
Redes - TP3

TRABALHO REALIZADO POR:

CARLOS MIGUEL LUZIA DE CARVALHO

RUBEN CÉSAR FERREIRA LUCAS

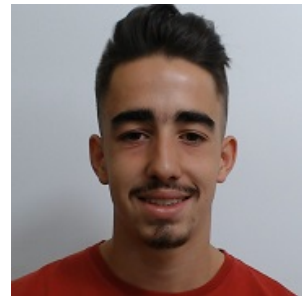
PAULO SILVA SOUSA



A89605
Carlos Carvalho



A89487
Ruben Lucas



A89465
Paulo Sousa

Índice

1	Captura e análise de Tramas Ethernet	1
2	Protocolo ARP	4
3	ARP Gratuito	7
4	Domínios de colisão	9
5	Conclusão	11

1 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.

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

No.	Time	Source	Destination	Protocol	Length	Info
8	0.160648	172.26.71.54	193.137.9.150	HTTP	427	GET / HTTP/1.1
9	0.165462	193.137.9.150	172.26.71.54	HTTP	198	HTTP/1.1 301

> Frame 9: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface en0, id 0
✓ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
> Destination: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
> Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.71.54
> Transmission Control Protocol, Src Port: 80, Dst Port: 49649, Seq: 1, Ack: 362, Len: 132
> Hypertext Transfer Protocol

Endereço MAC destino → a4:83:e7:e1:e9:30

Endereço MAC origem → 00:d0:03:ff:94:00

2. Identifique a que sistemas se referem. Justifique.

No caso do destino o endereço físico é referente ao router com que se está a comunicar. Relativamente á origem, o endereço físico refere-se á máquina que está a ser utilizada (ao nosso computador).

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

Como podemos ver na figura a cima (alinea 1) o Type é 0x0800 o que significa que a camada superior está a usar o protocolo IPv4.

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.

```
> Frame 8: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface en0, :
> Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:
> Internet Protocol Version 4, Src: 172.26.71.54, Dst: 193.137.9.150
> Transmission Control Protocol, Src Port: 49649, Dst Port: 80, Seq: 1, Ack: 1, Len: 361
< Hypertext Transfer Protocol
  < GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: elearning.uminho.pt\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML
    Accept-Language: pt-pt\r\n
0000  00 d0 03 ff 94 00 a4 83 e7 e1 e9 30 08 00 45 02  ....0..E.
0010  01 9d 00 00 40 00 40 06 7a e9 ac 1a 47 36 c1 89  ....@.@.z...G6..
0020  09 96 c1 f1 00 50 e6 86 09 47 76 89 0b 33 80 18  ....P...Gv...3..
0030  08 02 16 92 00 00 01 01 08 0a 0a fc 46 1f fc 06  .........F...
0040  9e a2 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 55 70 67  g.uminho .pt..Upg
0070  72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65  rade-Ins ecur-Re
```

Sendo que o 'G' aparece na linha 0x0040 no byte caracterizado por 47 temos 66 bytes desde o início até ao carater 'G'. Relativamente a percentagem da sobrecargaria introduzida pela pilha protocolar, uma vez que sabemos através do parametro Frame que a trama tem 427 bytes é aproximadamente $15,45 \rightarrow (66/427)*100$

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)).

```
> Frame 8: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface en0, id 0
< Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Source: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 172.26.71.54, Dst: 193.137.9.150
  > Transmission Control Protocol, Src Port: 49649, Dst Port: 80, Seq: 1, Ack: 1, Len: 361
  > Hypertext Transfer Protocol
```

Como podemos ver na imagem acima, o campo FCS não aparece no campo Ethernet logo não existem tramas com erros.

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

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

No.	Time	Source	Destination	Protocol	Length	Info
8	0.160648	172.26.71.54	193.137.9.150	HTTP	427	GET / HTTP/1.1
9	0.165462	193.137.9.150	172.26.71.54	HTTP	198	HTTP/1.1 301


```
> Frame 8: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
> Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
> Source: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
> Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.26.71.54, Dst: 193.137.9.150
> Transmission Control Protocol, Src Port: 49649, Dst Port: 80, Seq: 1, Ack: 1, Len: 361
> Hypertext Transfer Protocol
```

Como podemos ver na figura o endereço ethernet da fonte é a4:83:e7:e1:e9:30 e corresponde ao endereço físico do router com que estamos a comunicar.

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

Como podemos ver na figura do exercício 6, o endereço ethernet do destino é 00:d0:03:ff:94:00 e corresponde ao endereço físico da interface ativo do nosso computador.

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

Como podemos ver na imagem, os protocolos contidos na trama são Hypertext Transfer Protocol (HTTP), Internet Protocol Version 4 (IPV4), Ethernet II e Transmission Control Panel (TCP).

2 Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP. Verifique o conteúdo da cache ARP do seu computador.

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

```
~ 13:23:07
> arp -a
? (172.26.254.254) at 0:d0:3:ff:94:0 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
```

Para observar o protocolo ARP em operação, apague novamente a cache ARP e assegure-se que o cache do browser está vazia. Inicie a captura de tráfego com o Wireshark, e aceda a <http://alunos.uminho.pt>. Efectue também um ping para um host da sala de aula que esteja a ser usado por outro grupo. Pare a captura de tráfego e tente localizar o tráfego ARP. Se necessário, limite os protocolos visíveis apenas a protocolos abaixo do nível IP. Para tal, seleccione Analyze->Enabled Protocols e remova a selecção da opção IPv4 e IPv6. Responda às seguintes perguntas:

```
~ 13:30:20
> sudo arp -d -a
Password:
172.26.254.254 (172.26.254.254) deleted
224.0.0.251 (224.0.0.251) deleted

~ 3s 13:30:28
> arp -a
```

Cache esvaziada

No.	Time	Source	Destination	Protocol	Length	Info
30	8.169483	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.71.54
31	8.178094	ComdaEnt_ff:94:00	Apple_e1:e9:30	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

>	Frame 30: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
>	Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
>	Destination: Broadcast (ff:ff:ff:ff:ff:ff)
>	Source: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
>	Type: ARP (0x0806)
>	Address Resolution Protocol (request)

Para realizar o comando ping teríamos de estar ligados à rede do DI.

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?

```
> Frame 30: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

O endereço de origem é a4:83:e7:e1:e9:30 e o endereço de destino é ff:ff:ff:ff:ff:ff. Este endereço de destino é utilizado uma vez que o nosso dispositivo não está conectado ao dispositivo ao qual queremos enviar a mensagem, logo, temos de utilizar o endereço de broadcast para enviar a mensagem a todos os dispositivos. Assim, o dispositivo pretendido consegue responder com o seu MAC adress.

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

Como é observável na figura da alinea acima o campo type tem o valor 0x0806 o que indica que camada acima está a usar o protocolo ARP.

12. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? (Se necessário, consulte a RFC do protocolo ARP <http://tools.ietf.org/html/rfc826.html>).

```
> Frame 30: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), 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: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  Sender IP address: 172.26.71.54
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254
```

Conseguimos perceber que se trata efetivamente de um pedido ARP porque, na imagem acima, está descrito que se trata de um request.

O ARP contém endereços IP e Mac. Concluimos que o protocolo ARP permite converter um endereço IP no endereço Mac da interface ativa respetiva.

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

Não conseguimos fazer o ping porque estavam a usar o primeiro ARP do Router. Sendo assim, não conseguimos responder a esta pergunta.

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

No.	Time	Source	Destination	Protocol	Length	Info
30	8.169483	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.71.54
31	8.178094	ComdaEnt_ff:94:00	Apple_e1:e9:30	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
<pre> > Frame 31: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0 < Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_e1:e9:30 (a4:83:e7:e1:e9:30) > Destination: Apple_e1:e9:30 (a4:83:e7:e1:e9:30) > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00) 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: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00) Sender IP address: 172.26.254.254 Target MAC address: Apple_e1:e9:30 (a4:83:e7:e1:e9:30) Target IP address: 172.26.71.54 </pre>						

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

```
> Frame 31: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0
✓ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  > Destination: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: ARP (0x0806)
    Padding: 0000000000000000000000000000000000000000
✓ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
Opcode: reply (2)
  Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Sender IP address: 172.26.254.254
  Target MAC address: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  Target IP address: 172.26.71.54
```

O campo opcode tem o valor 2 e significa que o endereço 172.26.254.254 recebe a mensagem de request e está a comunicar o seu endereço mac de volta.

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

```
0000 a4 83 e7 e1 e9 30 00 d0 03 ff 94 00 08 06 00 01 00000000
0010 08 00 06 04 00 02 00 d0 03 ff 94 00 ac 1a fe fe 00000000
0020 a4 83 e7 e1 e9 30 ac 1a 47 36 00 00 00 00 00 00 00000000
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00000000
```

Como podemos ver na figura, a resposta ao pedido ARP está entre 23-28 bytes.

3 ARP Gratuito

Um ARP Gratuito envolve o envio de um ARP request ou ARP reply gratuito, i.e. um host faz um pedido ou uma resposta ARP sem que, segundo a especificação ARP (RFC826), haja necessidade de o fazer. Este procedimento, embora possa parecer desnecessário, aporta várias vantagens ao funcionamento da rede.

Uma vantagem imediata é permitir a deteção de conflitos de endereços IP na rede local. Assim, um ARP gratuito é usado primariamente para um host determinar se um outro host na rede tem o mesmo endereço IP que o originador do pedido. Todos os hosts enviam um ARP gratuito independentemente do endereço IP lhe ter sido atribuído ou não dinamicamente. Quando um host se liga a uma rede e recebe o endereço IP, por exemplo via servidor DHCP (Dynamic Host Configuration Protocol), ou mesmo quando possui um endereço IP estático, o host envia, pelo menos, um pedido ARP gratuito.

Adicionalmente, o envio de um ARP gratuito permite informar os hosts e/ ou switches da rede local sobre um endereço MAC particular, i.e. equivale a anunciar um novo endereço MAC para que todos os sistemas na rede possam atualizar as suas tabelas ARP.

Arranque o Wireshark na sua máquina nativa e inicie a captura de dados. Desligue e volte a ligar a sua ligação à rede local, ou force o pedido de atribuição de um novo endereço IP à interface em uso. Pare a captura de tráfego. Utilize o filtro de visualização ARP para facilitar a identificação dos pacotes respetivos.

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?

No.	Time	Source	Destination	Protoc ~	Length	Info
133	38.802484	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.71.54? (ARP Probe)
136	39.123064	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.71.54? (ARP Probe)
137	39.443550	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.71.54? (ARP Probe)
138	39.765284	Apple_e1:e9:30	Broadcast	ARP	42	ARP Announcement for 172.26.71.54
139	40.087464	Apple_e1:e9:30	Broadcast	ARP	42	ARP Announcement for 172.26.71.54
140	40.408369	Apple_e1:e9:30	Broadcast	ARP	42	ARP Announcement for 172.26.71.54
141	40.418044	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.71.54
142	40.421604	ComdaEnt_ff:94:00	Apple_e1:e9:30	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
143	40.462326	Apple_e1:e9:30	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.71.54
144	40.465370	ComdaEnt_ff:94:00	Apple_e1:e9:30	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

```
> Frame 140: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: Apple_e1:e9:30 (a4:83:e7:e1:e9:30), 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: Apple_e1:e9:30 (a4:83:e7:e1:e9:30)
  Sender IP address: 172.26.71.54
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.71.54
```

O ARP Gratuito, ao contrário do ARP, é usado para verificar se existe outro dispositivo na rede com o mesmo endereço IP, sendo que se for recebida uma resposta à solicitação do ARP Gratuito, irá acontecer um conflito caso o seu endereço IP seja usado. Assim seria esperado um request mas não seria esperada resposta, sendo que não pode haver mais do que um host com o mesmo IP

4 Domínios de colisão

Uma rede local onde existam vários equipamentos ligados através de um meio partilhado comum constitui o que é denominado um domínio de colisão. Esta designação decorre da possibilidade de vários hosts poderem coincidir temporalmente no envio de uma trama, causando uma interferência mútua (colisão) que deteriora as tramas originalmente enviadas.

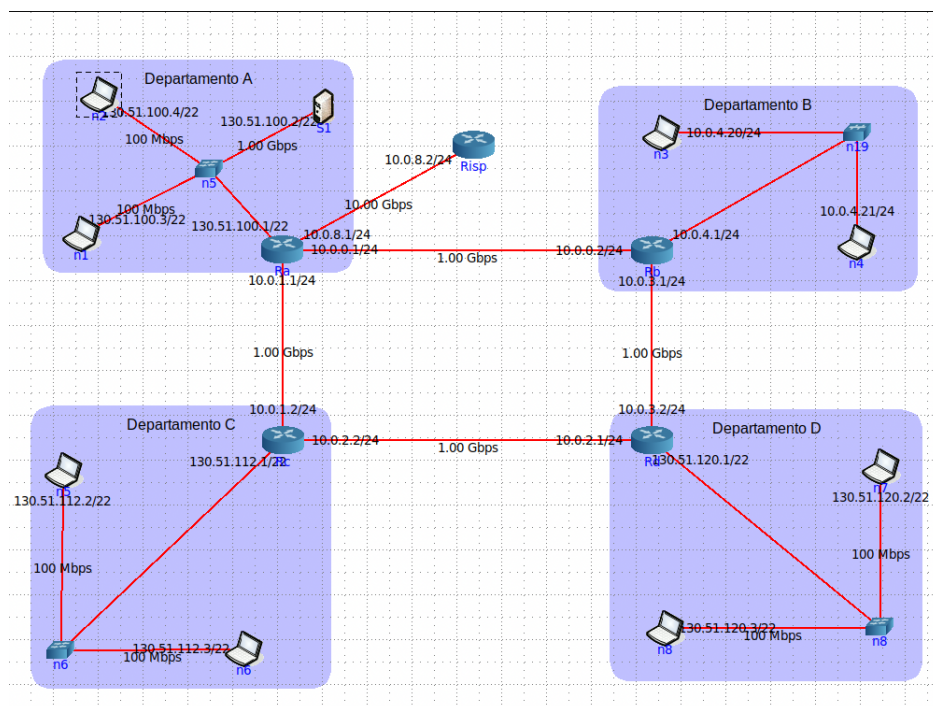
Num domínio de colisão, apenas um dispositivo pode transmitir num determinado instante e os restantes ficam à escuta para prevenir colisões. Por esse facto, a largura de banda é partilhada entre os diversos dispositivos. Na presença de uma colisão os dispositivos envolvidos têm que retransmitir a mesma trama Ethernet algum tempo depois. As normas Ethernet implementam um método de controlo de acesso ao meio denominado CSMA/CD (estudado nas aulas teóricas), que prevê a resolução de colisões.

Os domínios de colisão existem em segmentos de rede com equipamentos interligados via hubs partilhados (repetidores) e também em redes sem fios (Wi-Fi).

As redes mais modernas usam comutadores de rede (switches) para eliminar as colisões. Conectando cada dispositivo a uma porta do comutador, cada porta constitui um domínio de colisão (se a comunicação for half-duplex) ou são eliminados se a comunicação for full-duplex.

Ative o emulador CORE e carregue a topologia de rede com a solução de subnetting que construiu no âmbito do TP2. Substitua o switch do departamentos B por um hub (repetidor).

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.



```
root@n1:/tmp/pycore.33643/n1.conf - + x
root@n1:/tmp/pycore.33643/n1.conf# ping 130.51.100.4
PING 130.51.100.4 (130.51.100.4) 56(84) bytes of data.
64 bytes from 130.51.100.4: icmp_seq=1 ttl=64 time=0.079 ms
64 bytes from 130.51.100.4: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 130.51.100.4: icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from 130.51.100.4: icmp_seq=4 ttl=64 time=0.056 ms
64 bytes from 130.51.100.4: icmp_seq=5 ttl=64 time=0.047 ms
64 bytes from 130.51.100.4: icmp_seq=6 ttl=64 time=0.085 ms
64 bytes from 130.51.100.4: icmp_seq=7 ttl=64 time=0.054 ms
^C
--- 130.51.100.4 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 613ms
rtt min/avg/max/ndev = 0.044/0.055/0.079/0.015 ms
root@n1:/tmp/pycore.33643/n1.conf#

root@S1:/tmp/pycore.33643/S1.conf - + x
root@S1:/tmp/pycore.33643/S1.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
01:57:57.451306 IP 130.51.100.1 > 224.0.0.5: OSPFv2, Hello, length 44
14:57:57.587163 IP fe80::200:ff:feaa:8 > ff02::5: OSPFv3, Hello, length 36
14:58:07.488724 IP 130.51.100.1 > 224.0.0.5: OSPFv2, Hello, length 44
14:58:07.987829 IP fe80::200:ff:feaa:8 > ff02::5: OSPFv3, Hello, length 36

4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@S1:/tmp/pycore.33643/S1.conf#

root@n2:/tmp/pycore.33643/n2.conf - + x
length 64
14:58:09.706752 IP 130.51.100.3 > 130.51.100.4: ICMP echo request, id 68, seq 5, length 64
14:58:09.706771 IP 130.51.100.4 > 130.51.100.3: ICMP echo reply, id 68, seq 5, length 64
14:58:10.631377 ARP, Request who-has 130.51.100.3 tell 130.51.100.4, length 28
14:58:10.631422 ARP, Request who-has 130.51.100.4 tell 130.51.100.3, length 28
14:58:10.631430 ARP, Reply 130.51.100.4 is-at 00:00:00:aa:00:0c (oui Ethernet), length 28
14:58:10.631431 ARP, Reply 130.51.100.3 is-at 00:00:00:aa:00:0d (oui Ethernet), length 28
14:58:10.736700 IP 130.51.100.3 > 130.51.100.4: ICMP echo request, id 68, seq 6, length 64
14:58:10.736733 IP 130.51.100.4 > 130.51.100.3: ICMP echo reply, id 68, seq 6, length 64
14:58:11.750645 IP 130.51.100.3 > 130.51.100.4: ICMP echo request, id 68, seq 7, length 64
14:58:11.750667 IP 130.51.100.4 > 130.51.100.3: ICMP echo reply, id 68, seq 7, length 64
22 packets captured
22 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.33643/n2.conf#
```

tcpdump nos dispositivos do departamento A

```
root@n3:/tmp/pycore.33643/n3.conf - + x
length 64
15:11:11.686581 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 4, length 64
length 64
15:11:12.718860 IP 130.51.100.3 > 130.51.104.2: ICMP echo request, id 26, seq 5, length 64
15:11:12.718910 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 5, length 64
15:11:12.949938 IP 130.51.104.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:11:12.949912 IP fe80::200:ff:feaa:14 > ff02::5: OSPFv3, Hello, length 36
15:11:13.735352 ARP, Request who-has 130.51.104.1 tell 130.51.104.2, length 28
15:11:13.735363 ARP, Request who-has 130.51.104.2 tell 130.51.104.1, length 28
15:11:13.736109 ARP, Reply 130.51.104.2 is-at 00:00:00:aa:00:15 (oui Ethernet), length 28
15:11:13.736116 ARP, Reply 130.51.104.1 is-at 00:00:00:aa:00:14 (oui Ethernet), length 28
15:11:13.736133 IP 130.51.100.3 > 130.51.104.2: ICMP echo request, id 26, seq 6, length 64
15:11:13.736144 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 6, length 64
18 packets captured
18 packets received by filter
0 packets dropped by kernel
root@n3:/tmp/pycore.33643/n3.conf#

root@n4:/tmp/pycore.33643/n4.conf - + x
length 64
15:11:11.686586 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 4, length 64
length 64
15:11:12.718857 IP 130.51.100.3 > 130.51.104.2: ICMP echo request, id 26, seq 5, length 64
length 64
15:11:12.718915 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 5, length 64
15:11:12.949936 IP 130.51.104.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:11:12.949911 IP fe80::200:ff:feaa:14 > ff02::5: OSPFv3, Hello, length 36
15:11:13.735350 ARP, Request who-has 130.51.104.1 tell 130.51.104.2, length 28
15:11:13.735362 ARP, Request who-has 130.51.104.2 tell 130.51.104.1, length 28
15:11:13.736116 ARP, Reply 130.51.104.1 is-at 00:00:00:aa:00:14 (oui Ethernet), length 28
15:11:13.736117 ARP, Reply 130.51.104.2 is-at 00:00:00:aa:00:15 (oui Ethernet), length 28
15:11:13.736132 IP 130.51.100.3 > 130.51.104.2: ICMP echo request, id 26, seq 6, length 64
15:11:13.736146 IP 130.51.104.2 > 130.51.100.3: ICMP echo reply, id 26, seq 6, length 64
18 packets captured
18 packets received by filter
0 packets dropped by kernel
root@n4:/tmp/pycore.33643/n4.conf#

root@n1:/tmp/pycore.33643/n1.conf - + x
64 bytes from 130.51.104.2: icmp_seq=3 ttl=62 time=0.066 ms
64 bytes from 130.51.104.2: icmp_seq=4 ttl=62 time=0.092 ms
64 bytes from 130.51.104.2: icmp_seq=5 ttl=62 time=0.138 ms
64 bytes from 130.51.104.2: icmp_seq=6 ttl=62 time=0.083 ms
64 bytes from 130.51.104.2: icmp_seq=7 ttl=62 time=0.075 ms
64 bytes from 130.51.104.2: icmp_seq=8 ttl=62 time=0.072 ms
64 bytes from 130.51.104.2: icmp_seq=9 ttl=62 time=0.071 ms
^C
--- 130.51.104.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 817ms
rtt min/avg/max/ndev = 0.063/0.100/0.200/0.063 ms
root@n1:/tmp/pycore.33643/n1.conf# ping 130.51.104.2
PING 130.51.104.2 (130.51.104.2) 56(84) bytes of data.
64 bytes from 130.51.104.2: icmp_seq=1 ttl=62 time=0.060 ms
64 bytes from 130.51.104.2: icmp_seq=2 ttl=62 time=0.212 ms
64 bytes from 130.51.104.2: icmp_seq=3 ttl=62 time=0.107 ms
64 bytes from 130.51.104.2: icmp_seq=4 ttl=62 time=0.142 ms
64 bytes from 130.51.104.2: icmp_seq=5 ttl=62 time=0.145 ms
64 bytes from 130.51.104.2: icmp_seq=6 ttl=62 time=0.079 ms
^C
--- 130.51.104.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 514ms
rtt min/avg/max/ndev = 0.060/0.120/0.212/0.053 ms
root@n1:/tmp/pycore.33643/n1.conf#
```

tcpdump nos dispositivos do departamento B

Como podemos ver nas imagens acima apresentadas, no caso do departamento A, os dados enviados a um Computador não são partilhados com outro que esteja ligado à mesma rede.

Já no departamento B, onde trocamos o switch por um hub, quando fazemos ping ao computador n3, a informação é partilhada com o computador n4.

5 Conclusão

Com este trabalho conseguimos aprofundar conhecimentos sobre a Ethernet e a sua organização e conhecer melhor o protocolo ARP, utilizando o Wireshark para de melhor forma responder as perguntas sugeridas. Com o uso desta ferramenta foi nos permitida a observação dos protocolos envolvidos de entre outras propriedades do protocolo ARP.

Abordamos também o ARP Grátis verificando a utilidade deste, sendo que permite informar a hosts ou switches novos endereços MAC para que todos os sistemas de rede possam atualizar as suas tabelas ARP.

Também conseguimos aprofundar melhor a diferença entre um switch e um hub e os impactos que estes tem no tráfego de rede.