TP3 - Camada de Ligação Lógica

Engenharia Informática
Universidade do Minho
2019/2020

Grupo - PL6.G06

Paulo Lima | a89983

Mafalda Costa | a83919

Maria Silva | a83840

Objetivo

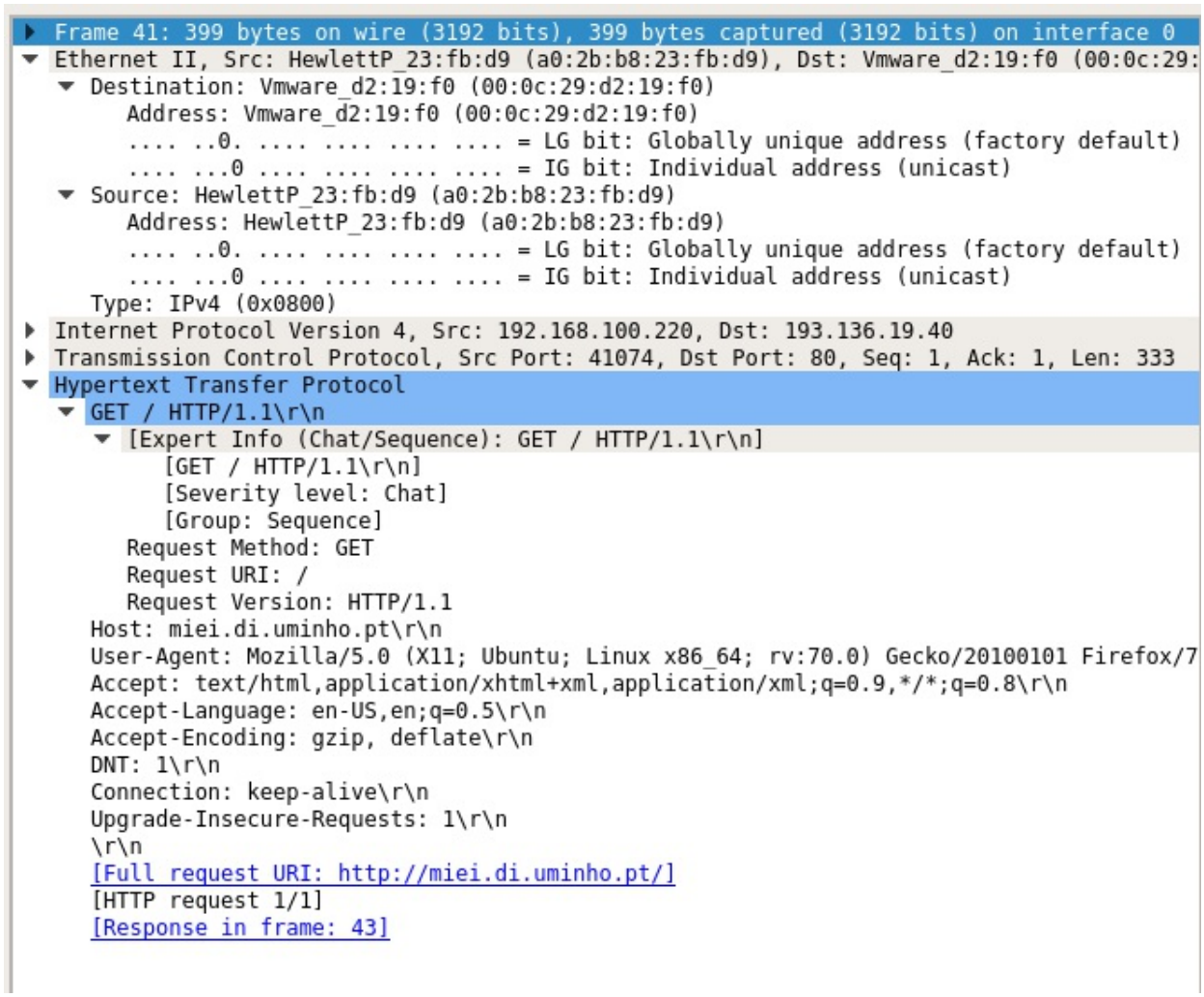
- Ganhar conhecimentos a nível da camada de ligação lógica
- Utilização as tecnologias Ethernet e o protocolo ARP

Questões e Respostas

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 o [a0:2b::b8:23:fb:d9] e o endereço MAC de destino é o [00:0c:29:d2:19:f0].



2) Identifique a que sistemas se referem. Justifique.

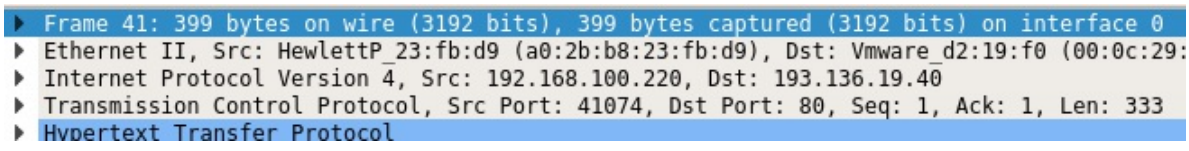
O endereço mac refere-se a um endereço físico atribuído a uma interface de rede.
Como podemos observar na imagem, a origem(source) refere-se ao endereço físico do nosso computador e o destination refere-se ao endereço físico do router com o qual estamos a comunicar.

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

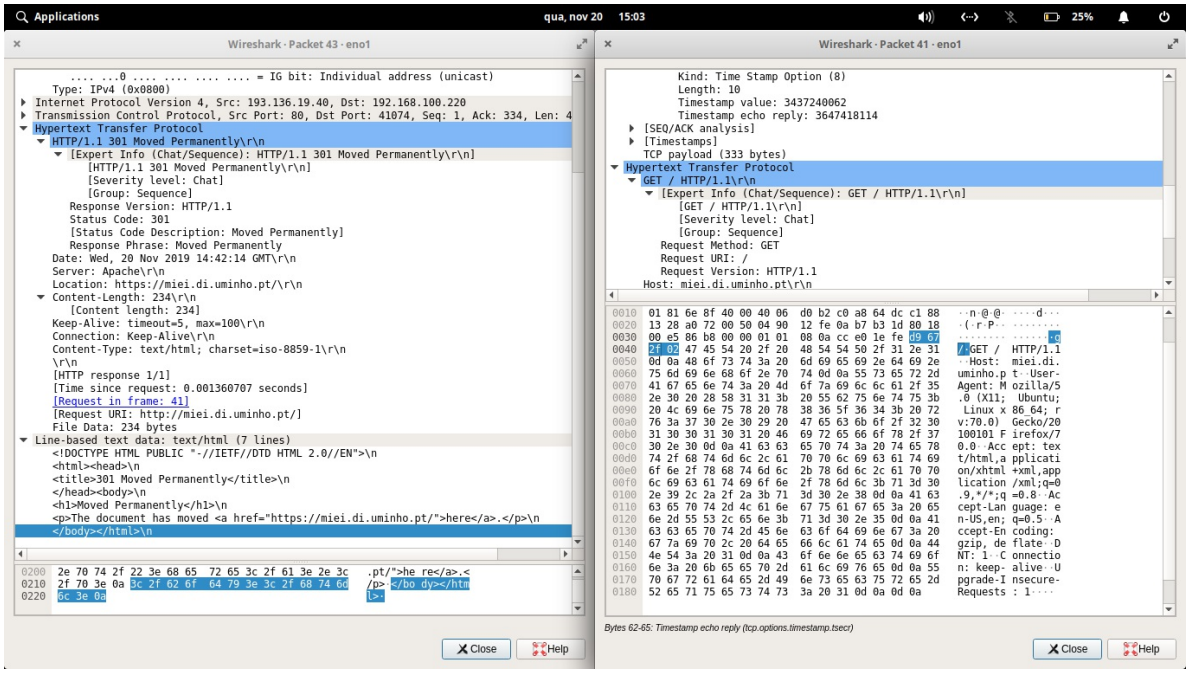
O valor hexadecimal do campo Type é [0x0800] o que significa que se trata do tipo IPv4.

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.

- Foram capturados 399 bytes.



- O caractere "G" encontra-se no byte 65.
- A percentagem da sobrecarga introduzida pela pilha protocolar é dada por: ((65*100)/399) 16,290726%



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?

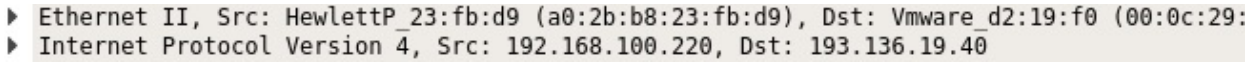
- O campo FCS não está a ser utilizado pois como foi utilizada uma rede ethernet que é considerada muito segura, não existiu necessidade de inserir esse campo.

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

O endereço MAC origem é o [00:0c:29:d2:19:f0] e o endereço IP correspondente o [193.136.19.40]. Este endereço corresponde ao endereço de destino do link dado (http://miei.di.uminho.pt).

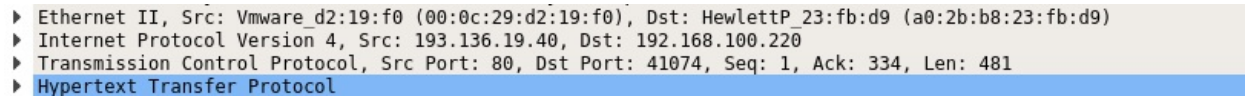
7) Qual é o endereço MAC do destino? A que sistema corresponde?

O endereço MAC destino é o [a0:2b:b8:23:fb:d9] e o endereço IP correspondente o [192.168.100.220] corresponde ao nosso endereço, que deu origem ao pedido inicial.



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

Os protocolos existentes são: IP, TCP, Ethernet e HTTP.



4 - Protocolo ARP

```
root@hostlinuz:/home/linux/Documents/NON GIT/escola/3ano/rc/tp3# ping -c 6 192.168.100.190
PING 192.168.100.190 (192.168.100.190) 56(84) bytes of data.
64 bytes from 192.168.100.190: icmp_seq=1 ttl=64 time=0.706 ms
64 bytes from 192.168.100.190: icmp_seq=2 ttl=64 time=0.344 ms
64 bytes from 192.168.100.190: icmp_seq=3 ttl=64 time=0.347 ms
64 bytes from 192.168.100.190: icmp_seq=4 ttl=64 time=0.349 ms
64 bytes from 192.168.100.190: icmp_seq=5 ttl=64 time=0.394 ms
64 bytes from 192.168.100.190: icmp_seq=6 ttl=64 time=0.332 ms

--- 192.168.100.190 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5101ms
rtt min/avg/max/mdev = 0.332/0.412/0.706/0.132 ms
```

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

- Os valores hex source e destination na trama são(estao na foto).

```
root@hostlinuz:/home/linux/Documents/NON GIT/escola/3ano/rc/tp3# arp -d -a
gateway (172.26.254.254) at 00:d0:03:ff:94:00 [ether] on wlp1s0
```

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 endereço de origem é o [192.168.100.203], e o endereço de destino é o endereço de broadcast [0.0.0.0]. A nossa tabela ARP não tem um endereço MAC associado ao ip destino do ping. Por isso perguntamos a todos os dispositivos associados à rede e apenas o que se identificar responde/manda um "reply".

```
676 14.674997720  BizlinkK_07:8b:e5  Broadcast          ARP      42 Who has 192.168.100.190? Tell 192.168.100.203
677 14.675339650  AsustekC_0f:38:da  BizlinkK_07:8b:e5  ARP      60 192.168.100.190 is at 54:a0:50:0f:38:da
```

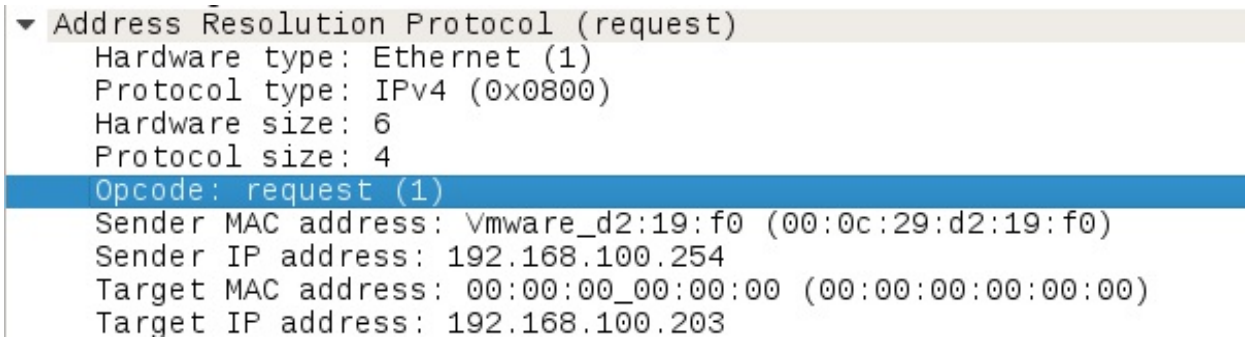
11) Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?

O valor hexadecimal do campo "Type" da trama ethernet é (0x0806), o que indica que estamos a usar o protocolo ARP.

```
Type: ARP (0x0806)
```

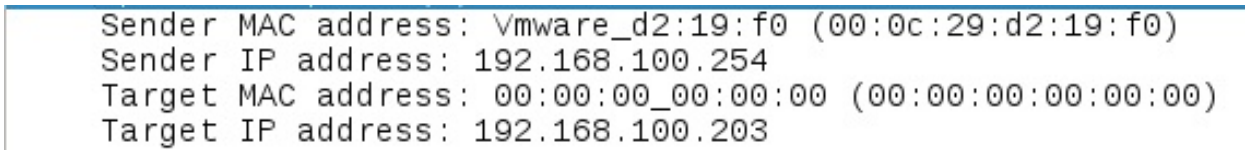
12) Qual o valor do campo ARP opcode? O que especifica?

O valor do campo ARP opcode é 1, o que especifica um request.



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

Temos endereços de IP e MAC, sendo que através do envio de um request pelo broadcast conseguimos informar todos os IPs presentes de forma a que apenas o Target IP responda com o seu endereço MAC correspondente.



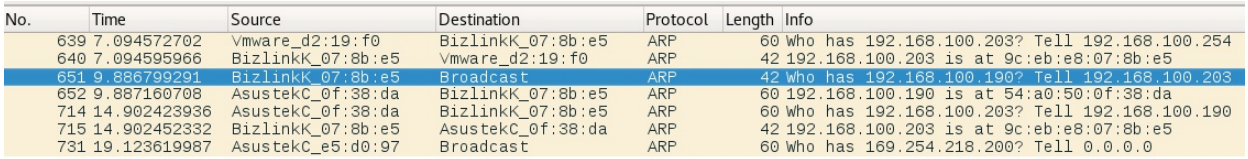
14) Explicite que tipo de pedido ou pergunta é feito pelo host de origem?

É efetuado um pedido do tipo ARP. Como inicialmente não existe nenhuma associação do IP ao MAC então é enviada uma mensagem ARP para todos os hosts da rede de forma a que o endereço requisitado responda.

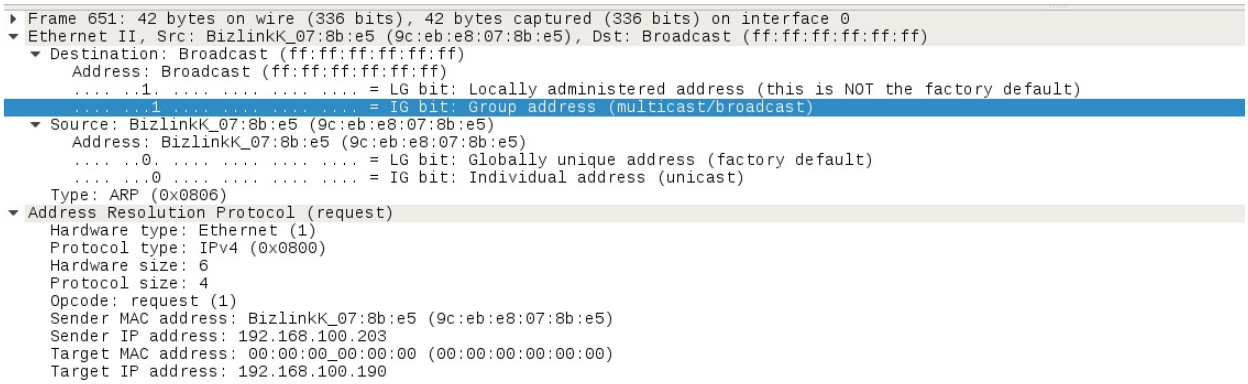
15) Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.

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

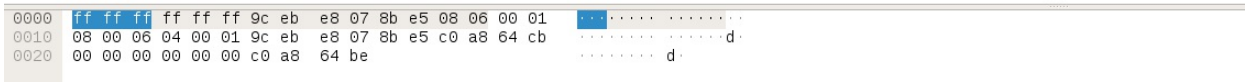
O valor do ARP opcode é 2 o que especifica um reply. Sabemos assim que o IP a que demos ping está a responder.



No.	Time	Source	Destination	Protocol	Length	Info
639	7.094572702	Vmware_d2:19:f0	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.254
640	7.094595966	BizlinkK_07:8b:e5	Vmware_d2:19:f0	ARP	42	192.168.100.203 is at 9c:eb:e8:07:8b:e5
651	9.886799291	BizlinkK_07:8b:e5	Broadcast	ARP	42	Who has 192.168.100.190? Tell 192.168.100.203
652	9.887160708	AsustekC_0f:38:da	BizlinkK_07:8b:e5	ARP	60	192.168.100.190 is at 54:a0:50:0f:38:da
714	14.902423936	AsustekC_0f:38:da	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.190
715	14.902452332	BizlinkK_07:8b:e5	AsustekC_0f:38:da	ARP	42	192.168.100.203 is at 9c:eb:e8:07:8b:e5
731	19.123619987	AsustekC_e5:d0:97	Broadcast	ARP	60	Who has 169.254.218.200? Tell 0.0.0.0



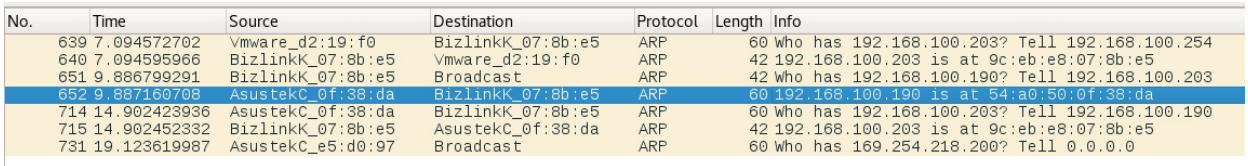
```
▸ Frame 651: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▾ Ethernet II, Src: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
      Address: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
    Sender IP address: 192.168.100.203
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.100.190
```



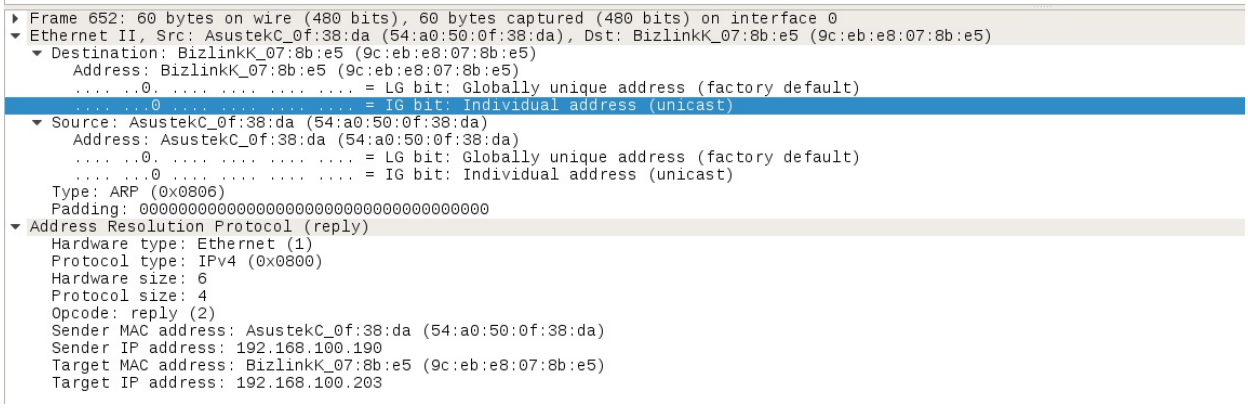
```
0000  ff ff ff ff ff ff 9c eb  e8 07 8b e5 08 06 00 01   ···· ···· ····
0010  08 00 06 04 00 01 9c eb  e8 07 8b e5 c0 a8 64 cb   ···· ···· ····d·
0020  00 00 00 00 00 00 c0 a8  64 be                     ···· ····d·
```

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

A respota ao pedido ARP encontra-se entre os 22 e os 27 bytes.



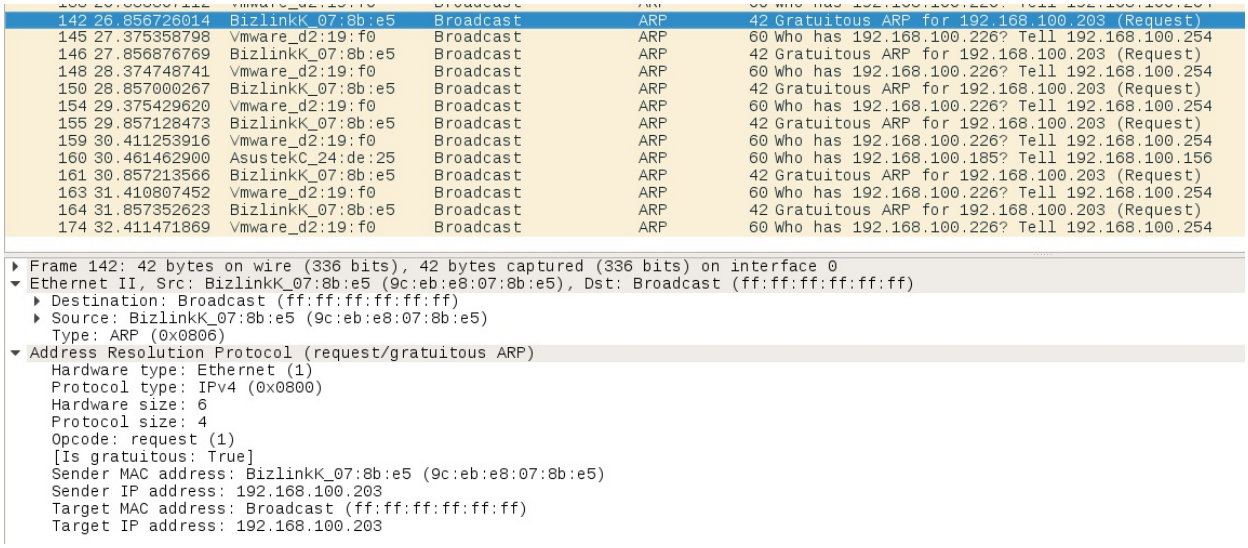
No.	Time	Source	Destination	Protocol	Length	Info
639	7.094572702	Vmware_d2:19:f0	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.254
640	7.094595966	BizlinkK_07:8b:e5	Vmware_d2:19:f0	ARP	42	192.168.100.203 is at 9c:eb:e8:07:8b:e5
651	9.886799291	BizlinkK_07:8b:e5	Broadcast	ARP	42	Who has 192.168.100.190? Tell 192.168.100.203
652	9.887160708	AsustekC_0f:38:da	BizlinkK_07:8b:e5	ARP	60	192.168.100.190 is at 54:a0:50:0f:38:da
714	14.902423936	AsustekC_0f:38:da	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.190
715	14.902452332	BizlinkK_07:8b:e5	AsustekC_0f:38:da	ARP	42	192.168.100.203 is at 9c:eb:e8:07:8b:e5
731	19.123619987	AsustekC_e5:d0:97	Broadcast	ARP	60	Who has 169.254.218.200? Tell 0.0.0.0



```
▸ Frame 652: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▾ Ethernet II, Src: AsustekC_0f:38:da (54:a0:50:0f:38:da), Dst: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
  ▾ Destination: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
      Address: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: AsustekC_0f:38:da (54:a0:50:0f:38:da)
      Address: AsustekC_0f:38:da (54:a0:50:0f:38:da)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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: AsustekC_0f:38:da (54:a0:50:0f:38:da)
    Sender IP address: 192.168.100.190
    Target MAC address: BizlinkK_07:8b:e5 (9c:eb:e8:07:8b:e5)
    Target IP address: 192.168.100.203
```

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?

O Target IP do request ARP gratuito é diferente do request normal, sendo que o Target IP é igual ao Sender IP, logo apenas o router é responde ao request.



5 - Domínios de colisão

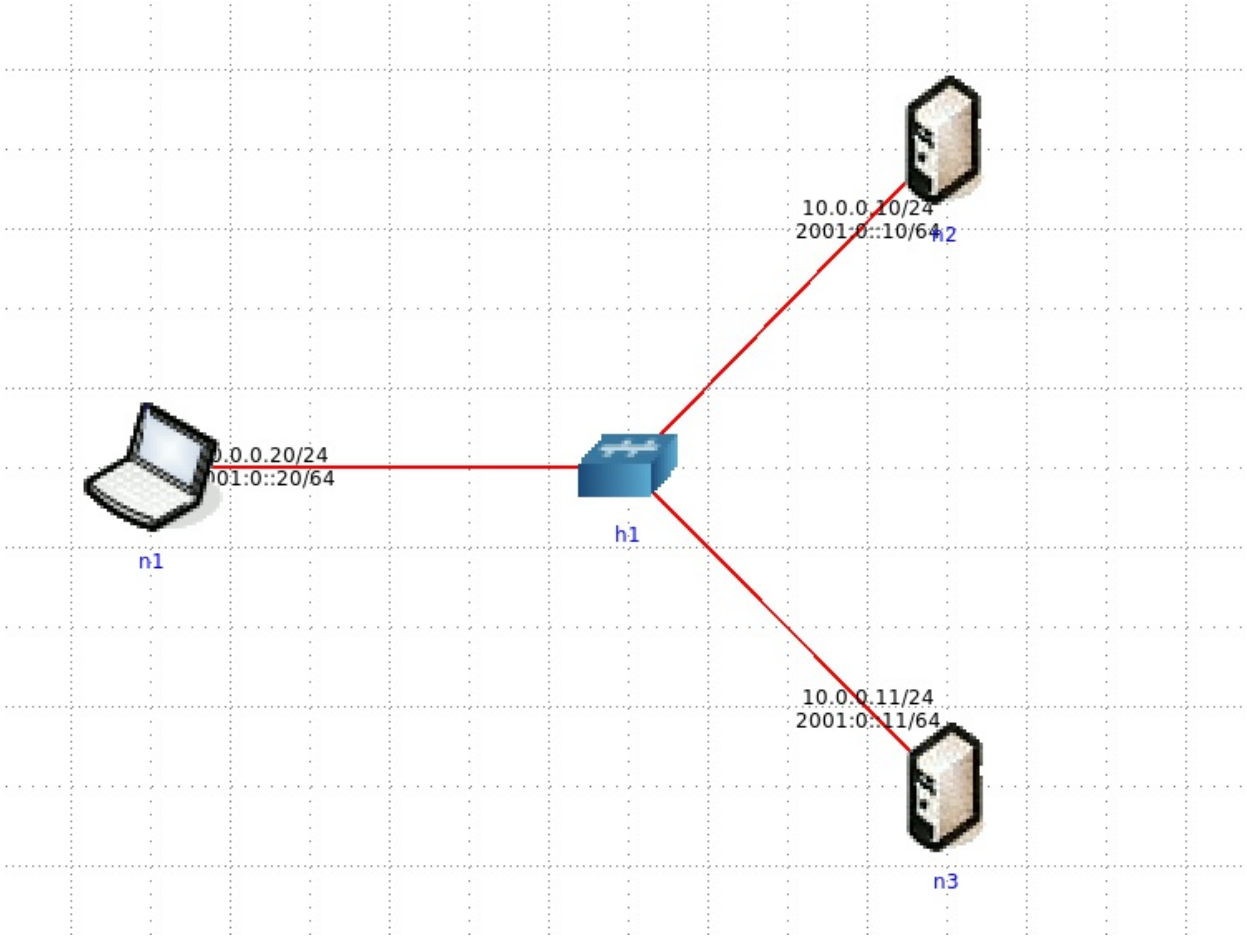
17) Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

```
root@n1:/tmp/pycore.33317/n1.conf# ping -c 1 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_seq=1 ttl=64 time=0.155 ms

--- 10.0.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.155/0.155/0.155/0.000 ms
root@n1:/tmp/pycore.33317/n1.conf#
```

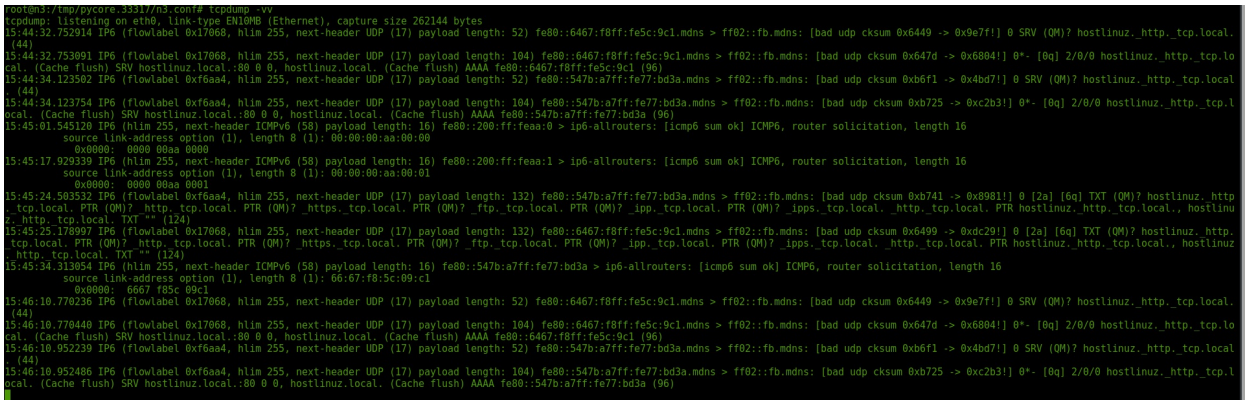
Comando ping no terminal n1

Um hub é um dispositivo que une várias portas num único segmento. Por isso, os hosts n2 e n3 recebem um tráfego uniforme, com a exceção do tráfego enviado por eles próprios.



Topologia

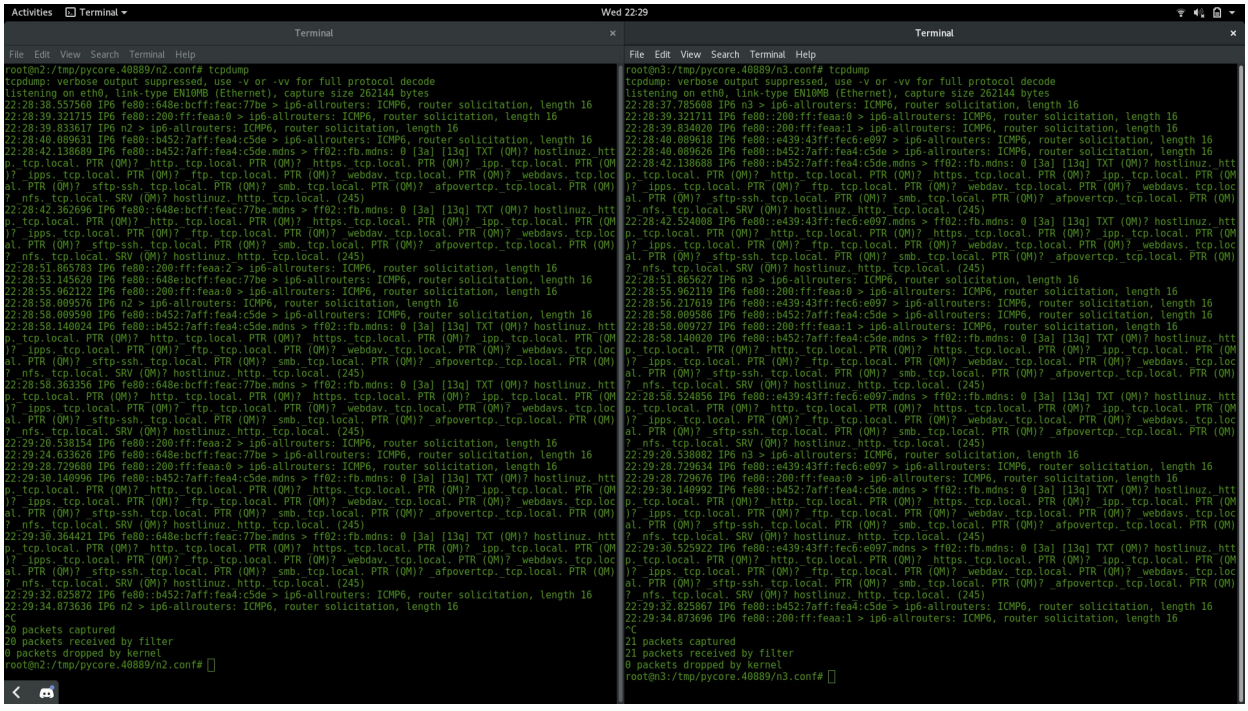
Comando tcdump no terminal n2 : hub



Comando tcdump no terminal n3 : hub

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.

Com um switch ao invés de o tráfego ser enviado para todos os dispositivos (como acontece com um hub), o tráfego é apenas direcionado para um só nó. Com os switch o risco de existir colisões é menor, sendo que estes dispositivos segmentam a rede internamente e cada porta do dispositivo corresponde a um domínio de colisão diferente. Os hub, ao enviarem informação para todos os hosts, concentram toda esta informação num único canal de transmissão aumentando a probabilidade de colisões.



Comando tcdump no terminal n2 e n3 : switch

Conclusões

Com este trabalho expandimos o nosso conhecimento acerca de tramas Ethernet e dos protocolos a esta associados. Sabemos que as estão organizadas em bytes, exploramos, através delas, o conceito de mac adress, desenvolvemos o nosso conhecimento acerca do protocolo HTTP. Este protocolo permite comunicar informação com a World Wide Web, através do FCS (Frame Check Sequence) garantimos que a informação enviada é a correta.

Quanto ao protocolo ARP, conluimos que este permite que diferentes PC's se encontrem numa rede ethernet. Através do protocolo ARP decobrimos o mac adress de um certo IP da rede em que nos encontramos. Quando um PC quer comunicar com outro mas não sabe o endereço físico deste, apenas o IP adress, é enviada uma mensagem de broadcast de forma a questionar-se a quem pertence esse IP, ao que o outro PC responde com o seu endereço físico.

Cada um dos protocolos existentes é utilizado com um objetivo específico, estes são depois, estruturados através de camadas lógicas que facilitam a ligação de redes.

Compreendemos a diferença entre o uso de um hub e um switch e as consequências do uso de cada um na nossa topologia, concluindo que o uso de um switch é mais vantajoso pois diminui o número de colisões entre pacotes.