Universidade do Minho
Mestrado Integrado em Engenharia Informática

Redes de Computadores
2019/2020

TP3: Camada de Ligação Lógica
Ethernet e Protocolo ARP
Grupo 05

Ana Afonso
A85762

João Diogo Mota
A80791

Márcia Teixeira
A80943

1. Questões e Respostas

1.1 Captura e análise de tramas Ethernet

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

Endereço MAC de origem: 3c:52:82:e6:4d:7b

Endereço MAC de destino: 00:0c:29:d2:19:f0

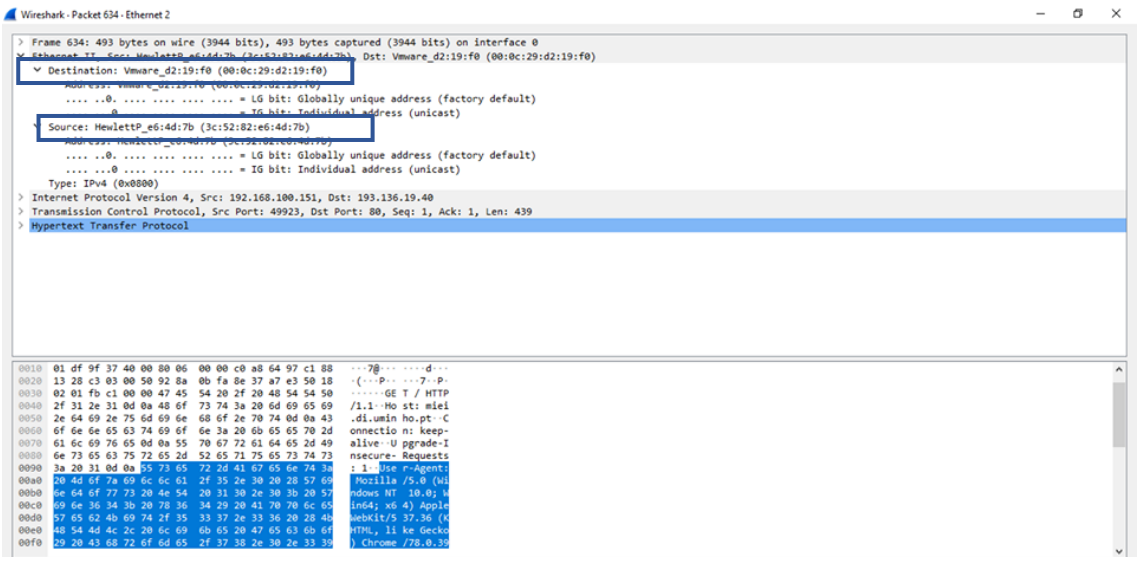


Figura 1: Conteúdo da trama Ethernet que contém a mensagem HTTP GET – Endereços MAC de origem e destino

Questão 2
Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem, indicado na Figura 1 no campo "*Source*", corresponde à interface da máquina nativa (computador onde foi realizado o exercício).

O endereço MAC de destino, indicado na Figura 1 no campo "*Destination*", corresponde ao *router* da rede local à qual a máquina nativa está conectada.

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

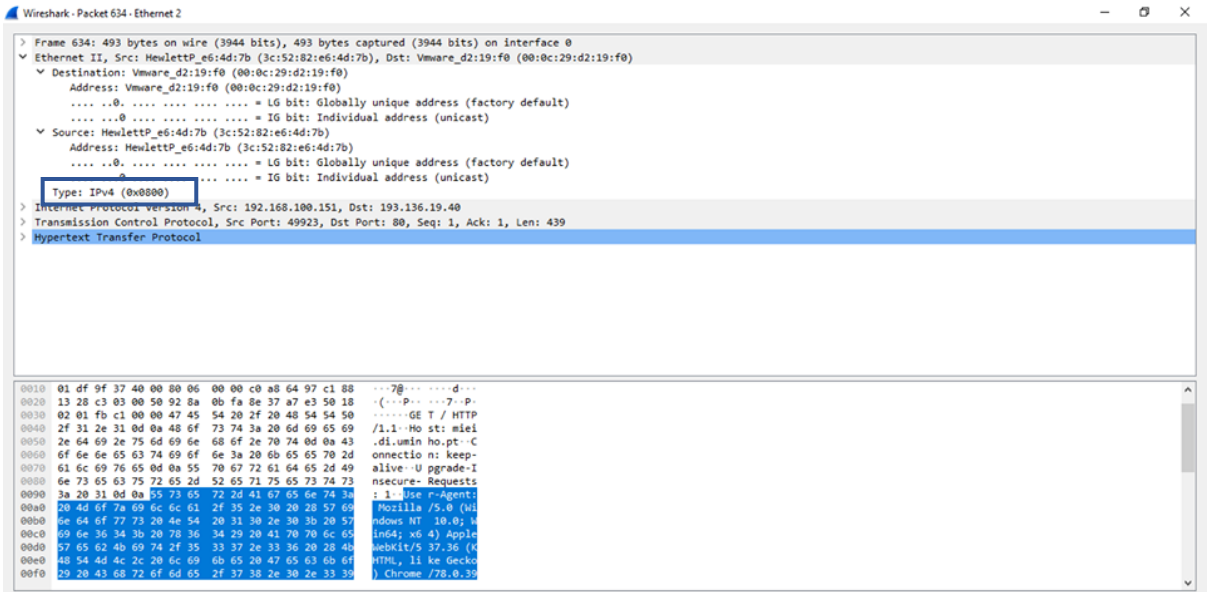


Figura 2: Conteúdo da trama Ethernet que contém a mensagem HTTP GET – Campo "Type"

O valor em hexadecimal do campo *Type* é 0x(0800). Este valor indica qual o protocolo utilizado. Como vemos na Figura 2, este é o IPv4.

Questão 4

Quantos bytes são usados desde o início da trama até ao carater ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.

Desde o início da trama até ao caracter ASCII "G" (em hexadecimal 0x47) do método HTTP GET foram usados 54 *bytes*. Sendo que no total foram usados 493 *bytes*, a percentagem da sobrecarga introduzida pela pilha protocolar no envio do HTTP GET, é de 10,95% (dado por 54/493 *100).

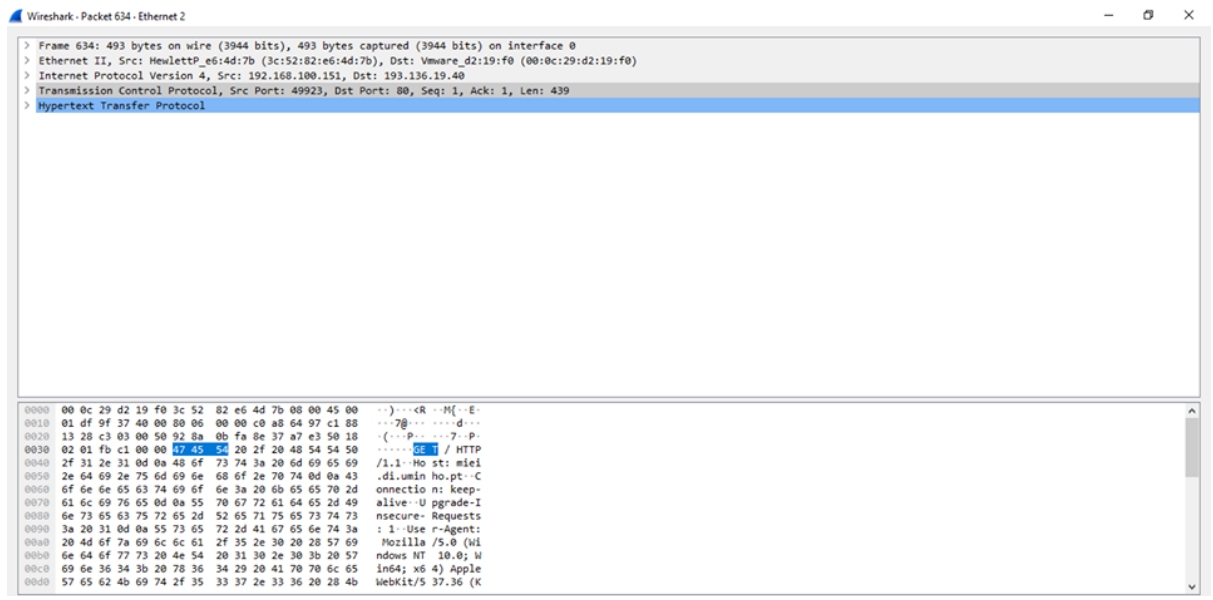


Figura 3: Conteúdo da trama Ethernet que contém a mensagem HTTP GET - Análise da percentagem da sobrecarga

Questão 5

Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para deteção de erros não está a ser usado. Em sua opinião, porque será?

Através da análise do conteúdo da trama, podemos concluir que o campo FCS (*Frame Check Sequence)* não está a ser usado, uma vez que não se encontra o campo no seu conteúdo. Esta inutilização deve-se ao facto de estarmos a usar ligação por cabo, onde este tipo de erros são muito raros, sendo por isso o campo FCS omitido.

Questão 6

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

Endereço Ethernet da fonte: (00:0c:29:d2:19:f0)
Este endereço corresponde ao *router* da rede local, dado que se trata do conteúdo da trama *Ethernet* que contém a resposta HTTP.

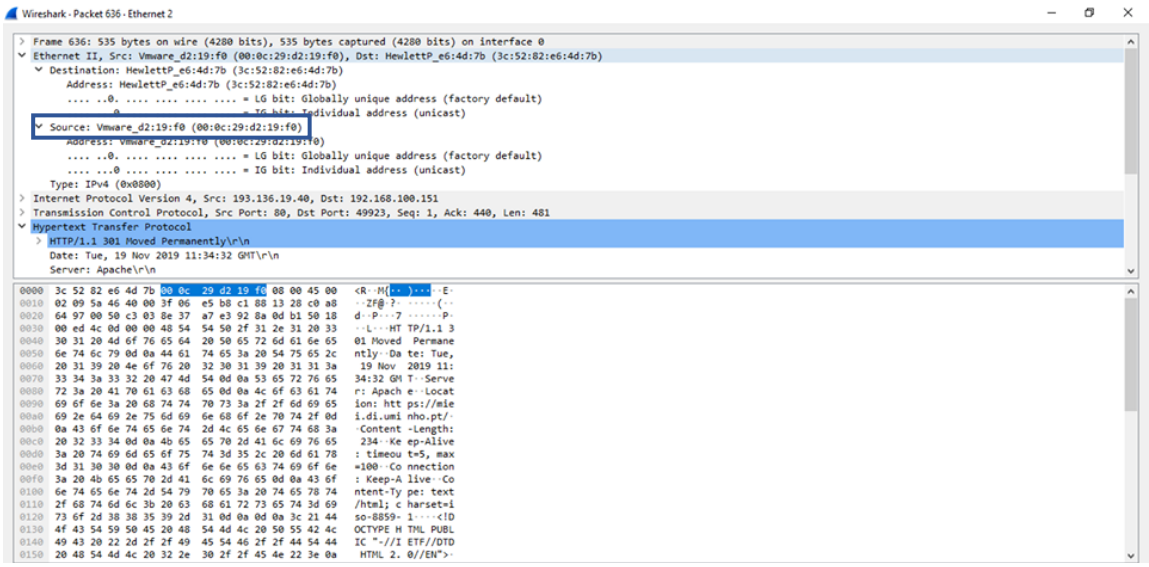


Figura 4: Conteúdo da trama Ethernet que contém a mensagem de resposta HTTP – Endereço Ethernet da fonte

<u>Questão 7</u>
Qual é o endereço MAC do destino? A que sistema corresponde?

Endereço MAC do destino: 3c:52:82:e6:4d:7b
Este endereço corresponde à máquina de que foi enviado o HTTP GET.

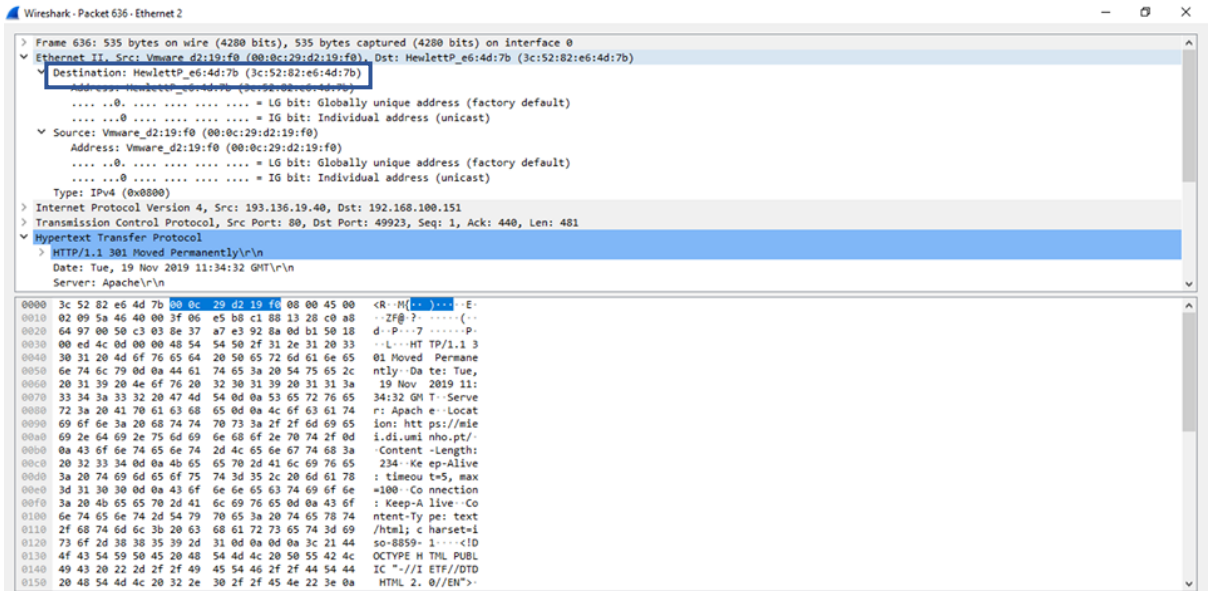


Figura 5: Conteúdo da trama Ethernet que contém a mensagem de resposta HTTP – Endereço MAC do destino

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

Os protocolos existentes na trama recebida são: IPv4 (*Internet Protocol Version 4),* TCP (*Transmission Control Protocol),* HTTP (*Hypertext Transfer Protocol),* e MAC *(Medium Access Protocol).*

1.2 Protocolo ARP

Questão 9
Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.

```
C:\Users\Ana Beatriz>arp -a

Interface: 192.168.100.151 --- 0xe
  Internet Address      Physical Address      Type
  192.168.100.196       54-ab-3a-5b-2f-c1     dynamic
  192.168.100.254       00-0c-29-d2-19-f0     dynamic
  192.168.100.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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

C:\Users\Ana Beatriz>
```

Figura 6: Tabela ARP

O objetivo do protocolo ARP é mapear endereços IP para endereços MAC. Esse mapeamento está registado numa tabela ARP.

- ***Internet Address***: Representa o endereço IP
- ***Physical Address***: Representa o endereço MAC relativo
- ***Type***: Indica o tipo de endereçamento

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. Todos os direitos reservados.

C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

Interface: 192.168.100.151 --- 0xe
  Internet Address      Physical Address      Type
  192.168.100.254       00-0c-29-d2-19-f0     dynamic
  192.168.100.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>
```

*Figura 7: Execução do comando arp -d * e resultante tabela ARP*

Questão 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?

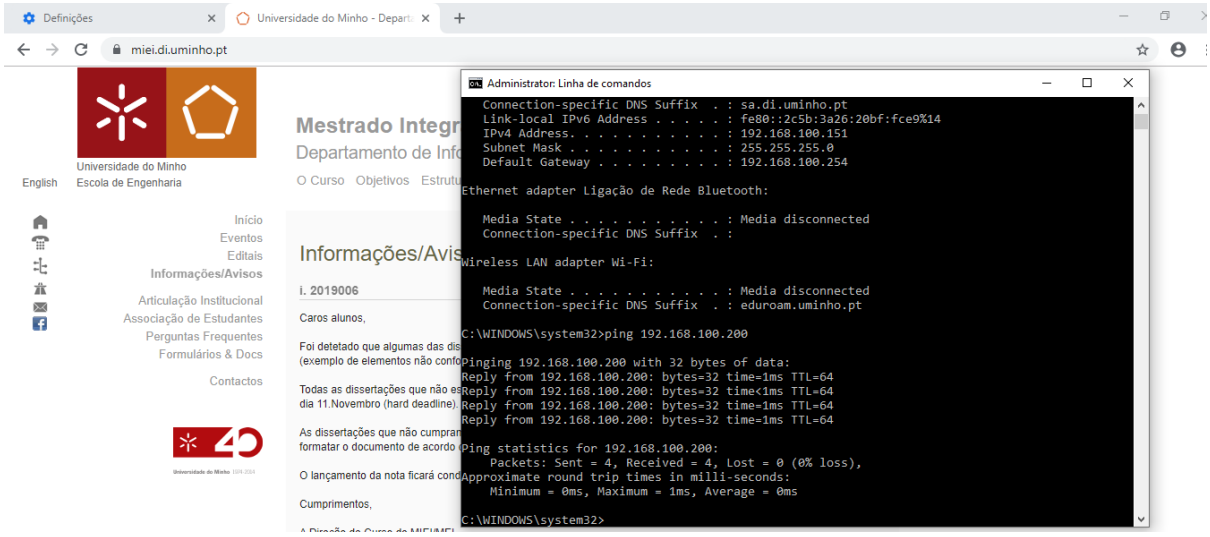


Figura 9: Execução do comando ping para um host da sala de aula/ acesso ao site fornecido

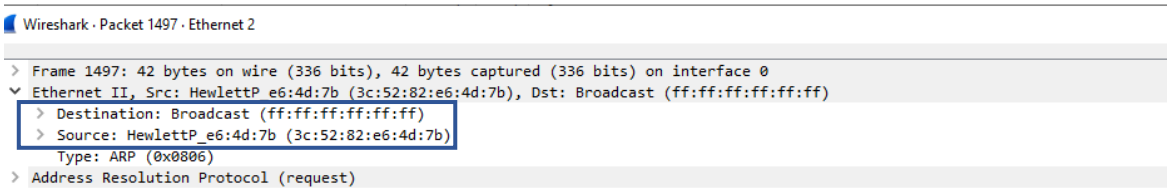


Figura 8: Conteúdo da trama com a mensagem ARP Request

Source : 3c:52:82:e6:4d:7b
Destination : ff:ff:ff:ff:ff:ff

O endereço destino usado é o de *Broadcast*, dado que, desta forma, é possível que a trama enviada numa rede local seja recebida e processada por todos os nós da mesma.

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

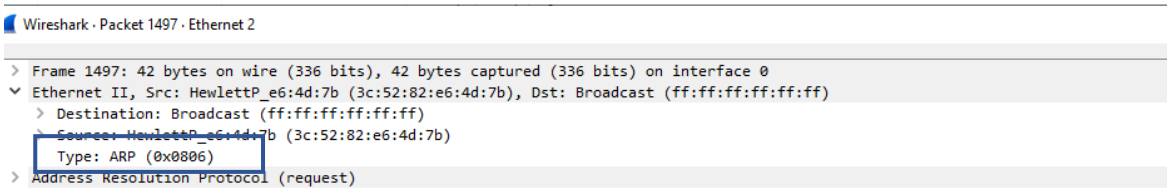


Figura 10: Conteúdo da trama com a mensagem ARP Request - análise do campo Type

O valor hexadecimal do campo *Type* é 0x0806 e indica o protocolo usado (ARP).

Questão 12
Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP (http://tools.ietf.org/html/rfc826.html).

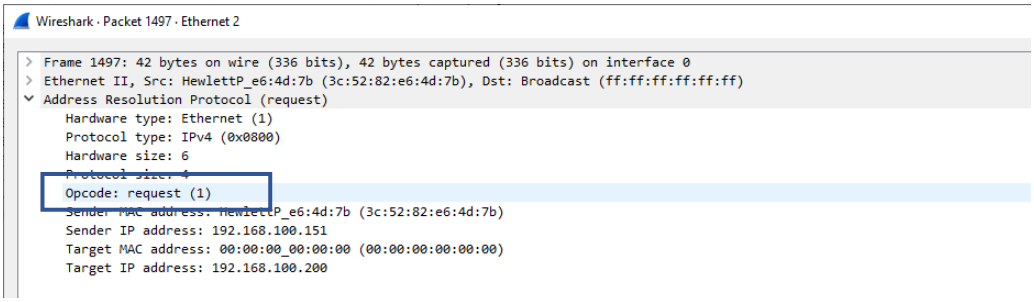


Figura 11: Conteúdo da trama com mensagem ARP Request - Campo opcode

O valor do campo ARP *opcode* é "*request* (1)", que especifica o que esta trama se trata de uma resposta.

Questão 13
Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

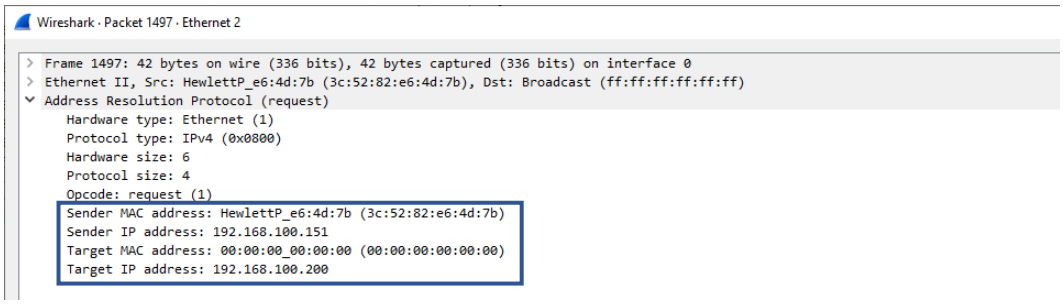
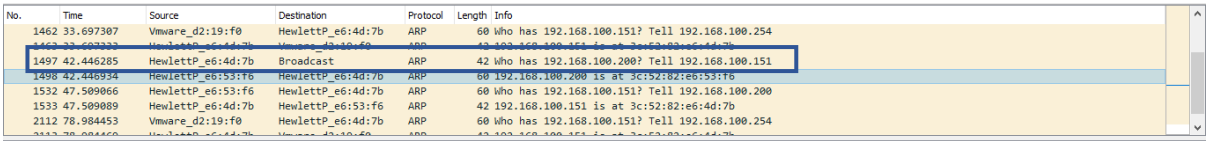


Figura 12: Conteúdo da trama com a mensagem ARP Request - Tipo de endereços

O tipo de endereços que está contido na mensagem ARP são os IP e MAC *Addresses.*

Os endereços de IP e MAC da origem dizem respeito à máquina nativa. No que diz respeito aos endereços do destino, podemos verificar que o endereço MAC se encontra com o valor 00:00:00:00:00:00, dado que no momento de envio da trama, este valor é desconhecido.

Questão 14
Explicite que tipo de pedido ou pergunta é feito pelo host de origem?



No.	Time	Source	Destination	Protocol	Length	Info
1462	33.697307	Vmware_d2:19:f0	HewlettP_e6:4d:7b	ARP	60	Who has 192.168.100.151? Tell 192.168.100.254
1497	42.446285	HewlettP_e6:4d:7b	Broadcast	ARP	42	Who has 192.168.100.200? Tell 192.168.100.151
1498	42.446934	HewlettP_e6:53:f6	HewlettP_e6:4d:7b	ARP	60	192.168.100.200 is at 3c:52:82:e6:53:f6
1532	47.509066	HewlettP_e6:53:f6	HewlettP_e6:4d:7b	ARP	60	Who has 192.168.100.151? Tell 192.168.100.200
1533	47.509089	HewlettP_e6:4d:7b	HewlettP_e6:53:f6	ARP	42	192.168.100.151 is at 3c:52:82:e6:4d:7b
2112	78.984453	Vmware_d2:19:f0	HewlettP_e6:4d:7b	ARP	60	Who has 192.168.100.151? Tell 192.168.100.254

Figura 13: Tipo de pedido efetuado pelo host de origem

Como podemos verificar pela Figura 13 , o *host* de origem pergunta "*Who has 192.168.100.200? Tell 192.168.100.151*", com o intuito de descobrir qual o endereço MAC correspondente a esse endereço IP.

Questão 15
Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

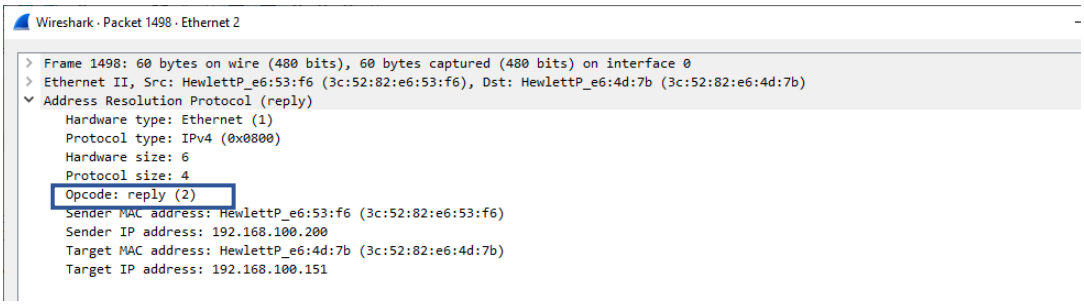


Figura 14: Conteúdo trama com a mensagem de resposta

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

O valor do campo ARP *opcode* é "*reply* (2)", especificando que se trata de uma trama de resposta.

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

A resposta ao pedido ARP está entre os *bytes* 6-12 da camada MAC *Ethernet*, que diz respeito ao endereço MAC origem.

Questão 16

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?

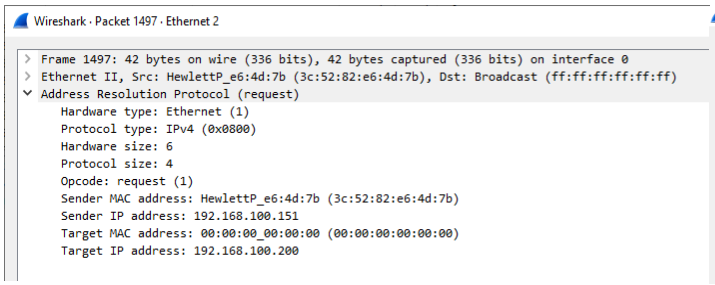


Figura 15: Pacote de pedido ARP

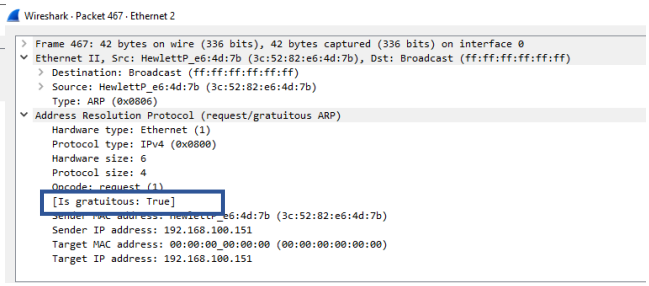


Figura 16: Pacote de pedido ARP gratuito

Um ARP gratuito é enviado sempre que um *host* se liga a uma rede, onde lhe é atribuído um endereço de IP, em que o principal objeto é determinar se um outro *host* na rede tem o mesmo IP que este.

Sendo assim, a distinção entre um pedido ARP gratuito dos restantes pedidos ARP reside na existência de uma *flag* "*is gratuitous : True*" e conseguimos verificar que o endereço IP da origem é igual ao endereço IP do destino.

1.3 Domínios de colisão

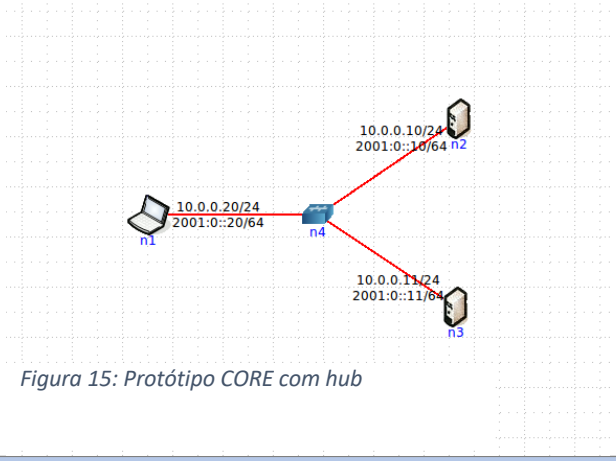


Figura 15: Protótipo CORE com hub

Questão 17
Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

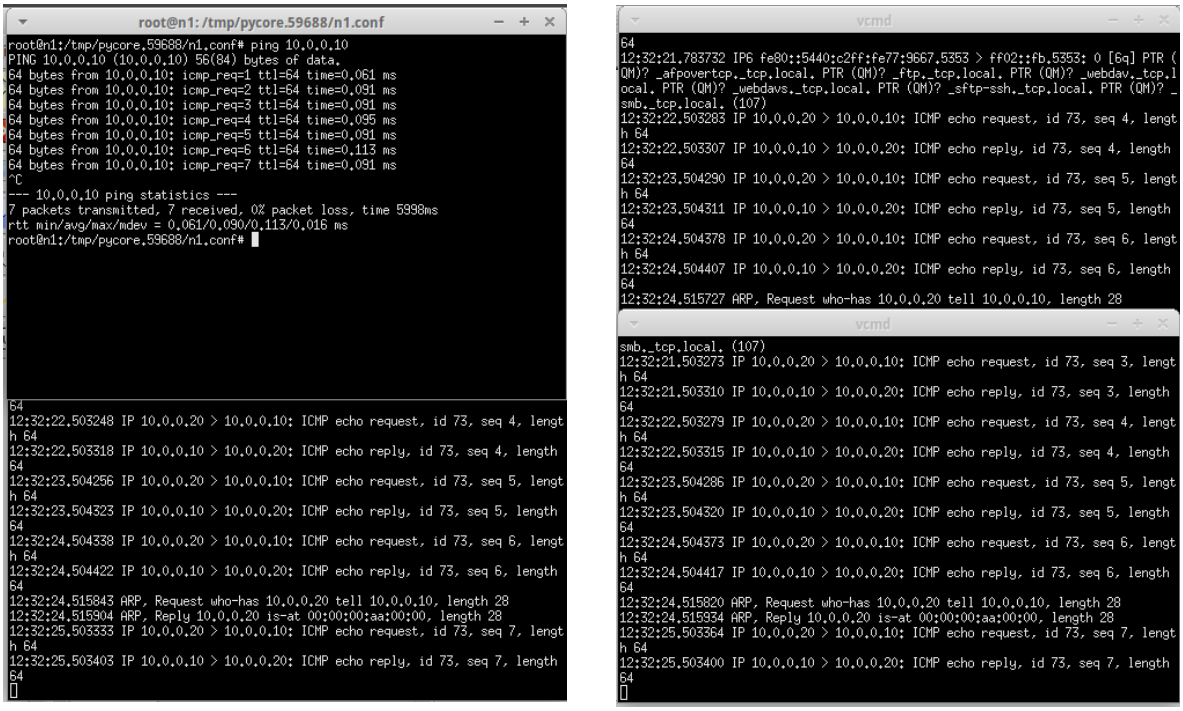


Figura 16: Execução dos comandos ping tcpdump de n1 para n2

Com a presença do *hub*, todos os servidores recebem os pacotes, dado que este, quando recebe um pacote de dados, reencaminha-os para todos os componentes dessa sub-rede.

Questão 18

Na topologia de rede substitua o hub por um switch. Repita os procedimentos que realizou na pergunta anterior. 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.

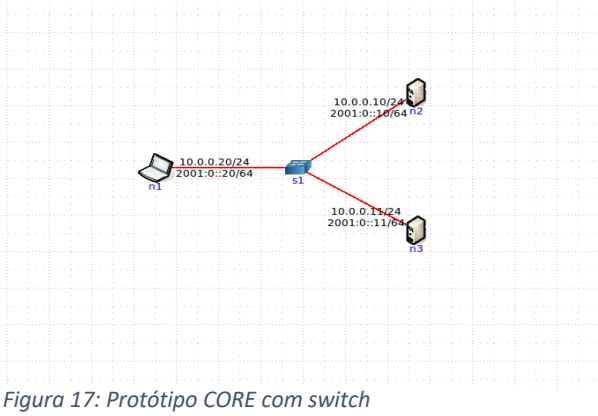


Figura 17: Protótipo CORE com switch

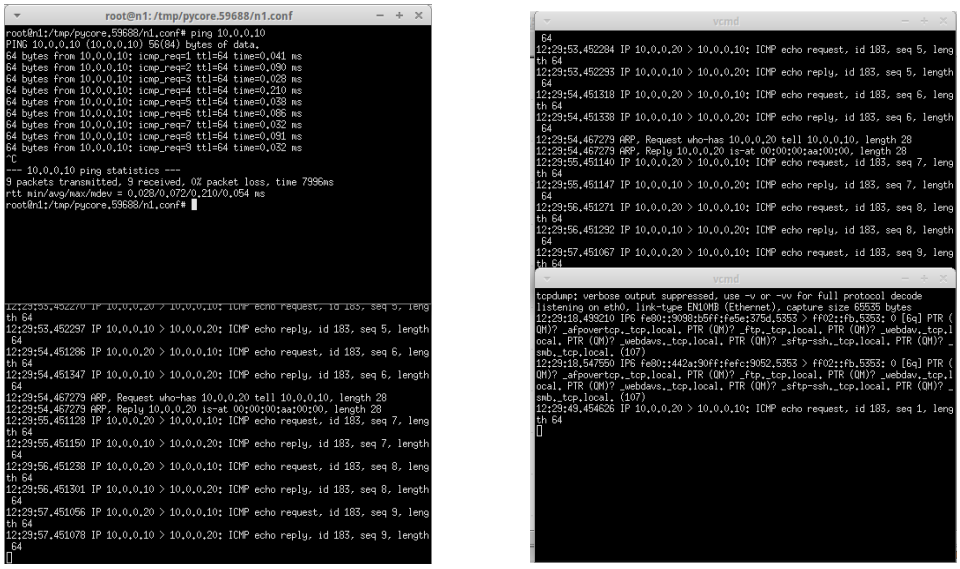


Figura 18: Execução dos comandos ping tcpdump de n1 para n2

Com o *switch*, o servidor n3 não é capaz de visualizar o tráfego emitido entre n1 e n2, visto que apenas captura um pacote que corresponde a um pacote "ARP Broadcast" enviado, de modo a conhecer o endereço MAC para onde o pacote deverá ser enviado, contrariamente ao que aconteceria na presença do hub.

Desta forma, pode-se concluir que o número de colisões nos *switches* são menores do que nos *hubs*, uma vez que nos *CH* a transmissão da mensagem recebida por todos os nodos da rede ocorre através de apenas um canal de comunicação (o que potencia colisões frequentes). Enquanto que os *switches* limitam o envio de mensagens apenas para o destino pretendido (o que reduz o número de colisões).

2. Conclusões

Ao longo da realização do proposto no enunciado, bem como do presente relatório o grupo pôde aprofundar os conhecimentos previamente adquiridos em contexto teórico, nomeadamente desde os endereços MAC, passando pelo *Address Resolution Protocol* (ARP) e Ethernet até à interligação de redes locais.
Numa primeira etapa, utilizou-se o *Wireshark* com a vista à efetuação de capturas para posteriores considerações acerca dos resultados obtidos, onde foram analisadas as tramas Ehternet, protocolos e deteção de erros, não descartando o aperfeiçoamento da definição prévia do protocolo ARP.
Numa segunda etapa, fez-se uso do emulador *CORE* para a elaboração de topologias a fim de ser possível ao grupo comparar em que medida a utilização dos *switches* e *hubs* afeta o número de colisões nas tramas, onde foi possível concluir a viabilidade do primeiro relativamente ao segundo.
Em suma, a bagagem recolhida da experiência prática do uso destas duas ferramentas e consequente análise do significado inerente ao obtido fomentou a capacidade de extrair conclusões práticas que se apresentam em concordância com os conceitos teóricos apreendidos.