

Redes de Computadores

Trabalho Prático 3: Nível de Ligação Lógica: Ethernet e Protocolo ARP

Ana Rita Peixoto, Sara Queirós, and Sofia Santos

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89612,a89491,a89615}@alunos.uminho.pt

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 <http://elearning.uminho.pt>.

Pare a captura do Wireshark.

Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o começo da respectiva mensagem HTTP RESPONSE proveniente do servidor.

No sentido de proceder à análise do tráfego, selecione a trama Ethernet que contém a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP está no interior de um segmento TCP que é transportado num datagrama IP que, por sua vez, está encapsulado no campo de dados de uma 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 HTTP GET.

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 use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o mínimo detalhe necessário para responder à pergunta.

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

Endereço MAC da origem: fc:01:7c:9b:c3:4b

Endereço MAC do destino: 00:d0:03:ff:94:00

No.	Time	Source	Destination	Protocol	Length	Info
564	10.423256360	172.26.87.84	194.210.238.74	HTTP	761	GET /filestreamingservice/files/a136d294-e546-408a-bb32-
601	10.437739983	194.210.238.74	172.26.87.84	HTTP	804	HTTP/1.1 200 OK (application/x-chrome-extension)
658	11.072394288	193.137.9.150	172.26.87.84	HTTP	198	HTTP/1.1 301

Frame 657: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface wlo1, id 0
 Ethernet II, Src: NonHalPr_9b:c3:4b (fc:01:7c:9b:c3:4b), Dst: ComdaEnt_ff:94:00 (00:00:03:ff:94:00)
 Destination: ComdaEnt_ff:94:00 (00:00:03:ff:94:00)
 Source: NonHalPr_9b:c3:4b (fc:01:7c:9b:c3:4b)
 Type: IPv4 (0x0800)

Fig. 1. Endereços MAC da mensagem HTTP GET.

Exercício 2. Identifique a que sistemas se referem. Justifique.

A origem refere-se ao nosso computador e o destino refere-se ao servidor do *elearning.uminho.pt*. Podemos verificar isto através do comando *ip link*, que nos permite consultar o endereço MAC do nosso computador.

```
ip link
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT group default qlen 1000
    link/ether fc:01:7c:9b:c3:4b brd ff:ff:ff:ff:ff:ff
    altnam wlp2s0
```

Fig. 2. Endereço MAC do computador, obtido através do comando *ip link***Exercício 3.** Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

O valor do campo Type é 0x0800, tal como podemos observar na fig. 1, e representa o protocolo de camada superior utilizado, neste caso IPv4.

Exercício 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.

66 bytes.

$66/487 = 13.55\%$ de overhead

0000	00 d0 03 ff 94 00 fc 01 7c 9b c3 4b 08 00 45 00K..E..
0010	01 e2 14 78 40 00 40 06 56 10 ac 1a 57 54 c1 89	...x@.@..V...WT..
0020	09 96 9f 64 00 50 42 c8 90 1d 5b b8 c7 40 80 18	...d PB...[...@..
0030	01 f6 35 ed 00 00 01 01 08 0a f0 be 1c ea b3 16	..5.....
0040	95 82 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20 65 6c 65 61 72 6e 69 6e	..Host: elearnin
0060	67 2e 75 6d 69 6e 68 6f 2e 70 74 0d 0a 43 6f 6e	g.uminho .pt..Con
0070	6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c	nection: keep-al
0080	69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	ive..Upg rade-Ins
0090	65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Re quests:

Bytes 66-68: Request Method (http.request.method)

Fig. 3. O caractere ASCII "G" corresponde ao byte 66. Como a contagem começa a partir do 0 este é o 67º byte.

Exercício 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)).

Através do uso de um *display filter*, podemos ver que não foi detetada nenhuma trama com erros, isto é, nenhuma trama contém o campo FCS.

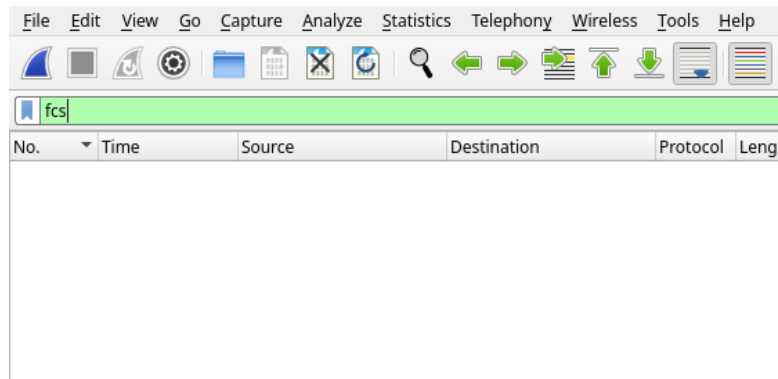


Fig. 4. Resultado de aplicar o *display filter* "fcs" (o filtro é *case insensitive*).

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

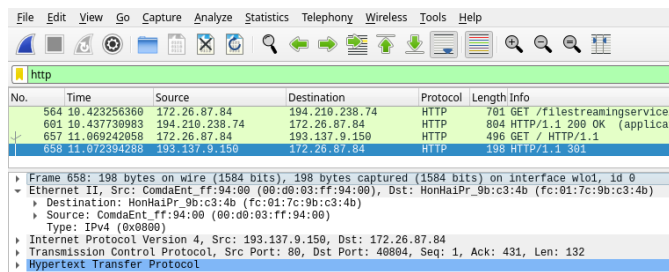


Fig. 5. Trama que contém o primeiro byte da resposta HTTP.

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

O endereço Ethernet da fonte é 00:d0:03:ff:94:00 e corresponde ao *default gateway* da rede local. Como o servidor não se encontra na rede local, não é diretamente alcançável por nós, logo as tramas serão trocadas entre o nosso computador e o *default gateway*, ao invés de ser diretamente com o servidor.

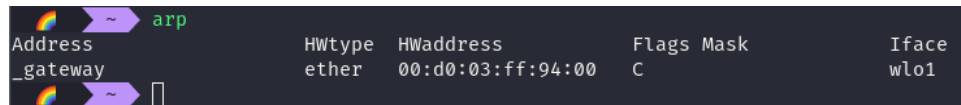
Exercício 7. Qual é o endereço MAC do destino? A que sistema corresponde?

O endereço MAC do destino é fc:01:7c:9b:c3:4b e corresponde à interface ethernet do nosso computador.

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

Ethernet, IPv4 e TCP.

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



Address	HWtype	HWaddress	Flags	Mask	Iface
_gateway	ether	00:d0:03:ff:94:00	C		wlo1

Fig. 6. Tabela ARP do nosso computador.

A coluna *Address* corresponde ao endereço, neste caso apenas temos o *gateway* da rede local. A coluna *HWtype* diz-nos o tipo de protocolo de camada física usado, e a coluna *HWaddress* o endereço MAC, neste caso endereço Ethernet visto que o protocolo de camada física também é do tipo Ethernet. 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 este registo foi obtido dinamicamente pelo protocolo ARP, e não introduzido manualmente. A coluna *Mask* corresponde à máscara de subrede. Por último, a coluna *Iface* dá-nos a interface de rede, no nosso caso wlo1.

Exercício 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?

O endereço MAC origem é 74:70:fd:b4:83:45 e o endereço destino é ff:ff:ff:ff:ff:ff (endereço de *broadcast*). O endereço destino utilizado é o de *broadcast* porque a máquina que envia o *ARP request* necessita de saber qual o endereço MAC destino. Assim, envia a mensagem para o endereço de *broadcast* (o que significa que envia para todas as interfaces) e espera uma resposta da máquina destino com o seu endereço MAC. Assim que receber a resposta, adiciona o seu valor à tabela ARP.

```

▼ Ethernet II, Src: IntelCor_b4:83:45 (74:70:fd:b4:83:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_b4:83:45 (74:70:fd:b4:83:45)
    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: IntelCor_b4:83:45 (74:70:fd:b4:83:45)
  Sender IP address: 172.26.53.225
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254

```

Fig. 7. Pedido ARP.

Alínea b) Em que posição da mensagem ARP está a resposta ao pedido ARP ?

Está presente no campo *Sender MAC address*.

Exercício 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?

É possível identificar que o pedido ARP é gratuito através da flag "*Is gratuitous*", que está assinalada a *true*. No caso do pedido ARP gratuito, os campos "*Sender IP address*" e "*Target IP address*" são iguais.

```

▼ Ethernet II, Src: IntelCor_b4:83:45 (74:70:fd:b4:83:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_b4:83:45 (74:70:fd:b4:83:45)
  Type: ARP (0x0806)
▼ 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_b4:83:45 (74:70:fd:b4:83:45)
  Sender IP address: 172.26.53.225
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.53.225

```

Fig. 10. Pedido ARP gratuito.

Exercício 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.

Como é possível ver na figura abaixo, no departamento B, onde a rede é partilhada, devido ao uso de um repetidor, o computador n13 (130.56.104.3) consegue ver as tramas enviadas pelo computador n14 (130.56.104.2), nomeadamente o *echo request* e o *echo reply* entre este e o computador com endereço 130.56.104.4, resultado do comando *ping 130.56.104.4* executado por n14. Por outro lado, no departamento A, onde a rede é comutada, devido ao uso de um *switch*, o computador n10 (130.56.96.3) não captura as tramas enviadas pelo computador n9 (130.56.96.2) ao servidor s1 (130.56.96.4). São capturadas outras tramas, mas não têm nada a ver com o comando *ping 130.56.96.4* executado por n9.

```

[root@n10 n10.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
20:14:31.878894 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
20:14:31.882316 IP n10.42527 > 192.168.1.1.domain: 5384+ PTR? 5.0.0.224.in-addr.arpa. (40)
20:14:31.882485 IP _gateway > n10: ICMP net 192.168.1.1 unreachable, length 76
20:14:31.882583 IP n10.44787 > 192.168.1.1.domain: 5384+ PTR? 5.0.0.224.in-addr.arpa. (40)
20:14:31.882724 IP _gateway > n10: ICMP net 192.168.1.1 unreachable, length 76
20:14:31.883666 IP n10.55832 > 192.168.1.1.domain: 62483+ PTR? 1.1.168.192.in-addr.arpa. (42)
20:14:33.879834 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
^C20:14:34.105407 IPo fe80::208:ff:feaa:8 > ff02::5: OSPFv3, Hello, length 36

8 packets captured
25 packets received by filter
0 packets dropped by kernel
[root@n10 n10.conf]#

[root@n9 n9.conf]# ping 130.56.96.4
PING 130.56.96.4 (130.56.96.4) 56(84) bytes of data.
64 bytes from 130.56.96.4: icmp_seq=1 ttl=64 time=0.319 ms
64 bytes from 130.56.96.4: icmp_seq=2 ttl=64 time=0.335 ms
64 bytes from 130.56.96.4: icmp_seq=3 ttl=64 time=0.316 ms
64 bytes from 130.56.96.4: icmp_seq=4 ttl=64 time=0.340 ms
64 bytes from 130.56.96.4: icmp_seq=5 ttl=64 time=0.321 ms
^C
--- 130.56.96.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 0.316/0.326/0.340/0.009 ms
[root@n9 n9.conf]#

[root@n13 n13.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
20:14:32.601085 IP 130.56.104.2 > 130.56.104.4: ICMP echo request, id 54623, seq 1, length 64
20:14:32.601261 IP 130.56.104.4 > 130.56.104.2: ICMP echo reply, id 54623, seq 1, length 64
^C20:14:32.603737 IP n13.54711 > 192.168.1.1.domain: 7282+ PTR? 4.104.56.130.in-addr.arpa. (43)

3 packets captured
36 packets received by filter
2 packets dropped by kernel
[root@n13 n13.conf]#

[root@n14 n14.conf]# ping 130.56.104.4
PING 130.56.104.4 (130.56.104.4) 56(84) bytes of data.
64 bytes from 130.56.104.4: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 130.56.104.4: icmp_seq=2 ttl=64 time=0.338 ms
64 bytes from 130.56.104.4: icmp_seq=3 ttl=64 time=0.339 ms
64 bytes from 130.56.104.4: icmp_seq=4 ttl=64 time=0.352 ms
64 bytes from 130.56.104.4: icmp_seq=5 ttl=64 time=0.341 ms
64 bytes from 130.56.104.4: icmp_seq=6 ttl=64 time=0.370 ms
^C
--- 130.56.104.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5061ms
rtt min/avg/max/mdev = 0.338/0.351/0.370/0.013 ms
[root@n14 n14.conf]#

```

Fig. 11. Comandos *tcpdump* e *ping* executados no departamento A (em cima) e no departamento B (em baixo).

1 Conclusão

Com este trabalho prático conseguimos consolidar os temas abordados nas aulas teóricas relativos à camada de ligação lógica, mais especificamente o uso da tecnologia Ethernet e do protocolo ARP. Desta forma é possível verificar que estas temáticas têm aplicações práticas úteis e importantes, e não são apenas matéria para memorizar. Podemos ver também a importância destas tecnologias na nossa sociedade atual, devido à quantidade enorme de dispositivos que as utilizam para o seu correto funcionamento.