Nível de Ligação Lógica: Redes Ethernet e Protocolo ARP

Filipa Rebelo and Joana Oliveira

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
email: {a90234,a87956}@alunos.uminho.pt

Captura e análise de Tramas Ethernet

Exercício 1

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

Uma vez que este se encontra encriptado, o acesso ao endereço indicado foi recusado. No entanto, é ainda possível saber quais os endereços MAC de origem e de destino.
Endereço MAC origem: 34:e1:2d:4b:b8:b0
Endereço MAC destino: 00:d0:03:ff:94:00

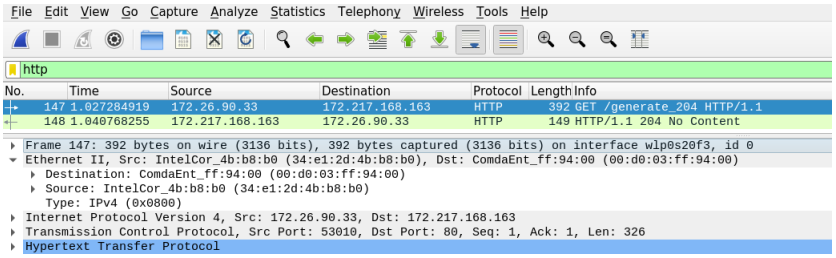

Fig. 1. Endereços MAC

Exercício 2

Identifique a que sistemas se referem. Justifique.

O endereço *Source* refere-se à interface da nossa máquina, ou seja de onde é enviada a trama. O endereço *Destination* refere-se à interface do router da rede local a que estamos ligados.

Exercício 3

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

O valor hexadecimal do campo Type é 0x0800, que representa o protocolo IPv4.

Exercício 4

Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (Application Data Protocol: http-over-tls)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

Observando a Figura 2 verifica-se que temos 66 bytes até ao início dos dados do nível aplicacional.
Assim, tendo sido já usados 392 bytes até ao momento, a sobrecarga é de:

$$\frac{66}{392} * 100 = 16.84\%$$

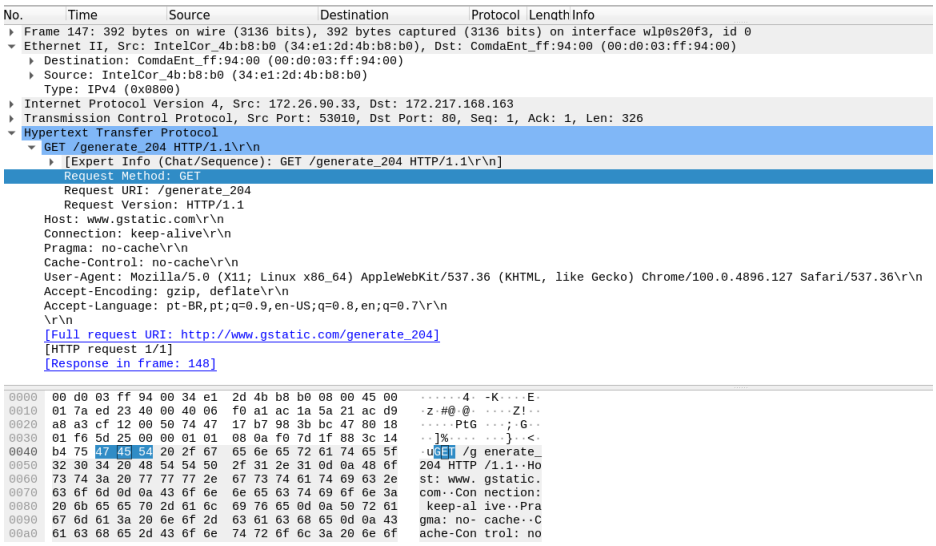

Fig. 2. Trama que contém o pedido HTTP

Exercício 5

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

O endereço Ethernet da fonte encontra-se no campo *Source* com o valor 00:d0:03:ff:94:00. Este corresponde ao *gateway* da rede local, uma vez que o servidor não se encontra na rede local e apenas conhecemos os IPs das redes locais e do *gateway*.

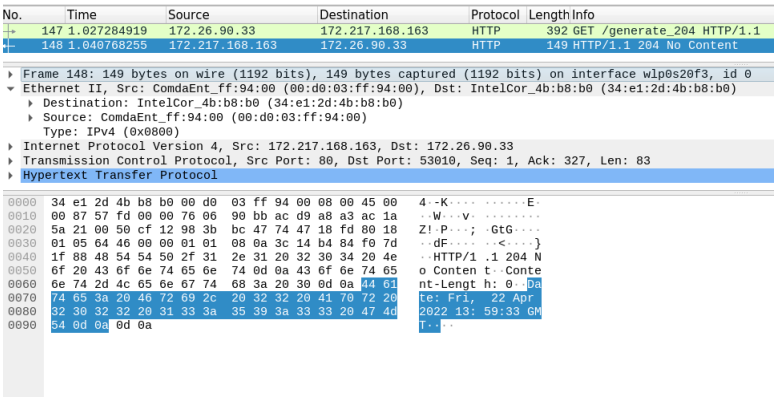

Fig. 3. Trama que contém a resposta HTTP

Exercício 6

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

O endereço MAC do destino, presente no campo *Destination* da figura anterior, é 34:e1:2d:4b:b8:b0 e corresponde à interface ethernet da nossa máquina.

Exercício 7

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

Os protocolos contidos na trama são IPv4, Ethernet, TCP e HTML.

Protocolo ARP

Exercício 8

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

A coluna *Adress* contém os endereços IP ou nome dos hosts e neste caso apenas contém o *gateway* da rede local. A coluna *HWtype* permite indicar que as

conexões são conexões Ethernet. A coluna *HWadress* contém os endereços MAC de cada dispositivo. A coluna *Flags* permite saber, por exemplo, se um endereço MAC foi aprendido ou introduzido manualmente. Neste caso, como o seu valor é C é possível saber que este registo foi aprendido dinamicamente através do protocolo ARP. A coluna *Mask* corresponde à máscara de sub-rede. Por fim, a coluna *Iface* representa a interface de rede, que neste caso corresponde a wlo1.

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

Fig. 4. Tabela ARP

Para a realização das perguntas seguintes, e devido à impossibilidade de fazer ping para outros hosts da sala de aula, foi-nos proposto que fizéssemos uma simulação no Core através do uso de um router, um switch e dois portáteis. A topologia criada pode ser observada na figura seguinte.

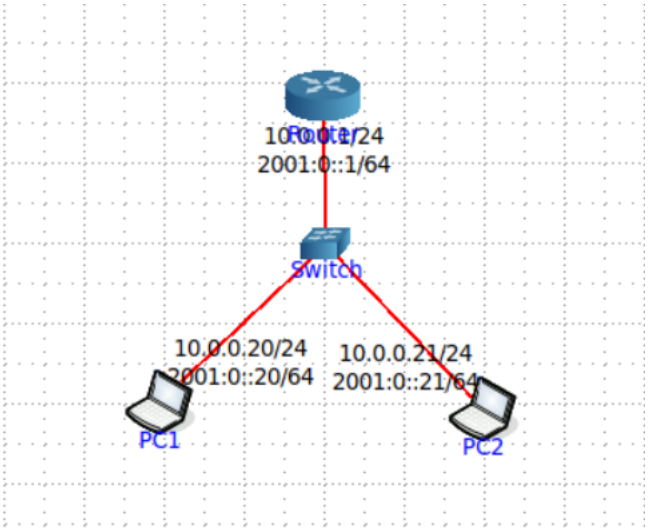

Fig. 5. Rede auxiliar

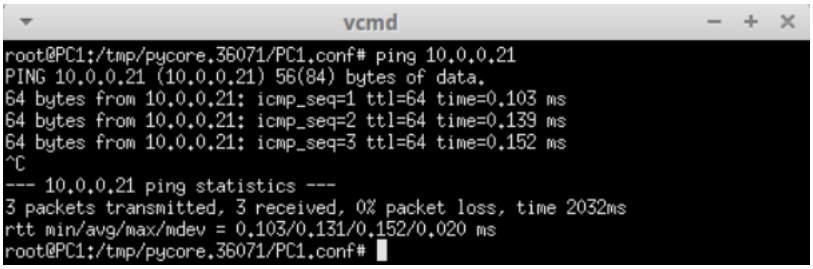

Fig. 6. Comando ping

Exercício 9

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?

Através da figura seguinte é possível observar que o endereço origem é 00:00:00:aa:00:01 e o endereço destino é ff:ff:ff:ff:ff:ff (broadcast).
O endereço destino é o de broadcast, o que permite enviar a mensagem para todos os hosts da rede. O host que tenha o IP destino correspondente irá então responder com o seu endereço MAC e este será adicionado à tabela ARP.

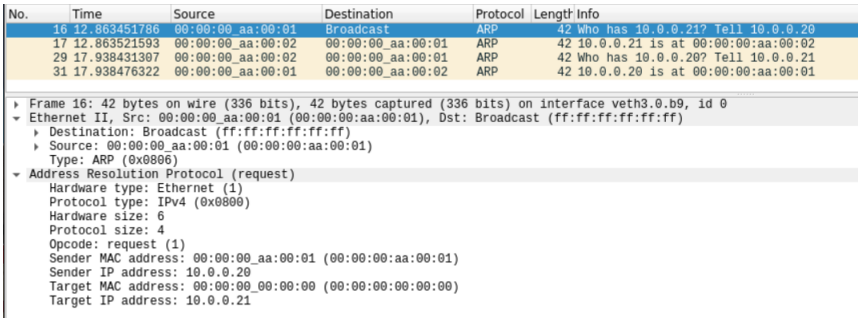

Fig. 7. Pedido ARP

Exercício 10

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

O valor hexadecimal é 0x0806 e indica que se trata de uma mensagem ARP.

Exercício 11

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

Tal como visto na alínea anterior esta trata-se de uma mensagem ARP. Analisando o campo *Opcode* vemos que este contém valor 1, juntamente com a palavra *request*, o que nos permite confimar que se trata de um pedido ARP.
Os tipos de endereços contidas na mensagem ARP são endereços IP e MAC, tanto de origem como de destino.

Exercício 12

Explicite que tipo de pedido ou pergunta é feita pelo host de origem.

O pedido feito pelo host de origem é "Who has 10.0.0.21? Tell 10.0.0.20". Este pedido é então enviado a todos os hosts da rede com o objetivo de saber o endereço MAC do endereço IP especificado, que deverá ser depois enviado para o host origem.

Exercício 13

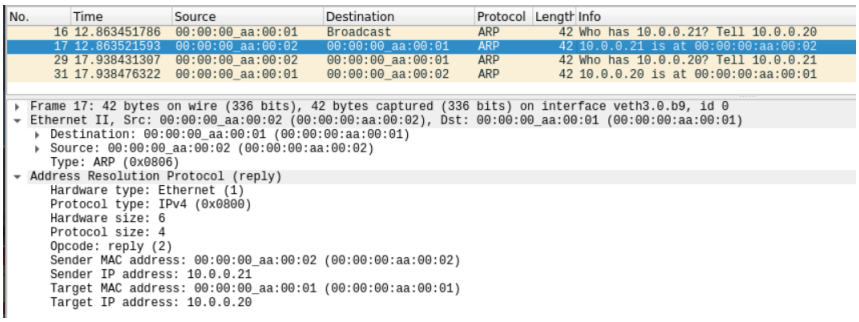

Fig. 8. Resposta ARP

Alínea 13a) Qual o valor do campo ARP opcode? O que especifica?

O valor do campo opcode é 2, o que significa que se trata de de uma resposta (ARP Reply) a um pedido anterior.

Alínea 13b) Em que campo da mensagem ARP está a resposta ao pedido ARP?

A resposta encontra-se no campo *Sender MAC adress*.

Exercício 14

Na situação em que efetua um ping a outro host, assuma que este está diretamente ligado ao mesmo router, mas noutra subrede, e que todas as tabelas ARP se encontram inicialmente vazias. Esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do host destino.

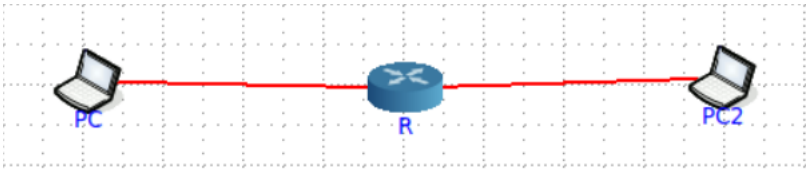

Fig. 9. Exemplo de rede

				ICMP
			IP Origem: IP PC	
			IP Destino: IP PC2	
AC Destino: ?	MAC Origem: MAC PC	Tipo: 0x800 (IPv4)		Payload
			MAC Origem: MAC PC	MAC Destino: 00:00:00:00:00:00
			IP Origem: IP PC	IP Destino: IP R
AC Destino: ff:ff:ff:ff:ff:ff	MAC Origem: MAC PC	Tipo: 0x806 (ARP)		Payload
			MAC Origem: MAC R	MAC Destino: MAC PC
			IP Origem: IP R	IP Destino: IP PC
AC Destino: MAC PC	MAC Origem: MAC R	Tipo: 0x806 (ARP)		Payload
				ICMP
			IP Origem: IP PC	
			IP Destino: IP PC2	
AC Destino: MAC R	MAC Origem: MAC PC	Tipo:0x800 (IPv4)		Payload

Fig. 10. Diagrama das mensagens trocadas entre PC e Router

				ICMP
			IP Origem: IP PC	
			IP Destino: IP PC2	
MAC Destino: ?	MAC Origem: MAC R	Tipo: 0x800 (IPv4)	Payload	
			MAC Origem: MAC R	MAC Destino: 00:00:00:00:00:00
			IP Origem: IP R	IP Destino: IP PC2
MAC Destino: ff:ff:ff:ff:ff:ff	MAC Origem: MAC R	Tipo: 0x806 (ARP)	Payload	
			MAC Origem: MAC PC2	MAC Destino: MAC R
			IP Origem: IP PC2	IP Destino: IP R
MAC Destino: MAC R	MAC Origem: MAC PC2	Tipo: 0x806 (ARP)	Payload	
				ICMP
			IP Origem: IP PC	
			IP Destino: IP PC2	
MAC Destino: MAC PC2	MAC Origem: MAC R	Tipo: 0x800 (IPv4)	Payload	

Fig. 11. Diagrama das mensagens trocadas entre Router e PC2

Domínios de colisão

Exercício 15

Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces do dispositivo de interligação no departamento A (LAN partilhada) e no departamento B (LAN comutada) quando se gera tráfego intra-departamento (por exemplo, fazendo ping IPaddr da Bela para Monstro, da Jasmine para o Alladin, etc.) Que conclui?

Na topologia representada na Figura 12 foi substítuido o switch existente no departamento A por um hub e adicionado um novo portátil, tanto no departamento A como no B, de modo a permitir correr o comando *tcdump* e ver o como flui o tráfego em ambos os departamentos.
No Departamento A, departamento onde ocorreu a substituição do switch para hub, ao ser realizado um ping de Bela para Monstro verifica-se que todos os hosts da interface recebem os pacotes enviados pela Bela. Isto é comprovado pelo facto de o PC1 capturar tramas tais como *echo request* e *echo reply* enviadas entre os dois outros portáteis.
No departamento B, departamento em que o switch ainda é utilizado, ao efetuar um ping de Jasmine para Alladin verifica-se que apenas o Alladin recebe os pacotes enviados por Jasmine e apenas Jasmine recebe a resposta enviada por Aladin. Isto é confirmado pelo facto de o PC2 não conseguir capturar quaisquer tramas enviadas entre os dois portáteis, sendo que as tramas existentes na Figura 16 nada têm a ver com o ping efetuado.
Assim conclui-se que, para diminuir as colisões, os switches são a melhor opção, uma vez que este apenas envia os pacotes para o host indicado, ao contrário do hub envia para todos os dispositivos a que esteja ligado.

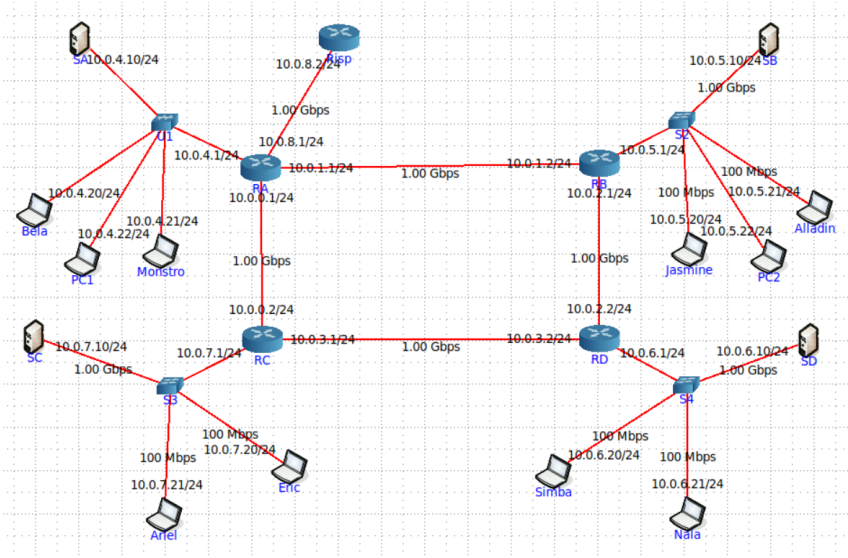

Fig. 12. Topologia Core

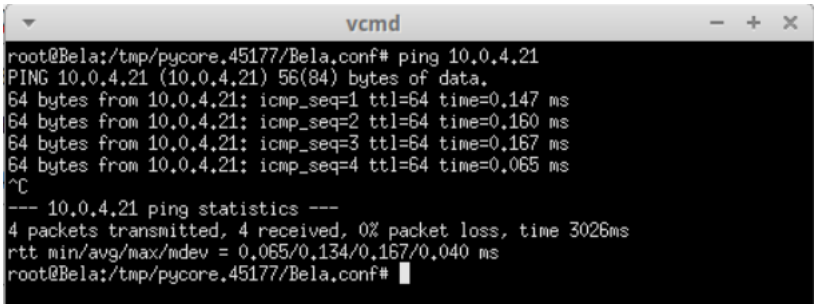

Fig. 13. Ping de Bela para Monstro

Fig. 14. Tcpdump no PC1

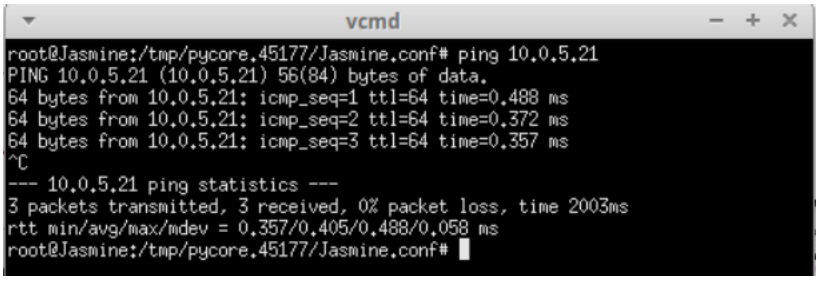

Fig. 15. Ping de Jasmine para Alladin

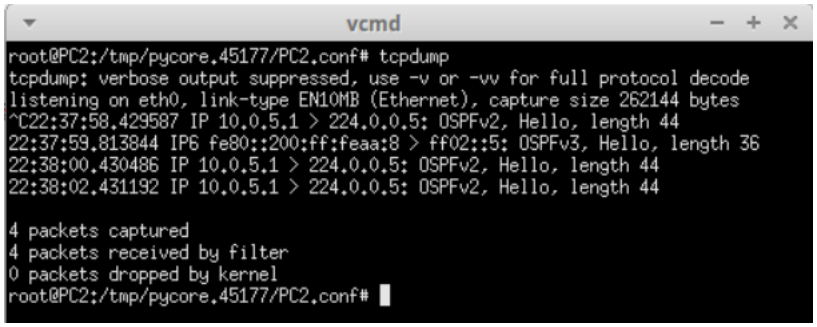

Fig. 16. Tcpdump no PC2

Exercício 16

Construa manualmente a tabela de comutação do switch do Departamento B, atribuindo números de porta à sua escolha

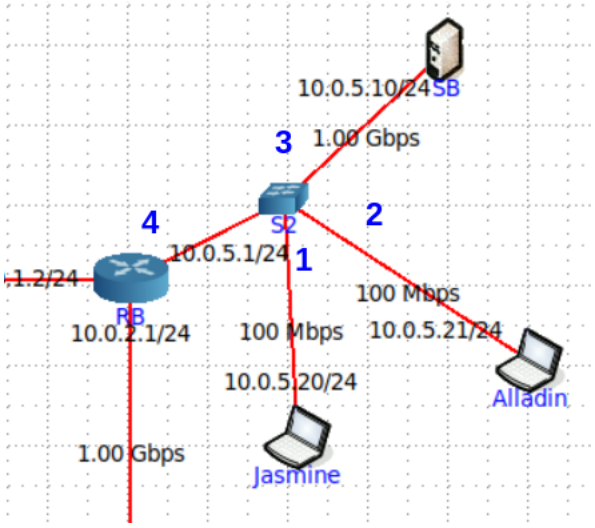

Fig. 17. Númeração das interfaces no Departamento B

MAC Adress	Interface	TTL
00:00:00:aa:00:0e	1	64
00:00:00:aa:00:0f	2	64
00:00:00:aa:00:09	3	64
00:00:00:aa:00:08	4	64

Fig. 18. Tabela de comutação

Conclusão

Através da realização deste trabalho foi possível consolidar os conhecimentos obtidos nas aulas teóricas sobre o **Nível de Ligação Lógica**, nomeadamente os conceitos de **Ethernet** e **Protocolo ARP**.
Para tal foi então utilizado o **Wireshark**, que nos permitiu capturar e visualizar o conteúdo dos diversos pacotes e o **CORE** que nos permitiu verificar a diferença entre switches e hubs e o seu impacto na deteção e correção de erros.
Foi ainda abordado o protocolo ARP, nomeadamente as suas tabelas e o conteúdo das mensagens enviadas através do mesmo.
Por fim, acreditamos ter cumprido o objetivo deste trabalho e obtido conhecimento importante em conceitos como captura e análise de tramas ethernet, protocolo ARP e domínios de colisão.