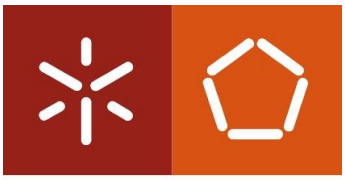

Universidade do Minho

Departamento de Informática

TP3:
Grupo Nº 7

João Teixeira (A85504)

José Ferreira (A83683)

Miguel Solino (A86435)

27 de Novembro de 2019

Conteúdo

Capítulo 1

3. Captura e análise de tramas Ethernet

1.1 Exercício 1

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

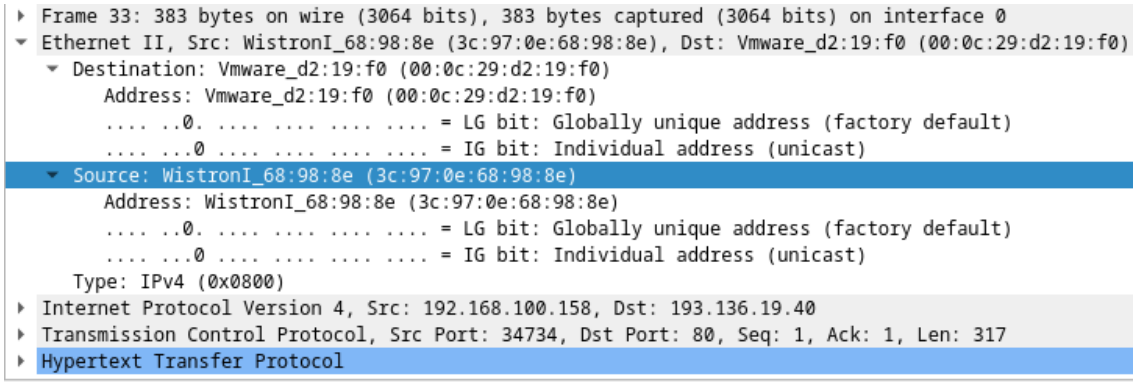

Figura 1.1: endereço MAC

Observando a figura 1.1, vemos que o endereço MAC de origem é 3c:97:0e:68:98:8e e o destino é 00:0c:29:d2:19:f0.

1.2 Exercício 2

Identifique a que sistemas se referem. Justifique.
Estes dois endereços estão em dois campos diferentes, *Source* e *Destination*.
O primeiro corresponde à interface da nossa máquina nativa. O segundo corresponde ao router da rede local à qual estamos ligados.

1.3 Exercício 3

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

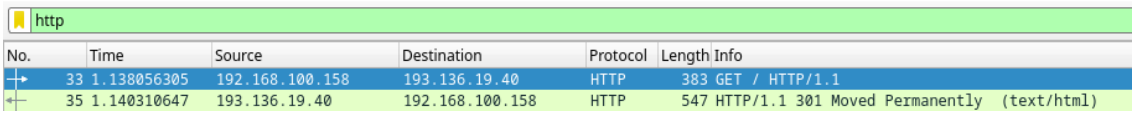

Figura 1.2: Tramas HTTP

Como podemos observar na figura 1.2, no campo Type da trama Ethernet está o valor 0x0800, que indica que o protocolo utilizado ao nível da rede é IPv4.

1.4 Exercício 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.

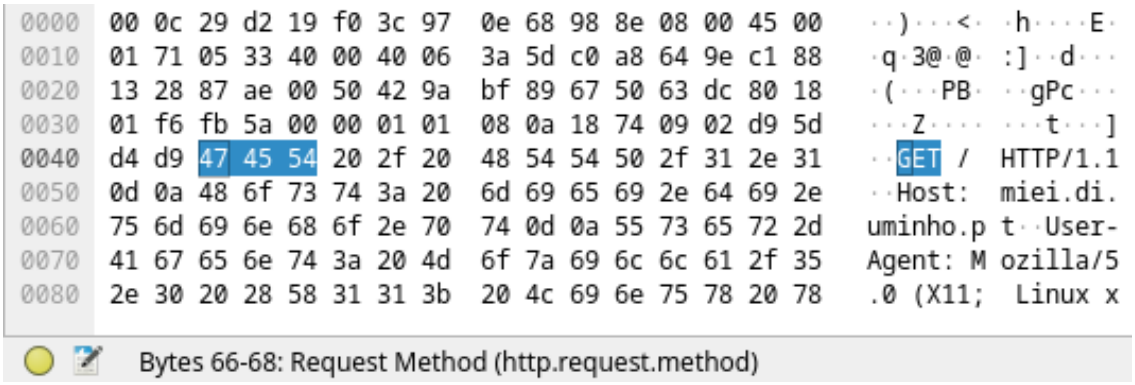

Figura 1.3: bytes até ao G

Observando a figura 1.3, reparamos que até ao caractere ASCII "G"são usados 65 bytes.
No total são utilizados 383 bytes, logo para verificar a sobrecarga fazemos o cálculo (65/383) * 100 = 16.97%

1.5 Exercício 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?
Visualizando a trama reparamos que o campo FCS (*Frame Check Sequence*) não aparece. Isto deve-se a estarmos a utilizar uma conexão por rede wired (neste caso Ethernet) e este tipo é normalmente muito robusto e pouco suscetível a erros, ao contrário das redes Wireless em que este campo já é normal aparecer.

1.6 Exercício 6

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

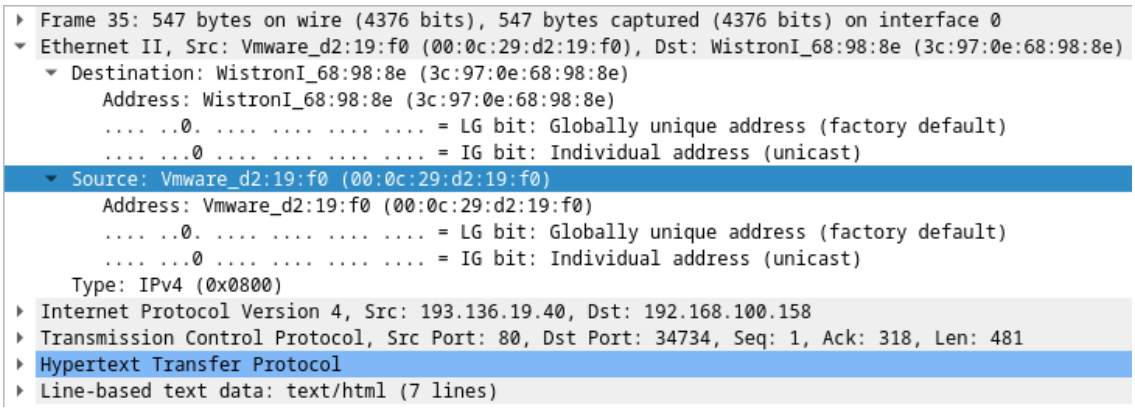

Figura 1.4: Trama Ethernet

Como é mostrado na figura 1.4, o endereço Ethernet da fonte (*Source*) é 00:0c:29:d2:19:f0 que corresponde ao router da rede local à qual estamos ligados.

1.7 Exercício 7

Qual é o endereço MAC do destino? A que sistema corresponde?
Observando outra vez a figura 1.4 repara-se que o endereço Ethernet no campo Destination é 3c:97:0e:68:98:8e e este corresponde à interface ativa da nossa máquina nativa.

1.8 Exercício 8

Atendendo ao conceito de desencapsulamento protocolar, identifique os vários
Os protocolos contidos na trama mostrada na figura 1.4 são: Ethernet II, IPv4 (*Internet Protocol Version 4*), TCP (*Transmission Control Protocol*) e HTTP (*Hypertext Transfer Protocol*).

Capítulo 2

4. Protocolo ARP

2.1 Exercício 9

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

```
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   00:0c:29:d2:19:f0   C                     enp0s25
_gateway                 ether   00:d0:03:ff:94:00   C                     wlp3s0
```

Figura 2.1: Tabela ARP

A tabela ARP pode ser comparada a um histórico de comunicações, ou seja, mapeia o endereço IP para o endereço MAC dos sistemas que comunicaram recentemente. A primeira coluna representa os endereços IP, a segunda os endereços MAC e a terceira o tipo do endereçamento usado.

```
$ sudo arp -d -a
_gateway (192.168.100.254) at 00:0c:29:d2:19:f0 [ether] on enp0s25
_gateway (172.26.254.254) at 00:d0:03:ff:94:00 [ether] on wlp3s0
```

Figura 2.2: ARP cleanup

2.2 Exercício 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?

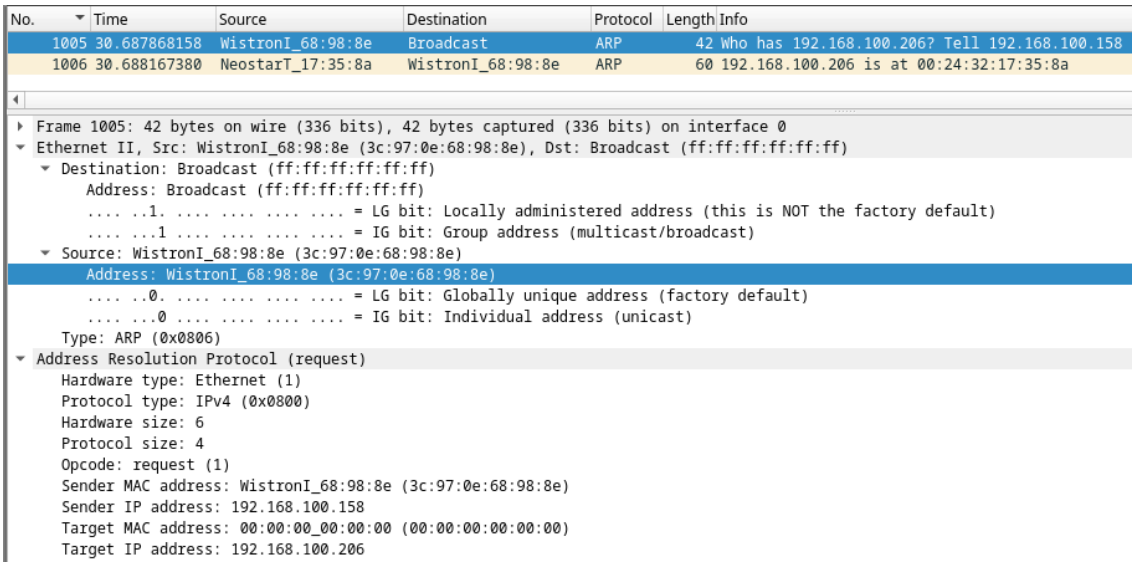

Figura 2.3: pedido ARP

Na trama Ethernet (figura 2.3) o endereço de origem é 3c:97:0e:68:98:8e e o de destino é ff:ff:ff:ff:ff:ff. É usado este endereço de destino para que todos os endereços conectados à rede recebam a mensagem com o pedido.

2.3 Exercício 11

Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?
Observando a figura 2.3, vemos que o campo Type tem o valor 0x0806, indicando que o campo de dados pertence ao ARP.

2.4 Exercício 12

Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP.

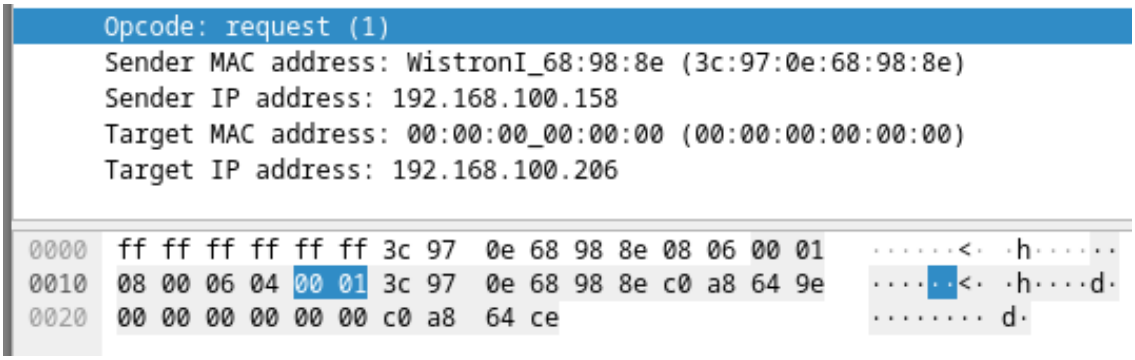

Figura 2.4: campo ARP opcode

Como podemos observar na figura 2.4, o campo ARP opcode tem o valor 0x0001. Isso significa que o pacote é um pedido ou uma resposta, sendo neste caso um pedido.

2.5 Exercício 13

Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?
A mensagem ARP contém os endereços IP de destino e de origem e sendo que se trata de um ARP request então também só mostra o endereço MAC do endereço IP da origem.

2.6 Exercício 14

Explicite que tipo de pedido ou pergunta é feito pelo host de origem?
A pergunta que é feita pela nossa máquina é "Quem tem o endereço 192.168.100.206? Diga 192.168.100.158". Logo, como resposta vamos obter o endereço MAC do equipamento que tiver o endereço indicado na pergunta.

2.7 Exercício 15

Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.
a. Qual o valor do campo ARP opcode? O que expecífica?

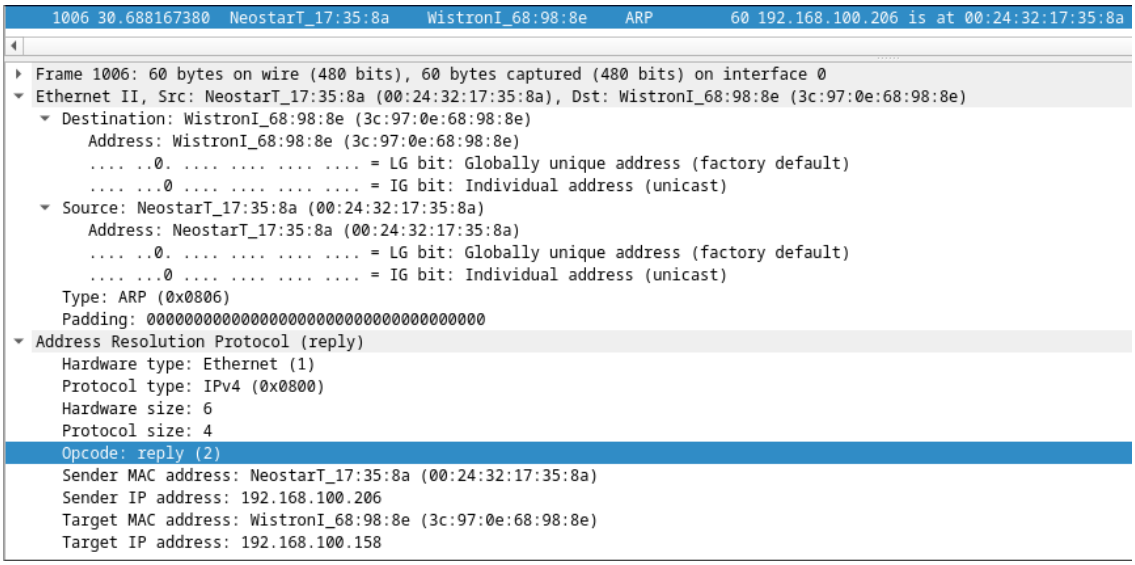

Figura 2.5: campo ARP opcode

Como podemos observar na figura 2.5, o valor do campo ARP opcode é 0x0002, o que significa que se trata de uma resposta ao pedido ARP feito anteriormente.
b. Em que posição da mensagem ARP está a resposta ao pedido ARP?

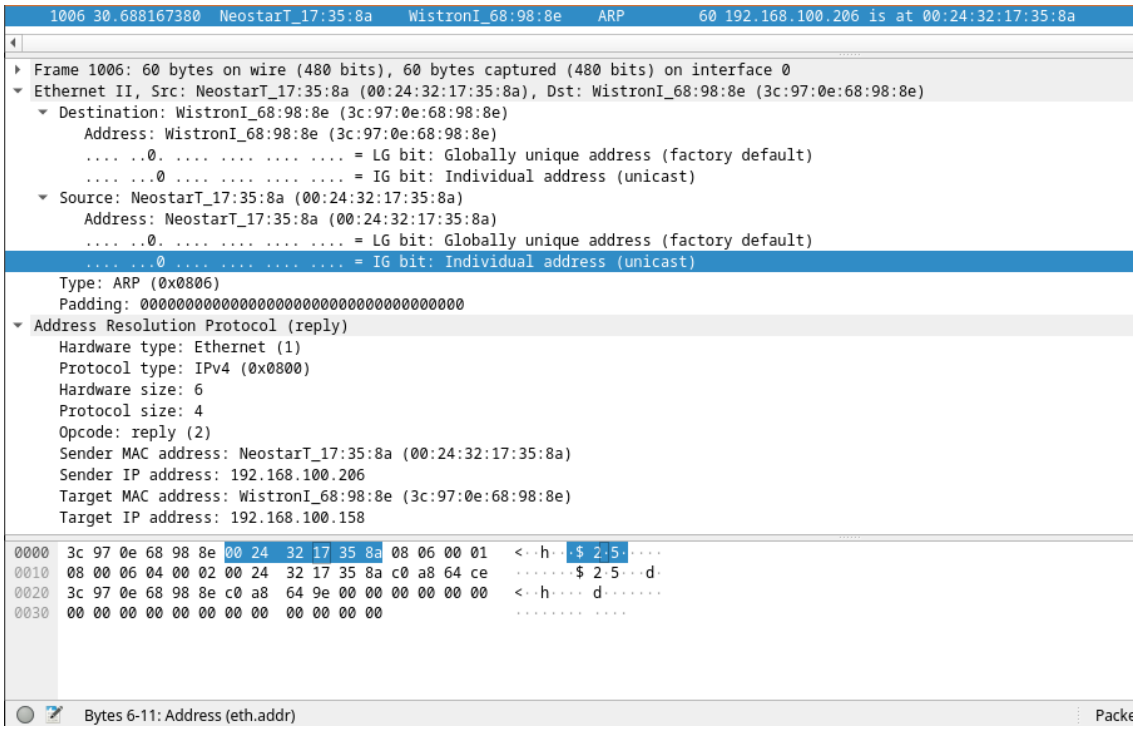

Figura 2.6: pedido ARP

Observando a figura 2.6, a resposta ao pedido ARP está entre os bytes 6 e 11.

2.8 Exercício 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 enviado?

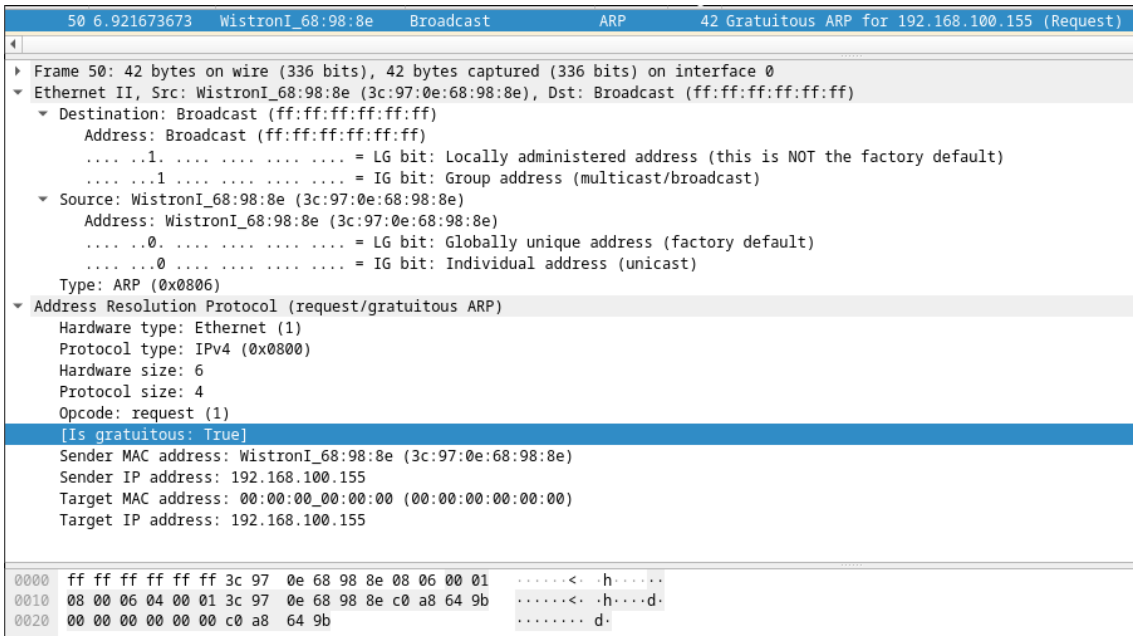

Figura 2.7: pacote de pedido ARP gratuito

Observando as figuras 2.7 e 2.3, reparamos que existem algumas diferenças.
A primeira diferença é que apresenta uma flag *Is gratuitous*: True, indicando que se trata de um pedido ARP gratuito.
A outra é que o Sender e Target MAC address são iguais.
Ao ser um ARP gratuito é esperado que não exista resposta, mas caso contrário acontecesse significaria que conectado à rede existe outro equipamento com o mesmo endereço que o nosso.

Capítulo 3

5. Domínios de colisão

3.1 Exercício 17

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

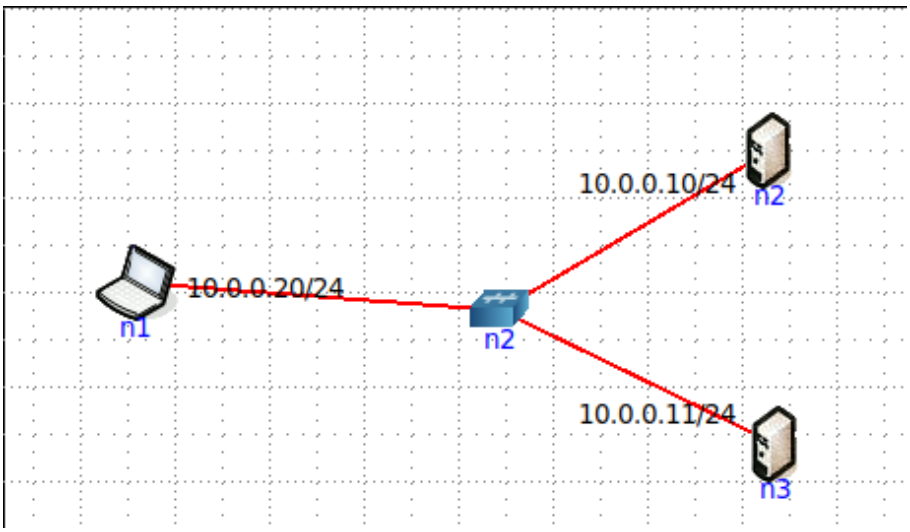

Figura 3.1: Topologia Core

```
root@n1:/tmp/pycore.43697/n1.conf# ping -c 2 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=0.141 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.863 ms

--- 10.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.141/0.502/0.863/0.361 ms
```

Figura 3.2: ping de n1 para n2

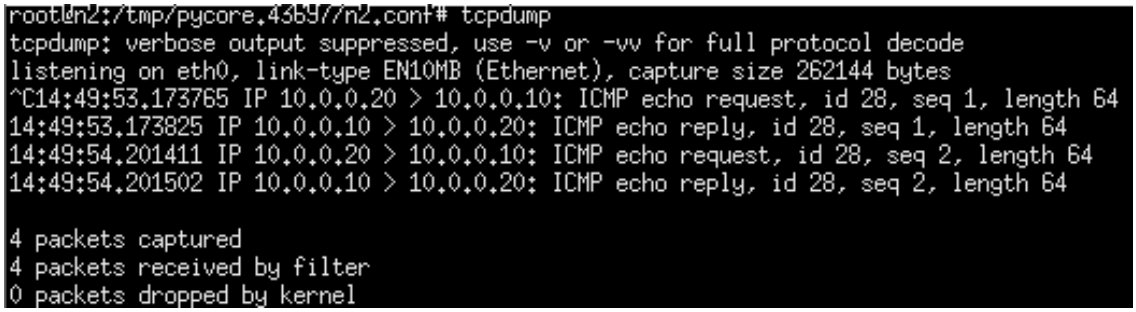

Figura 3.3: tcpdump em n2

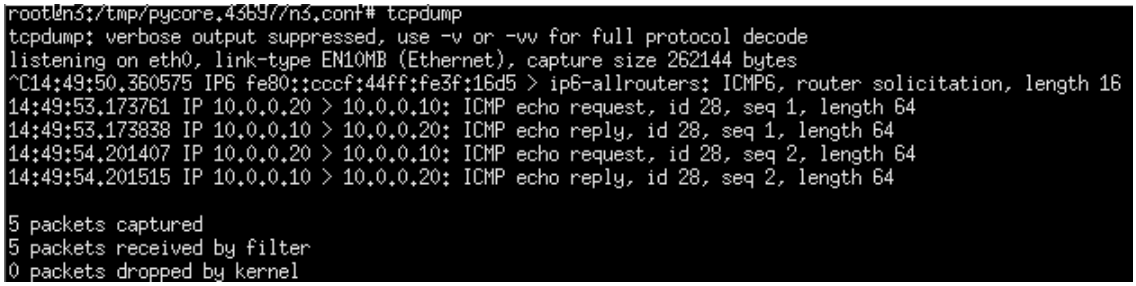

Figura 3.4: tcpdump em n3

Analisando as figuras 3.2, 3.3 e 3.4 reparamos que os dois servidores receberam os pacotes. Isso deve-se ao facto de o hub ao receber o ping do laptop n1 para o servidor n2, reencaminha-os para todos os dispositivos que estejam conectados à rede.

3.2 Exercício 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.

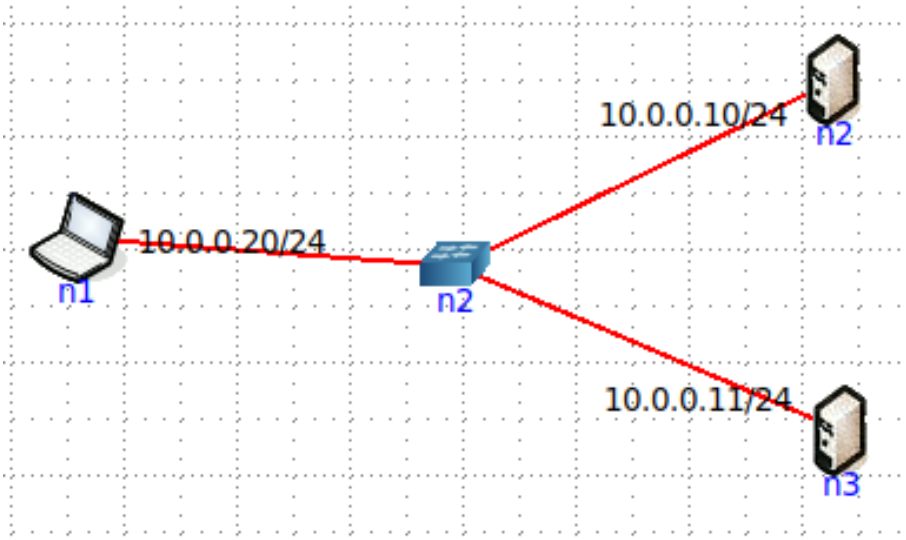

Figura 3.5: Topologia Core

```
root@n2:/tmp/pycore.43697/n2.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C14:54:14.727159 IP 10.0.0.20 > 10.0.0.10: ICMP echo request, id 38, seq 1, length 64
14:54:14.727207 IP 10.0.0.10 > 10.0.0.20: ICMP echo reply, id 38, seq 1, length 64
14:54:15.728905 IP 10.0.0.20 > 10.0.0.10: ICMP echo request, id 38, seq 2, length 64
14:54:15.728953 IP 10.0.0.10 > 10.0.0.20: ICMP echo reply, id 38, seq 2, length 64

4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Figura 3.6: tcpdump em n2

```
root@n3:/tmp/pycore.43697/n3.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

Figura 3.7: tcpdump em n3

Observando as figuras 3.6 e 3.7, reparamos que apenas o servidor de destino do ping recebeu os pacotes.
Tal acontece porque o pedido foi enviado para um switch que envia diretamente para o host e não envia para todos como é feito por um hub. Ou seja, ao contrário do hub, com o switch não acontecem colisões frequentemente pois este envia para cada host as informações usando vários canais de comunicação.
Concluindo assim que os switches são mais viáveis do que os hubs.

Capítulo 4

Conclusão

A realização deste trabalho proporcionou nos a oportunidade de aprofundar os nossos conhecimentos relativamente a Ethernet, Endereços MAC, Address Resolution Protocol (ARP) e Interligação de Redes Locais.
Utilizando a ferramenta Wireshark e o Core conseguimos capturar e analisar tramas Ethernet, ou seja, o essencial para colocarmos em prática e aprimorar os nossos conhecimentos relacionados com os tópicos anteriormente referidos.
Se dividirmos o trabalho por partes é possível dividir em 3. Na primeira parte o foco foi baseado na utilização de uma conexão por Ethernet. Na segunda foi focado nos pacotes ARP e na terceira a comparação entre Hubs e Switches. Resumindo, achamos que maior parte do capitulo Link Layer foi abrangido e relembrado.