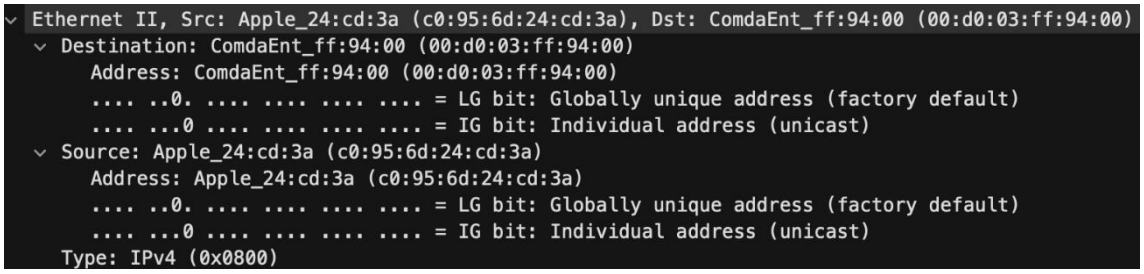
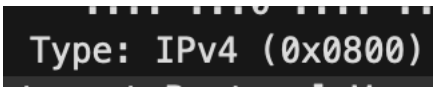
3. Captura e análise de Tramas Ethernet
Questões e Respostas

1. Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.



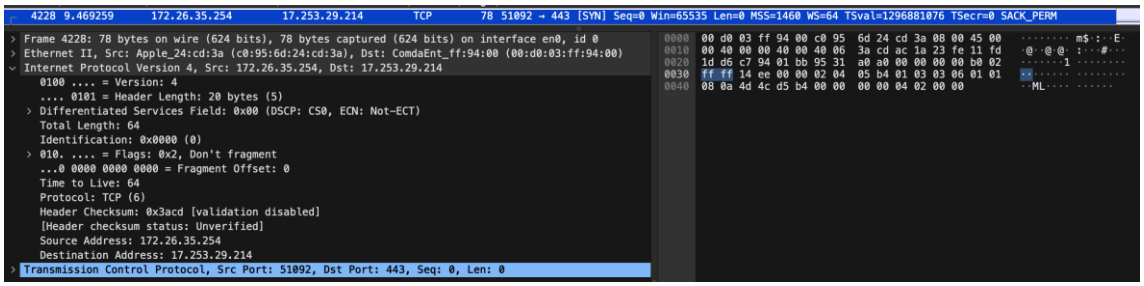
Neste caso, os endereços MAC de origem e destino são **00:d0:03:ff:94:00** (www.uminho.pt) e **c0:95:6d:24:cd:3a (Maquina nativa)** respetivamente.

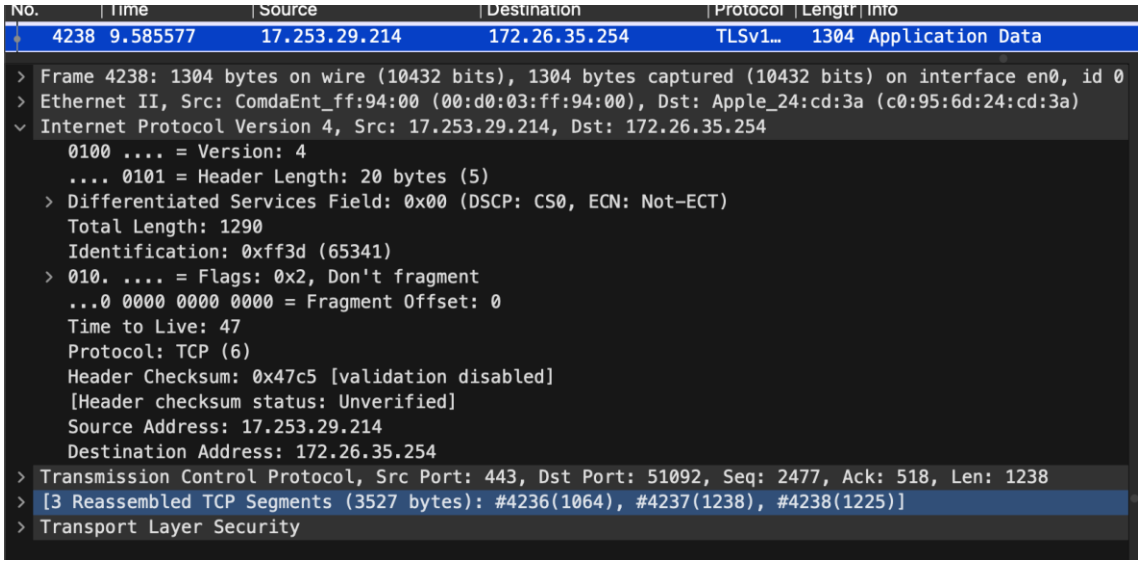
2. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?



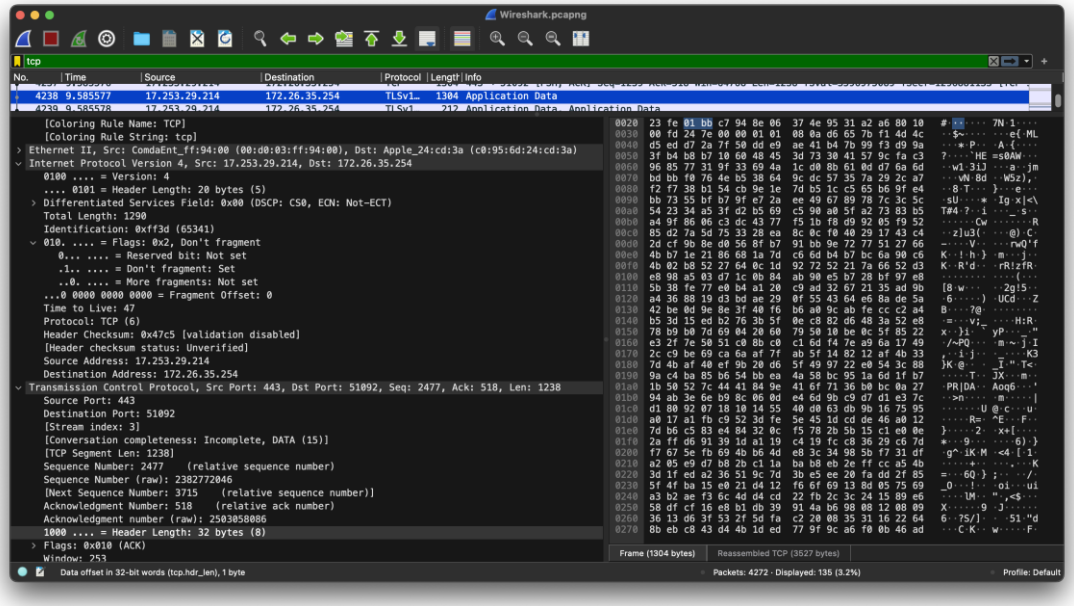
O valor é 0x0800 e significa que é do conteúdo está encapsulado é do tipo IPv4.

3. 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, no caso de HTTPS)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.



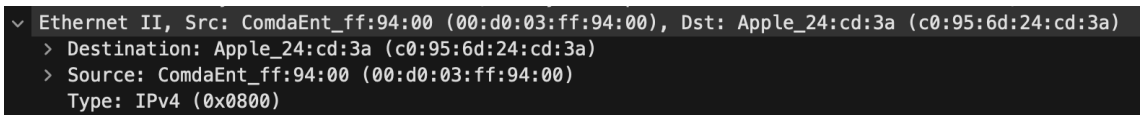


Como podemos observar a partir destas duas imagens, são usados 1226 bytes,1304-78=1226.



Tendo em conta que o header length da ethernet ocupa 14 bytes, o do IPV4 20 e o do TCP 32, concluímos que são precisos 66 bytes para o encapsulamento protocolar. (66/1304)*100 = 5,06% de sobrecarga.

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



O endereço é 00:d0:03:ff:94:00 e corresponde ao router da Universidade.

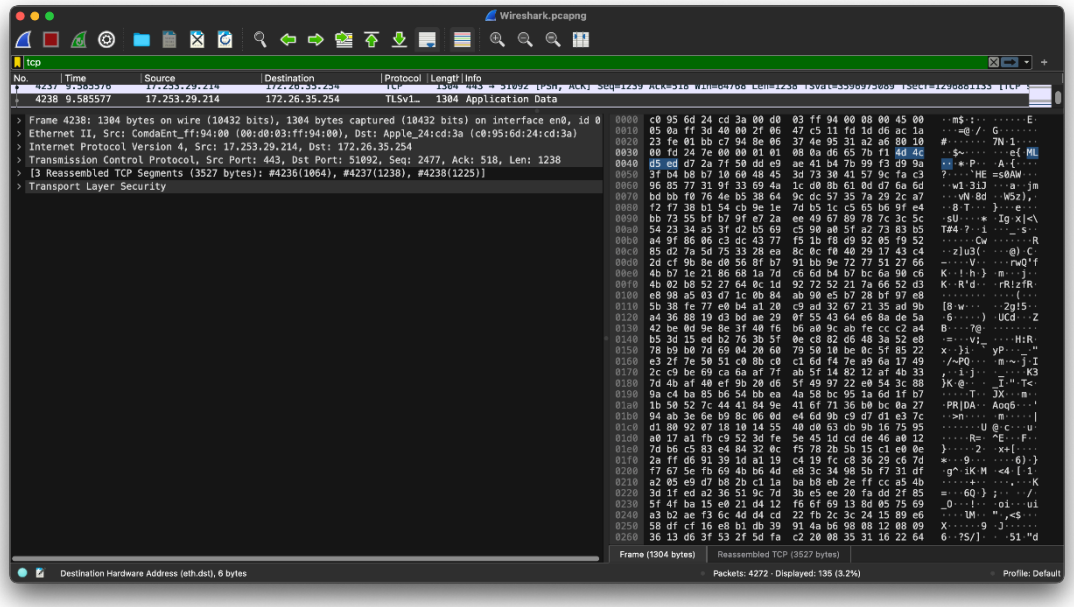
Destination: Apple_24:cd:3a (c0:95:6d:24:cd:3a)

5. Qual é o endereço MAC do destino? A que sistema (host) corresponde?

```
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_24:cd:3a (c0:95:6d:24:cd:3a)
  > Destination: Apple_24:cd:3a (c0:95:6d:24:cd:3a)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
```

O endereço de destino é c0:95:6d:24:cd:3a e corresponde à máquina que estamos a usar.

6. Atendendo ao conceito de encapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. Justifique, indicando em que campos dos cabeçalhos capturados se baseou.



Os protocolos contidos na recebida são os Ethernet (1),IPV4, TCP(6) e TLS ().

```
Frame 4238: 1304 bytes on wire (10432 bits), 1304 bytes captured (10432 bits) on interface en0, id 0
  Section number: 1
  Interface id: 0 (en0)
    Interface name: en0
    Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
```

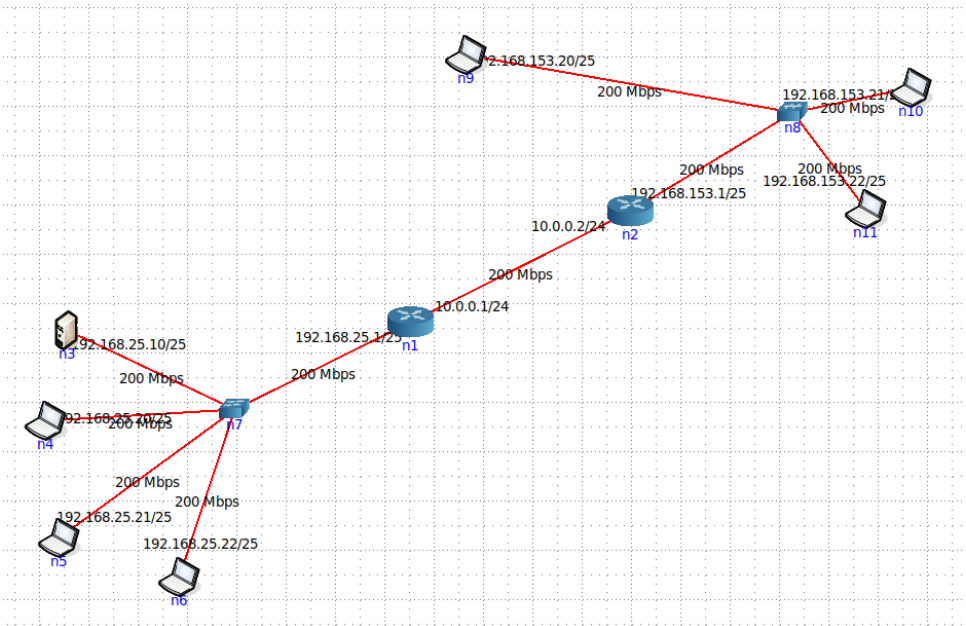
```
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_24:cd:3a (c0:95:6d:24:cd:3a)
  > Destination: Apple_24:cd:3a (c0:95:6d:24:cd:3a)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
```

```
Internet Protocol Version 4, Src: 17.253.29.214, Dst: 172.26.35.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1290
    Identification: 0xff3d (65341)
  v 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: TCP (6)
    Header Checksum: 0x47c5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 17.253.29.214
    Destination Address: 172.26.35.254
```

```
Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 3522
      Encrypted Application Data: 6930a6a3eb1aabc5656795b77b0a32d01718c99f82c08fe42f8fd03665eef21f5…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

4. Protocolo ARP

1. Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp -a. a. Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela. b. Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.



a) Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.

```
root@n11:/tmp/pycore.35691/n11.conf# arp -a
? (192.168.153.20) at 00:00:00:aa:00:08 [ether] on eth0
? (192.168.153.1) at 00:00:00:aa:00:03 [ether] on eth0
```

O primeiro campo indica o endereço ip de cada dispositivo (como por exemplo 192.168.153.20), o segundo é endereço mac (00:00:00:aa:00:08)e o terceiro é a interface (eth0).

b) Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.

O equipamento com maior tabela Arp é o router n1 (departamento A) pois precisa de manter um grande número de conexões entre os dispositivos dos dois departamentos.

```
root@n1:/tmp/pycore.35691/n1.conf# arp -a
? (192.168.25.10) at 00:00:00:aa:00:04 [ether] on eth1
? (10.0.0.2) at 00:00:00:aa:00:01 [ether] on eth0
? (192.168.25.22) at 00:00:00:aa:00:07 [ether] on eth1
? (192.168.25.20) at 00:00:00:aa:00:05 [ether] on eth1
root@n1:/tmp/pycore.35691/n1.conf#
```

2. Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).

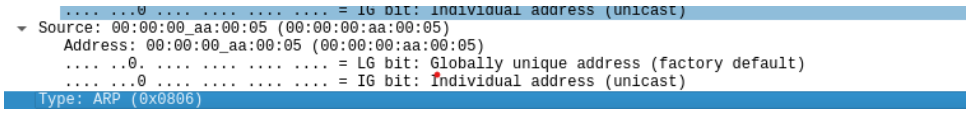
a. Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

```
▾ Ethernet II, Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05), Dst: 00:00:00_aa:00:02 (00:00:0
  ▾ Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
      Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 00:00:00_aa:00:05 (00:00:00:aa:00:05)
      Address: 00:00:00_aa:00:05 (00:00:00:aa:00:05)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
```

Destino - 00:00:00:aa:00:02
Source - 00:00:00:aa:00:05

O endereço mac é constituído por 6 bytes escritos em hexadecimal. Os primeiros 3 bytes são fixos e identificam o fabricante do dispositivo. Os outros são para identificar o dispositivo em si.

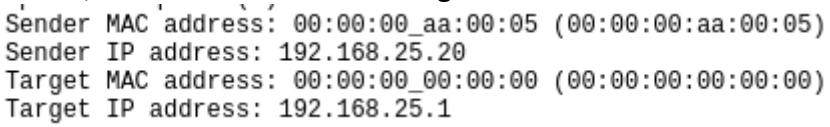
b. Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?



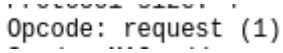
O valor do campo Tipo é 0x0806 e identifica que o conteúdo da mensagem é do tipo ARP.

c. Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.

A primeira maneira de identificar que se trata um pedido arp é existência dos endereços MAC e IP, tanto do sender com o target.



O campo opcode também server para identificar que se trata de um pedido arp pois tem o seu valor igual a 1.



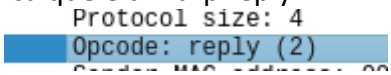
d. Explicite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?

O host esta basicamente a procura do endereço Mac do dispositivo do destino, perguntando a todos os dispositivos ate encontrar o destino.

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

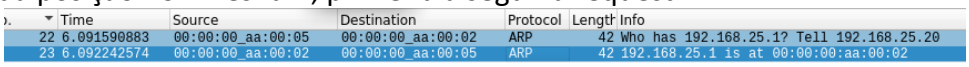
a. Qual o valor do campo ARP opcode? O que especifica?

O valor do campo é 2 e significa que é um arp reply.

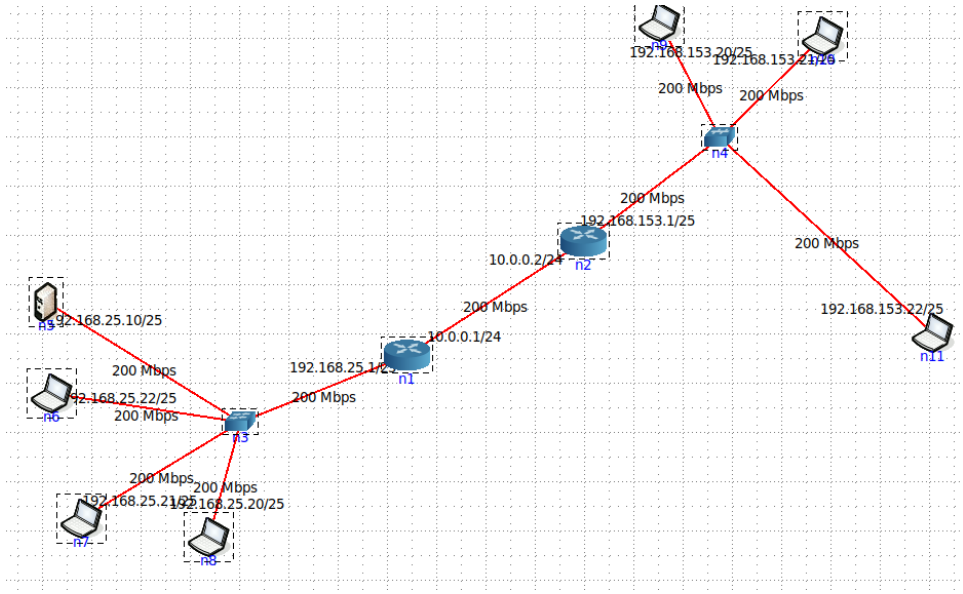


b. Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?

Segunda posição no wireshark, primeira a seguir a request.

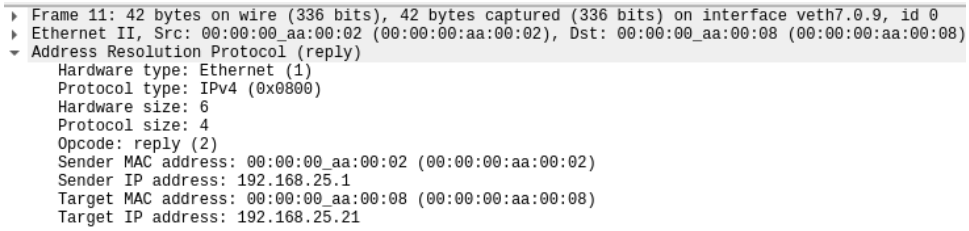


c. Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.

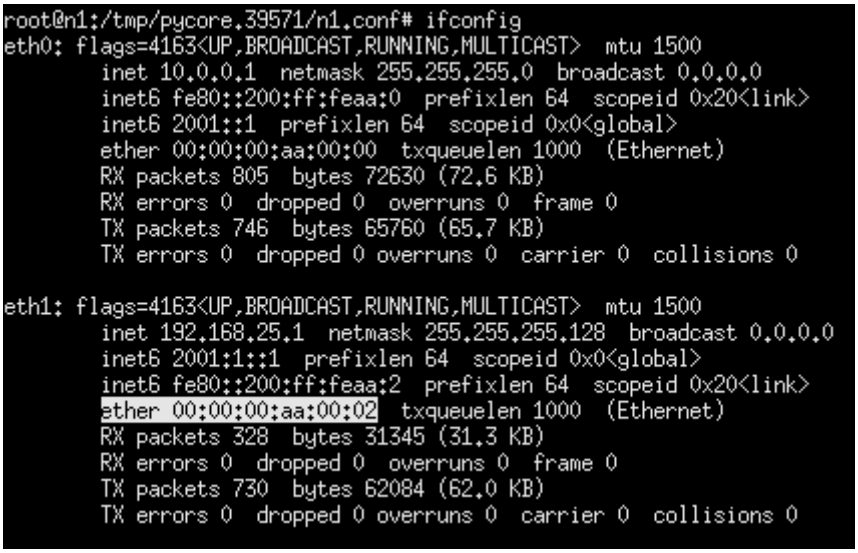


(tivemos de refazer a arquitetura no core devido ao core travar).

O destino corresponde ao n7 que tem o endereço MAC 00:00:00:aa:00:08.



A origem é o router n1 com endereço MAC 00:00:00:aa:00:02 .



d. Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

O modo de comunicaçao usado é o unicast devido ao sender já saber o caminho para o destino.

4. Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada.

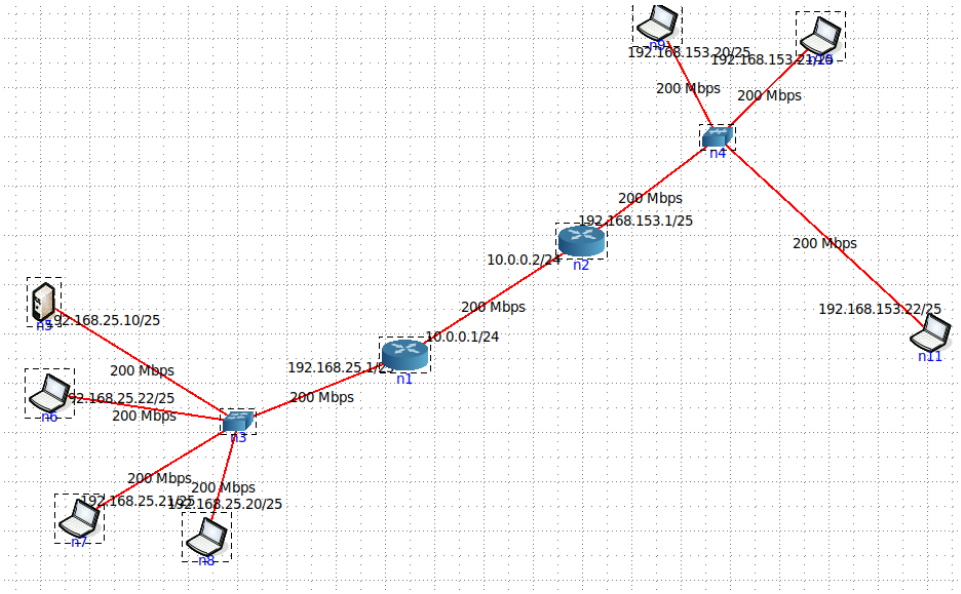
Não devido os valor Mac já estam nas tabelas não é necessário enviar uma mensagem arp.

5. Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.

Na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede são os campos de hardware size e protocol size onde ambos indicam o numero de bytes usados em cada protocolo.

```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
```

6. Na situação em que efetua um ping a um PC não local à sua sub-rede, 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 sistema destino (represente apenas os nós intervenientes). Assuma que todas as tabelas ARP se encontram inicialmente vazias.



O trajeto do ping foi do n7 -> n1-> n2 -> n11.

Primeiramente o pc faz N7 arp-request e chega n1. Quando chega ao n1 o router faz arp-reply para o N7. De seguida o n1 faz arp-request ao n2 e o n2 faz arp-reply para o n1. Quando chega ao n2, o mesmo vai fazer arp-request e chega ao n11 que de seguida vai fazer arp replay para o n2.
As mensagens ICMP são enviadas normalmente (a mensagem arp não as afetam).

5. Domínios de colisão

1. 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 é gerado 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.

Ao gerar tráfego intra-departamento com origem no departamento B e destino no A apenas o dispositivo de destino consegue ver o tráfego através do tcpdump devido a ser usada uma switch. Quanto a tráfego de A para B, qualquer dispositivo em B consegue observar tráfego de A para B independentemente do dispositivo de destino, ou seja, ao enviar tráfego de A para o PC p1 em B é possível observar esse tráfego em p2 ou p3 (pertencentes a B) devido a ser utilizado um hub.
Este comportamento justifica-se devido ao funcionamento de switches e hubs. Um hub envia tráfego para todos os dispositivos conectados, independentemente do destino do pacote. Um switch geralmente envia tráfego apenas para o destino pretendido devido à existência de uma tabela de comutação da switch que indica qual interface deve ser usada.

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

Porta	Endereço MAC
1	00:00:00:aa:00:07
2	00:00:00:aa:00:06
3	00:00:00:aa:00:05
4	00:00:00:aa:00:04
5	00:00:00:aa:00:03

Conclusões

Realizado o trabalho notamos que foi uma grande ajuda para perceber melhor os temas que o mesmo aborda, a nossa maior dificuldade foi no protocolo ARP mas acreditamos que fizemos um bom trabalho.