

Redes de Computadores

Trabalho Prático N°3

Nível de Ligação Lógica: Ethernet e Protocolo ARP

Alexandra Candeias, Pedro Araújo, and Tiago Ribeiro

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89521,a70699,a76420}@alunos.uminho.pt

1 Introdução

A elaboração do presente relatório tem o intuito de responder às questões colocadas ao longo do guião do *Trabalho Prático 3* (TP3), cujo o foco é o estudo da tecnologia *Ethernet* e do protocolo *Address Resolution Protocol* (ARP). As questões realizadas têm como objectivo primordial a consolidação de conhecimentos sobre este dois tópicos.

Assim sendo, na secção 2 são expostas as questões presentes no TP3 e apresentadas respostas às mesmas. Na secção 3, são realizadas as devidas conclusões.

2 Questões e Respostas

Esta secção tem o intuito de responder às questões colocadas no guião do TP3.

2.1 Captura e análise de Tramas Ethernet

No.	Time	Source	Destination	Protocol	Length	Info
19	3.989180	172.26.22.142	216.58.215.142	QUIC	1392	Client Hello
20	3.910461	172.26.22.142	193.137.9.150	DNS	82	Standard query 0x8e68 A wpad.eduroam.uminho.pt
21	3.910627	172.26.22.142	193.137.9.150	TCP	66	59536 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	3.912022	193.137.16.65	172.26.22.142	DNS	136	Standard query response 0x8e68 No such name A wpad.eduroam.uminho.pt SOA dns.uminho.pt
23	3.912508	172.26.22.142	172.26.255.255	NDNS	92	Name query NB WPAD-000
24	3.913141	172.26.22.142	224.0.0.251	NDNS	70	Standard query 0x0000 A wpad.local, "Q" question
25	3.913600	fe80::fdb8:febb:15b::ff02::fb	ff02::fb	NDNS	90	Standard query 0x0000 A wpad.local, "Q" question
26	3.913937	fe80::fdb8:febb:15b::ff02::11:3	ff02::11:3	LLMNR	84	Standard query 0x5973 A wpad
27	3.914845	172.26.22.142	224.0.0.252	LLMNR	64	Standard query 0x5973 A wpad
28	3.915005	193.137.9.150	172.26.22.142	TCP	66	80 → 59536 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1250 WS=256 SACK_PERM=1
29	3.915090	172.26.22.142	193.137.9.150	TCP	54	59536 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
30	3.915546	172.26.22.142	193.137.9.150	HTTP	513	GET / HTTP/1.1
31	3.928316	193.137.9.150	172.26.22.142	HTTP	186	HTTP/1.1 301
32	3.921306	193.137.9.150	172.26.22.142	TCP	54	80 → 59536 [FIN, ACK] Seq=133 Ack=600 Win=262400 Len=0
33	3.921370	172.26.22.142	193.137.9.150	TCP	54	59536 → 80 [ACK] Seq=460 Ack=134 Win=66048 Len=0
34	3.923497	172.26.22.142	193.137.9.150	TCP	54	59536 → 80 [FIN, ACK] Seq=460 Ack=134 Win=66048 Len=0
35	3.925062	193.137.9.150	172.26.22.142	TCP	54	80 → 59536 [ACK] Seq=134 Ack=461 Win=262400 Len=0
36	3.928983	172.26.22.142	193.137.9.150	TCP	66	59537 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37	3.931221	193.137.9.150	172.26.22.142	TCP	66	443 → 59537 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1250 WS=256 SACK_PERM=1
38	3.931282	172.26.22.142	193.137.9.150	TCP	54	59537 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0

> Frame 38: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF{SCDAEF33-B1AB-482E-944A-460AA09FB87}, id 0
> Ethernet II, Src: IntelCor_86:2d:c4 (30:3a:64:86:2d:c4), Dst: CondaEnt_ff:94:00 (00:00:03:ff:94:00)
> Destination: CondaEnt_ff:94:00 (00:00:03:ff:94:00)
> Source: IntelCor_86:2d:c4 (30:3a:64:86:2d:c4)
> Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.26.22.142, Dst: 193.137.9.150
> Transmission Control Protocol, Src Port: 59536, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
> Hypertext Transfer Protocol

Fig. 1.

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

R: Como é possível visualizar na Figura 1, o endereço *MAC* de origem é o 30:3a:64:86:2d:c4 e de destino 00:d0:03:ff:94:00.

2. Identifique a que sistemas se referem. Justifique.

R: Os endereços *MAC* anteriormente referidos presentes na Figura 1, são, respetivamente, o do host local e o do router do primeiro nó.

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

R: O valor do *type* em hexadecimal é 0x0800, isto significa que irá ser usado o protocolo IPv4 para a transmissão desta trama.

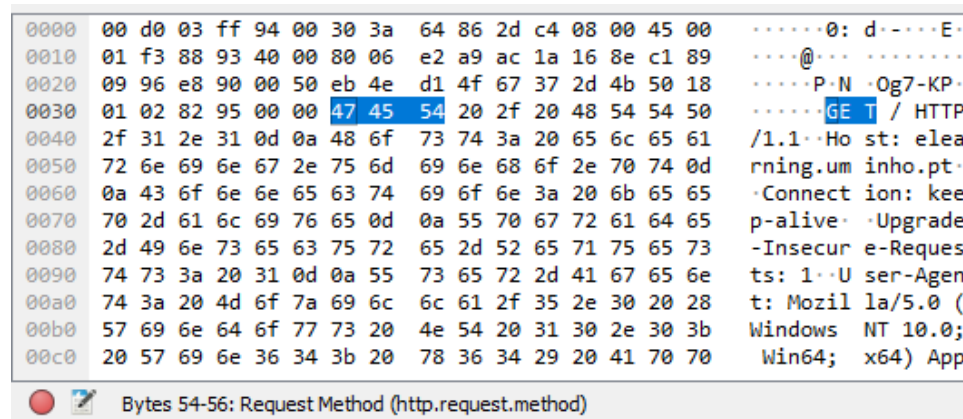


Fig. 2.

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.

R: Como observável na Figura 2, serão usados 54 Bytes desde o início da trama até ao caractere “G”. De modo a calcular o *overhead* usar-se-à o quociente entre o total de Bytes que a trama possui e os Bytes de cabeçalho, i.e., *overhead*. Neste caso o total de Bytes da trama é 512 Bytes, temos então um *overhead*, em percentagem, de $(54/512) * 100 = 10.5\%$.

5. Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)).

R: Não foram detetadas tramas com erros, através da verificação do campo FCS, uma vez que o *WireShark* ignora todas as tramas com erros.

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

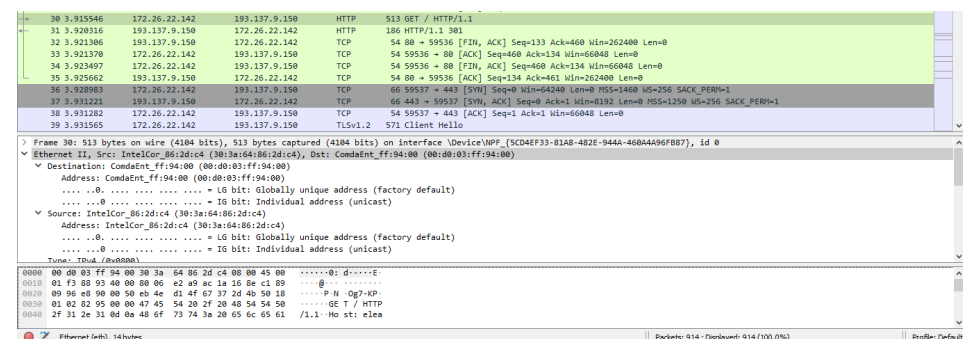


Fig. 3.

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

R: Como representado pela Figura 3, o endereço *Ethernet* da fonte é o 30:3a:64:86:2d:c4. Este corresponde ao endereço da máquina nativa.

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

R: Recorrendo de novo à Figura 3, o endereço *MAC* de destino é o 00:d0:03:ff:94:00 e corresponde ao endereço do router.

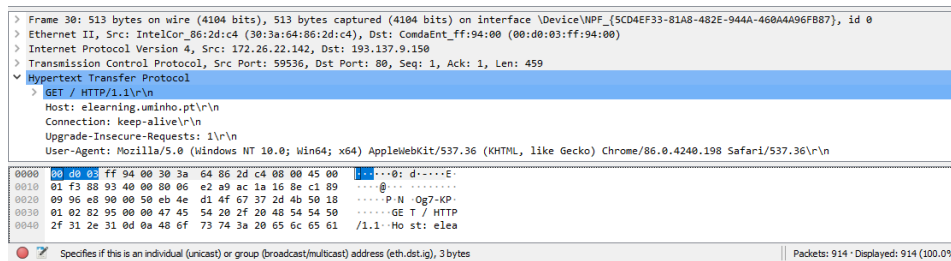


Fig. 4.

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

R: Na Figura 4, a encapsular a trama recebida são usados os protocolos seguintes: HTTP (Hypertext Transfer Protocol), TCP (Transmission Control Protocol) e IP (Internet Protocol).

2.2 Protocolo ARP

```
Interface: 192.168.56.1 --- 0x4
Internet Address      Physical Address      Type
192.168.56.255        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

Interface: 172.26.22.142 --- 0xa
Internet Address      Physical Address      Type
172.26.254.254        00-d0-03-ff-94-00    dynamic
172.26.255.255        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
```

Fig. 5. Resultado do comando `arp -a`

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

R: Seguindo a Figura 5, observamos que a coluna *Internet Address* corresponde ao endereço *IPv4* que corresponde a cada *IP* um endereço *MAC*. A coluna do *Physical Address*

corresponde por sua vez a endereços *MAC* que foram descobertos ao longo das várias transmissões de tramas. A coluna *Type* corresponde ao tipo de linha adicionada, isto é, se o registo adicionado é do tipo estático ou dinâmico.

```
C:\WINDOWS\system32>ping 172.26.74.74

Pinging 172.26.74.74 with 32 bytes of data:
Reply from 172.26.22.142: Destination host unreachable.

Ping statistics for 172.26.74.74:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Control-C
^C
```

Fig. 6. Limitação após a tentativa de implementação do comando ping

```
C:\WINDOWS\system32>ping 172.26.74.74

Pinging 172.26.74.74 with 32 bytes of data:
Reply from 172.26.22.142: Destination host unreachable.

Ping statistics for 172.26.74.74:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Control-C
^C
```

Fig. 7. Inexistência de resposta ao ARP Request

Devido à existência de limitações na *Rede Eduroam* não é possível obter a resposta ao comando *ping*, como observado na Figura 6 que em consequência não irá permitir ter acesso à resposta dada pelo ARP request, Figura 7. Deste modo é necessário o uso do emulador *CORE* de forma a colmatar tais limitações.

```
C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

Interface: 192.168.56.1 --- 0x4
    Internet Address      Physical Address        Type
    224.0.0.22            01-00-5e-00-00-16      static
    239.255.255.250       01-00-5e-7f-ff-fa      static

Interface: 172.26.22.142 --- 0xa
    Internet Address      Physical Address        Type
    224.0.0.22            01-00-5e-00-00-16      static
    239.255.255.250       01-00-5e-7f-ff-fa      static
```

Fig. 8. Execução do comando arp -d * e resultado obtido

No.	Time	Source	Destination	Protocol	Length	Info
604	25.216907126	00:00:00:aa:00:12		0x0800	100	IPv4
605	25.216934368	00:00:00:aa:00:12		0x0800	100	IPv4
606	25.357466778	9a:26:3a:59:80:a0		0x86dd	72	IPv6
607	25.357486295	9a:26:3a:59:80:a0		0x86dd	72	IPv6
608	25.357495445	9a:26:3a:59:80:a0		0x86dd	72	IPv6
609	26.243031173	00:00:00:aa:00:12		0x0800	100	IPv4
610	26.243058596	00:00:00:aa:00:12		0x0800	100	IPv4
611	26.368501500	00:00:00:aa:00:14	44 Who has 130.71.96.3? Tell 130.71.96.1	ARP	44	
612	26.368525057	00:00:00:aa:00:12	44 130.71.96.3 is at 00:00:00:aa:00:12	ARP	44	
613	26.368535471	00:00:00:aa:00:12	44 130.71.96.3 is at 00:00:00:aa:00:12	ARP	44	
614	26.368550032	00:00:00:aa:00:12		0x0800	100	IPv4
615	27.264577384	00:00:00:aa:00:12		0x0800	100	IPv4
616	28.288414368	00:00:00:aa:00:12		0x0800	100	IPv4
617	28.288441845	00:00:00:aa:00:12		0x0800	100	IPv4
618	29.312565229	00:00:00:aa:00:12		0x0800	100	IPv4
619	29.312592580	00:00:00:aa:00:12		0x0800	100	IPv4
620	30.336791988	00:00:00:aa:00:12		0x0800	100	IPv4
621	30.336819460	00:00:00:aa:00:12		0x0800	100	IPv4
622	30.336819460	00:00:00:aa:00:12		0x0800	100	IPv4

▶ Frame 611: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0						
Linux cooked capture						
▼ 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:00:14 (00:00:00:aa:00:14)						
Sender IP address: 130.71.96.1						
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)						
Target IP address: 130.71.96.3						

0000	00 03 00 01 00 06 00 00 00 aa 00 14 00 00 08 066
0010	00 01 08 00 06 04 00 01 00 00 00 aa 00 14 82 47G

Frame (frame), 44 bytes

Packets: 1188 · Displayed: 1188 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Fig. 9.

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?

R: O endereço origem encontra-se identificado como 00:00:00:aa:00:14. Por sua vez o endereço de destino, identificado como endereço Broadcast, assume o valor 00:00:00:00:00:00. Este identificador associado ao destino foi atribuído por default, uma vez que, numa fase inicial o host não tem conhecimento de qual o real endereço MAC do destinatário. Neste sentido, é necessário fazer este pedido em Broadcast de modo a que o destino se identifique perante o pedido do seu endereço MAC.

No.	Time	Source	Destination	Protocol	Length	Info
607	25.357486295	9a:26:3a:59:80:a0		0x86dd	72	IPv6
608	25.357495445	9a:26:3a:59:80:a0		0x86dd	72	IPv6
609	26.243031173	00:00:00:aa:00:12		0x0800	100	IPv4
610	26.243058596	00:00:00:aa:00:12		0x0800	100	IPv4
611	26.368501500	00:00:00:aa:00:14	44 Who has 130.71.96.3? Tell 130.71.96.1	ARP	44	
612	26.368525057	00:00:00:aa:00:12	44 130.71.96.3 is at 00:00:00:aa:00:12	ARP	44	
613	26.368535471	00:00:00:aa:00:12	44 130.71.96.3 is at 00:00:00:aa:00:12	ARP	44	
614	26.368550032	00:00:00:aa:00:12		0x0800	100	IPv4
615	27.264577384	00:00:00:aa:00:12		0x0800	100	IPv4
616	28.288414368	00:00:00:aa:00:12		0x0800	100	IPv4
617	28.288441845	00:00:00:aa:00:12		0x0800	100	IPv4
618	29.312565229	00:00:00:aa:00:12		0x0800	100	IPv4
619	29.312592580	00:00:00:aa:00:12		0x0800	100	IPv4
620	30.336791988	00:00:00:aa:00:12		0x0800	100	IPv4
621	30.336819460	00:00:00:aa:00:12		0x0800	100	IPv4
622	30.727285129	00:00:00:aa:00:03	44 Who has 10.0.1.1? Tell 10.0.1.2	ARP	44	
623	30.727315354	00:00:00:aa:00:03	44 Who has 10.0.1.1? Tell 10.0.1.2	ARP	44	
624	30.727285129	00:00:00:aa:00:03	44 Who has 10.0.1.1? Tell 10.0.1.2	ARP	44	

▶ Frame 611: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0						
Linux cooked capture						
Packet type: Unicast to another host (3)						
Link-layer address type: 1						
Link-layer address length: 6						
Source: 00:00:00:aa:00:14 (00:00:00:aa:00:14)						
Unused: 0000						
Protocol: ARP (0x0806)						
▼ Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						

0000	00 03 00 01 00 06 00 00 00 aa 00 14 00 00 08 066
0010	00 01 08 00 06 04 00 01 00 00 00 aa 00 14 82 47G
0020	00 01 00 00 00 00 00 00 82 47 00 03G

Link-layer address type (sl.hatype), 2 bytes

Packets: 1188 · Displayed: 1188 (100.0%)

Fig. 10.

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

R: Usando a Figura 10 como referência, valor do tipo da trama em hexadecimal é *0x0806* e indica que se trata de uma trama do tipo *ARP*.

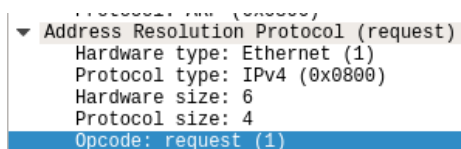


Fig. 11. ARP Request

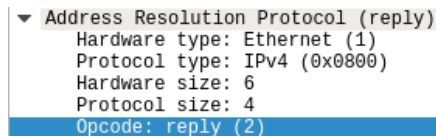


Fig. 12. ARP Reply

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

R: Analisando a Figura 11 é possível observar que o campo *Opcode* se encontra com o valor 1, indicando tratar-se de um pedido ARP. No caso da Figura 12, onde este campo se encontra com o valor 2, tratando-se de uma ARP reply. Como observável na Figura 10, na mensagem ARP estão contidos os endereços MAC do host fonte e do Broadcast, respetivamente. Aquando da executado de um pedido ARP, é enviado o MAC associado ao pedido, uma vez que, inicialmente não se sabe qual o endereço MAC que executou o envio do mesmo. Assim, como não se sabe em que endereço MAC se encontra o destino, é necessário enviar esta trama com o endereço MAC em Broadcast.

611	26.368373827	00:00:00:aa:00:14	ARP	44	Who has 130.71.96.3? Tell 130.71.96.1
612	26.368501500	00:00:00:aa:00:14	ARP	44	Who has 130.71.96.3? Tell 130.71.96.1
613	26.368525957	00:00:00:aa:00:12	ARP	44	130.71.96.3 is at 00:00:00:aa:00:12
614	26.368535471	00:00:00:aa:00:12	ARP	44	130.71.96.3 is at 00:00:00:aa:00:12
615	27.264550032	00:00:00:aa:00:12	0x0800	100	IPv4
616	27.264577384	00:00:00:aa:00:12	0x0800	100	IPv4
617	28.288414368	00:00:00:aa:00:12	0x0800	100	IPv4
618	28.288441845	00:00:00:aa:00:12	0x0800	100	IPv4
619	29.312565229	00:00:00:aa:00:12	0x0800	100	IPv4
Packet type: Unicast to another host (3)					
Link-layer address type: 1					
Link-layer address length: 6					
Source: 00:00:00:aa:00:12 (00:00:00:aa:00:12)					
Unused: 0060					
Protocol: 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:00:12 (00:00:00:aa:00:12)					
Sender IP address: 130.71.96.3					
Target MAC address: 00:00:00:aa:00:14 (00:00:00:aa:00:14)					
Target IP address: 130.71.96.1					
0000	00 03 00 01 00 06 00 00	00 aa 00 12 06 6b 08 06K..		
0010	00 01 08 00 06 04 00 02	00 00 00 aa 00 12 82 47G		
0020	00 03 00 00 00 aa 00 14	82 47 60 01G		
Opcode (arp.opcode), 2 bytes					

Fig. 13.

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

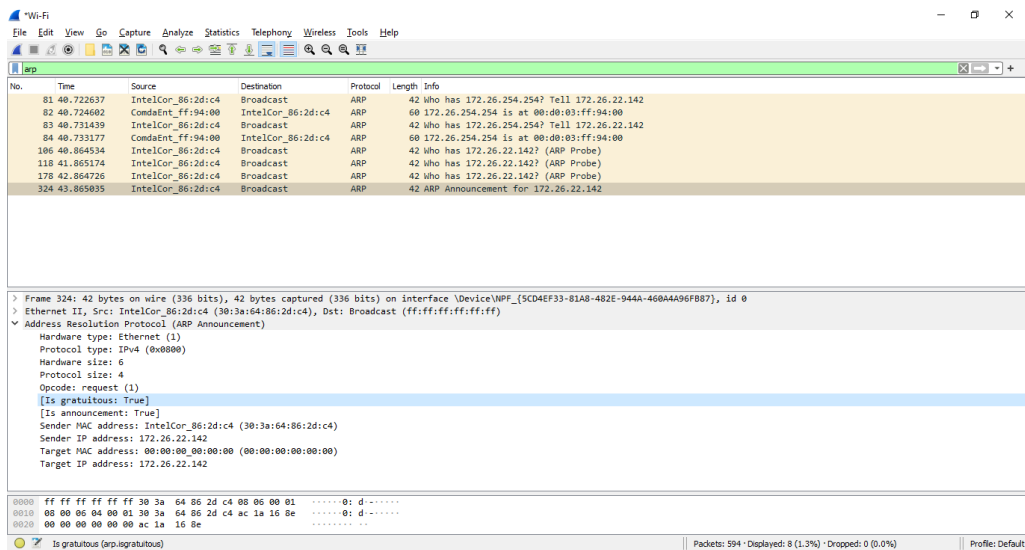
R: A pergunta colocada é “Who has 130.71.96.3?” sendo que a resposta é “Tell 130.71.96.1”. Com esta pergunta e, consequente resposta, obtém-se o endereço MAC do destino, sendo este também registado nas tabelas ARP dos routers ligados ao host fonte.

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

a: O valor do *Opcode* é reply (2) que especifica o código da operação a ser transmitida.

b: A mensagem encontra-se logo após o pedido ARP (ARP request).

2.3 ARP Gratuito



No.	Time	Source	Destination	Protocol	Length	Info
81	40.722637	IntelCor_86:2d:c4	Broadcast	ARP	42	who has 172.26.254.254? Tell 172.26.22.142
82	40.724602	ComdaEnt_ff:94:00	IntelCor_86:2d:c4	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
83	40.731439	IntelCor_86:2d:c4	Broadcast	ARP	42	who has 172.26.254.254? Tell 172.26.22.142
84	40.733177	ComdaEnt_ff:94:00	IntelCor_86:2d:c4	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
106	40.864534	IntelCor_86:2d:c4	Broadcast	ARP	42	who has 172.26.22.142? (ARP Probe)
118	41.865174	IntelCor_86:2d:c4	Broadcast	ARP	42	who has 172.26.22.142? (ARP Probe)
178	42.864726	IntelCor_86:2d:c4	Broadcast	ARP	42	who has 172.26.22.142? (ARP Probe)
324	43.865035	IntelCor_86:2d:c4	Broadcast	ARP	42	ARP Announcement for 172.26.22.142

Frame 324: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5CD4EF33-81A8-482E-944A-460A4A96F8B7}, id 0
Ethernet II, Src: IntelCor_86:2d:c4 (30:3a:64:86:2d:c4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (ARP Announcement)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: True]
[Is announcement: True]
Sender MAC address: IntelCor_86:2d:c4 (30:3a:64:86:2d:c4)
Sender IP address: 172.26.22.142
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.22.142

0000 ff ff ff ff ff 30 3a 64 86 2d c4 00 00 00 010: d-----
0010 00 00 04 00 01 30 3a 64 86 2d c4 ac 1a 16 8e0: d-----
0020 00 00 00 00 00 ac 1a 16 8e
Is gratuitous (arp.isgratuitous) Packets: 594 · Displayed: 8 (1.3%) · Dropped: 0 (0.0%) Profile: Default

Fig. 14.

15. 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?

R: O pacote de pedido de ARP gratuito inicia na trama número 106, como observável pela Figura 14, e inicia perguntando se o IP já atribuído à máquina é válido e/ou se já existe em alguma interface na rede. Depois de confirmar que o IP é válido, é então anunciado a toda a rede o IP atribuído à interface da máquina. O que difere de um pedido ARP normal é um campo adicional/flag que identifica o mesmo como ARP gratuito. Este pedido não necessita de uma resposta pois só está a anunciar qual o endereço MAC do IP da máquina atual.

2.4 Domínios de Colisão

16. 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 gera 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.

R:

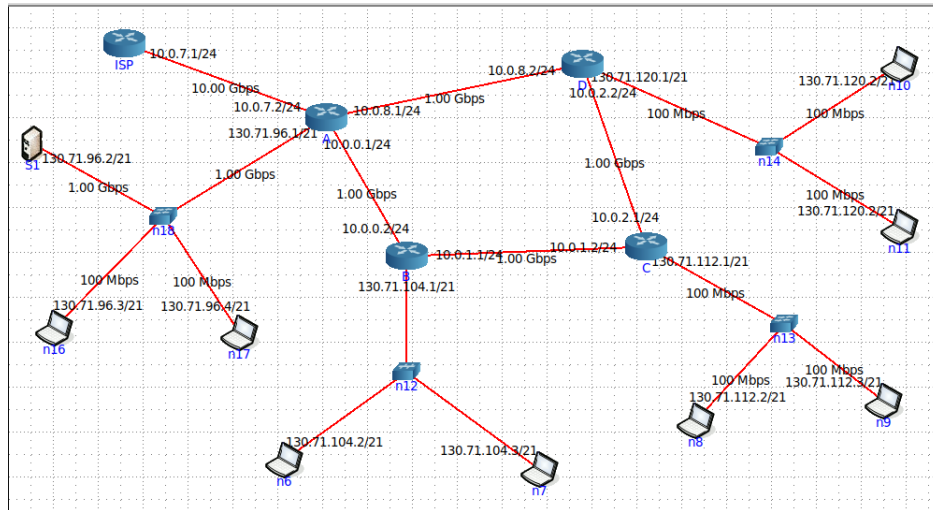


Fig. 15.

Recordando a Topologia efetuada no TP2, Figura 15, é possível observar a substituição do switch do departamento B por um repetidor(hub).

```

root@n8: /tmp/pycore.42383/n8.conf
root@n8: /tmp/pycore.42383/n8.conf# ping 130.71.96.3
PING 130.71.96.3 (130.71.96.3) 56(84) bytes of data.
64 bytes from 130.71.96.3: icmp_seq=1 ttl=61 time=0.217 ms
64 bytes from 130.71.96.3: icmp_seq=2 ttl=61 time=0.268 ms
^C
--- 130.71.96.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.217/0.242/0.268/0.029 ms
root@n8: /tmp/pycore.42383/n8.conf# ping 130.71.104.3
PING 130.71.104.3 (130.71.104.3) 56(84) bytes of data.
64 bytes from 130.71.104.3: icmp_seq=1 ttl=62 time=0.188 ms
64 bytes from 130.71.104.3: icmp_seq=2 ttl=62 time=0.376 ms
^C
--- 130.71.104.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.188/0.282/0.376/0.094 ms
root@n8: /tmp/pycore.42383/n8.conf#

```

Fig. 16.

Executando o comando ping, Figura 16, do host n8 do departamento C para, numa primeira instância, o servidor S1 do departamento A e, em seguida um ping para o host n6 do departamento B, concluímos os seguintes resultados:


```
root@n6: /tmp/pycore.42383/n6.conf
root@n6: /tmp/pycore.42383/n6.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
^C11:01:21.934682 IP 130.71.104.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:21.935402 IP6 fe80::200:ff:feaa:16 > ff02::5: OSPFv3, Hello, length 36
11:01:23.922518 IP6 fe80::200:ff:feaa:15 > ip6-allrouters: ICMP6, router solicit
ation, length 16
11:01:31.934922 IP 130.71.104.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:31.938633 IP6 fe80::200:ff:feaa:16 > ff02::5: OSPFv3, Hello, length 36
11:01:33.480563 ARP, Request who-has 130.71.104.3 tell 130.71.104.1, length 28
11:01:33.480610 ARP, Reply 130.71.104.3 is-at 00:00:00:aa:00:15 (oui Ethernet),
length 28
11:01:33.480625 IP 130.71.112.2 > 130.71.104.3: ICMP echo request, id 28, seq 1,
length 64
11:01:33.480673 IP 130.71.104.3 > 130.71.112.2: ICMP echo reply, id 28, seq 1, l
ength 64
11:01:34.482388 IP 130.71.112.2 > 130.71.104.3: ICMP echo request, id 28, seq 2,
length 64
11:01:34.482545 IP 130.71.104.3 > 130.71.112.2: ICMP echo reply, id 28, seq 2, l
ength 64
11:01:38.515144 ARP, Request who-has 130.71.104.1 tell 130.71.104.3, length 28
11:01:38.515374 ARP, Reply 130.71.104.1 is-at 00:00:00:aa:00:16 (oui Ethernet),
length 28
13 packets captured
13 packets received by filter
0 packets dropped by kernel
root@n6: /tmp/pycore.42383/n6.conf#
```

Fig. 17.

No departamento A, como o comutador é um switch, o servidor S1 não obteve qualquer trama direccionada aos hosts do seu departamento, como é possível verificar na Figura 17

```
root@S1: /tmp/pycore.42383/S1.conf
root@S1: /tmp/pycore.42383/S1.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol d
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 b
^C11:00:21.918563 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 4
11:00:21.947455 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:00:31.922116 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:00:31.950961 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:00:32.721349 IP6 fe80::200:ff:feaa:e > ip6-allrouters: ICMP6, rou
tion, length 16
11:00:41.923545 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:00:41.960928 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:00:50.047535 ARP, Request who-has 130.71.96.3 tell 130.71.96.1, le
11:00:51.925407 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:00:51.970794 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:00:57.297497 IP6 fe80::200:ff:feaa:f > ip6-allrouters: ICMP6, rou
tion, length 16
11:01:01.925776 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:01.977706 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:01:03.441564 IP6 fe80::200:ff:feaa:10 > ip6-allrouters: ICMP6, rou
tion, length 16
11:01:04.461489 IP6 fe80::c039:cfff:fe8a:4b3f.mdns > ff02::fb.mdns: 0
QM)? _ipps._tcp.local. PTR (QM)? _ipps._tcp.local. (45)
11:01:07.373134 IP6 fe80::408:89ff:feb8:85fb.mdns > ff02::fb.mdns: 0
M)? _ipps._tcp.local. PTR (QM)? _ipps._tcp.local. (45)
11:01:11.926624 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:11.985853 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:01:21.936604 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:21.995554 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:01:23.922227 IP6 fe80::408:89ff:feb8:85fb > ip6-allrouters: ICMP6,
icitation, length 16
11:01:31.937182 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:31.998263 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le
11:01:40.305999 IP6 fe80::c039:cfff:fe8a:4b3f > ip6-allrouters: ICMP6
licitation, length 16
11:01:41.937977 IP 130.71.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:01:42.003074 IP6 fe80::200:ff:feaa:11 > ff02::5: OSPFv3, Hello, le

26 packets captured
26 packets received by filter
0 packets dropped by kernel
root@S1: /tmp/pycore.42383/S1.conf#
```

Fig. 18.

Enquanto que no departamento B, como o comutador é um repetidor (hub), no host n6, é observável a chegada de tramas redirecionadas aos hosts vizinhos deste departamento, isto é, tramas respectivas ao host n7.

Conclui-se que um switch é uma ferramenta mais indica para redireccionar tráfego e assim torna mais fácil o controlo de colisões, uma vez que o repetidor (hub) simplesmente se encontra a “repetir” todo o tráfego que chega ao mesmo.

3 Conclusões

Com este trabalho foi possível aprofundar o conhecimento sobre a Ethernet e respetivos pedidos de comunicação através do protocolo ARP. O desenvolvimento do trabalho associado ao presente relatório envolveu a utilização do simulador de redes *CORE*, e da ferramenta de captura e análise de tramas *Wireshark*. A utilização conjunta destas ferramentas permitiu a clara observação das técnicas de encapsulamento usadas para transferência de processos, com foco primordial no protocolo ARP. Foi possível averiguar as técnicas associadas a este protocolo no que toca à informação dos endereços envolvidos, bem como à análise de pedidos de pedidos e respostas do mesmo. A análise do funcionamento do protocolo ARP Gratuito permitiu evidenciar as diferenças de operação entre estes protocolos, tendo sido a mais fundamental a ausência da necessidade de uma resposta.

Este trabalho permitiu salientar os benefícios da utilização de redes Ethernet, nomeadamente associados à facilidade da comunicação e transmissão de informação, bem como o papel fundamental dos protocolos ARP para o seu correto funcionamento.