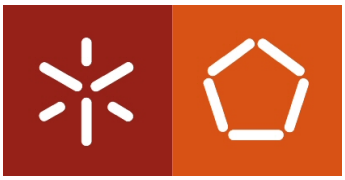


Universidade do Minho

Departamento de Informática

Relatório de Redes de Computadores
Grupo 3

Inês Alves (A81368) João Lopes (A80397)
Sofia Teixeira (a80624)

30 de Novembro de 2018

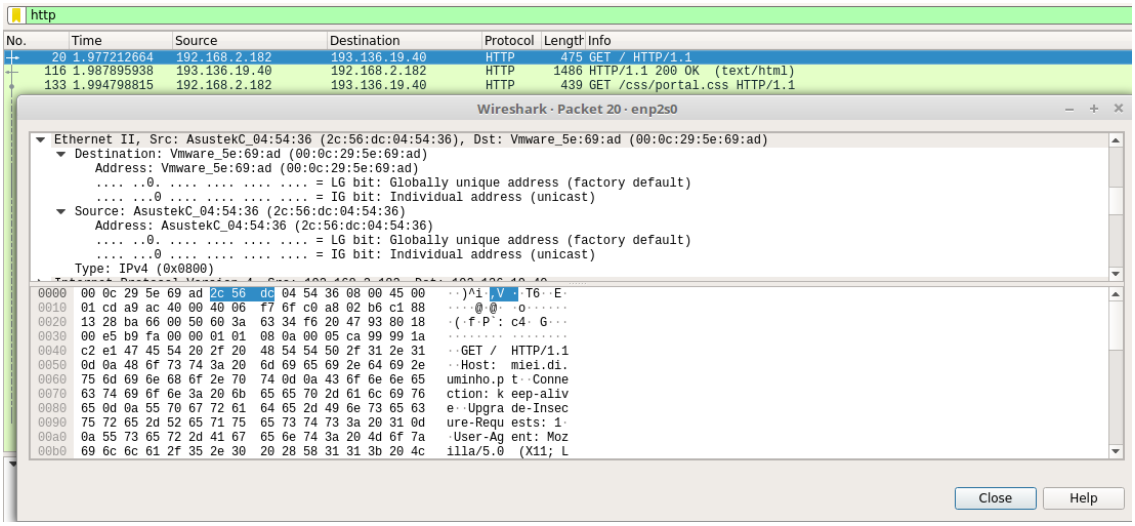
Conteúdo

1 Questões e Respostas

1.1 Pergunta 3: Captura e análise de Tramas Ethernet

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

O endereço MAC de origem é 2c:56:dc:04:54:36 e o de destino é 00:0c:29:5e:69:ad, como podemos verificar pela imagem seguinte:

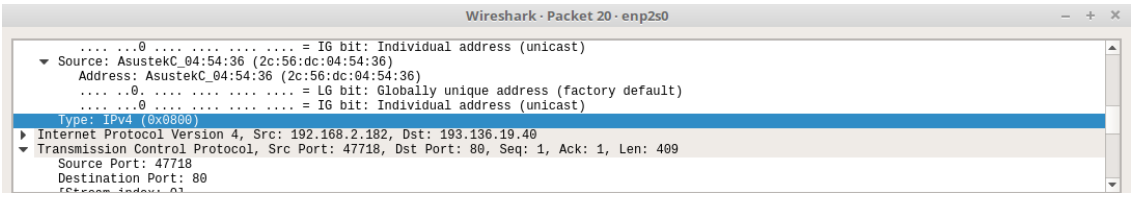


2. Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem identifia o sistema de origem, o AsustekC, e o endereço MAC de destino identifica o sistema de destino, o Vmware, que se trata da interface que conecta a rede em que nos encontramos à exterior.

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

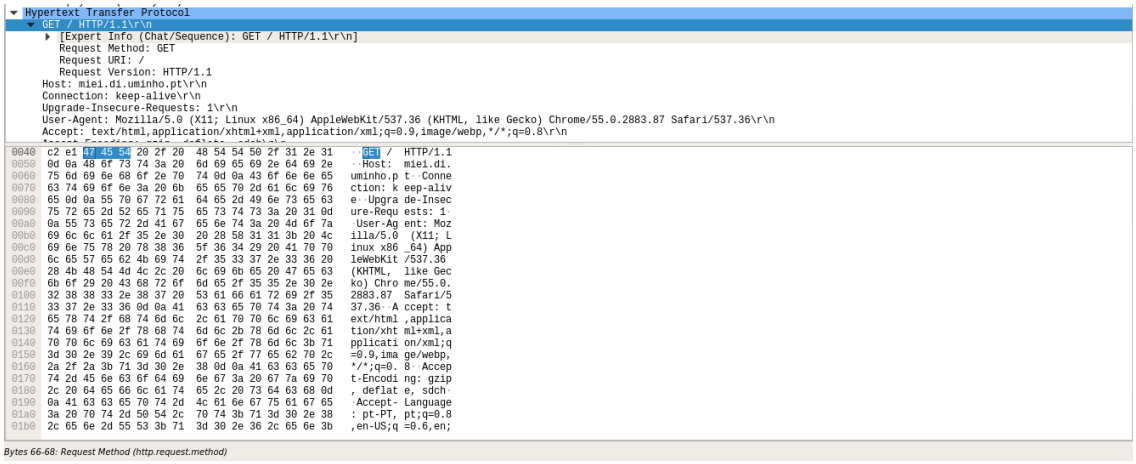
O valor hexadecimal do campo Type é 0x0800.



Indica o tipo de dados que a trama encapsula. Neste caso indica que se trata do 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.

São usados 66 bytes, como mostra a figura seguinte:



Cálculo da sobrecarga:

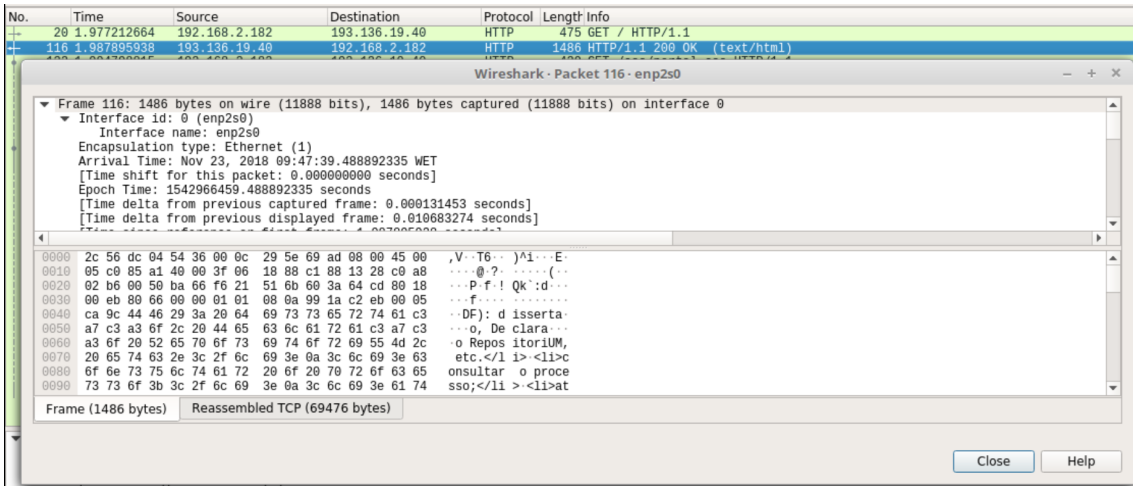
$$\frac{66 * 100}{475} = 13.9\%$$

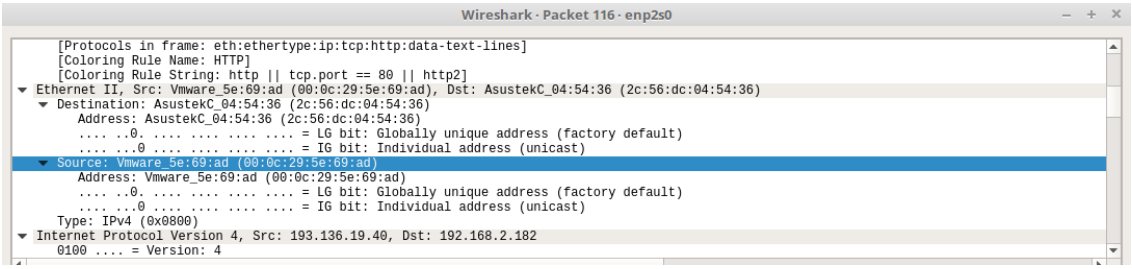
5. Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para deteção de erros não está a ser usado. Em sua opinião, porque será?

Pode-se concluir que o Frame Check Sequence não está a ser usado uma vez que este não aparece na captura da trama. Visto que a quantidade de erros que surgem é bastante baixa, as NICs, estando numa rede wired, não é consideram que compense usar o FCS devido ao seu elevado custo.

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

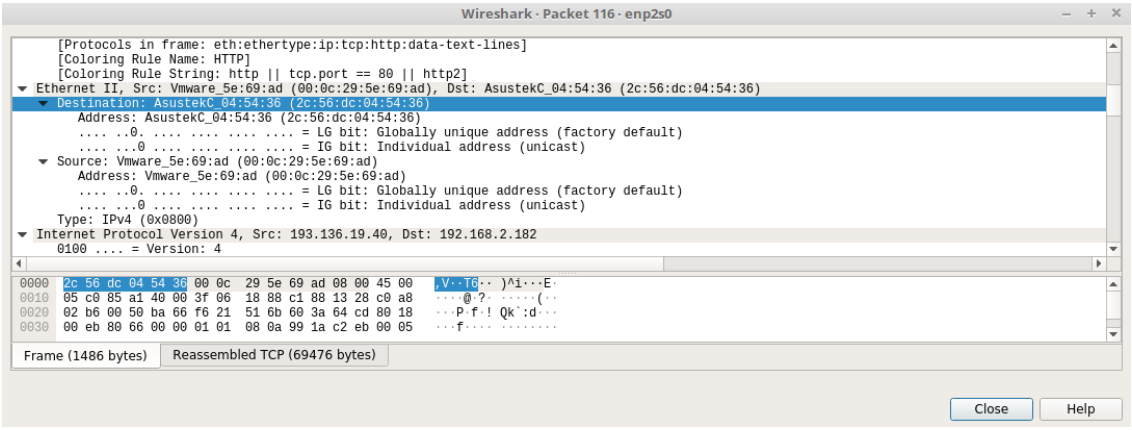
O endereço Ethernet da fonte é 00:0c:29:5e:69:ad. Corresponde ao endereço físico do router ao qual estamos ligados.





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

O endereço MAC de destino é 2c:56:dc:04:54:36. Corresponde à interface ativa da máquina que usamos.



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

Identificamos os protocolos HTTP (Hypertext Transfer Protocol), Ethernet, TCP (Transmition Control Protocol) e, como referido acima, IPv4 (Internet Protocol Version 4).

1.2 Pergunta 4: Protocolo ARP

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

Na primeira coluna vemos representado o endereço IP 192.168.100.254; na segunda coluna o endereço MAC 00:0c:29:d2:19:f0; por fim, a terceira coluna representa a rede Ethernet.

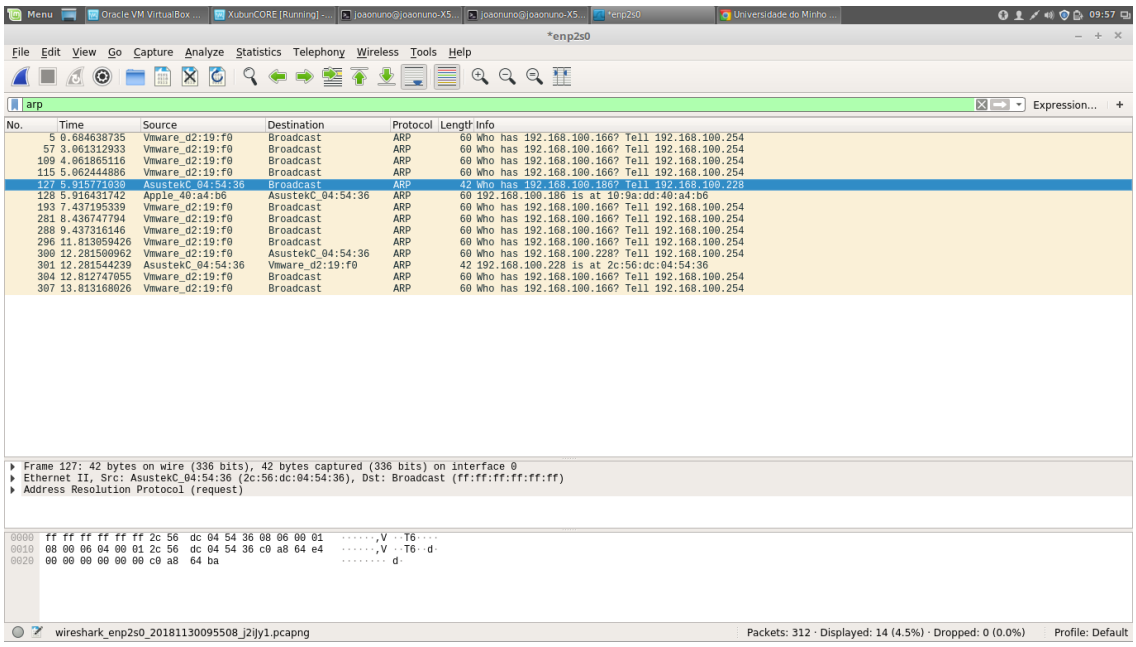
```
joaonuno@joaonuno-X556UF ~ $ arp -a
gw.sa.di.uminho.pt (192.168.100.254) at 00:0c:29:d2:19:f0 [ether] on enp2s0
```

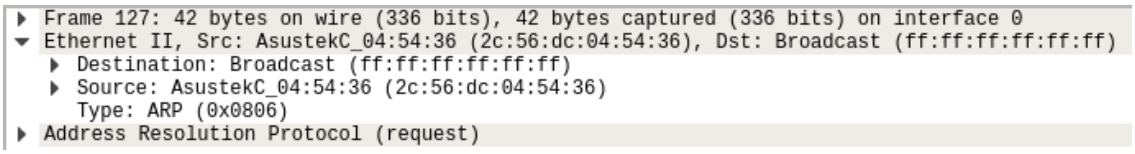
Inicie a captura de tráfego com o Wireshark, e aceda a http://miei.di.uminho.pt. Efectue também um ping para um host da sala de aula (e.g. ping 192.168.100.xxx) que esteja a ser usado por outro grupo. Pare a captura de tráfego e tente localizar o tráfego ARP. Se necessário, limite os protocolos visíveis 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:

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 valor hexadecimal do endereço origem é 2c:56:dc:04:54:36 e o endereço de destino é ff:ff:ff:ff:ff:ff (Broadcast). Este endereço de destino é usado uma vez que o nosso dispositivo não está diretamente conectado ao dispositivo para o qual queremos enviar a mensagem e, portanto, é necessário enviar uma mensagem para todos os dispositivos da rede para que assim o dispositivo pretendido possa responder com o seu endereço MAC.

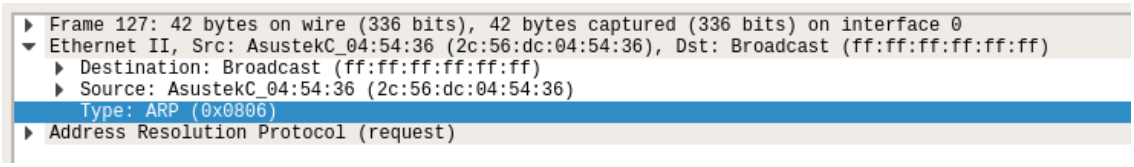
```
joaonuno@joaonuno-X556UF ~ $ ping 192.168.100.186
PING 192.168.100.186 (192.168.100.186) 56(84) bytes of data.
64 bytes from 192.168.100.186: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 192.168.100.186: icmp_seq=2 ttl=64 time=0.707 ms
64 bytes from 192.168.100.186: icmp_seq=3 ttl=64 time=0.574 ms
64 bytes from 192.168.100.186: icmp_seq=4 ttl=64 time=0.693 ms
64 bytes from 192.168.100.186: icmp_seq=5 ttl=64 time=0.769 ms
64 bytes from 192.168.100.186: icmp_seq=6 ttl=64 time=0.742 ms
64 bytes from 192.168.100.186: icmp_seq=7 ttl=64 time=0.767 ms
64 bytes from 192.168.100.186: icmp_seq=8 ttl=64 time=0.504 ms
^C
--- 192.168.100.186 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7002ms
rtt min/avg/max/mdev = 0.504/0.730/1.085/0.161 ms
```





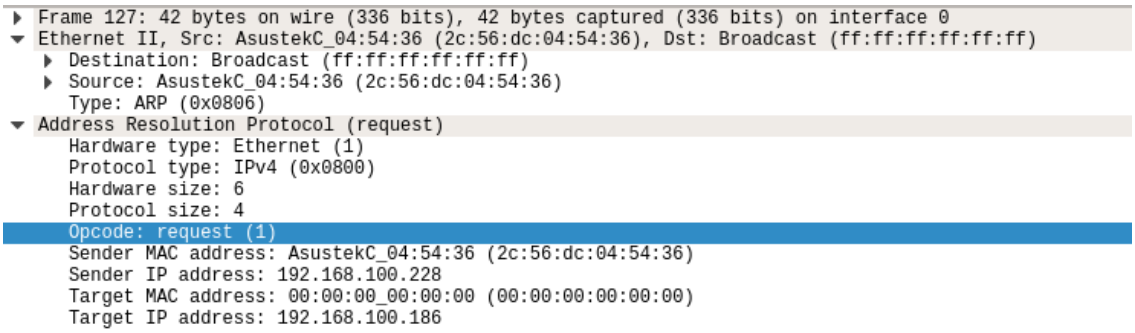
11. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?

Como podemos verificar na figura seguinte, o valor hexadecimal do campo tipo da trama Ethernet é 0x0806, indicando que a camada acima está a usar o protocolo ARP.



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.*

O valor do campo ARP opcode é 1, o que indica que a nossa máquina está a efetuar um request. Deste modo, concluímos que está a ser realizado um pedido de resposta aos dispositivos cujo ip corresponde ao indicado no request.



13. Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Como podemos observar na figura, na mensagem ARP podemos identificar endereços IP e MAC. O protocolo ARP permite obter o endereço MAC da máquina de destino, usando o endereço IP. Este processo consiste no envio de broadcast para procurar a máquina com o IP pretendido. Visto que o endereço MAC de destino é 00:00:00:00:00:00, podemos então concluir que o endereço MAC de destino não é conhecido e o arp está a enviar o broadcast.

```
▸ Frame 127: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▾ Ethernet II, Src: AsustekC_04:54:36 (2c:56:dc:04:54:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: AsustekC_04:54:36 (2c:56:dc:04:54:36)
    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: AsustekC_04:54:36 (2c:56:dc:04:54:36)
    Sender IP address: 192.168.100.228
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.100.186
```

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

Ao fazer ping, o host de origem envia um request a todos os dispositivos na rede a perguntar se algum dos dispositivos tem o IP que procura: "Who has 192.168.100.186?". Este request vai causar que, caso exista um dispositivo com o determinado IP, este mande uma resposta com o seu endereço MAC.

15. Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.

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

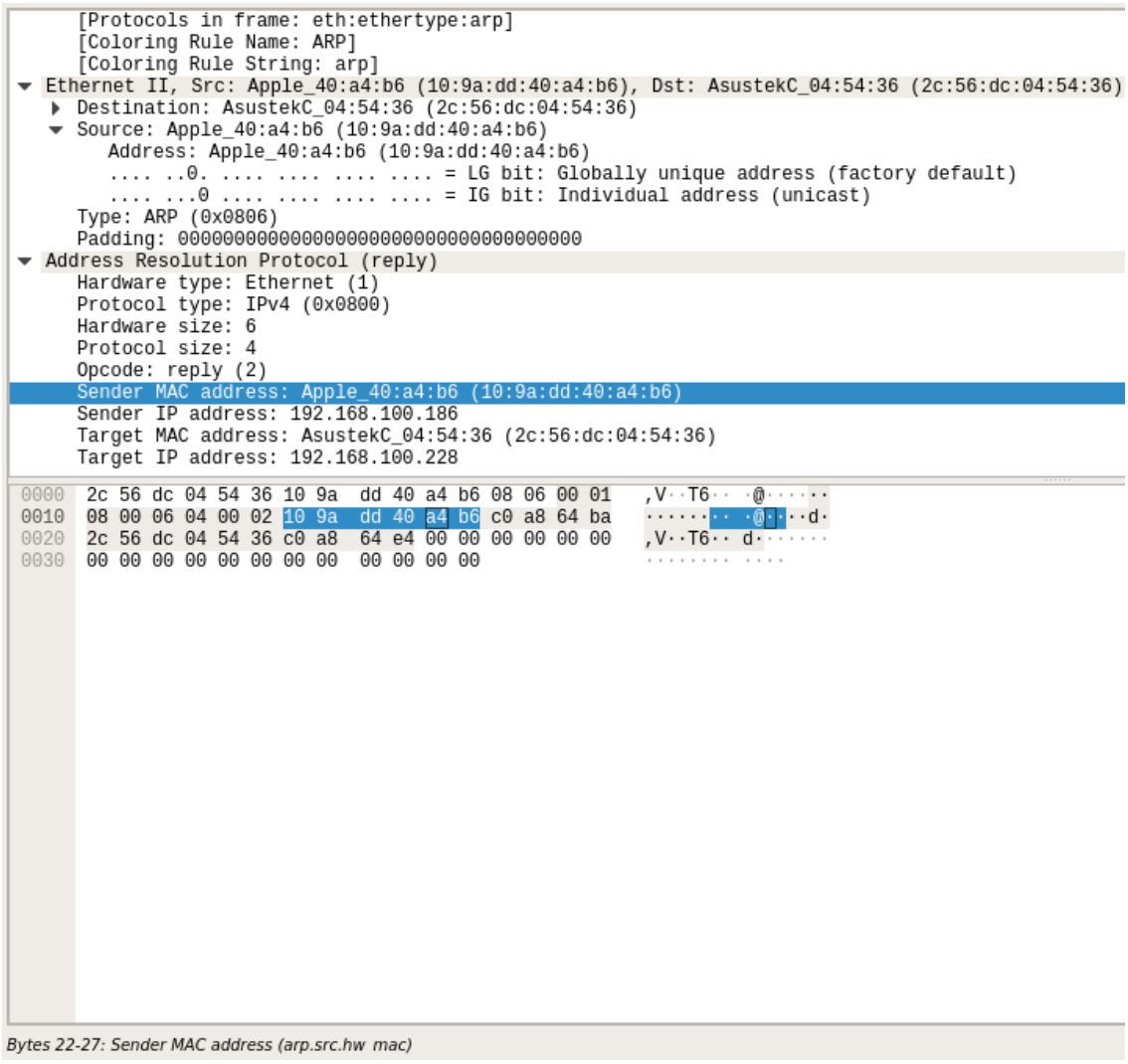
O campo ARP opcode tem o valor 2. Este valor revela que se trata da resposta - reply(2) - obtida ao request previamente efetuado pela nossa máquina.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.684638735	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
57	3.061312933	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
109	4.061865116	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
115	5.062444886	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
127	5.915771030	AsustekC_04:54:36	Broadcast	ARP	42	Who has 192.168.100.186? Tell 192.168.100.228
128	5.916431742	Apple_40:a4:b6	AsustekC_04:54:36	ARP	60	192.168.100.186 is at 10:9a:dd:40:a4:b6
193	7.437195339	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
281	8.436747794	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
288	9.437316146	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
296	11.813059426	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
300	12.281500962	Vmware_d2:19:f0	AsustekC_04:54:36	ARP	60	Who has 192.168.100.228? Tell 192.168.100.254
301	12.281544239	AsustekC_04:54:36	Vmware_d2:19:f0	ARP	42	192.168.100.228 is at 2c:56:dc:04:54:36
304	12.812747055	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254
307	13.813168026	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.166? Tell 192.168.100.254

```
▸ Frame 128: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▾ Ethernet II, Src: Apple_40:a4:b6 (10:9a:dd:40:a4:b6), Dst: AsustekC_04:54:36 (2c:56:dc:04:54:36)
  ▸ Destination: AsustekC_04:54:36 (2c:56:dc:04:54:36)
  ▸ Source: Apple_40:a4:b6 (10:9a:dd:40:a4:b6)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_40:a4:b6 (10:9a:dd:40:a4:b6)
    Sender IP address: 192.168.100.186
    Target MAC address: AsustekC_04:54:36 (2c:56:dc:04:54:36)
    Target IP address: 192.168.100.228
```

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

A resposta ao pedido ARP está entre 22-27 bytes, como está demonstrado no fim da figura seguinte. Obtivemos esta informação através da secção *Sender MAC Adress*.



1.3 Pergunta 5: ARP Gratuito

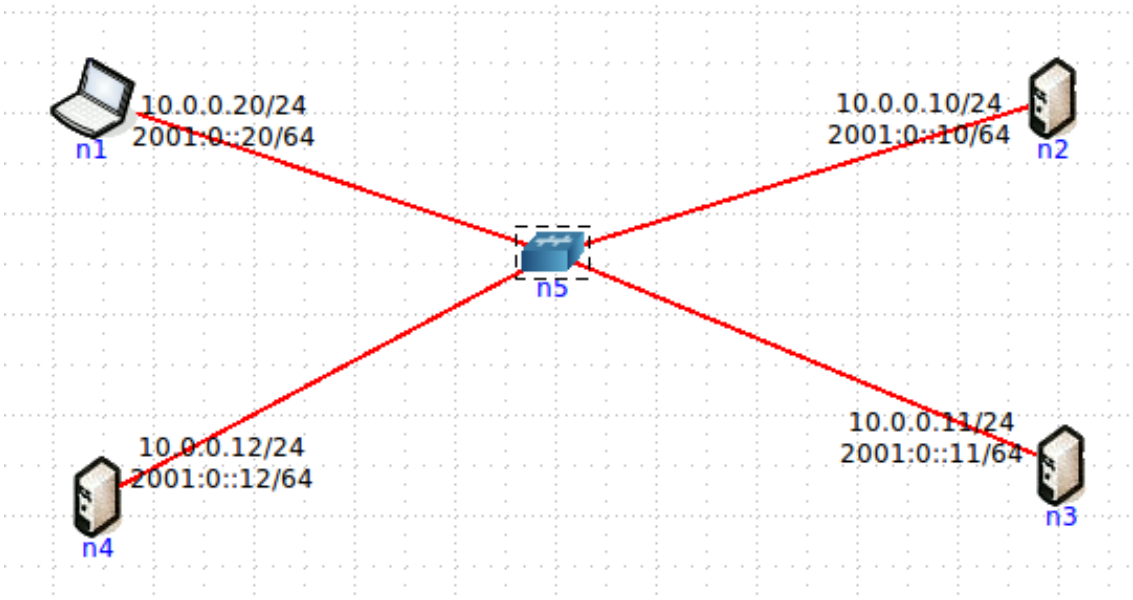
16. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado?

1	0.000000000	Vmware_d2:19:f0	Broadcast	ARP	60 Who has 192.168.100.208? Tell 192.168.100.254
3	0.999603927	Vmware_d2:19:f0	Broadcast	ARP	60 Who has 192.168.100.208? Tell 192.168.100.254
26	5.582985338	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)
30	6.583124407	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)
37	7.103045986	AsustekC_04:54:36	Broadcast	ARP	42 Who has 192.168.100.254? Tell 192.168.100.228
38	7.103433554	Vmware_d2:19:f0	AsustekC_04:54:36	ARP	60 192.168.100.254 is at 00:0c:29:d2:19:f0
72	7.583219383	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)
103	8.583377185	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)
152	9.583476611	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)
193	10.583554822	AsustekC_27:fc:41	Broadcast	ARP	60 Gratuitous ARP for 192.168.100.200 (Reply)

Os ARPs gratuitos são usados para verificar se existe outro dispositivo na rede com o mesmo endereço IP. Se for recebida uma resposta à solicitação do ARP gratuito, será concluído que irá

ocorrer um conflito caso o seu endereço IP seja usado. Assim, seria suposto aparecer o request e não ser obtida qualquer resposta, visto que não seria suposto haver mais nenhum host com o mesmo IP.

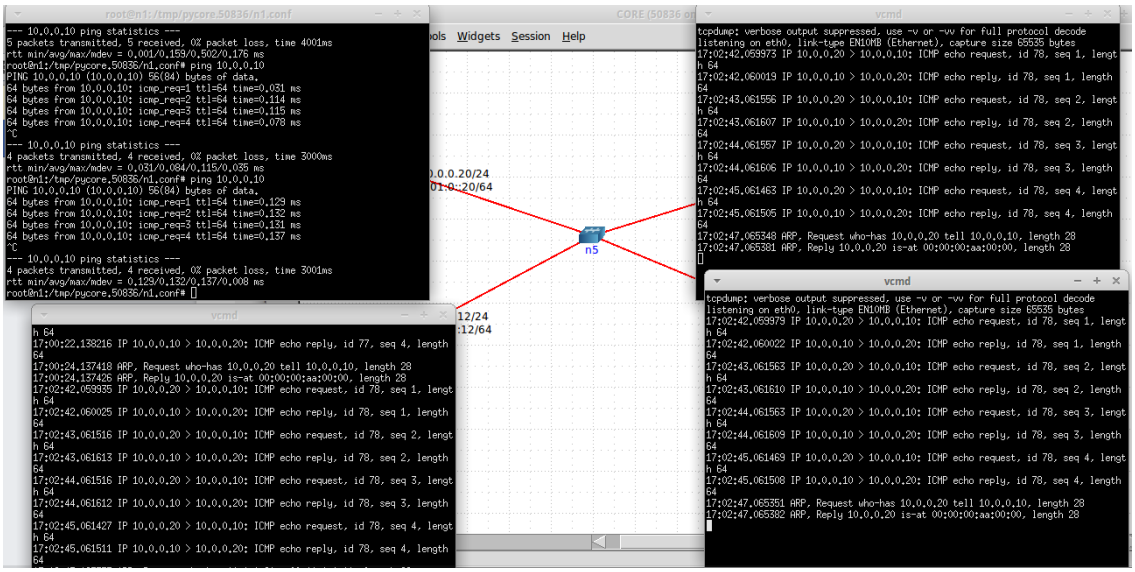
1.4 Pergunta 6: Domínios de colisão



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

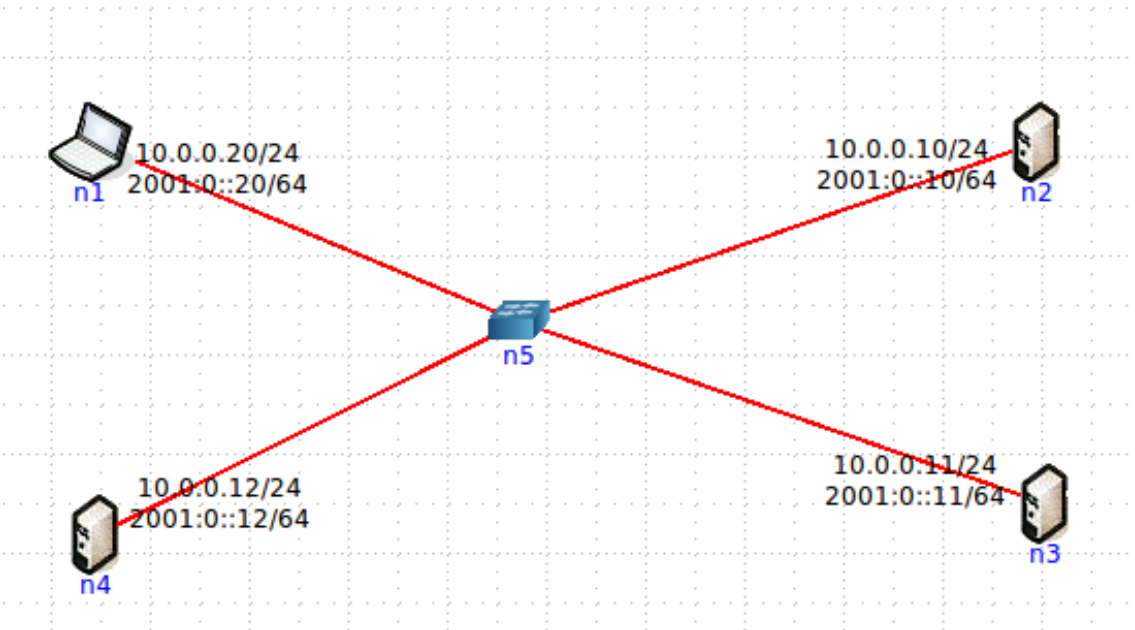
Com a opção tcpdump, o *hub* redireciona o tráfego para as interfaces de todos os dispositivos, com exceção do que está a enviar (n1). Visto isto, podemos concluir que, embora a mensagem fosse apenas para o dispositivo n2, esta é enviada desnecessariamente para o n3 e n4.

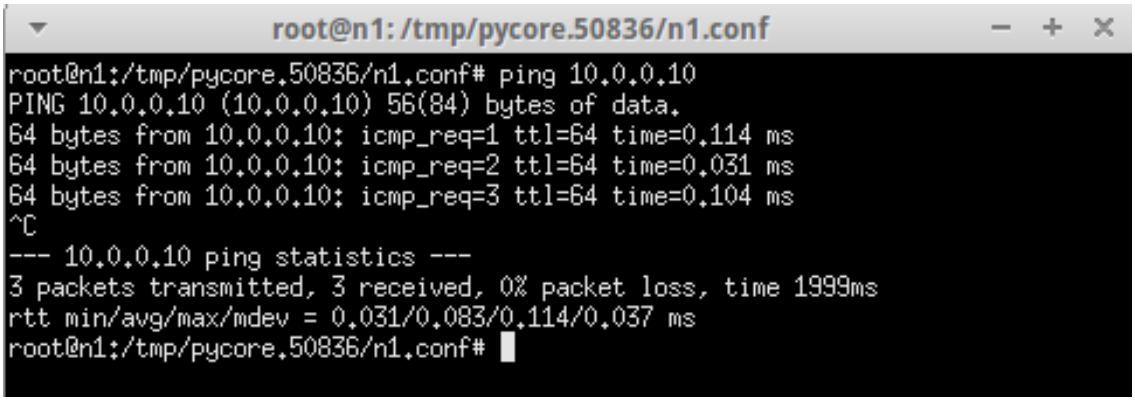
```
root@n1: /tmp/pycore.50836/n1.conf
root@n1:/tmp/pycore.50836/n1.conf# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_req=1 ttl=64 time=0.070 ms
64 bytes from 10.0.0.10: icmp_req=2 ttl=64 time=0.502 ms
64 bytes from 10.0.0.10: icmp_req=3 ttl=64 time=0.098 ms
64 bytes from 10.0.0.10: icmp_req=4 ttl=64 time=0.001 ms
64 bytes from 10.0.0.10: icmp_req=5 ttl=64 time=0.128 ms
^C
--- 10.0.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.001/0.159/0.502/0.176 ms
root@n1:/tmp/pycore.50836/n1.conf#
```

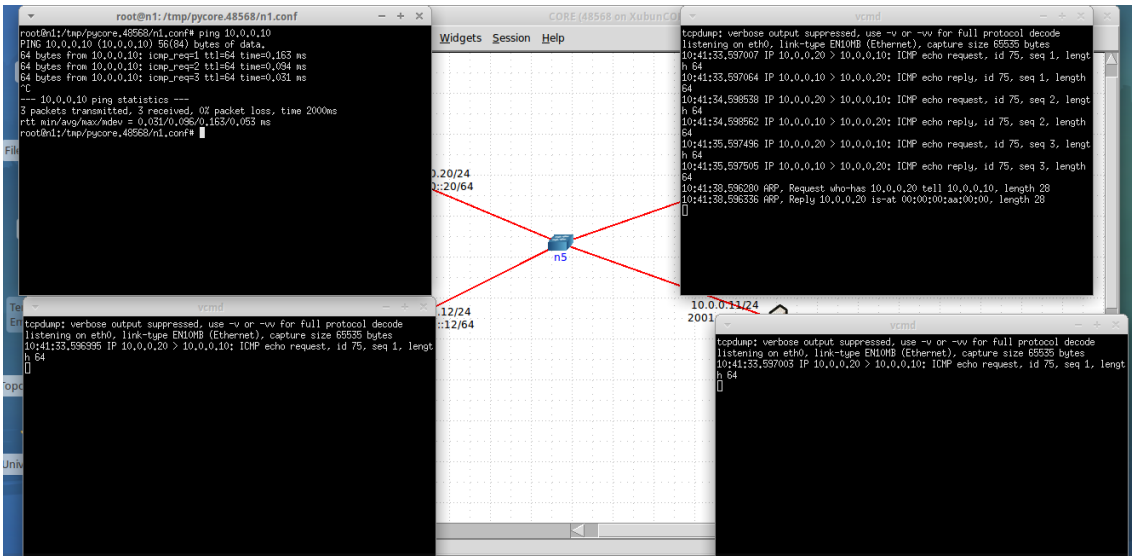


18. Na topologia de rede substitua o *hub* por um switch. Repita os procedimentos que realizou na pergunta anterior. Comente os resultados obtidos quanto à utilização de *hub*s e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.

Com a substituição de um *hub* por um switch observamos que o tráfego não flui nas interfaces dos outros dispositivos, fluindo apenas para n2, como era suposto. Nos restantes dispositivos n3 e n4, é recebido apenas o envio arp broadcast. Podemos assim concluir que os *hubs*, devido ao uso de um único canal constantemente partilhado por todos os dispositivos na redes que faz com que a mensagem seja partilhada para todos, está muito mais propício a colisões do que o switch as evita limitando a mensagem para o destino pretendido através de portas para cada interface.




root@n1: /tmp/pycore.50836/n1.conf
root@n1:/tmp/pycore.50836/n1.conf# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_req=1 ttl=64 time=0.114 ms
64 bytes from 10.0.0.10: icmp_req=2 ttl=64 time=0.031 ms
64 bytes from 10.0.0.10: icmp_req=3 ttl=64 time=0.104 ms
^C
--- 10.0.0.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.031/0.083/0.114/0.037 ms
root@n1:/tmp/pycore.50836/n1.conf#


Widgets
Session
Help
n5
10.0.0.11/24

2 Conclusão

Este projeto foi dividido em diferentes fases, identificadas neste mesmo relatório.

Na primeira parte deste relatório foi feita uma captura, seguida da análise de uma trama Ethernet com a mensagem HTTP GET, estudando assim os vários campos do cabeçalho da trama referida.

Foi também estudado o protocolo ARP, fazendo outra captura onde foram analisadas duas tramas: a do pedido e a da resposta. Para além disso, foi feita uma pesquisa do ARP gratuito e as suas vantagens e desvantagens.

Por fim, foi feita uma topologia no CORE, onde foram verificadas as diferenças de usar um *hub* e um *Switch* para conectar vários dispositivos. Nesta fase foram identificadas diversas vantagens e desvantagens em ambos os dispositivos, consolidando o nosso conhecimento acerca dos mesmos.