço MAC destino. Envia em *broadcast*, o que significa que envia o pedido para todas as interfaces, e espera pela resposta da máquina destino com o respetivo endereço MAC.

```
▶ Frame 19: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.e8, 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)
  ▶ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  Sender IP address: 172.16.0.10
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.16.0.1
```

Figura 8: Pedido ARP.

3.5 Pergunta 10

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

3.6 Resposta 10

O valor é 0x0806. Indica que se trata do protocolo ARP.

3.7 Pergunta 11

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

3.8 Resposta 11

Podemos verificar que se trata de um pedido ARP, uma vez que o campo opcode contém "request" e código 1. Na mensagem estão contidos o IP e MAC origem, como também o IP destino (o MAC destino não está presente visto que foi apagado da tabela ARP previamente).

3.9 Pergunta 12

Explicita o tipo de pedido ou pergunta é feita pelo host de origem.

3.10 Resposta 12

"Who has 172.16.0.1? Tell 172.16.0.10" A máquina origem quer saber quem tem o endereço IP 172.16.0.1, logo pergunta a todos os *hosts* qual deles é que tem esse endereço, e pede feedback (com o endereço MAC destino) para o endereço IP 172.16.0.10.

3.11 Pergunta 13

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

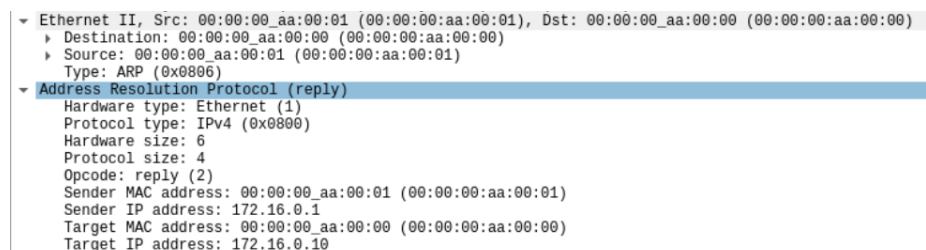


Figura 9: ARP reply.

3.11.1 Pergunta a

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

3.11.2 Resposta a

O valor do campo opcode é "reply (2)", indicando que se trata de uma mensagem *ARP reply*. O código 2 significa que é do tipo *ARP reply*.

3.11.3 Pergunta b

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

3.11.4 Resposta b

No campo *Sender MAC address*.

3.12 Pergunta 14

Na situação em que efetua um ping a outro host, assuma que este está diretamente ligado ao mesmo router, mas noutra subrede, e que todas as tabelas ARP se encontram inicialmente vazias. Esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do host destino.

3.13 Resposta 14

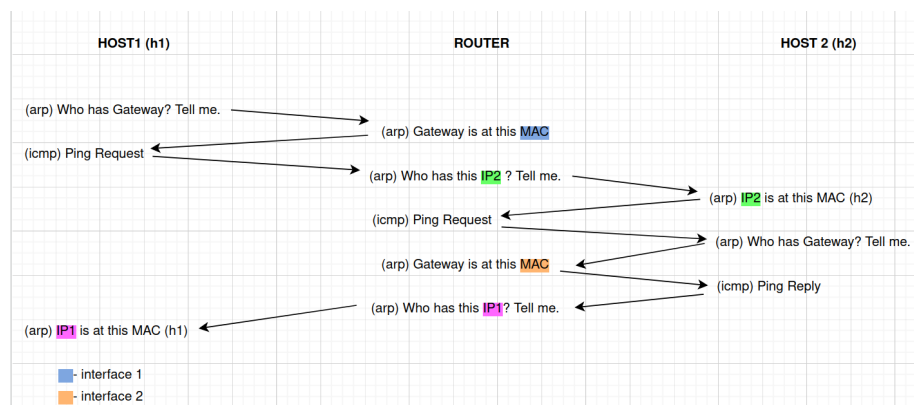


Figura 10: Diagrama ARP e ICMP.

4 Domínios de colisão

4.1 Pergunta 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?

4.2 Resposta 15

No departamento A, departamento na qual se trocou o *switch* por um *hub*, após executar o comando ping do computador Bela (192.168.134.228) para o computador Monstro(192.168.134.226) e executar o comando tcpdump no *hostSA*(192.168.134.227) é possível verificar o envio de tramas entre os computadores anteriormente mencionados, tais como o echo request e o echo reply. No departamento B foi mantido o *switch* e executaram-se os mesmos comandos, o comando ping do computador Jasmine(192.168.134.196) para Alla-

din(192.168.134.195) e o comando tcpdump no *hostSB*(192.168.134.193), e após uma breve análise foi possível verificar que executando o comando tcpdump este não captura as tramas enviadas do computador Jasmine para o Alladin, capturando outras tramas que não estavam relacionadas com o comando ping executado.

```

root@SB:/tmp/pycore.42923/SB.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15:58:08.491156 IP 192.168.134.226 > 224.0.0.5: OSPFv2, Hello, length 44
15:58:08.963960 ARP, Request who-has 192.168.134.226 tell 192.168.134.228, length 28
15:58:09.964058 ARP, Reply 192.168.134.226 is-at 00:00:00:aa:00:17 (oui Ethernet II), length 28
15:58:09.965274 IP 192.168.134.228 > 192.168.134.226: ICMP echo request, id 27, seq 1, length 64
15:58:09.965434 IP 192.168.134.226 > 192.168.134.228: ICMP echo reply, id 27, seq 1, length 64
15:58:09.965792 IP 192.168.134.228 > 192.168.134.226: ICMP echo request, id 27, seq 2, length 64
15:58:09.966067 IP 192.168.134.226 > 192.168.134.228: ICMP echo reply, id 27, seq 2, length 64
15:58:10.492751 IP 192.168.134.225 > 224.0.0.5: OSPFv2, Hello, length 44
15:58:10.664351 IP6 fe80::289e:5dff:fe63:12af.ndna > ff02::fb.ndna: 0 [2q] PTR (00)7 _lppa_tcp.local. PTR (00)7 _lpp_tcp.local. (45)
15:58:10.980819 IP 192.168.134.228 > 192.168.134.226: ICMP echo request, id 27, seq 3, length 64
15:58:10.980923 IP 192.168.134.226 > 192.168.134.228: ICMP echo reply, id 27, seq 3, length 64
15:58:11.429157 IP6 fe80::200:ff:feaa:16 > ip6-allrouters: ICMP6, router solicitation, length 16
15:58:12.005274 IP 192.168.134.228 > 192.168.134.226: ICMP echo request, id 27, seq 4, length 64
15:58:12.006391 IP 192.168.134.226 > 192.168.134.228: ICMP echo reply, id 27, seq 4, length 64
15:58:12.493072 IP 192.168.134.225 > 224.0.0.5: OSPFv2, Hello, length 44
15:58:12.521459 IP6 fe80::200:ff:feaa:18 > ff02::5: OSPFv3, Hello, length 36

16 packets captured
16 packets received by filter
0 packets dropped by kernel
root@SB:/tmp/pycore.42923/SB.conf#

root@SB:/tmp/pycore.42923/SB.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15:58:16.555942 IP 192.168.134.193 > 224.0.0.5: OSPFv2, Hello, length 44
15:58:20.559354 IP 192.168.134.193 > 224.0.0.5: OSPFv2, Hello, length 44

4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@SB:/tmp/pycore.42923/SB.conf#

root@Jasmine:/tmp/pycore.42923/Jasmine.conf# ping 192.168.134.195
PING 192.168.134.195 (192.168.134.195) 56(84) bytes of data:
64 bytes from 192.168.134.195: icmp_seq=1 ttl=64 time=0.41 ms
64 bytes from 192.168.134.195: icmp_seq=2 ttl=64 time=0.320 ms
64 bytes from 192.168.134.195: icmp_seq=3 ttl=64 time=0.572 ms
64 bytes from 192.168.134.195: icmp_seq=4 ttl=64 time=0.142 ms
^C
--- 192.168.134.195 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3045ms
rtt min/avg/max/ndev = 0.142/0.861/2.412/0.908 ms
root@Jasmine:/tmp/pycore.42923/Jasmine.conf#

root@Beia:/tmp/pycore.42923/Beia.conf# ping 192.168.134.226
PING 192.168.134.226 (192.168.134.226) 56(84) bytes of data:
64 bytes from 192.168.134.226: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 192.168.134.226: icmp_seq=2 ttl=64 time=0.444 ms
64 bytes from 192.168.134.226: icmp_seq=3 ttl=64 time=0.356 ms
64 bytes from 192.168.134.226: icmp_seq=4 ttl=64 time=0.951 ms
^C
--- 192.168.134.226 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/ndev = 0.356/0.930/1.970/0.641 ms
root@Beia:/tmp/pycore.42923/Beia.conf#

```

Figura 11: Comandos executados no departamento A e no departamento B

4.3 Pergunta 16

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

4.4 Resposta 16

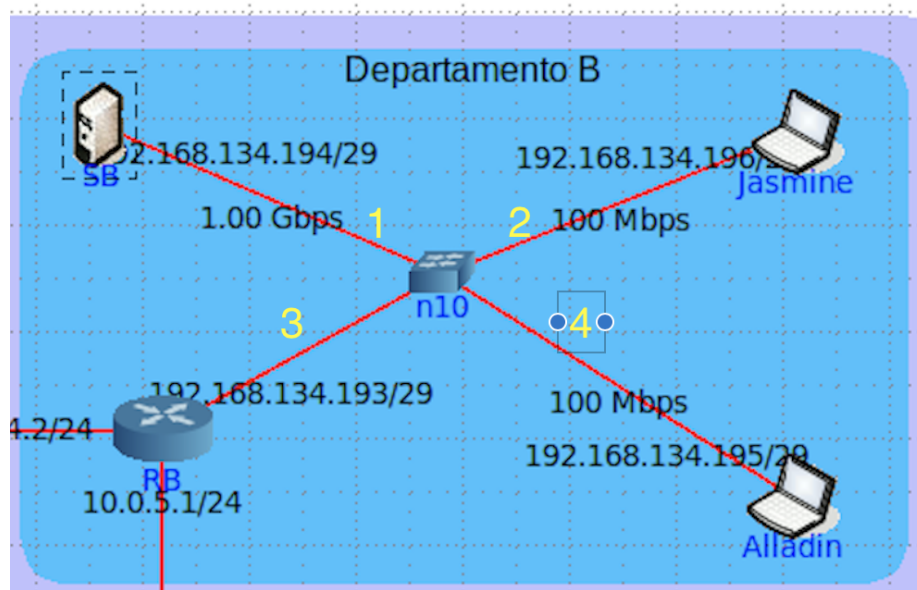


Figura 12: Topologia

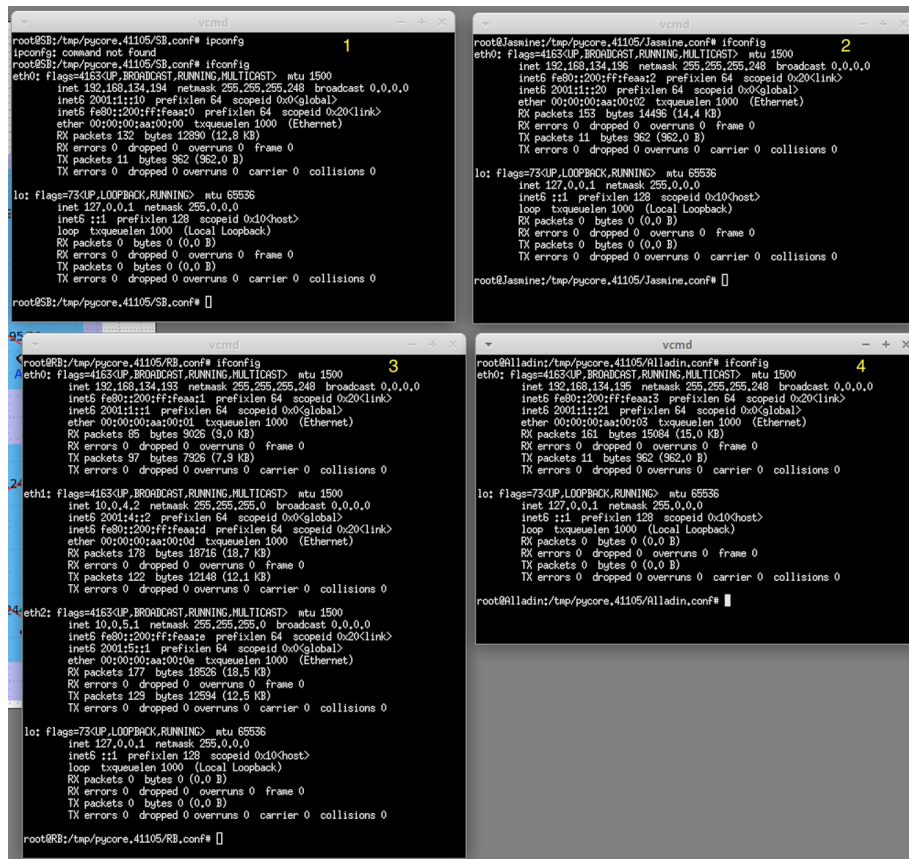


Figura 13: Comando ifconfig

Interface	Endereços Mac	TTL
1	00:00:00:aa:00:00	20
2	00:00:00:aa:00:02	20
3	00:00:00:aa:00:01	20
4	00:00:00:aa:00:03	20

Figura 14: Tabela de comutação do switch

5 Conclusão

A realização deste trabalho prático permitiu aos elementos da equipa de trabalho consolidar os conhecimentos adquiridos nas aulas acerca de captura e análise de tramas *Ethernet*, protocolo ARP e sobre domínios de colisão. Alado a isto, este trabalho permitiu também um maior domínio sobre o uso de aplicações relacionadas com os temas supramencionados.