TP3: Camada de Ligação Lógica: Ethernet e Protocolo ARP

Adriana Gonçalves, Eduardo Semanas, and Leonardo Neri

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {ae4481,a75536,a80056}@alunos.uminho.pt

Introdução Este trabalho realizado no âmbito da unidade curricular de Redes de Computadores pretende explorar e compreender o funcionamento da camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP (Address Resolution Protocol). Abordaremos ainda o conceito de domínio de colisão e o uso de diferentes equipamentos de interligação de redes.

Resolução das questões:

3. Captura e análise de Tramas Ethernet

```
leonardo@Holmes:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 28:d2:44:1f:cc:47
          inet addr:192.168.2.167  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::be8:48fc:c56d:f683/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1672 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:761789 (761.7 KB)  TX bytes:318989 (318.9 KB)
          Interrupt:20 Memory:f2500000-f2520000
```

Figura 1: Interface de rede utilizada

```
▸ Frame 50: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0
▾ Ethernet II, Src: LcfcHefe_1f:cc:47 (28:d2:44:1f:cc:47), Dst: Vmware_5e:69:ad (00:0c:29:5e:69:ad)
  ▾ Destination: Vmware_5e:69:ad (00:0c:29:5e:69:ad)
      Address: Vmware_5e:69:ad (00:0c:29:5e:69:ad)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: LcfcHefe_1f:cc:47 (28:d2:44:1f:cc:47)
      Address: LcfcHefe_1f:cc:47 (28:d2:44:1f:cc:47)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.2.167, Dst: 193.136.19.40
▸ Transmission Control Protocol, Src Port: 57550, Dst Port: 80, Seq: 1, Ack: 1, Len: 385
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: miei.di.uminho.pt\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,pt;q=0.8\r\n
    \r\n
    [Full request URI: http://miei.di.uminho.pt/]
    [HTTP request 1/7]
    [Response in frame: 102]
    [Next request in frame: 119]
```

Figura 2: Trama Ethernet com a mensagem HTTP GET

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

Endereço de origem: 28:d2:44:1f:cc:47
Endereço de destino: 00:0c:29:5e:69:ad

3.2) Identifique a que sistemas se referem. Justifique.

O 28:d2:44:1f:cc:47 corresponde ao endereço MAC da interface ativa do nosso computador (Source) e o 00:0c:29:5e:69:ad corresponde ao endereço MAC do equipamento (Destination).

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

O valor hexadecimal do campo type é 0x0800 e refere-se ao protocolo, neste caso IPv4, que é encapsulado no *payload*.

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.

O tamanho do frame é 451 bytes, e o tamanho do payload TCP, que é onde o método HTTP GET está encapsulado, é 385 bytes. Logo, o overhead gerado até o caracter 'G' é 451 - 385 = 66 bytes.

O caracter 'G' é o primeiro octeto do payload encapsulado pelo TCP.

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

O campo FCS não está presente, isto significa que não há qualquer controle de erros feitos na camada de ligação de dados.

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

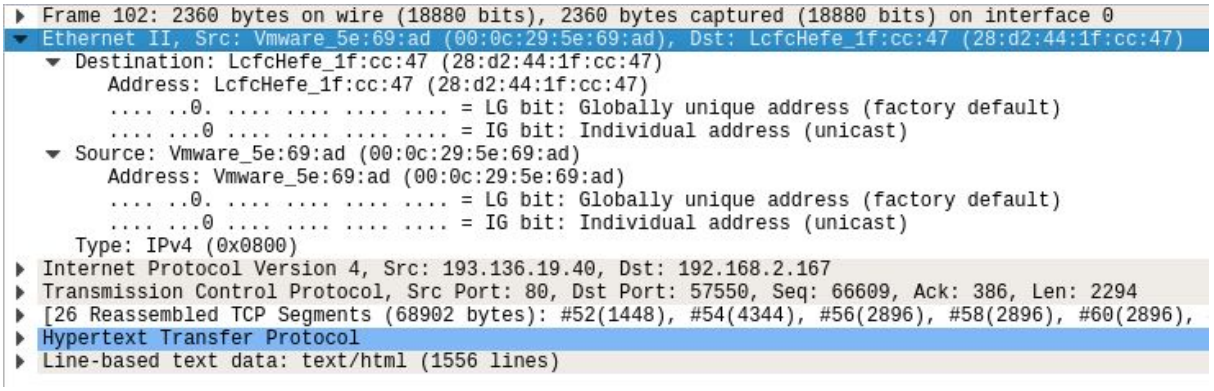

Figura 3: Primeiro pacote de resposta HTTP

O endereço Ethernet da fonte é 00:0c:29:5e:69:ad que corresponde ao endereço do host miei.di.uminho.pt

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

O endereço MAC do destino é 28:d2:44:1f:cc:47, que corresponde ao endereço da interface eth0 (como mostra a Figura 1) do nosso computador.

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

Protocolo Ethernet, correspondente à camada de ligação de dados.
Protocolo IP, correspondente à camada de rede.
Protocolo TCP, correspondente à camada de transporte.
Protocolo HTTP, correspondente à camada de aplicação.

4. Protocolo ARP

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

A coluna *Internet Address* é referente aos endereços que serão acedidos. A segunda coluna contém os endereços MAC necessários para chegar ao IP. A terceira coluna corresponde ao tipo de endereçamento utilizado.

```
C:\Users\Eduar_000>arp -a

Interface: 192.168.100.176 --- 0x5
  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
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     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
```

Figura 4: Tabela ARP antes do comando ping

```
C:\Users\Eduar_000>arp -a

Interface: 192.168.100.176 --- 0x5
  Internet Address      Physical Address      Type
  192.168.100.156       70-4d-7b-48-4b-b4     dynamic
  192.168.100.169       08-62-66-b5-70-2e     dynamic
  192.168.100.254       00-0c-29-d2-19-f0     dynamic
  192.168.100.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figura 5: Tabela ARP depois do comando ping

4.10) 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?

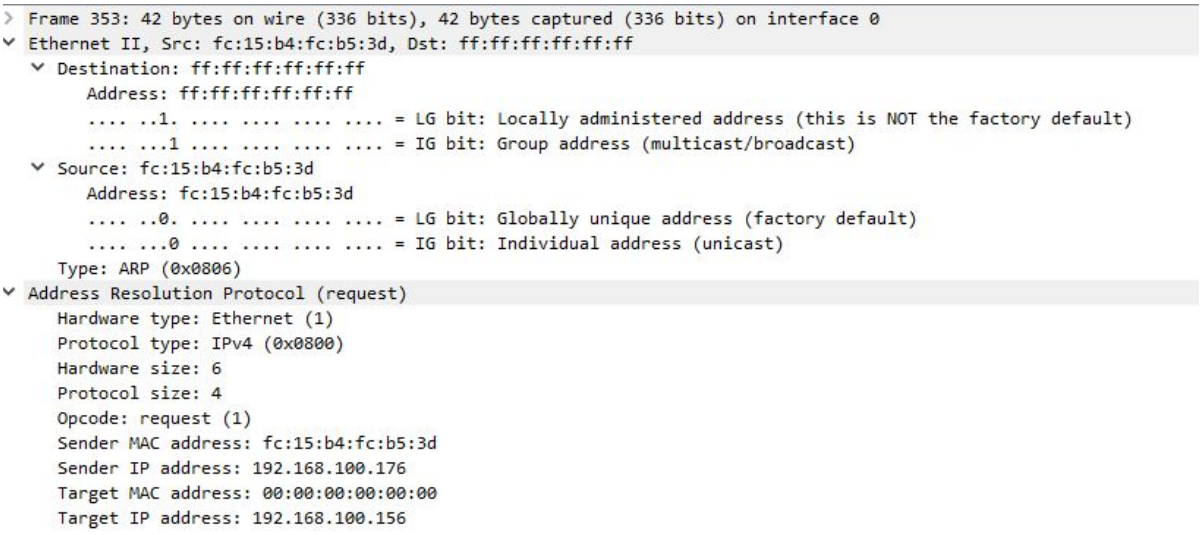

Figura 6: Trama Ethernet capturada contendo um ARP Request

Endereço de origem: fc:15:b4:fc:b5:3d
Endereço de destino: 00:0c:29:d2:19:f0
O endereço de destino usado corresponde ao endereço do router.

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

O valor hexadecimal do campo tipo é 0x0806 e indica que está a ser usado o protocolo ARP.

4.12) 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.

Opcode indica o código da operação conforme definido na RFC 826.
O valor 1 significa ARP Request.

4.13) Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Endereços da camada 2 (MAC Address) e da camada 3 (IPv4), concluo que o ARP faz o mapeamento de endereços da camada 2 com endereços da camada 3.

4.14) Explicite que tipo de pedido ou pergunta é feita pelo *host* de origem?

O pedido é um ARP request, com o objetivo de obter o endereço pretendido.

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

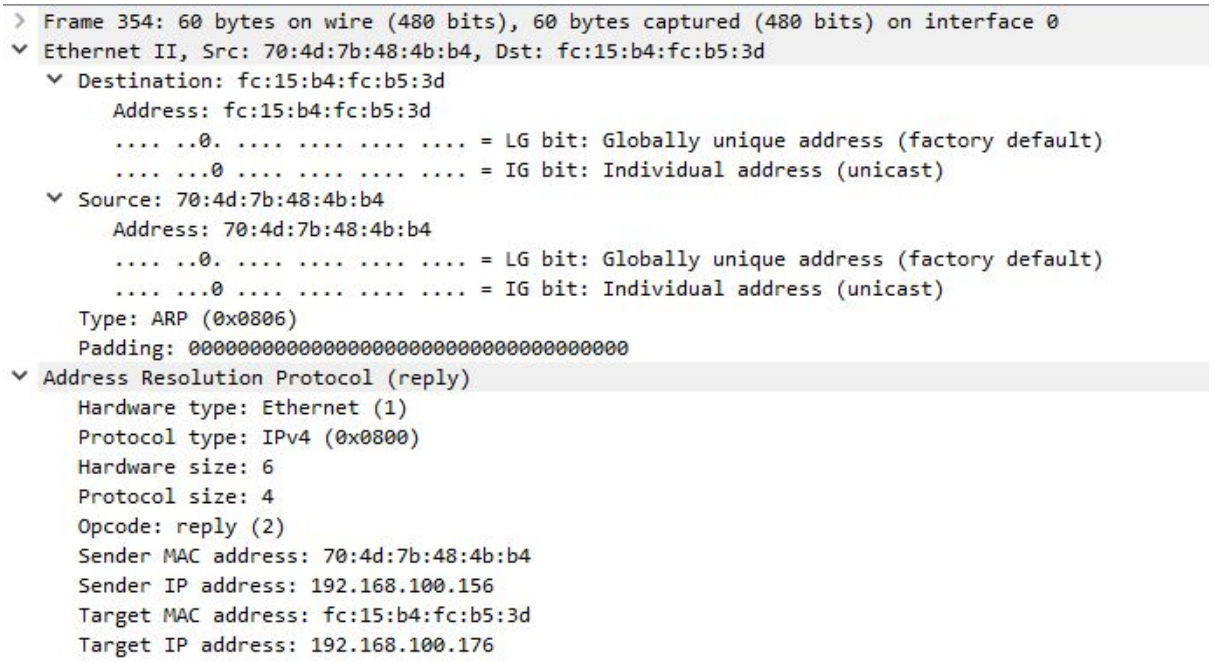

Figura 7: Trama Ethernet contendo um ARP Reply

a. **Qual o valor do campo ARP *opcode*? O que especifica?**
   O valor do campo opcode é 2, especificado um ARP Reply.

b. **Em que posição da mensagem ARP está a resposta ao pedido ARP?**
   Sender IP address e Sender MAC address.

5. ARP Gratuito

5.16) 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?

```
> Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: fc:15:b4:fc:b5:3d, Dst: ff:ff:ff:ff:ff:ff
  > Destination: ff:ff:ff:ff:ff:ff
  > Source: fc:15:b4:fc:b5:3d
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: fc:15:b4:fc:b5:3d
    Sender IP address: 192.168.100.176
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 192.168.100.254
```

Figura 8: Trama Ethernet de um ARP gratuito

Um ARP gratuito é um ARP Request que tem como destino o broadcast e o resultado esperado é um ARP Reply com o endereço MAC solicitado.

6. Domínios de Colisão

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

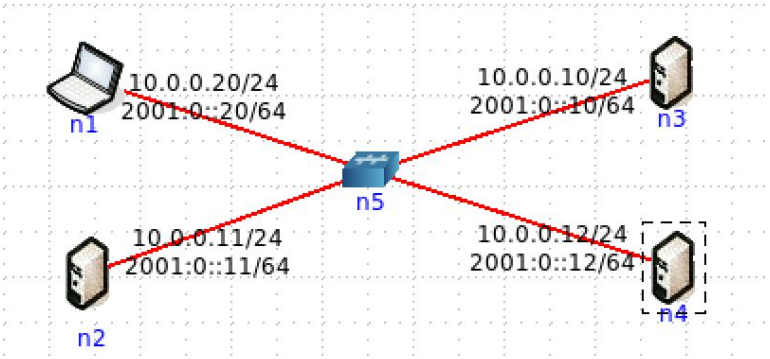

Figura 9: Rede com Hub

O hub ao receber um pacote de dados, encaminha-o para todos os dispositivos que fazem parte da rede a que ele pertence, pois a função deste é replicar o sinal e enviá-lo para todos

os outros equipamentos que lhe estão ligados. Assim, apesar de ser realizada uma transferência de dados entre os hosts n1 e n2, a informação é enviada para todos os endereços MAC presentes nessa rede.

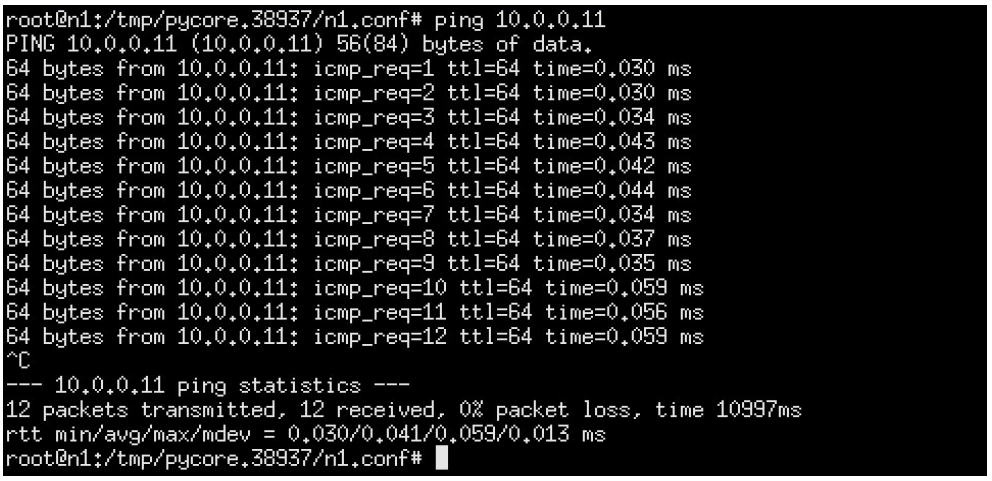

Figura 10: Ping do laptop n1 para o servidor n2

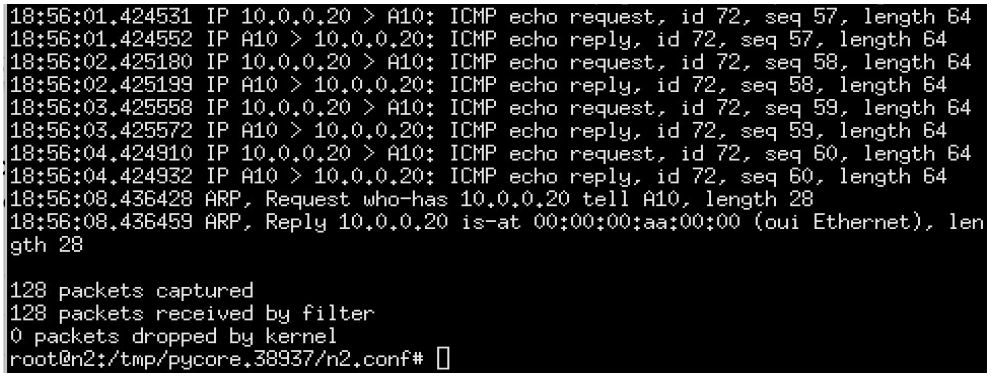

Figura 11: Tcpdump em n2

Figura 12: Tcpdump em n3

```
18:56:00.424902 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 56, length 64
18:56:01.424528 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 57, length 64
18:56:01.424561 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 57, length 64
18:56:02.425177 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 58, length 64
18:56:02.425205 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 58, length 64
18:56:03.425556 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 59, length 64
18:56:03.425577 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 59, length 64
18:56:04.424906 IP 10.0.0.20 > A10: ICMP echo request, id 72, seq 60, length 64
18:56:04.424941 IP A10 > 10.0.0.20: ICMP echo reply, id 72, seq 60, length 64
18:56:08.436444 ARP, Request who-has 10.0.0.20 tell A10, length 28
18:56:08.436458 ARP, Reply 10.0.0.20 is-at 00:00:00:aa:00:00 (oui Ethernet), len
gth 28

128 packets captured
128 packets received by filter
0 packets dropped by kernel
root@n4:/tmp/pycore.38937/n4.conf#
```

Figura 13: Tcpdump em n4

6.18) 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.

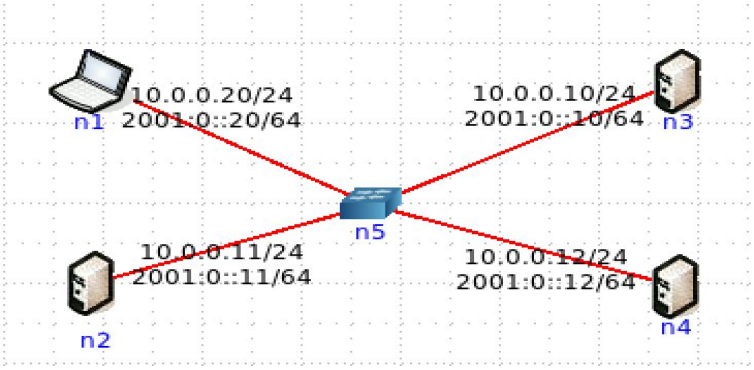

Figura 14: Rede com Switch

O hub permite detetar (caso aconteça) colisões entre tramas, enviando um sinal que permite que a trama em conflito volte à máquina de origem e fique à espera até que o hub termine a sua operação atual. Por outro lado, o switch permite evitar colisões de tramas ao impossibilitar que dados que são irrelevantes a certos dispositivos circulem na rede. Ao analisarmos o tráfego nos dispositivos podemos concluir que nos hosts n1 e n2 verificou-se captura de dados, e no n3 e n4 não se observa qualquer tráfego. Ou seja, como o comando ping foi executado apenas entre n1 e n2, a transferência de dados apenas é relevante para eles próprios, não realizando qualquer tráfego nos restantes.

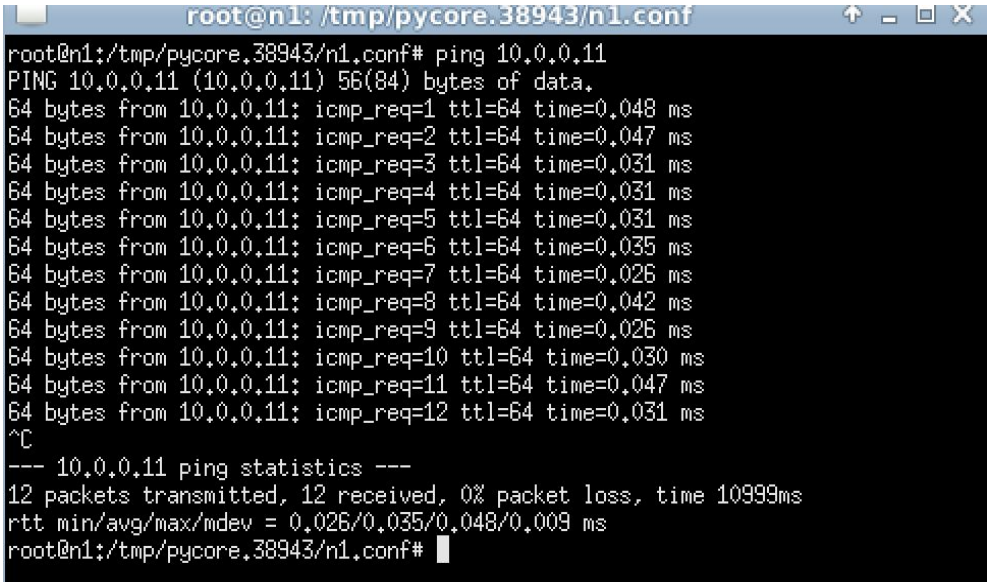

Figura 15: Ping do laptop n1 para o servidor n2

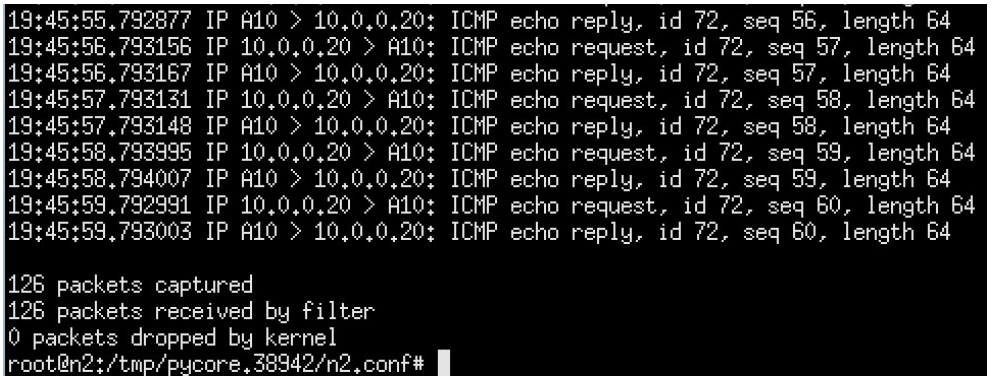

Figura 16: Tcpdump em n2

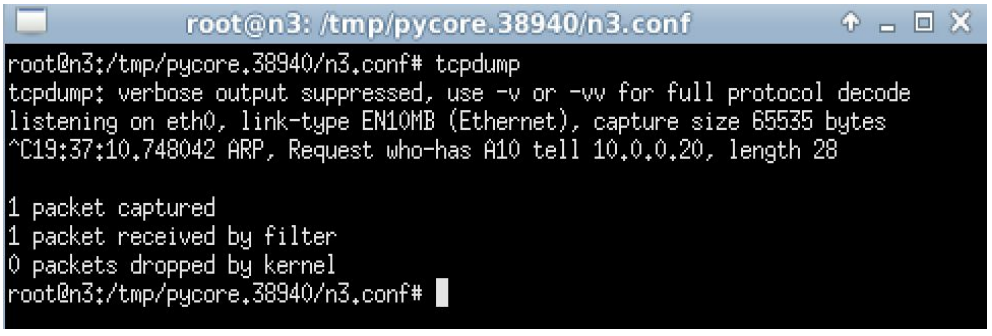

Figura 17: Tcpdump em n3

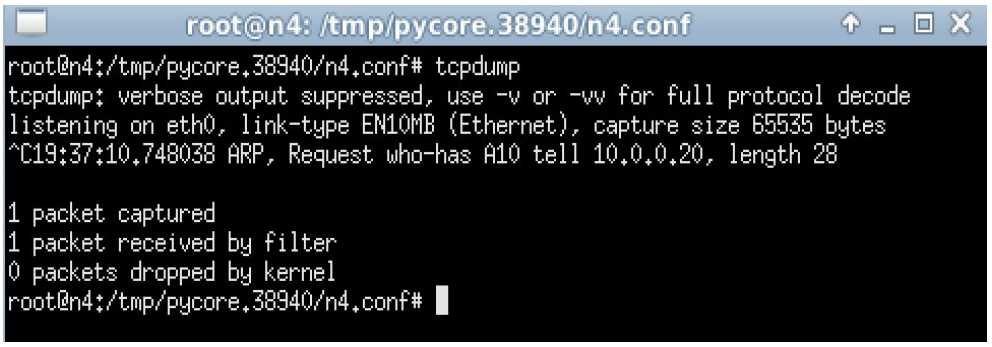

Figura 18: Tcpdump em n4

Conclusões

Este trabalho foi-nos proposto com o intuito de estudar a camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP. Foram-nos apresentados vários novos conceitos como o anteriormente referido “ARP” (Address Resolution Protocol) e “endereços MAC” (endereço de 48 bits em formato hexadecimal), entre outros.

Na primeira parte deste trabalho foi-nos pedido que capturássemos e analisássemos uma “Trama de Ethernet” através do software “Wireshark”. Após do uso do software referido fomos capazes de obter os dados pretendidos conseguindo assim responder a questões relativas à Trama de Ethernet pretendida, interpretativas da mesma. Esta parte premitiu-nos obter um melhor entendimento dos diferentes campos de informação referentes a uma dada Trama de Ethernet, por exemplo os campos referentes ao endereço de destino e de origem de pedidos realizados na trama.

Passando para a segunda parte foi-nos proposto um estudo relativo ao protocolo ARP. Recorrendo ao comando “arp -a” foi-nos possível responder as perguntas relativas à “cache ARP” da máquina que utilizámos nesta parte. Após isto realizámos um “ARP request” através do comando “ping [endereço de outra máquina na mesma rede]” realizando uma captura da Trama Ethernet correspondente através do Wireshark, isto permitiu-nos responder às restantes perguntas desta parte, relativas tanto ao pedido em si como à resposta obtida.

Relativamente à terceira parte do trabalho os conhecimentos pretendidos foram muito idênticos à parte anterior, sendo esta referente a pedidos/respostas ARP “gratuitos” que são, basicamente, pedidos que aconteceram sem intervenção nossa.

Chegando à quarta e última parte passámos a utilização do software “core”, simulando uma rede que contenha um “hub” ou um “switch”. Através dos comandos “ping” e “tcpdump” conseguimos responder às questões pedidas, obtendo assim uma melhor compreensão da diferença entre os dois dispositivos utilizados nas diferentes alíneas.

De um ponto de vista introspectivo pensamos ser seguro dizer que conseguimos obter as informações e os conhecimentos respectivos pretendidos, tendo assim um maior conhecimento sobre redes computacionais.