

RC TP3 PL54

Artur Luís

Carlos Pina

Luís Ferreira

May 2023

Índice

1	Captura e análise de Tramas Ethernet	3
1.1	Questão 1	3
1.2	Questão 2	4
1.3	Questão 3	4
1.4	Questão 4	5
1.5	Questão 5	6
1.6	Questão 6	6
2	Protocolo ARP	7
2.1	Questão 1	8
2.1.1	Alínea A	8
2.1.2	Alínea B	8
2.2	Questão 2	8
2.2.1	Alínea A	9
2.2.2	Alínea B	9
2.2.3	Alínea C	9
2.2.4	Alínea D	9
2.3	Questão 3	10
2.3.1	Alínea A	10
2.3.2	Alínea B	10
2.3.3	Alínea C	10
2.3.4	Alínea D	11
2.4	Questão 4	12
2.5	Questão 5	12
2.6	Questão 6	12
3	Domínios de colisão	13
3.1	Questão 1	13
3.2	Questão 2	13
4	Conclusões	14

1 Captura e análise de Tramas Ethernet

“No seu browser, acesse ao URL <https://alunos.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, SYNACK, ACK ativas).”

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.26.30.116	162.55.131.196	SSL	106	Continuation Data
2	0.056740	162.55.131.196	172.26.30.116	SSL	90	Continuation Data
3	0.110476	172.26.30.116	162.55.131.196	TCP	54	49750 → 443 [ACK] Seq=53 Ack=37 Win=510 Len=0
10	1.712223	172.26.30.116	193.137.9.171	TCP	66	58274 → 443 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	1.735334	193.137.9.171	172.26.30.116	TCP	66	443 → 58274 [SYN, ACK] Seq=1 Ack=1 Win=12500 Len=0 MSS=1250 WS=0 SACK_PERM=1

> Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{80FCE783-659C-4EA3-B946-7FE5000780A9}, Id 0

Ethernet II, Src: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)

Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)

Source: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.26.30.116, Dst: 193.137.9.171

Transmission Control Protocol, Src Port: 58274, Dst Port: 443, Seq: 0, Len: 0

0000 00 34 23 c5 40 00 89 06 c4 bd e5 d6 f2 e0 00 45 00 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0010 09 ab c4 62 01 bb 17 3d fa 13 00 00 00 00 00 02 05 b4 01 03 03 00 01 01

0020 fa f0 95 e9 00 00 02 04 05 b4 01 03 03 00 01 01

0030

0040 04 02

Figure 1: Conexão entre Cliente e Servidor

1.1 Questão 1

“Anotar os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.”

▼ Ethernet II, Src: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)	
> Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)	
> Source: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0)	
Type: IPv4 (0x0800)	

Figure 2: Endereço MAC de Origem

▼ Ethernet II, Src: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)	
> Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)	
> Source: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0)	
Type: IPv4 (0x0800)	

Figure 3: Endereço MAC de Destino

- O Endereço MAC de Origem, que representa o nosso computador é (c4:bd:e5:d6:f2:e0). Como o primeiro a enviar um pedido de acesso é o nosso computador, o primeiro pedido tem como origem o nosso PC. Dessa forma, na 1ª trama capturada podemos ver o endereço de origem que somos nós.

O Endereço de Destino, que representa o servidor da Uminho tem MAC (00:d0:03:ff:94:00).

1.2 Questão 2

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

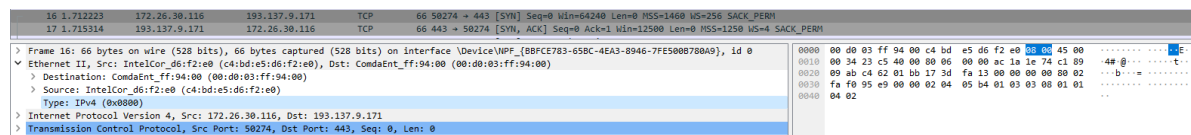


Figure 4: Campo Type: IPv4

- O campo hexadecimal "type" representa o tipo de payload que está encapsulado na trama. Neste caso, como o tipo é 0x0800, isso significa (e é assumido pelo wireshark) que é do tipo IPv4.

1.3 Questão 3

“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, no caso de HTTPS)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.”

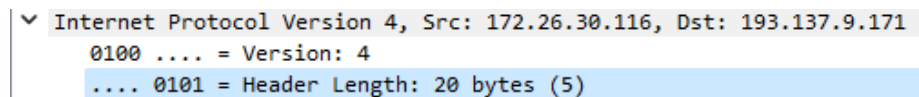


Figure 5: Tamanho cabeçalho IP

- O cabeçalho IP tem 20 bytes.

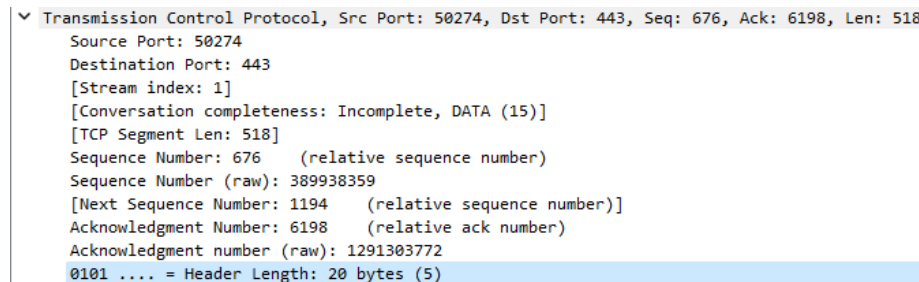


Figure 6: Tamanho cabeçalho TCP

- O cabeçalho TCP tem 32 bytes.

- O tamanho de um cabeçalho Ethernet é de 14 octetos, logo o nº de bytes no Encapsulamento Protocolar é de $20+32+14 = 66$ bytes.

```
▼ Frame 30: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface
  Section number: 1
  > Interface id: 0 (\Device\NPF_{8BFCE783-65BC-4EA3-8946-7FE500B780A9})
  Encapsulation type: Ethernet (1)
  Arrival Time: Apr 27, 2023 17:26:11.174907000 Hora de Verão de GMT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1682612771.174907000 seconds
  [Time delta from previous captured frame: 0.000108000 seconds]
  [Time delta from previous displayed frame: 0.000108000 seconds]
  [Time since reference or first frame: 1.745969000 seconds]
  Frame Number: 30
  Frame Length: 572 bytes (4576 bits)
```

Figure 7: Tamanho cabeçalho Pacote

- Como o tamanho do pacote é de 572 bytes, a sobrecarga imposta pela pilha protocolar é dada pela fórmula $(20+20+14)/572$, que em percentagem corresponde a 9.44%.

“Baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP proveniente do servidor.”

1.4 Questão 4

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

```
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00),
  > Destination: IntelCor_d6:f2:e0 (c4:bd:e5:d6:f2:e0)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Type: IPv4 (0x0800)
```

Figure 8: Endereços de Origem e Destino da Trama

- A fonte tem endereço Ethernet (00:d0:03:ff:94:00), e este endereço corresponde ao router Ethernet ao qual a máquina está conectada.

1.5 Questão 5

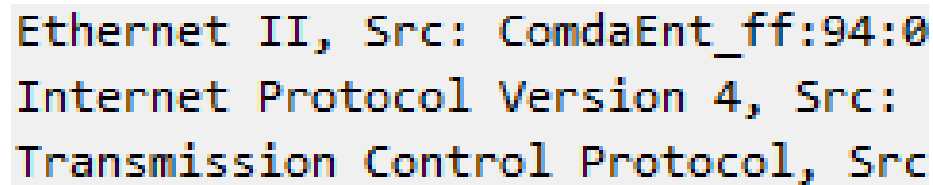
“Qual é o endereço MAC do destino? A que sistema (host) corresponde?”

- O Endereço destino é (c4:bd:e5:d6:f2:e0) e corresponde ao endereço físico da nossa máquina. Como é possível verificar na Fig.8.

1.6 Questão 6

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

Justifique, indicando em que campos dos cabeçalhos capturados se baseou.”



Ethernet II, Src: ComdaEnt_ff:94:0
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src:

Figure 9: Protocolos contidos na Trama

- Como podemos verificar, os protocolos contidos são Ethernet, IPv4 (Internet Protocol Version 4) e TCP (Transmission Control Protocol).

2 Protocolo ARP

“Crie uma topologia de rede com dois departamentos, A e B. O departamento A usará os endereços 192.168.0+54.X/25, e o departamento B 192.168.128+54.X/25, sendo X o decimal atribuído automaticamente pelo CORE.

Adotando a terminologia usada no CORE, considere que o departamento A contém três PCs e um host (servidor) ligados a um switch, que por sua vez liga ao router RA. O departamento B tem três PCs ligados a um hub, que por sua vez liga ao router RB. Os dois routers estão ligados entre si por uma ligação física, cujo endereço de rede é atribuído automaticamente pelo CORE. Todos os links têm uma largura de banda de 200 Mbps. Para facilitar a configuração dos endereços de rede, comece por ligar apenas o switch e o hub aos routers e depois configure os endereços IP das interfaces do router de acordo com a regra definida. Seguidamente ligue os PCs e o servidor ao switch e ao hub, ficando assim automaticamente configurados com os endereços IP desejados.

Selecione um PC de um dos departamentos à sua escolha e inicie a captura de tráfego com o Wireshark do CORE. A partir desse sistema efetue ping para dois PCs localizados na outra rede (departamento). Pare a captura de tráfego no Wireshark e localize o tráfego ARP, usando o filtro arp.”

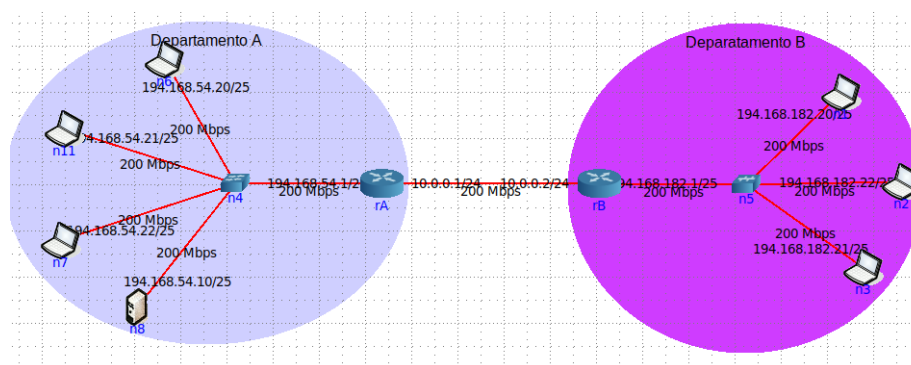


Figure 10: Topologia de rede

2.1 Questão 1

“Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp -a.”

```
root@n11:/tmp/pycore.36883/n11.conf# arp -a
? (194.168.54.1) at 00:00:00:aa:00:00 [ether] on eth0
```

Figure 11: Tabela ARP

2.1.1 Alínea A

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

- Após executar o comando arp -a obtivemos a tabela ARP. A primeira coluna corresponde ao IP do departamento em que foi executado o comando. Na segunda coluna temos o seu endereço MAC.

2.1.2 Alínea B

“Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.”

- Considerando a topologia completa, o equipamento com maior número de entradas na tabela ARP deverá ser o rB, pois foi este o router que teve que comunicar com mais equipamentos. Depois de executar os 2 pings para o departamento B, o n10 comunica com o rA, rA com n10 e rB com o rA, n2 e n3.

2.2 Questão 2

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

```
▶ Frame 33: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface vethb.0.83, id 0
▶ Ethernet II, Src: 00:00:00_aa:00:03 (00:00:00:aa:00:03), 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: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
  Sender IP address: 194.168.54.21
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 194.168.54.1
```

Figure 12: Trama Ethernet

2.2.1 Alínea A

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

- O valor hexadecimal dos endereços MAC origem é 194.168.54.21 e destino é ff:ff:ff:ff:ff:ff (Broadcast).

O endereço de destino ff:ff:ff:ff:ff:ff (Broadcast) é usado quando se pretende enviar um pacote para todos os dispositivos numa rede, em vez de apenas para um dispositivo específico. Ao usar o endereço de broadcast, o pacote é enviado para todos os dispositivos na rede, permitindo que cada dispositivo receba e processe o pacote.

2.2.2 Alínea B

“Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?”

- O campo Tipo tem valor (0x0806), o que indica o uso do protocolo ARP.

2.2.3 Alínea C

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

- A Trama endereça a mensagem a todos os equipamentos na rede (faz broadcast) e tem o tipo ARP (0x8006).

2.2.4 Alínea D

“Explicite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?”

- O *Host* pergunta na rede a quem pertence o endereço IP indicado. A mensagem é enviada a todos os equipamentos na rede. O equipamento com esse endereço IP envia assim o seu endereço MAC diretamente para o *Host* origem.

2.3 Questão 3

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

```
▶ Frame 34: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface vethb.0.83, id 0
▶ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
  ▶ Destination: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
  ▶ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  Type: ARP (0x0806)
  ▼ 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:00:00 (00:00:00:aa:00:00)
    Sender IP address: 194.168.54.1
    Target MAC address: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
    Target IP address: 194.168.54.21
```

Figure 13: Resposta ARP

2.3.1 Alínea A

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

- O valor é 2 e especifica que a mensagem ARP é um reply.

2.3.2 Alínea B

“Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?”

- No cabeçalho Ethernet estão presentes 3 informações, o destino, a fonte e o tipo. O emissor é o equipamento procurado pelo host que emitiu o pedido ARP - Este envia o seu endereço ao host que o procurava.

2.3.3 Alínea C

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

```

root@n11:/tmp/pycore.36883/n11.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 194.168.54.21 netmask 255.255.255.128 broadcast 0.0.0.0
    inet6 2001::21 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:3 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:03 txqueuelen 1000 (Ethernet)
    RX packets 2195 bytes 178726 (178.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 6184 (6.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 340 (340.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 340 (340.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 14: ifconfig

```

root@n11:/tmp/pycore.36883/n11.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 194.168.54.1 0.0.0.0 UG 0 0 0 eth0
194.168.54.0 0.0.0.0 255.255.255.128 U 0 0 0 eth0

```

Figure 15: netstat -rn

```

root@n11:/tmp/pycore.36883/n11.conf# arp
Address HWtype HWaddress Flags Mask Iface
194.168.54.1 ether 00:00:00:aa:00:00 C

```

Figure 16: arp

-

2.3.4 Alínea D

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

- Quando um dispositivo envia uma solicitação ARP (ARP Request) para encontrar outro dispositivo na rede, a mensagem é enviada para todos os dispositivos (broadcast). O dispositivo procurado responde diretamente ao dispositivo que fez a solicitação (unicast), evitando a necessidade de enviar uma

resposta para todos os dispositivos novamente. Isso torna a comunicação mais eficiente e rápida.

2.4 Questão 4

“Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada.”

- O dispositivo guardou na sua tabela ARP a informação sobre como se comunicar com o router após enviar o primeiro "ping". Isso significa que não é preciso continuar a enviar "pings" sucessivos, porque o dispositivo já sabe como se dirigir ao router.

2.5 Questão 5

“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.”

- Podemos verificar que para a camada de ligação lógica o protocolo utilizado é o Ethernet com tamanho de endereços 6. O protocolo utilizado para a camada de rede é o IPv4 e o tamanho dos endereços é de 4.

2.6 Questão 6

“Na situação em que efetua um ping a um PC não local à sua sub-rede, 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 sistema destino (represente apenas os nós intervenientes). Assuma que todas as tabelas ARP se encontram inicialmente vazias.”

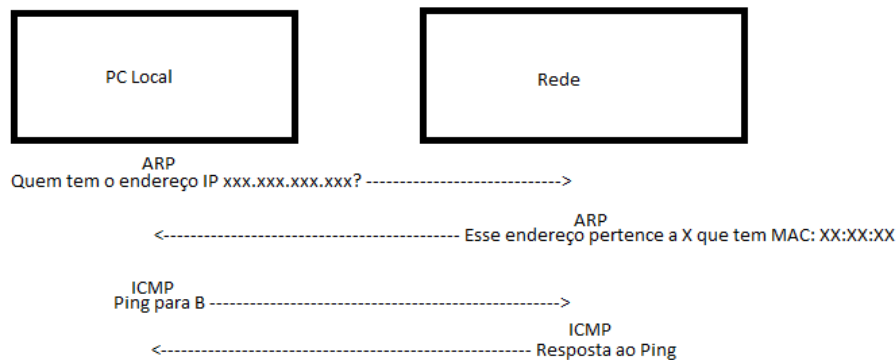


Figure 17: Diagrama De Mensagens

3 Domínios de colisão

“Considere a topologia de rede definida anteriormente.”

3.1 Questão 1

“Através da opção tcpdump, verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando é gerado tráfego intra-departamento (por exemplo, através do comando ping). Que conclui?

Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.”

-

3.2 Questão 2

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

-

4 Conclusões

- Com a realização deste trabalho prático, pudemos aprofundar o nosso conhecimento sobre a Ethernet e o protocolo ARP, aplicando na prática o que foi aprendido nas aulas teóricas. Foi uma oportunidade para consolidar a nossa aprendizagem e compreender melhor como ocorre a comunicação entre dispositivos numa rede.

Além disso, através da análise dos resultados obtidos, pudemos observar como a tabela ARP é essencial para a comunicação entre dispositivos numa rede, permitindo a identificação e resolução de endereços MAC e IP.

Em suma, este trabalho foi de grande importância para o nosso desenvolvimento acadêmico e aprimoramento dos nossos conhecimentos sobre redes de computadores.