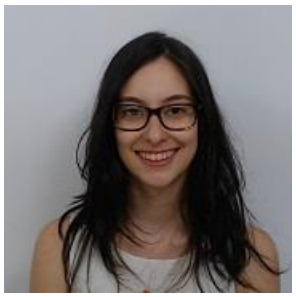
Relatório do Trabalho Prático 3

Redes de Computadores 2020/2021

a89506

Luís Miguel Lopes Pinto



a89599

Maria Beatriz Cardoso Gonçalves Barbosa e Moreira

a89574

Pedro Almeida Fernandes

Conteúdo

Captura e análise de Tramas Ethernet 3

1 Anote os endereços MAC de origem e de destino da trama capturada. 3

2 Identifique a que sistemas se referem. Justifique. 3

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

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. 4

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)). 4

6 Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique. 5

7 Qual é o endereço MAC do destino? A que sistema corresponde? 5

8 Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. 5

Protocolo ARP 6

9 Observe o conteúdo da tabela ARP. Diga o que significa cada umadas colunas. 6

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? 6

11 Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica? 7

12 Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? 8

13 Explicite que tipo de pedido ou pergunta é feita pelo host de origem? 9

14 Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. 9

a) Qual o valor do campo ARP opcode? O que especifica? 9

b) Em que posição da mensagem ARP está a resposta ao pedido ARP ? 9

ARP Gratuito 10

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? 10

Domínios de Colisão 11

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. 11

Conclusão 13

Captura e análise de Tramas Ethernet

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

R:. Endereço destino: (00:d0:03:ff:94:00)
Endereço origem: (b4:6b:fc:20:f5:e4)

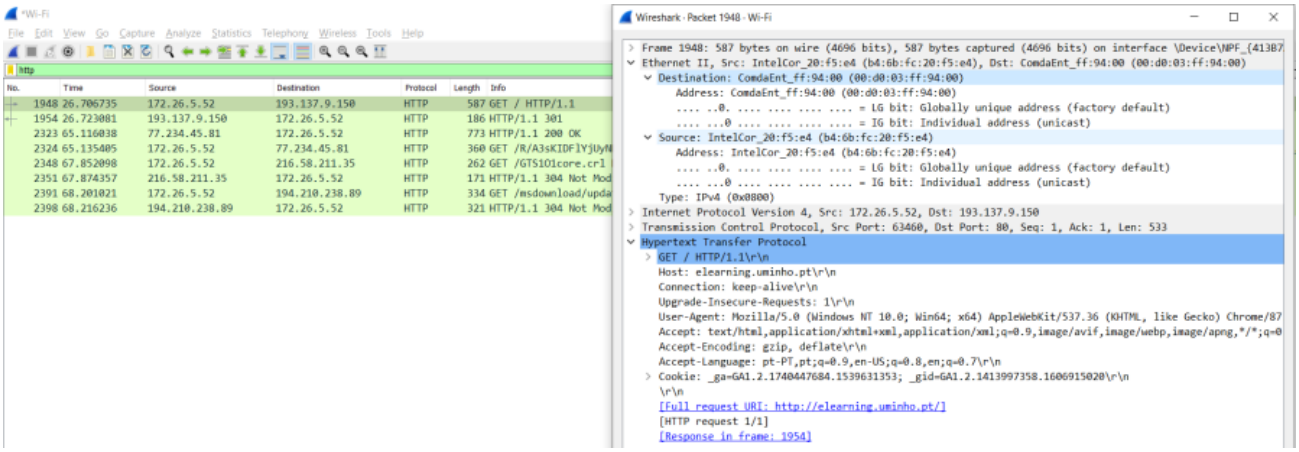


Figura 1 : Ilustração Pergunta 1

2 Identifique a que sistemas se referem. Justifique.

R:. Endereço origem- de onde é enviada a trama, i.e, interface ethernet nossa maquina.
Endereço Destino- envia trama para o servidor Web, i.e, interface router rede local pois a nossa maquina não conhece endereços fora da rede local.

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

R:. O valor hexadecimal é 0x0800. Isto significa que encapsula um pacote 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.

R:. 54 bytes. Logo, a sobrecarga introduzida pela pilha protocolar corresponde aproximadamente à 9.20%.
(54/587) * 100 = 9.20%

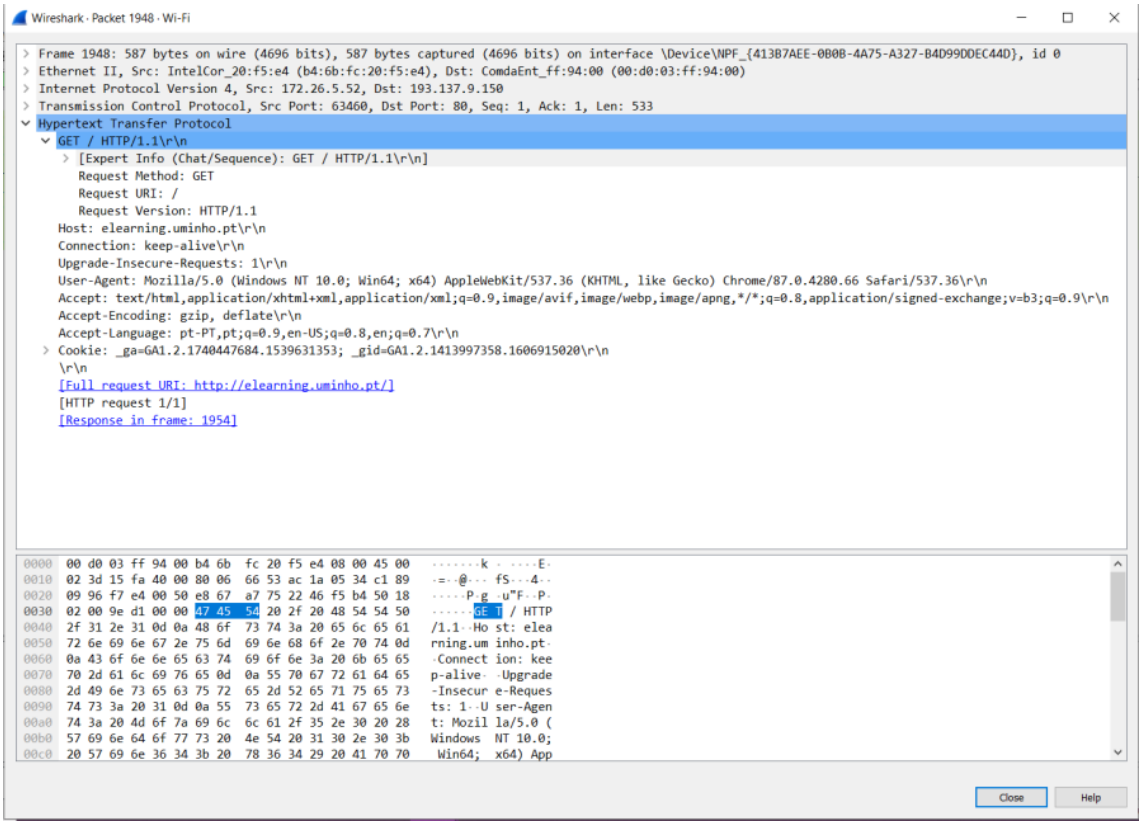


Figura 2: Ilustração Pergunta 4

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:. A rede ethernet é uma rede muito robusta (rede wired), assim sendo, é muito pouco suscetível a erros. Daí só ter sido detetada uma trama.

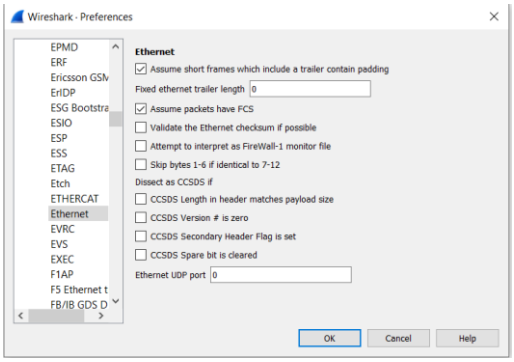


Figura 3: Ativação do Campo FCS

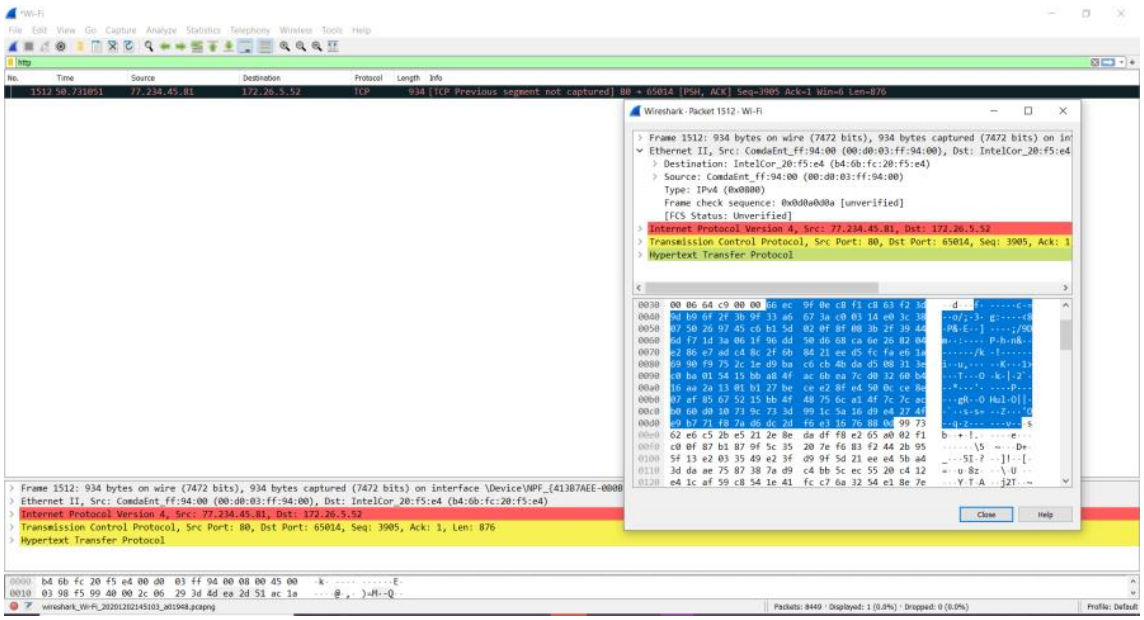


Figura 4: Trama detetada

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

R:. 00:d0:03:ff:94:00. Corresponde ao gateway da rede local pois só conseguimos saber o ip das redes locais e o gateway.

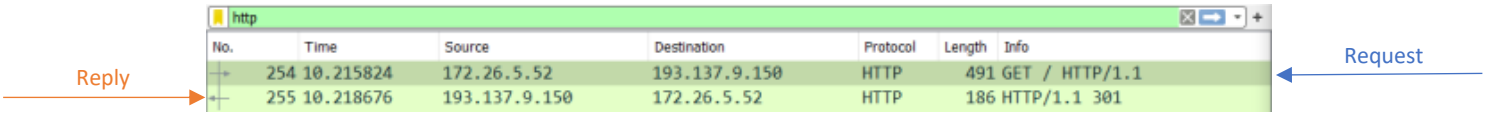


Figura 5: Ilustração da Pergunta 6

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

R:. 193.137.9.150. Corresponde à interface ethernet da nossa maquina.

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

R:. IPv4,Ethernet e TCP.

Protocolo ARP

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

R:. A Tabela ARP que resultou da execução do comando "arp -a" tem 3 colunas. A primeira tem os endereços IP de vários hosts, a segunda teus os endereços físicos (MAC) e a terceira indica o tipo da entrada (estática ou dinâmica).
Como pré-definido os endereços IP aparecem em notação decimal enquanto que os endereços MAC em notação hexadecimal.

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

C:\WINDOWS\system32>arp -a

Interface: 192.168.56.1 --- 0x9
  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: 172.26.5.52 --- 0xa
  Internet Address      Physical Address      Type
  172.26.254.254        00-d0-03-ff-94-00     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
```

Figura 6: apagar e reobter tabela arp

```
    46 12.322517    IntelCor_20:f5:e4   Broadcast           ARP         42 Who has 172.26.254.254? Tell 172.26.5.52
    47 12.324589    ComdaEnt_ff:94:00   IntelCor_20:f5:e4   ARP         60 172.26.254.254 is at 00:d0:03:ff:94:00
```

Figura 7: repreenchimento tabela arp

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 de origem é b4:6b:fc:20:f5:e4 (cujo nome é IntelCor_20:f5:e4) e corresponde ao MAC address do host que utilizamos.
Por sua vez o endereço de destino é ff:ff:ff:ff:ff:ff. Este endereço informa-nos que esta é uma ligação multipoint (Broadcast), uma vez que este encontra-se reservado para ligações em que a trama seja transmitida a todos os nós. Por sua vez o endereço de destino é 00:00:00:00:00:00. É necessário que isto aconteça, uma vez que nós não sabemos o endereço MAC destino (essa é justamente a informação que o pacote ARP pretende descobrir). Ou seja, ele sabe o endereço IP do destinatário e manda esta mensagem para descobrir o endereço MAC, pelo que esta mensagem é enviada a todos os hosts para que quando algum deles a receber e identificar o endereço ID como seu enviar um mensagem de reply onde segue o seu endereço MAC como Fonte.

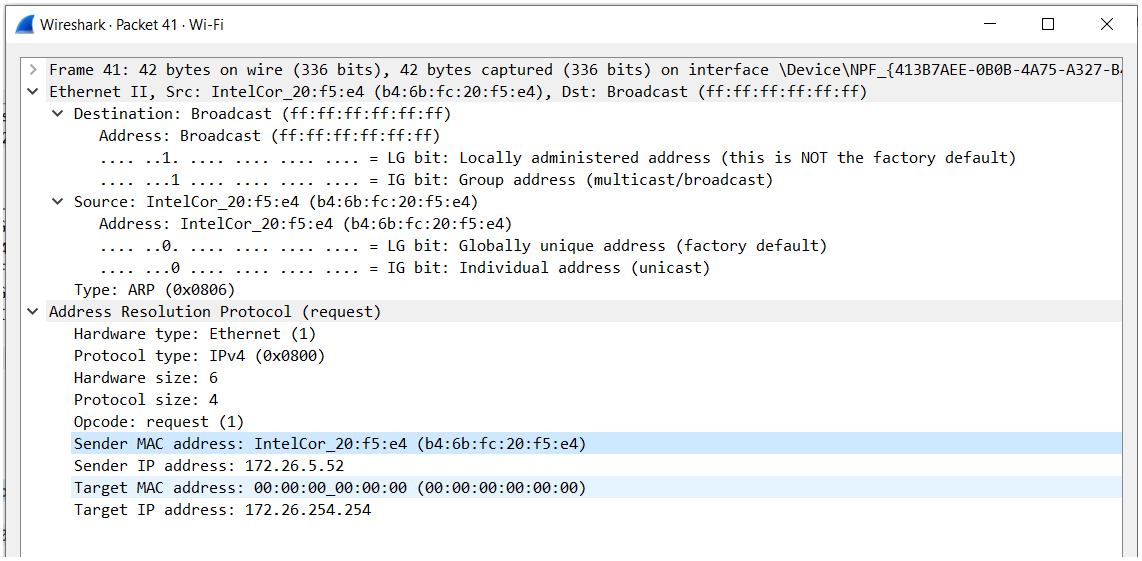


Figura 8: Ilustração exercício 10

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

R:. O valor hexadecimal do campo da trama Ethernet é 0x0806 e indica que se trama de uma mensagem ARP.

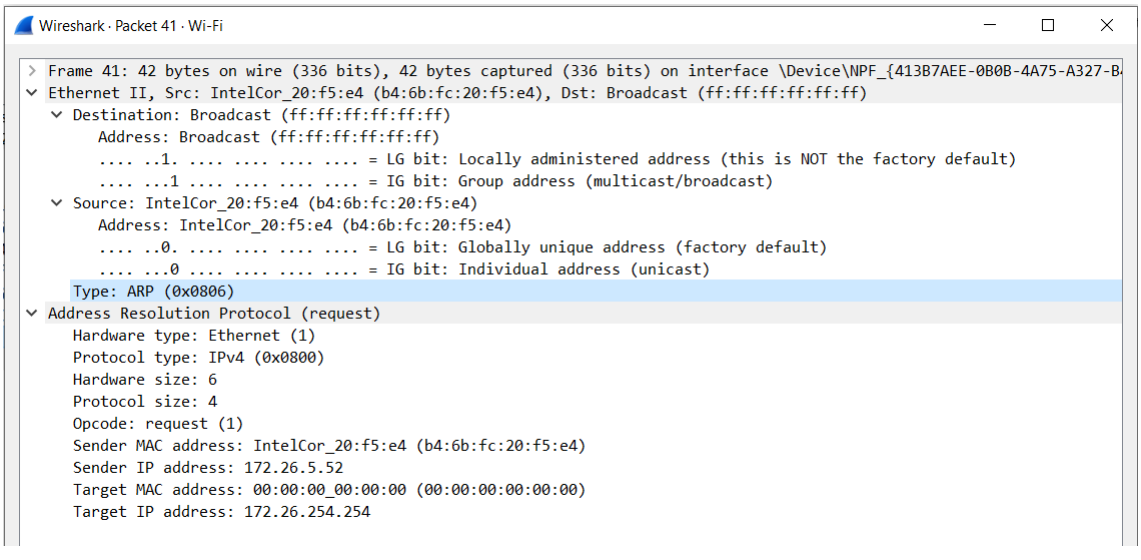


Figura 9: Ilustração exercício 11

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:. Como explicamos na alínea anterior estamos perante uma mensagem ARP e se verificarmos o ARP opcode tem valor 1, pelo que podemos concluir que é uma mensagem de request (ou seja, um pedido ARP).
Os endereços contidos na mensagem ARP são endereços MAC e endereços IP.
A mensagem ARP vem com estes dois tipos de endereços, para permitir a criação de linhas da tabela ARP com estes endereços, ou seja, para permitir que haja uma correspondência entre endereços IP e MAC estabelecida.

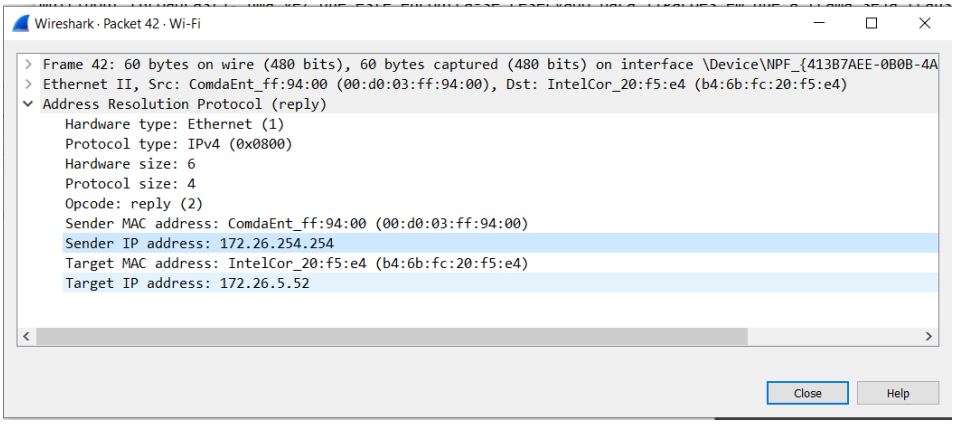


Figura 10: IP

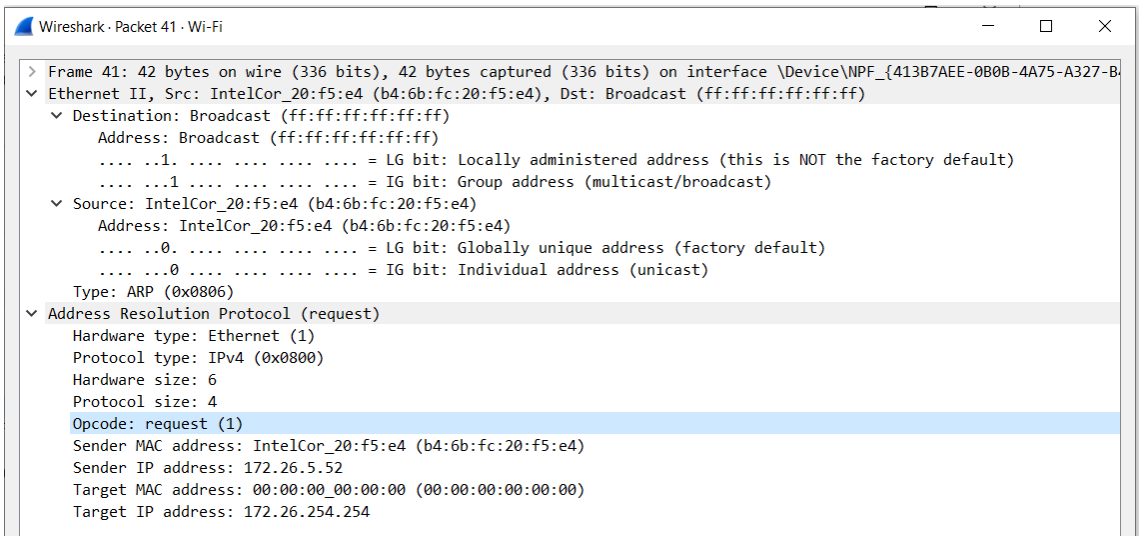


Figura 11: MAC

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

R:. A mensagem enviada é "Who has 192.168.1.1? Tell 192.168.1.5" e significa que o host 192.168.1.5 quer descobrir quem é o host 192.168.1.1, ou seja, qual é o endereço MAC associado a este endereço IP.

41	2.910007	IntelCor_20:f5:e4	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.5.52

Figura 12: Ilustração exercício 13 e endereços exercício 12

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

No.	Time	Source	Destination	Protocol	Length	Info
41	2.910007	IntelCor_20:f5:e4	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.5.52
42	2.911919	ComdaEnt_ff:94:00	IntelCor_20:f5:e4	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
199	12.994787	IntelCor_20:f5:e4	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.5.52
200	12.998188	ComdaEnt_ff:94:00	IntelCor_20:f5:e4	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

Figura 13: Ilustração exercício 14

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

R:. O valor do campo ARP opcode é 2 e especifica uma reply message (mensagem de resposta).

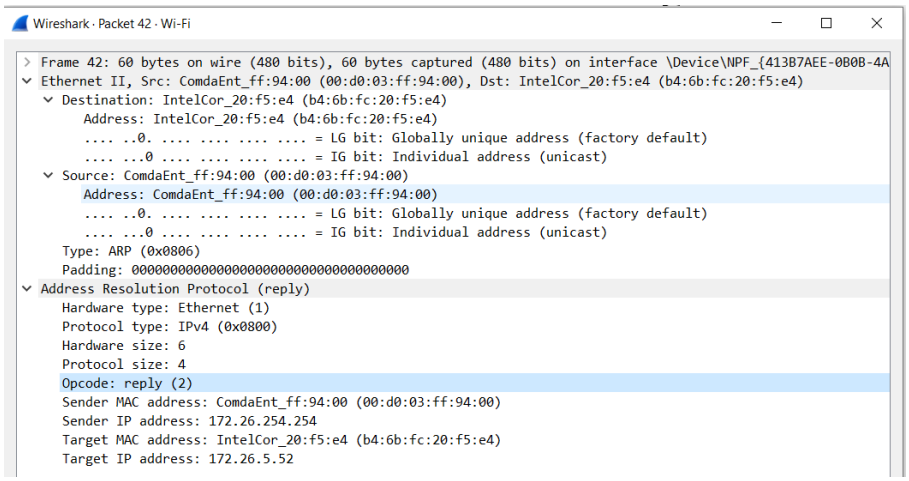


Figura 14: Ilustração exercício 14 a)

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

R:. A resposta ao pedido ARP vem na posição de origem (sender address), uma vez que quando o pedido chega ao host representado pelo ID-alvo esse host envia a mensagem de resposta e de modo que o seu endereço MAC torna-se a origem da mensagem (sender address).

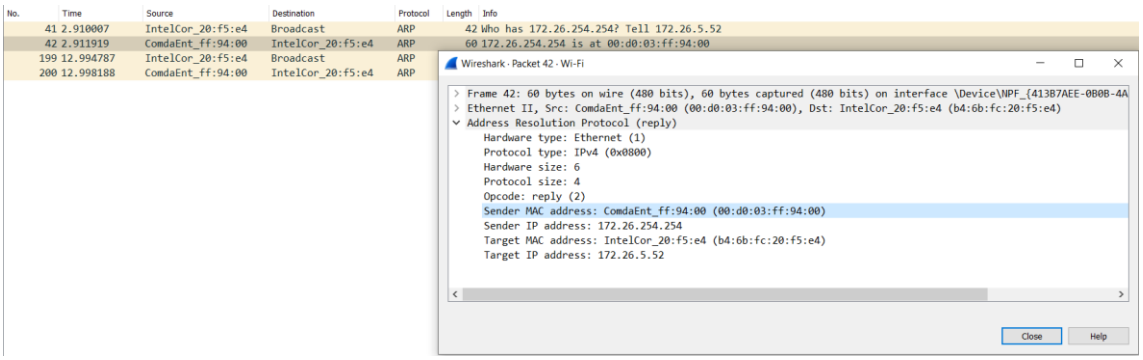


Figura 15: Ilustração Exercício 14 b)

ARP Gratuito

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?

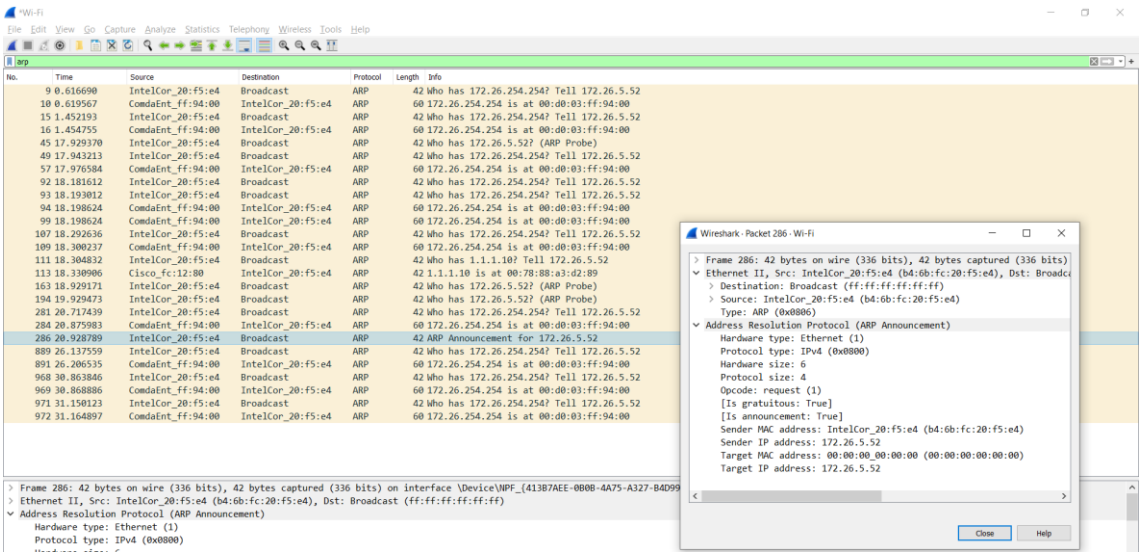


Figura 16 - Ilustração Exercício 15

R:. Os pedidos de ARP gratuito são diferentes dos restantes pedidos ARP uma que possui uma flag para indicar isso mesmo. Consegue-se visualizar isto com [Is gratuitous : True] na janela que se encontra em cima.

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.

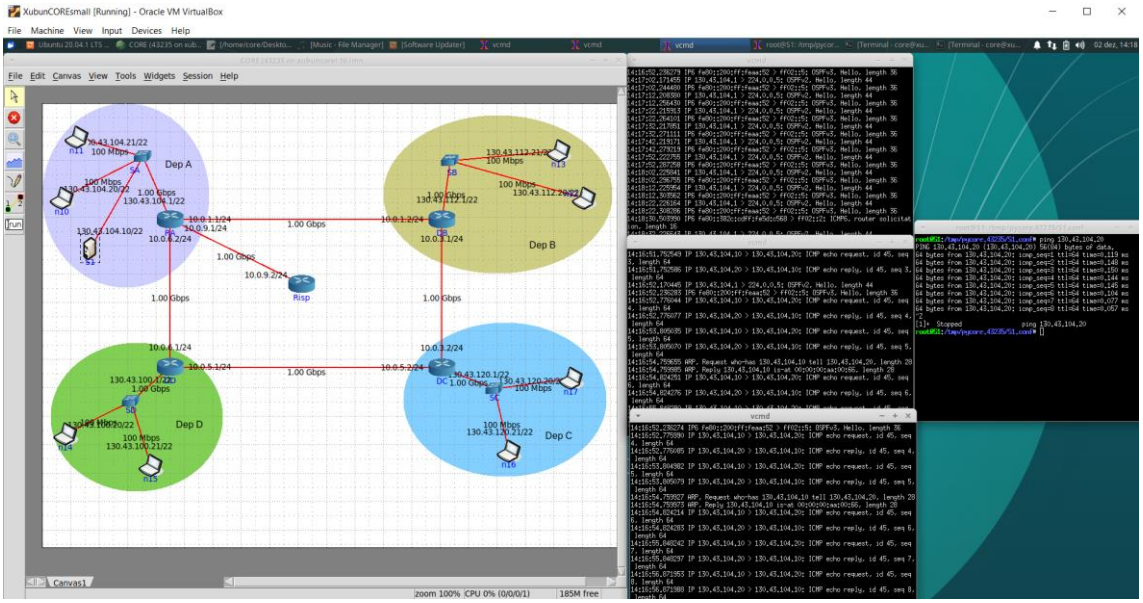


Figura 17 - Departamento A (Switch)

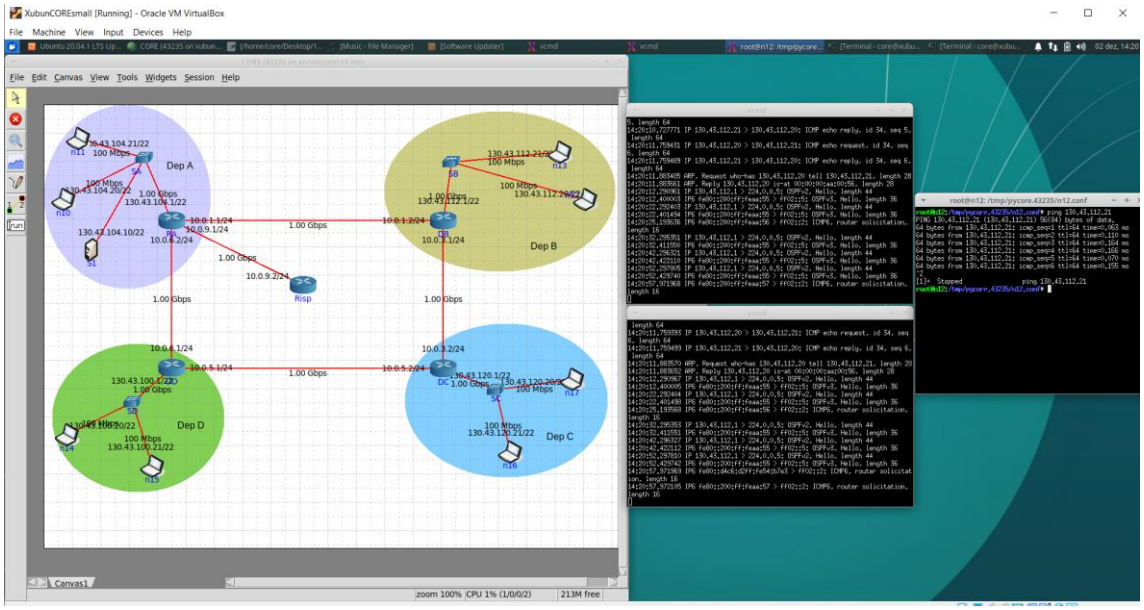


Figura 18 - Departamento B (Hub)

R:. As Interfaces do departamento A continuaram ligadas ao router através do switch enquanto que as interfaces passaram a fazer esta ligação a partir de um hub.

No Departamento B (departamento onde foi substituído o switch pelo hub) ao ser realizado um ping numa interface verifica-se ao analisar o tráfego dos hosts da interface, que todos estes recebem essa comunicação.

No Departamento A (departamento onde ainda é usado o switch) ao ser realizado o mesmo procedimento, ao analisar o tráfego dos hosts verifica-se que só os hosts envolvidos é que recebem essa comunicação, resolvendo assim o problema encontrado com o uso do hub.

Conclusão

Com este trabalho prático complementamos os conhecimentos obtidos nas aulas teóricas sobre o capitulo de Link Layer (nível de ligação lógica). Dentro desta focamo-nos nas temáticas de Ethernet e protocolo ARP (Address Resolution Protocol).

Primeiramente obtivemos um melhor entendimento sobre o funcionamento da interconexão entre redes locais através do envio de pacotes. Respetivamente a deteção e correção de erros, usamos como ferramenta de auxilio o campo FCS (Frame Check Sequence), conseguindo assim detetar as tramas danificadas. Visto que apenas foi detetada uma trama, comprovamos que a rede ethernet é robusta e pouco suscetível a erros.

De seguida, analisamos tabelas ARP e a forma como a sua construção e manutenção são levadas a cabo. Para a construção delas há duas alternativas. Por um lado, alguns dos endereços são obtidos através de uma metodologia de request/reply em que o host tem o endereço IP e manda uma mensagem a procurar o endereço MAC, que segue como fonte da resposta é inserido na tabela. O outro método corresponde à inserção de endereços MAC gratuitos, ou seja, o host recebe a resposta sem ter de enviar uma mensagem. Quanto à sua manutenção, concluímos que à medida que o tempo passa, as entradas da tabela não utilizadas vão sendo removidas.

Relativamente ao domínio da colisão com a troca de um dos switches do departamento B por um hub chegou-se à conclusão que os hubs deveriam ser sempre substituídos por switches.