

UNIVERSIDADE DO MINHO

Mestrado Integrado em Engenharia Informática



---

# REDES DE COMPUTADORES

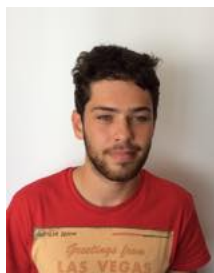
TP3 – Camada de Ligação Lógica: Ethernet e Protocolo ARP

Grupo 46

---



Davide Matos (A80970)



Francisco Freitas (A81580)



Maria Dias (A81611)

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

Origem: f8-32-e4-e6-c7-5a

Destino: 00-0c-29-d2-19-f0

No.	Time	Source	Destination	Protocol	Length	Info
1516	18.059041779	192.168.100.210	193.136.19.40	TCP	74	48042 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM.
1517	18.059338047	193.136.19.40	192.168.100.210	TCP	74	80 → 48040 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146.
1518	18.059364539	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535.
1519	18.059531296	193.136.19.40	192.168.100.210	TCP	74	80 → 48042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146.
1520	18.059545580	192.168.100.210	193.136.19.40	TCP	66	48042 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535.
1521	18.060135555	192.168.100.210	193.136.19.40	HTTP	442	GET / HTTP/1.1
1522	18.060746358	193.136.19.40	192.168.100.210	TCP	66	80 → 48040 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2832.
1523	18.063727768	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=1 Ack=377 Win=30080 Len=1448 TSval=2.
1524	18.063789531	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=1449 Win=32128 Len=0 TSval=1.
1525	18.063828546	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=1449 Ack=377 Win=30080 Len=1448 TSva.
1526	18.063841610	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=2897 Win=35072 Len=0 TSval=1.
1527	18.063958636	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=2897 Ack=377 Win=30080 Len=1448 TSva.
1528	18.063969934	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=4345 Win=37888 Len=0 TSval=1.
1529	18.064071195	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=4345 Ack=377 Win=30080 Len=1448 TSva.
1530	18.064084107	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=5793 Win=40832 Len=0 TSval=1.

▶ Frame 1521: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0  
 ▶ Ethernet II, Src: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a), Dst: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
   ▶ Destination: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
   ▶ Source: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
   Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 192.168.100.210, Dst: 193.136.19.40  
 ▶ Transmission Control Protocol, Src Port: 48040, Dst Port: 80, Seq: 1, Ack: 1, Len: 376  
 ▶ Hypertext Transfer Protocol

```

0000  00 0c 29 d2 19 f0 f8 32 e4 e6 c7 5a 08 00 45 00  ...2...Z..E.
0010  01 ac 96 01 40 00 40 06 a9 1f c0 a8 64 d2 c1 88  ...@...d...
0020  13 28 bb a8 00 50 67 b8 5e 22 7b dd 74 39 00 18  -(...Pg- A" { t9..
0030  00 e5 d5 33 00 00 01 01 08 0a 63 db d9 ad a8 d6  ...3...c.....
  
```

wireshark\_enp2s0\_20181126110713\_ZFPyYO.pcapng      Packets: 2115 · Displayed: 2115 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

2. Identifique a que sistemas se referem. Justifique.

O endereço de origem (f8-32-e4-e6-c7-5a) identifica o endereço MAC da máquina nativa (o *Wireshark* identifica-o como AsustekC). O endereço de destino (00-0c-29-d2-19-f0) refere-se ao endereço MAC do destino, que o *Wireshark* identifica como Vmware, e é a interface que liga a rede em que estamos à rede exterior.

3. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa? O campo Type da trama Ethernet tem o valor 0x0800, que identifica o protocolo IPv4, significando, portanto, que o payload da trama contém um datagrama IP.

▶ Frame 1521: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0  
 ▶ Ethernet II, Src: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a), Dst: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
   ▶ Destination: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
   ▶ Source: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
   Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 192.168.100.210, Dst: 193.136.19.40  
 ▶ Transmission Control Protocol, Src Port: 48040, Dst Port: 80, Seq: 1, Ack: 1, Len: 376  
 ▶ Hypertext Transfer Protocol

4. 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. Até ao caractere “G” vão 66 bytes. Uma vez que o comprimento total da trama é de 442 bytes, o overhead introduzido pela pilha protocolar é de ((66\*100)/442=) 14.93%.

No.	Time	Source	Destination	Protocol	Length	Info
1516	18.059041779	192.168.100.210	193.136.19.40	TCP	74	48042 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
1517	18.059338047	193.136.19.40	192.168.100.210	TCP	74	80 → 48040 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1518	18.059364539	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1519	18.059531296	193.136.19.40	192.168.100.210	TCP	74	80 → 48042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1520	18.059545580	192.168.100.210	193.136.19.40	TCP	66	48042 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1521	18.060135555	192.168.100.210	193.136.19.40	HTTP	442	GET / HTTP/1.1
1522	18.060746358	193.136.19.40	192.168.100.210	TCP	66	80 → 48040 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2832...
1523	18.063727768	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=1 Ack=377 Win=30080 Len=1448 TSval=2...
1524	18.063789531	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=1449 Win=32128 Len=0 TSval=1...
1525	18.063826546	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=1449 Ack=377 Win=30080 Len=1448 TSva...
1526	18.063841610	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=2897 Win=35072 Len=0 TSval=1...
1527	18.063958636	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=2897 Ack=377 Win=30080 Len=1448 TSva...
1528	18.063969934	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=4345 Win=37888 Len=0 TSval=1...
1529	18.064071195	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=4345 Ack=377 Win=30080 Len=1448 TSva...

▶ Frame 1521: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0  
 ▶ Ethernet II, Src: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a), Dst: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
 ▶ Destination: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
 ▶ Source: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 ▶ Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 192.168.100.210, Dst: 193.136.19.40  
 ▶ Transmission Control Protocol, Src Port: 48040, Dst Port: 80, Seq: 1, Ack: 1, Len: 376  
 ▶ Hypertext Transfer Protocol

```

0000  00 0c 29 d2 19 f0 f8 32  e4 e6 c7 5a 08 00 45 00  ... ..2 ..Z..E..
0010  01 ac 96 01 40 00 40 06  a9 1f c0 a8 64 d2 c1 88  ...@.@...d...
0020  13 28 bb a8 00 50 67 b8  5e 22 7b dd 74 39 80 18  (...Pg A" t9...
0030  00 e5 d5 33 00 09 01 01  08 0a 63 db 09 ad a8 d6  ...3...c....
0040  f7 c6 07 4c 50 29 2f 20  48 54 54 50 2f 31 2e 31  ... / HTTP/1.1
0050  00 0a 48 6f 73 74 3a 20  6d 69 65 69 2e 64 69 2e  ..Host: miel.di.
0060  75 6d 69 6e 68 6f 2e 70  74 0d 0a 43 6f 6e 6e 65  uminho.p t: Conne
0070  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76  ction: k eep-aliv
0080  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63  e..Upgra de-Insec
  
```

Bytes 66-68: Request Method (http.request.method)      Packets: 2115 · Displayed: 2115 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

5. Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para detecção de erros não está a ser usado. Em sua opinião, porque será?

Se o campo FCS não aparece na captura da trama, é porque ele não está a ser usado. Normalmente, as NICs, estando numa rede *wired*, não calculam este código de erros, pois o custo do cálculo relativamente à probabilidade de haver erros nestas redes, que é muito baixa, não compensa.

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

O endereço Ethernet da fonte é 00:0c:29:d2:19:f0.

Corresponde ao router da rede à qual estamos ligados.

No.	Time	Source	Destination	Protocol	Length	Info
1614	18.069250043	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=66609 Win=141696 Len=0 TSval...
1615	18.069361024	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=66609 Ack=377 Win=30080 Len=1448 TSv...
1616	18.069366631	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=68057 Win=140800 Len=0 TSval...
1617	18.069492711	193.136.19.40	192.168.100.210	HTTP	1486	HTTP/1.1 200 OK (text/html)
1618	18.069497498	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=69477 Win=139776 Len=0 TSval...
1619	18.091906845	192.168.100.210	193.136.19.40	TCP	74	48044 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
1620	18.092025658	192.168.100.210	193.136.19.40	TCP	74	48046 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
1621	18.092192559	192.168.100.210	193.136.19.40	TCP	74	48048 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
1622	18.092260480	192.168.100.210	193.136.19.40	TCP	74	48050 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM...
1623	18.092580539	193.136.19.40	192.168.100.210	TCP	74	80 → 48044 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1624	18.092602800	192.168.100.210	193.136.19.40	TCP	66	48044 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1625	18.092606312	193.136.19.40	192.168.100.210	TCP	74	80 → 48046 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1626	18.092611281	192.168.100.210	193.136.19.40	TCP	66	48046 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1627	18.092612583	193.136.19.40	192.168.100.210	TCP	74	80 → 48048 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...

▶ Frame 1617: 1486 bytes on wire (11888 bits), 1486 bytes captured (11888 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0), Dst: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 ▶ Destination: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 ▶ Source: Vmware\_d2:19:f0 (00:0c:29:d2:19:f0)  
 ▶ Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.210  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 48040, Seq: 68057, Ack: 377, Len: 1420  
 ▶ (48 Reassembled TCP Segments (69476 bytes): #1523(1448), #1525(1448), #1527(1448), #1529(1448), #1531(1448), #1533(1448), #1535(1448), #1537(1448))  
 ▶ Hypertext Transfer Protocol  
 ▶ Line-based text data: text/html (1573 lines)

Ethernet (eth), 14 bytes      Packets: 2115 · Displayed: 2115 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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

O endereço MAC do destino é f8:32:e4:e6:c7:5a e corresponde à interface ativa do computador.

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

A trama contém os protocolos IPv4 (Internet Protocol Version 4), Ethernet, TCP (Transmission Control Protocol) e HTTP (Hypertext Transfer Protocol), como podemos verificar na captura de ecrã seguinte.

No.	Time	Source	Destination	Protocol	Length	Info
1614	18.069250843	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=66609 Win=141696 Len=0 TSval=...
1615	18.069361024	193.136.19.40	192.168.100.210	TCP	1514	80 → 48040 [ACK] Seq=66609 Ack=377 Win=30080 Len=1448 TSv=...
1616	18.069366631	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=68057 Win=140800 Len=0 TSval=...
1617	18.069492711	193.136.19.40	192.168.100.210	HTTP	1486	HTTP/1.1 200 OK (text/html)
1618	18.069497498	192.168.100.210	193.136.19.40	TCP	66	48040 → 80 [ACK] Seq=377 Ack=69477 Win=139776 Len=0 TSval=...
1619	18.091906845	192.168.100.210	193.136.19.40	TCP	74	48044 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=...
1620	18.092025658	192.168.100.210	193.136.19.40	TCP	74	48046 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=...
1621	18.092192559	192.168.100.210	193.136.19.40	TCP	74	48048 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=...
1622	18.092268480	192.168.100.210	193.136.19.40	TCP	74	48050 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=...
1623	18.092580539	193.136.19.40	192.168.100.210	TCP	74	80 → 48044 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1624	18.092602800	192.168.100.210	193.136.19.40	TCP	66	48044 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1625	18.092606312	193.136.19.40	192.168.100.210	TCP	74	80 → 48046 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...
1626	18.092611281	192.168.100.210	193.136.19.40	TCP	66	48046 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=167535...
1627	18.092612583	193.136.19.40	192.168.100.210	TCP	74	80 → 48048 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146...

▶ Frame 1617: 1486 bytes on wire (11888 bits), 1486 bytes captured (11888 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_d2:19:f0 (08:0c:29:d2:19:f0), Dst: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 ▶ Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.210  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 48040, Seq: 68057, Ack: 377, Len: 1420  
 ▶ [48 Reassembled TCP Segments (69476 bytes): #1523(1448), #1525(1448), #1527(1448), #1529(1448), #1531(1448), #1533(1448), #1535(1448), #1537(1448)]  
 ▶ Hypertext Transfer Protocol  
 ▶ Line-based text data: text/html (1573 lines)

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

A primeira coluna representa o endereço IP (192.168.100.254). A segunda apresenta o endereço MAC (00:0c:29:d2:19:f0) e por fim aparece o tipo (Ethernet).

```
user@user-X555LJ:~$ arp -a
gw.sa.di.uminho.pt (192.168.100.254) at 00:0c:29:d2:19:f0 [ether] on enp2s0
```

10. 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?

Endereço de origem: f8:32:e4:e6:c7:5a.

O endereço destino tem que ser um que seja identificado por todas as máquinas da rede (endereço de broadcast – ff:ff:ff:ff:ff:ff), para que todas possam receber o pedido ARP. Desta forma, a máquina que contenha o endereço contido no pedido (192.168.100.204) irá responder a quem enviou o pedido com o seu endereço MAC, enquanto que as restantes máquinas não respondem.

\*enp2s0

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter  <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2082	28.188196459	AsustekC_a5:06:1d	Broadcast	0x0800	463	IPv4
2083	28.544499996	Cisco_46:85:6a	Spanning-tree-(for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2084	28.595645554	AsustekC_e6:c7:5a	Vmware_d2:19:f0	0x0800	65	IPv4
2085	28.637018885	Vmware_d2:19:f0	AsustekC_e6:c7:5a	0x0800	62	IPv4
2086	29.589294321	AsustekC_00:5c:b1	IPv4mcast_7f:ff:fa	0x0800	179	IPv4
2087	29.899223448	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 192.168.100.204? Tell 192.168.100.210
2088	29.899579057	RealtekS_68:06:6d	AsustekC_e6:c7:5a	ARP	60	192.168.100.204 is at 00:e0:4c:68:06:6d
2089	29.899587627	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2090	30.59059024	Cisco_46:85:6a	Spanning-tree-(for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2091	30.920672262	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2092	31.940646115	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2093	32.101877074	Cisco_46:85:6a	LOOP	60	Reply	
2094	32.545812074	Cisco_46:85:6a	Spanning-tree-(for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2095	32.591978313	AsustekC_00:5c:b1	IPv4mcast_7f:ff:fa	0x0800	179	IPv4

▶ Frame 2087: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

▶ Ethernet II, Src: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)

▶ Source: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)

▶ Type: ARP (0x0806)

▶ Address Resolution Protocol (request)

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

O valor do campo tipo da trama indica o tipo de dados da trama. Neste caso é ARP, como podemos ver na imagem apresentada na questão anterior, o que é assinalado pelo valor hexadecimal 0x0806,

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

O campo ARP opcode tem o valor 1 (em hexadecimal, 0x0001), identificando que se trata de um pedido ARP (request, como indica o próprio campo).

2087 29.899223448	AsustekC_e6:c7:5a	Broadcast	ARP	42 Who has 192.168.100.204? Tell 192.168.100.210
2088 29.899579057	RealtekS_68:06:6d	AsustekC_e6:c7:5a	ARP	60 192.168.100.204 is at 00:e0:4c:68:06:6d
2089 29.899587627	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98 IPv4
2090 30.550059024	Cisco_46:85:6a	Spanning-tree-(for-...	STP	60 Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2091 30.920672262	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98 IPv4
2092 31.940646115	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98 IPv4
2093 32.101877074	Cisco_46:85:6a	Cisco_46:85:6a	LOOP	60 Reply
2094 32.945812074	Cisco_46:85:6a	Spanning-tree-(for-...	STP	60 Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2095 32.591978313	AsustekC_00:5c:b1	IPv4mcast 7f:ff:fa	0x0800	179 IPv4
▶ Frame 2087: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0				
▶ Ethernet II, Src: AsustekC_e6:c7:5a (f8:32:e4:e6:c7:5a), 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: AsustekC_e6:c7:5a (f8:32:e4:e6:c7:5a)				
Sender IP address: 192.168.100.210				
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)				
Target IP address: 192.168.100.204				

13. Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Na mensagem ARP estão contidos endereços de tipo MAC e IP, como podemos constatar na figura seguinte, em que são apresentados os endereços da origem e do destino. Concluímos que não sabemos, neste ponto, qual é o endereço MAC do destino (é, aliás, aquilo que pretendemos descobrir), tendo apenas informação acerca do seu endereço IP. E, por isto, o endereço MAC do destino é 00:00:00:00:00:00.

▶ Frame 2087: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▶ Ethernet II, Src: AsustekC_e6:c7:5a (f8:32:e4:e6:c7:5a), 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: AsustekC_e6:c7:5a (f8:32:e4:e6:c7:5a)
Sender IP address: 192.168.100.210
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.100.204

14. Explícite que tipo de pedido ou pergunta é feita pelo host de origem?

O host de origem pergunta qual é a máquina que possui o endereço IP 192.168.100.204 ("Who has 192.168.100.204?"), para a qual fizemos ping, indicando também o seu endereço IP, para que a máquina que possui esse endereço IP lhe responda com o endereço MAC que lhe corresponde.

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

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

O campo opcode tem o valor 2, especificando que se trata da resposta ao pedido ARP (reply, como o próprio campo indica) anterior.



2087	29.899223448	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 192.168.100.204? Tell 192.168.100.210
2088	29.899579057	RealtekS_68:06:6d	AsustekC_e6:c7:5a	ARP	60	192.168.100.204 is at 00:e0:4c:68:06:6d
2089	29.89957627	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2090	30.550059024	Cisco_46:85:6a	Spanning-tree-(for...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2091	30.920672262	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2092	31.940646115	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2093	32.101877074	Cisco_46:85:6a	Cisco_46:85:6a	LOOP	60	Reply
2094	32.545812074	Cisco_46:85:6a	Spanning-tree-(for...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2095	32.591978313	AsustekC_00:5c:b1	IPv4mcast_7f:ff:fa	0x0800	179	IPv4

▶ Frame 2088: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 ▶ Ethernet II, Src: RealtekS\_68:06:6d (00:e0:4c:68:06:6d), Dst: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 ▼ Address Resolution Protocol (reply)  
   Hardware type: Ethernet (1)  
   Protocol type: IPv4 (0x0800)  
   Hardware size: 6  
   Protocol size: 4  
   Opcode: reply (2)  
   Sender MAC address: RealtekS\_68:06:6d (00:e0:4c:68:06:6d)  
   Sender IP address: 192.168.100.204  
   Target MAC address: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
   Target IP address: 192.168.100.210

- b) Em que posição da mensagem ARP está a resposta ao pedido ARP?  
 A resposta ao pedido ARP é o endereço MAC da origem e encontra-se na posição 23-28bytes, correspondendo à secção “Sender MAC address”.

No.	Time	Source	Destination	Protocol	Length	Info
2085	28.637018885	Vmware_d2:19:f0	AsustekC_e6:c7:5a	0x0800	62	IPv4
2086	29.589294321	AsustekC_00:5c:b1	IPv4mcast_7f:ff:fa	0x0800	179	IPv4
2087	29.899223448	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 192.168.100.204? Tell 192.168.100.210
2088	29.899579057	RealtekS_68:06:6d	AsustekC_e6:c7:5a	ARP	60	192.168.100.204 is at 00:e0:4c:68:06:6d
2089	29.89957627	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2090	30.550059024	Cisco_46:85:6a	Spanning-tree-(for...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2091	30.920672262	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2092	31.940646115	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2093	32.101877074	Cisco_46:85:6a	Cisco_46:85:6a	LOOP	60	Reply
2094	32.545812074	Cisco_46:85:6a	Spanning-tree-(for...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2095	32.591978313	AsustekC_00:5c:b1	IPv4mcast_7f:ff:fa	0x0800	179	IPv4
2096	32.964649773	AsustekC_e6:c7:5a	RealtekS_68:06:6d	0x0800	98	IPv4
2097	34.551070341	Cisco_46:85:6a	Spanning-tree-(for...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 6008 Por...
2098	35.091372413	AsustekC_97:88:ff	IPv6mcast_fb	0x86dd	107	IPv6

▶ Source: RealtekS\_68:06:6d (00:e0:4c:68:06:6d)  
   Type: ARP (0x0806)  
   Padding: 00000000000000000000000000000000  
 ▼ Address Resolution Protocol (reply)  
   Hardware type: Ethernet (1)  
   Protocol type: IPv4 (0x0800)  
   Hardware size: 6  
   Protocol size: 4  
   Opcode: reply (2)  
   Sender MAC address: RealtekS\_68:06:6d (00:e0:4c:68:06:6d)  
   Sender IP address: 192.168.100.204  
   Target MAC address: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
   Target IP address: 192.168.100.210

0000 f8 32 e4 e6 c7 5a 00 e0 4c 68 06 6d 08 06 00 01 2...Z...Lh.m...  
 0010 08 00 06 04 00 02 00 00 00 00 00 00 c0 a8 64 cc .....Lh...d...  
 0020 f8 32 e4 e6 c7 5a c0 a8 64 d2 00 00 00 00 00 00 2...Z...d...  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Sender MAC address (arp.src.hw\_mac), 6 bytes      Packets: 2193 · Displayed: 2193 (100.0%) · Dropped: 0 (0.0%)      Profile: Default

16. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado?  
 Recorrendo ao comando dhcliente que se segue na imagem abaixo, forçamos o pedido de atribuição de um novo IP à interface.

```

user@user-X555LJ:~$ sudo dhclient -v enp2s0
[sudo] password for user:
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp2s0/f8:32:e4:e6:c7:5a
Sending on LPF/enp2s0/f8:32:e4:e6:c7:5a
Sending on Socket/fallback
DHCPREQUEST of 192.168.73.162 on enp2s0 to 255.255.255.255 port 67 (xid=0x221513a1)
DHCNACK from 192.168.100.248 (xid=0xa1131522)
DHCPDISCOVER on enp2s0 to 255.255.255.255 port 67 interval 3 (xid=0x1d248877)
DHCPREQUEST of 192.168.100.210 on enp2s0 to 255.255.255.255 port 67 (xid=0x7788241d)
DHCPOFFER of 192.168.100.210 from 192.168.100.254
DHCPACK of 192.168.100.210 from 192.168.100.254
bound to 192.168.100.210 -- renewal in 150 seconds.
user@user-X555LJ:~$
  
```

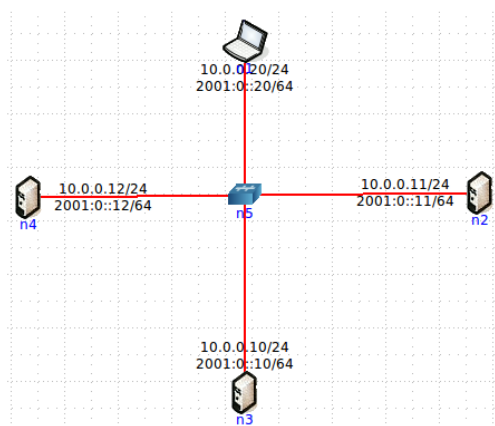
Observando a captura de ecrã seguinte, verificamos que este pedido se distingue dos restantes pedidos ARP por ter o mesmo IP de origem e destino (como podemos ver na primeira imagem, 192.245.10.139), o que nos permite saber se existe algum equipamento na rede com o mesmo endereço IP que o da máquina que envia a mensagem. No caso de existir, seria recebida uma mensagem de resposta, uma vez que o pedido é feito a qualquer equipamento que tenha o IP dado, e, existindo, enviaria uma mensagem ao remetente, indicando que existe. Assim, o objetivo do pedido ARP gratuito é evitar conflitos, verificando se existe alguém com o mesmo endereço IP da fonte. Uma vez que não se obteve resposta, concluímos que não existe mais nenhum host com aquele IP, o que coincide com o resultado esperado.

No.	Time	Source	Destination	Protocol	Length	Info
4	3.466742644	Vmware_d2:19:f0	AsustekC_e6:c7:5a	ARP	60	Who has 192.168.100.210? Tell 192.168.100.254
5	3.466766599	AsustekC_e6:c7:5a	Vmware_d2:19:f0	ARP	42	192.168.100.210 is at f8:32:e4:e6:c7:5a
6	3.493692444	AsustekC_e6:c7:5a	Vmware_d2:19:f0	ARP	42	Who has 192.168.100.254? Tell 192.168.100.210
7	3.494092017	Vmware_d2:19:f0	AsustekC_e6:c7:5a	ARP	60	192.168.100.254 is at 00:0c:29:d2:19:f0
69	34.846365979	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 169.254.10.139? Tell 0.0.0.0
72	36.089800061	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 169.254.10.139? Tell 0.0.0.0
74	37.179016295	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 169.254.10.139? Tell 0.0.0.0
77	39.180328828	AsustekC_e6:c7:5a	Broadcast	ARP	42	Gratuitous ARP for 169.254.10.139 (Request)
79	39.222241690	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 192.168.1.255? Tell 169.254.10.139
89	40.229610053	AsustekC_e6:c7:5a	Broadcast	ARP	42	Who has 192.168.1.255? Tell 169.254.10.139
100	41.180619735	AsustekC_e6:c7:5a	Broadcast	ARP	42	Gratuitous ARP for 169.254.10.139 (Request)

Frame 77: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 Ethernet II, Src: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
 Source: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 Type: ARP (0x0806)  
 Address Resolution Protocol (request/gratuitous ARP)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: request (1)  
 [Is gratuitous: True]  
 Sender MAC address: AsustekC\_e6:c7:5a (f8:32:e4:e6:c7:5a)  
 Sender IP address: 169.254.10.139  
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Target IP address: 169.254.10.139

0000 ff ff ff ff ff f8 32 e4 e6 c7 5a 00 00 .....2...Z...  
 0010 00 00 06 04 00 01 f8 32 e4 e6 c7 5a a9 fe 0a 8b .....2...Z...  
 0020 00 00 00 00 00 00 a9 fe 0a 8b .....  
 Ethernet (eth), 14 bytes  
 Packets: 171 · Displayed: 16 (9.4%) · Dropped: 0 (0.0%) · Profile: Default

17. Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?



Quando o laptop n1 faz ping para o host n2, a mensagem é transmitida para o hub, que a repete para os hosts n2, n3 e n4, e por isso conseguimos ver,

através do comando tcpdump, que todos os hosts receberam várias mensagens ARP de pedido e resposta, embora a mensagem fosse apenas destinada ao n2. Isto deve-se ao facto de os hubs serem dispositivos de interligação que operam a nível físico, ou seja, repetem o sinal que lhes chega através de uma porta de entrada para todas as outras portas, fazendo com que todos os dispositivos recebam a mensagem.

```

root@n4:/tmp/pycore.40307/n4.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
16:08:03.384734 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 1, length 64
16:08:03.384788 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 1, length 64
16:08:04.383703 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 2, length 64
16:08:04.383723 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 2, length 64
16:08:05.382372 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 3, length 64
16:08:05.382392 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 3, length 64
16:08:06.383286 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 4, length 64
16:08:06.383318 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 4, length 64
16:08:08.387225 ARP, Request who-has 10.0.0.20 tell A10, length 28
16:08:08.387236 ARP, Reply 10.0.0.20 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n4:/tmp/pycore.40307/n4.conf#

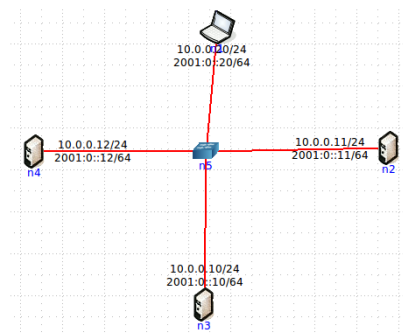
root@n3:/tmp/pycore.40307/n3.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:08:03.384734 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 1, length 64
16:08:03.384781 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 1, length 64
16:08:04.383706 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 2, length 64
16:08:04.383724 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 2, length 64
16:08:05.382375 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 3, length 64
16:08:05.382393 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 3, length 64
16:08:06.383292 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 4, length 64
16:08:06.383319 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 4, length 64
16:08:08.387227 ARP, Request who-has 10.0.0.20 tell A10, length 28
16:08:08.387238 ARP, Reply 10.0.0.20 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n3:/tmp/pycore.40307/n3.conf#

root@n2:/tmp/pycore.40307/n2.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
16:08:03.384740 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 1, length 64
16:08:03.384775 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 1, length 64
16:08:04.383705 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 2, length 64
16:08:04.383718 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 2, length 64
16:08:05.382374 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 3, length 64
16:08:05.382388 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 3, length 64
16:08:06.383289 IP 10.0.0.20 > A10: ICMP echo request, id 149, seq 4, length 64
16:08:06.383310 IP A10 > 10.0.0.20: ICMP echo reply, id 149, seq 4, length 64
16:08:08.387192 ARP, Request who-has 10.0.0.20 tell A10, length 28
16:08:08.387237 ARP, Reply 10.0.0.20 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.40307/n2.conf#

root@n1:/tmp/pycore.40307/n1.conf# ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_req=1 ttl=64 time=0.111 ms
64 bytes from 10.0.0.11: icmp_req=2 ttl=64 time=0.043 ms
64 bytes from 10.0.0.11: icmp_req=3 ttl=64 time=0.041 ms
64 bytes from 10.0.0.11: icmp_req=4 ttl=64 time=0.071 ms
--- 10.0.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2398ms
rtt min/avg/max/ndev = 0.041/0.065/0.111/0.029 ms
root@n1:/tmp/pycore.40307/n1.conf#

```

- Na topologia de rede substitua o hub por um switch. Repita os procedimentos que realizou na pergunta anterior. 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.  
A topologia fica com o aspeto seguinte:



Como podemos ver na imagem que se segue, ao substituir o hub por um switch, foram obtidos resultados diferentes. Desta vez, quando o laptop n1 faz ping para o host n2, a mensagem é primeiramente transmitida para o switch e este, ao contrário do que acontece com o hub, envia a mensagem para o host pretendido em vez de repetir o sinal



para todos os hosts a ele ligados. Assim, não vemos tráfego nos hosts n3 e n4, para além da captura do pacote ARP de broadcast. Este pacote deve-se ao facto de, quando uma trama chega a um switch e não consegue comutar com base nas entradas da tabela do switch, este difunde a mensagem através de todas as suas interfaces.

Os switches evitam colisões, limitando o envio das mensagens apenas para o destino pretendido. Ao ter várias portas para cada interface, os switches asseguram vários domínios de colisão, diminuindo a probabilidade destas acontecerem.

Os hubs, por outro lado, repetem a mensagem para todos os nodos ligados a ele, usando um único canal, o que aumenta em muito a probabilidade de ocorrerem colisões. Quando estas acontecem, é necessário proceder ao reenvio das mensagens, pelo que esta topologia pode tornar-se num grande peso para a rede.

The image shows three terminal windows from a network simulation. The top-left window (n1) shows a ping command to 10.0.0.11 and its statistics. The top-right window (n2) shows a tcpdump capture of several ICMP echo requests and replies between 10.0.0.20 and 10.0.0.11. The bottom window (n4) shows a tcpdump capture of an ARP request for 10.0.0.20. The windows are titled 'root@n1:/tmp/pycore.40307/n1.conf', 'root@n2:/tmp/pycore.40307/n2.conf', and 'root@n4:/tmp/pycore.40307/n4.conf'.

```

root@n1:/tmp/pycore.40307/n1.conf# ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_req=1 ttl=64 time=0.160 ms
64 bytes from 10.0.0.11: icmp_req=2 ttl=64 time=0.079 ms
64 bytes from 10.0.0.11: icmp_req=3 ttl=64 time=0.074 ms
64 bytes from 10.0.0.11: icmp_req=4 ttl=64 time=0.090 ms

--- 10.0.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.074/0.098/0.160/0.036 ms
root@n1:/tmp/pycore.40307/n1.conf#

root@n2:/tmp/pycore.40307/n2.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
^C16:13:34.507773 ARP, Request who-has A10 tell 10.0.0.20, length 28
16:13:34.507823 ARP, Reply A10 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
16:13:34.507861 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 1, length 64
16:13:34.507866 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 1, length 64
16:13:35.509516 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 2, length 64
16:13:35.509539 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 2, length 64
16:13:36.508513 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 3, length 64
16:13:36.508536 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 3, length 64
16:13:37.508170 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 4, length 64
16:13:37.508194 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 4, length 64
16:13:39.507950 ARP, Request who-has 10.0.0.20 tell A10, length 28
16:13:39.508032 ARP, Reply 10.0.0.20 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
12 packets captured
12 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.40307/n2.conf#

root@n4:/tmp/pycore.40307/n4.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
^C16:13:34.507776 ARP, Request who-has A10 tell 10.0.0.20, length 28
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@n4:/tmp/pycore.40307/n4.conf#

```

## CONCLUSÃO

Com a resolução deste trabalho, ficamos a compreender mais intimamente o funcionamento da camada de ligação lógica, tendo estudado atentamente a tecnologia Ethernet – o seu funcionamento e análise sucinta de tramas deste tipo -, bem como o protocolo ARP, que nos proporcionou um melhor entendimento dos mecanismos de mapeamento entre os endereços de rede e os endereços de uma tecnologia de ligação de dados.

Por fim, aprendemos acerca do funcionamento de dispositivos de interligação que operam a nível físico, mais especificamente o hub e o switch. Em relação a estes, vimos que o funcionamento de cada um tem características próprias, sendo que, dependendo do caso, um pode ser mais vantajoso do que outro, tal como vimos neste trabalho que o switch era mais apropriado para a questão apresentada.