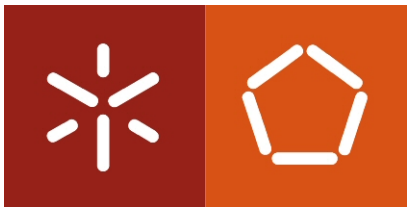

UNIVERSIDADE DO MINHO

MESTRADO INTEGRADO DE ENGENHARIA INFORMÁTICA

Redes de Computadores

TP3: Camada de Ligação Lógica: Ethernet e Protocolo ARP

Autores:

Frederico Pinto	A73639	
Pedro Silva	A78434	
Ricardo Leal	A75411	

1 de Abril de 2018

1 Introdução

Este trabalho prático foi proposto na disciplina de Redes de Computadores e divide-se em duas partes. Na primeira parte foi abordada a tecnologia Ethernet. Esta tecnologia é usada como norma de comunicação e ligação de dados

2 Parte I

2.1 Captura e análise de Tramas Ethernet

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

Origem: 60:02:92:10:57:46
Destino: c8:2a:14:58:01:60
Como podemos ver na Figura 1.

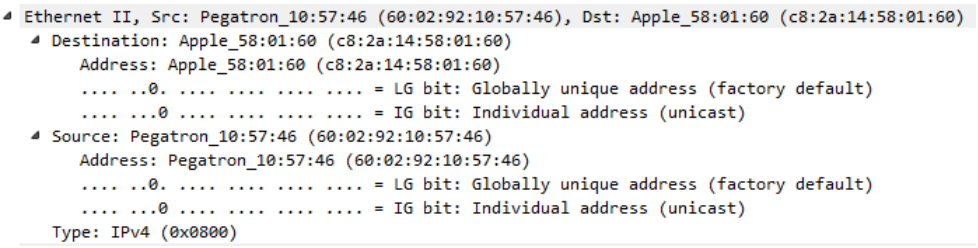

Figura 1. Campo Ethernet II da trama que suporta a mensagem HTTP GET.

2) Identifique a que sistemas se referem. Justifique.

O endereço de origem identifica o *laptop*, i.e., a nossa máquina nativa, enquanto que o endereço destino representa o *router* da rede Ethernet da sala de aula.

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

Pela Figura 1 constatamos que vale 0x0800 e identifica o protocolo utilizado a nível de rede, neste caso, 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.

Até ao caractere "G" são usados 54 bytes. No total, o tamanho da trama é de 646 bytes. Ora, concluímos que:

$$Overhead(\%) = \frac{54}{646} * 100 \approx 8.36\%$$

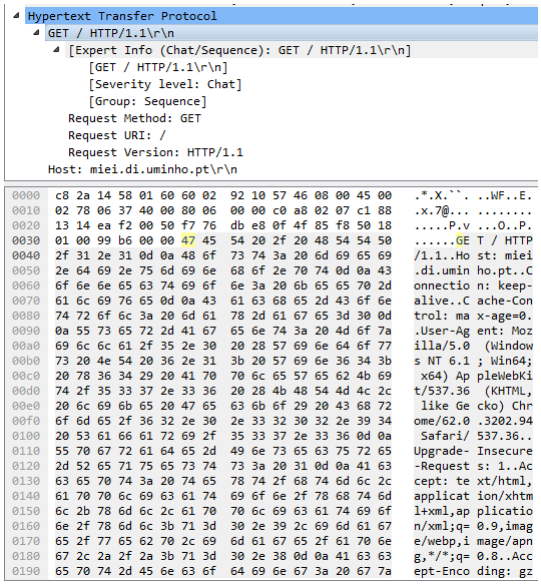

Figura 2. Parte da trama.

5) Em ligações com fios pouco susceptíveis a erros, nem sempre as NICs geram o código de detecção de erros. Através de visualização direta de uma trama capturada, verifique se o campo FCS está visível, i.e., se está a ser utilizado. Aceda à opção "Edit/Preferences/Protocols/Ethernet"e indique que é assumido o uso do campo FCS. Verifique qual o valor hexadecimal desse campo na trama capturada. Que conclui? Reponha a configuração original.

O campo FCS vale 0x0d0a0d0a, o que nos permite concluir que não foi gerado código de deteção de erros, como observamos na Figura 3.

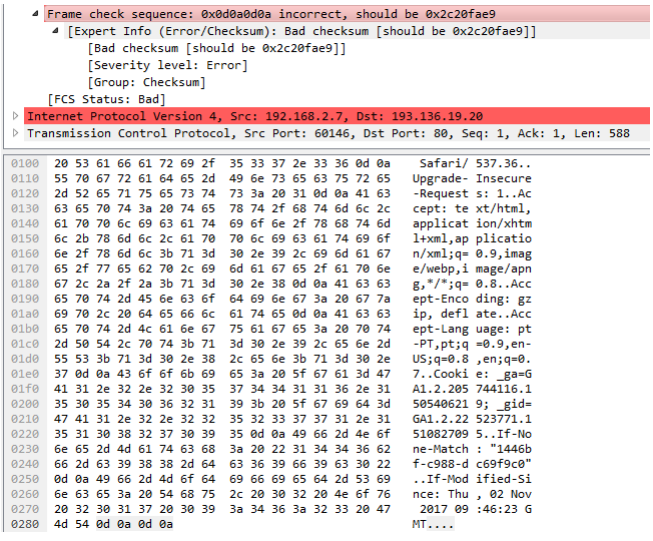

Figura 3. Frame em análise, vista conforme as configurações especificadas.

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

c8:2a:14:58:01:60, como verificamos na Figura 4, que identifica o *router* de acesso à rede da sala de aula.

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

Constatamos na Figura 4, que o endereço do destino é 60:02:92:10:57:46, associado à nossa máquina.

```
▲ Ethernet II, Src: Apple_58:01:60 (c8:2a:14:58:01:60), Dst: Pegatron_10:57:46 (60:02:92:10:57:46)
  ▲ Destination: Pegatron_10:57:46 (60:02:92:10:57:46)
       Address: Pegatron_10:57:46 (60:02:92:10:57:46)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▲ Source: Apple_58:01:60 (c8:2a:14:58:01:60)
       Address: Apple_58:01:60 (c8:2a:14:58:01:60)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figura 4. Campo Ethernet II da trama que suporta a resposta à mensagem inicial.

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

Desencapsulando progressivamente esta trama Ethernet, constatamos que os protocolos que a compõem são: Ethernet, IPv4, TCP e HTTP.

```
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 16, 2017 10:13:38.953454000 Hora padrão de GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1510827218.953454000 seconds
    [Time delta from previous captured frame: 0.000804000 seconds]
    [Time delta from previous displayed frame: 0.000804000 seconds]
    [Time since reference or first frame: 3.730242000 seconds]
    Frame Number: 39
    Frame Length: 185 bytes (1480 bits)
    Capture Length: 185 bytes (1480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▷ Ethernet II, Src: Apple_58:01:60 (c8:2a:14:58:01:60), Dst: Pegatron_10:57:46 (60:02:92:10:57:46)
▷ Internet Protocol Version 4, Src: 193.136.19.20, Dst: 192.168.2.7
▷ Transmission Control Protocol, Src Port: 80, Dst Port: 60146, Seq: 1, Ack: 593, Len: 131
▷ Hypertext Transfer Protocol

0000  60 02 92 10 57 46 c8 2a  14 58 01 60 08 00 45 00   `...WF.* .X.`..E.
0010  00 ab b8 c6 40 00 3f 06  eb 3a c1 88 13 14 c0 a8   ....@.?. .:......
0020  02 07 00 50 ea f2 0f 4f  85 f8 f7 76 de 38 50 18   ...P...O ...v.8P.
0030  19 70 1a 33 00 00 48 54  54 50 2f 31 2e 31 20 33   .p.3..HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified.
0050  0a 44 61 74 65 3a 20 54  68 75 2c 20 31 36 20 4e   .Date: T hu, 16 N
0060  6f 76 20 32 30 31 37 20  31 30 3a 31 33 3a 34 34   ov 2017  10:13:44
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0080  61 63 68 65 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   ache..Co nnection
0090  3a 20 63 6c 6f 73 65 0d  0a 45 54 61 67 3a 20 22   : close. .ETag: "
00a0  31 34 34 36 62 66 2d 63  39 38 38 2d 64 63 36 39   1446bf-c 988-dc69
00b0  66 39 63 30 22 0d 0a 0d  0a                       f9c0"... .
```

Figura 5. Protocolos definidos na trama em estudo.

2.2 Protocolo ARP

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

Dado que o protocolo ARP estabelece relações entre endereços do nível de rede e endereços do nível de ligação lógica, a tabela ARP trata de armazenar o mapeamento definido em *soft state*, como podemos ver na Figura 6, onde na primeira coluna se encontra o endereço MAC, na segunda o endereço IP associado e na terceira o tipo de encaminhamento utilizado, estático ou dinâmico.

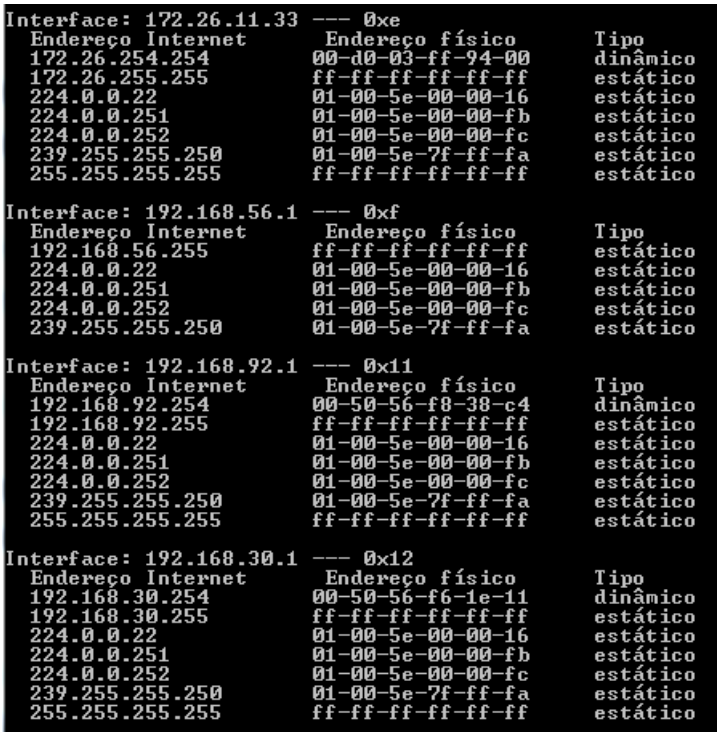

Figura 6. Tabela ARP.

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?
Origem: 60:02:92:10:57:46
Destino: ff:ff:ff:ff:ff:ff
O pedido ARP pretende determinar o endereço físico associado ao endereço IP 192.168.2.1, por forma a preencher a tabela ARP, pelo que necessita de enviar o pedido em *broadcast*, sendo expectável que seja recebida resposta *unicast* do *host* com esse endereço IP associado.

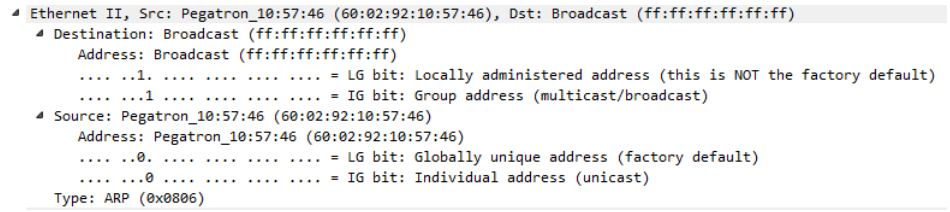

Figura 7. Campo Ethernet II do pedido ARP.

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

Pela Figura 7 constatamos que vale 0x0806, identificando ARP.
12) Qual o valor do campo ARP opcode? O que especifica?

0x0001, que representa *Request*. Serve para identificar se se trata de um pedido(request) ou de uma resposta a outro pedido(reply).

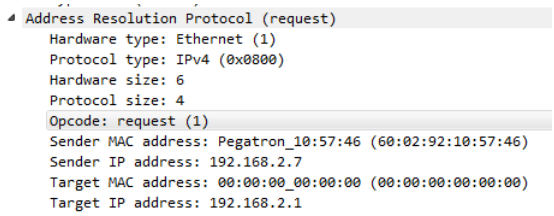

Figura 8. Informação ARP do pedido.

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

Endereços MAC e IPv4, pela Figura 8, dado que este protocolo define o mapeamento entre esses tipos de endereços.
14) Explicite que tipo de pedido ou pergunta é feita pelo host de origem?

Figura 9. Pedido efetuado.

15) Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.
a. Qual o valor do campo ARP opcode? O que especifica?
b. Em que posição da mensagem ARP está a resposta ao pedido ARP?

Na Figura 10 está representada a resposta ao pedido ARP. O campo opcode vale 0x0002, pelo que identifica que se trata da *reply* ao pedido efetuado, onde no campo *Sender MAC address* se encontra a resposta a este último, c8:2a:14:58:01:60.

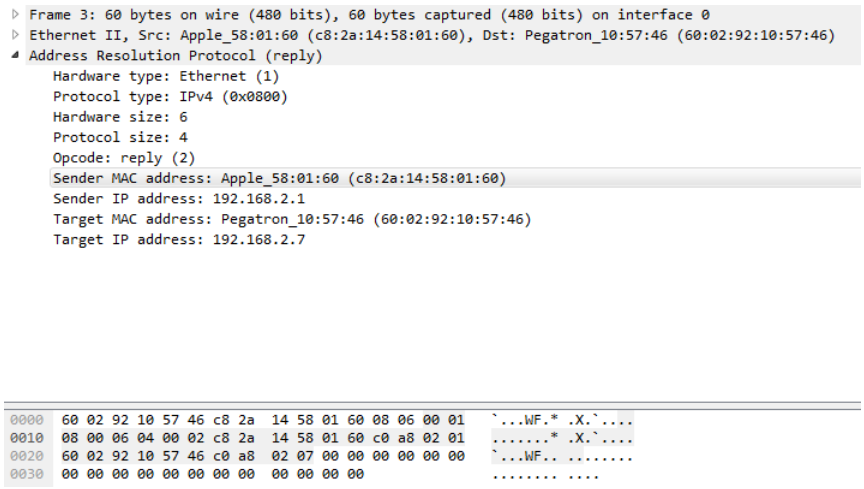

Figura 10. Resposta ao pedido ARP.

2.3 ARP numa topologia CORE

Preparamos a topologia CORE conforme o descrito:

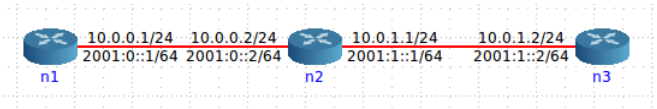

Figura 11. Topologia CORE.

16) Com auxílio do comando ifconfig obtenha os endereços Ethernet das interfaces dos diversos routers.

n_1: eth0 - 00:00:00:aa:00:00
n_2: eth0 - 00:00:00:aa:00:01
eth1 - 00:00:00:aa:00:02
n_3: eth1 - 00:00:00:aa:00:03

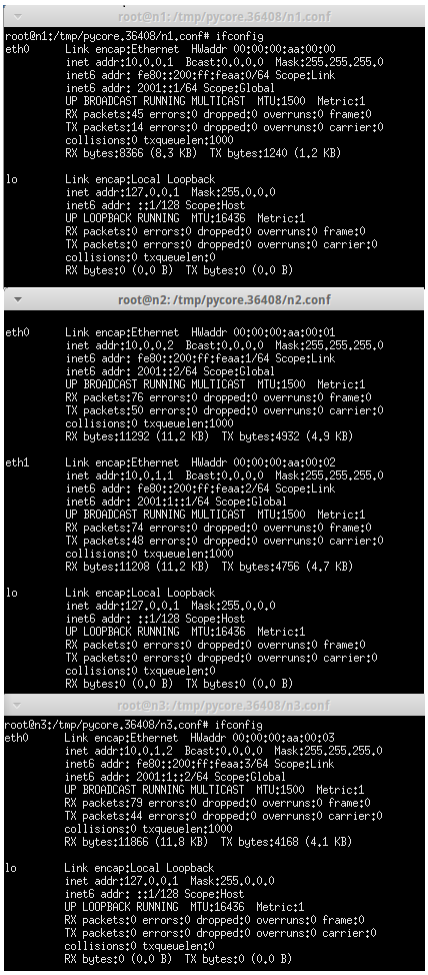

Figura 12. Resultado de executar o comando ifconfig nos *routers*.

17) Usando o comando arp obtenha as caches arp dos diversos sistemas.
Encontra-se o resultado obtido para n1, n2 e n3, nas figuras 13,14 e 15, respetivamente.

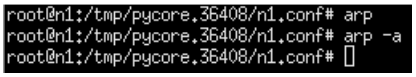

Figura 13. Resultado de executar os comandos arp e arp -a em n1.

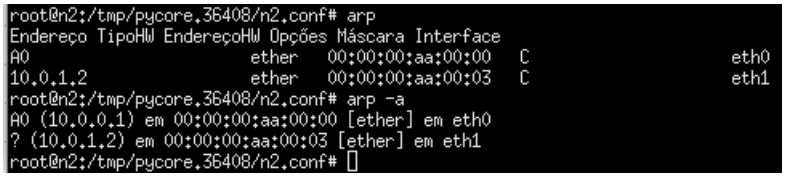

Figura 14. Resultado de executar os comandos arp e arp -a em n2.

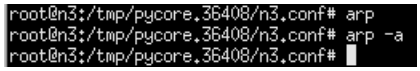

Figura 15. Resultado de executar os comandos arp e arp -a em n3.

18) Faça ping de n1 para n2. Que modificações observa nas caches ARP desses sistemas? Faça ping de n1 para n3. Consulte as caches ARP. Que conclui?

Na primeira fase, como mostra a Figura 16, é adicionada à tabela ARP de n1 uma entrada com a associação do endereço MAC de n2 e o seu respetivo endereço IP. Após o ping de n1 e n3, n3 passa a ter informação na sua tabela ARP relativa a n2, que possibilita a comunicação entre n1 e n2, como podemos ver na Figura 17.

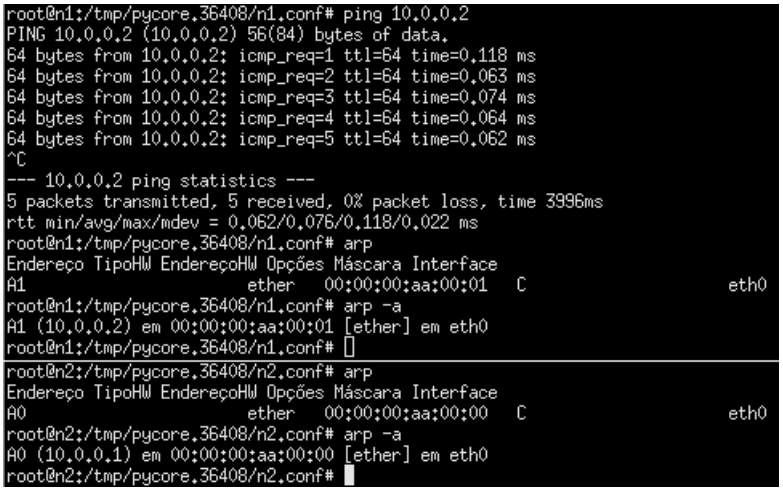

Figura 16. Alteração na tabela ARP de n1 e na de n2 após fazer ping de n1 para n2.

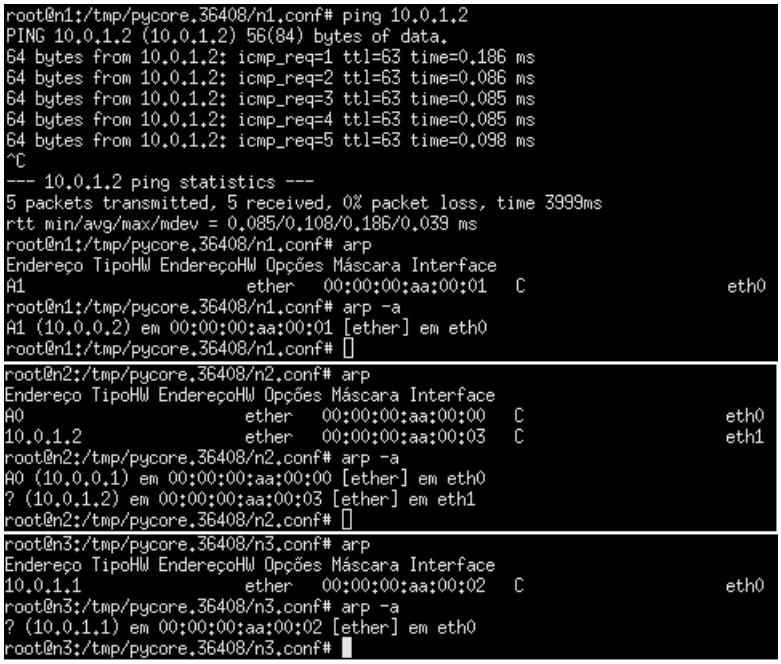

Figura 17. Alterações nas tabelas ARP dos sistemas após fazer ping de n1 para n3.

19) Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com endereço Ethernet inexistente. O que acontece?

Procedemos conforme o descrito, como mostra a Figura 18. Concluímos que n1 perde a conexão para n2 e, por consequência, para n3, como podemos verificar, por exemplo, na Figura 19.

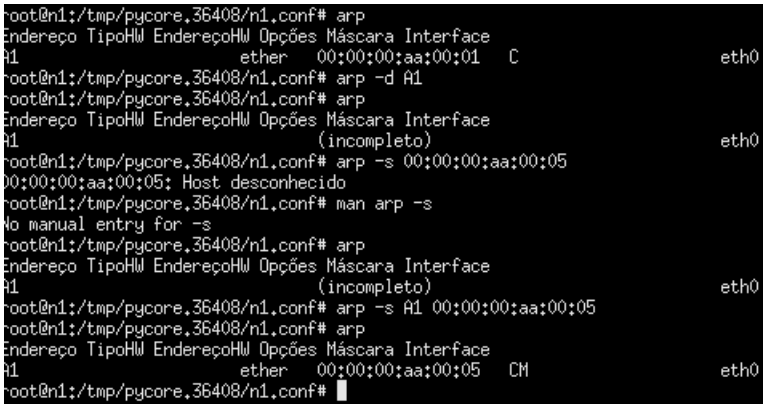

Figura 18. Remoção da entrada relativa a n2 da tabela ARP de n1 e inserção de um endereço Ethernet inexistente.

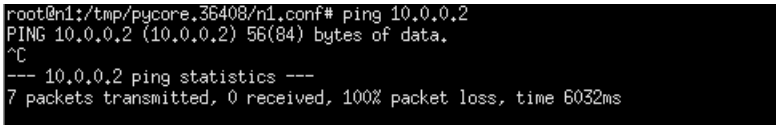

Figura 19. Ping de n1 para n2.

Alteramos a topologia conforme o descrito.

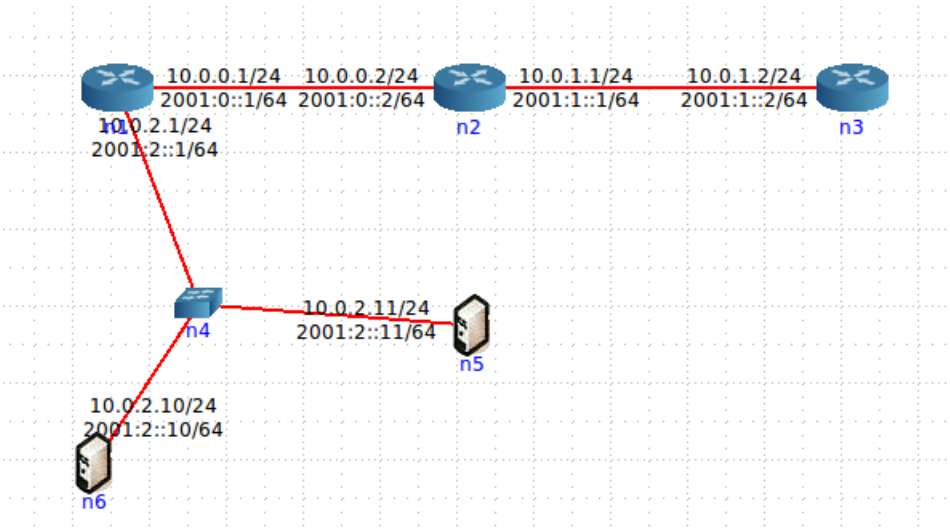

Figura 20. Topologia CORE após inserir n4, n5 e n6 à rede.

20) Faça ping de n6 para n5. Sem consultar a tabela ARP anote a entrada que, em sua opinião, é criada na tabela ARP de n6. Verifique, justificando, se a sua interpretação sobre a operação da rede Ethernet e protocolo ARP estava correto.

Dado que o CORE começou por atribuir endereços MAC aos routers da forma 00:00:aa:00:0x, $x \in [0, 3]$, é espectável que para a nova interface de n1 seja atribuido o endereço 00:00:aa:00:04, para n5 00:00:aa:00:05 e para n6 00:00:aa:00:06. Ora, ao fazer ping de n6 para n5, seria de esperar que a entrada criada na tabela ARP de n6 atribuirá ao endereço IP de n5, 10.0.2.11, o endereço MAC 00:00:aa:00:05, como verificamos na Figura 33.

```
root@n6:/tmp/pycore.36409/n6.conf# arp
root@n6:/tmp/pycore.36409/n6.conf# ping 10.0.2.11
PING 10.0.2.11 (10.0.2.11) 56(84) bytes of data.
64 bytes from 10.0.2.11: icmp_req=1 ttl=64 time=0.120 ms
64 bytes from 10.0.2.11: icmp_req=2 ttl=64 time=0.062 ms
64 bytes from 10.0.2.11: icmp_req=3 ttl=64 time=0.061 ms
64 bytes from 10.0.2.11: icmp_req=4 ttl=64 time=0.067 ms
64 bytes from 10.0.2.11: icmp_req=5 ttl=64 time=0.066 ms
^C
--- 10.0.2.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.061/0.075/0.120/0.023 ms
root@n6:/tmp/pycore.36409/n6.conf# arp
Endereço TipoHW EndereçoHW Opções Máscara Interface
10.0.2.11                ether   00:00:00:aa:00:05   C                     eth0
root@n6:/tmp/pycore.36409/n6.conf# arp -a
? (10.0.2.11) em 00:00:00:aa:00:05 [ether] em eth0
root@n6:/tmp/pycore.36409/n6.conf#
```

Figura 21. Tabela ARP de n6 após *ping* de n6 para n5.

3 Parte II

3.1 ARP Gratuito

1) Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Verifique quantos pacotes ARP gratuito foram enviados e com que intervalo temporal?

Na Figura 22 podemos ver um exemplo de pacote ARP gratuito enviado pelo nosso sistema. No total foram enviados 3 pacotes, com uma média de $\mu \approx 56.037552s$ entre eles.

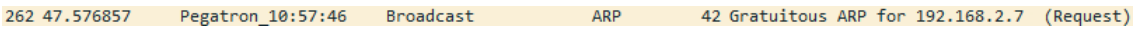

Figura 22. Exemplo de pedido ARP gratuito.

2) 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?

Podemos constatar, pela Figura 23, que o pedido ARP gratuito, para além da informação contida nos pedidos ARP habituais, apresenta uma flag *Is gratuitous* a indicar que se trata de um ARP gratuito. É esperado que o pedido não obtenha resposta, pois caso lhe enviassem, significaria que existe algum sistema na rede com o mesmo endereço IP do nosso dispositivo, identificando um conflito na rede local.

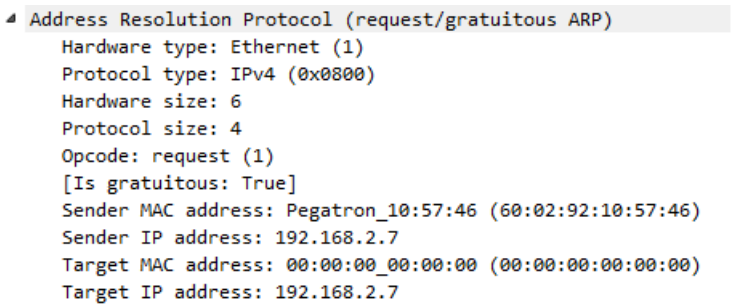

Figura 23. Campo ARP do pacote enviado.

3.2 Dominios de Colisão

1) Faça ping de n1 para n4. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

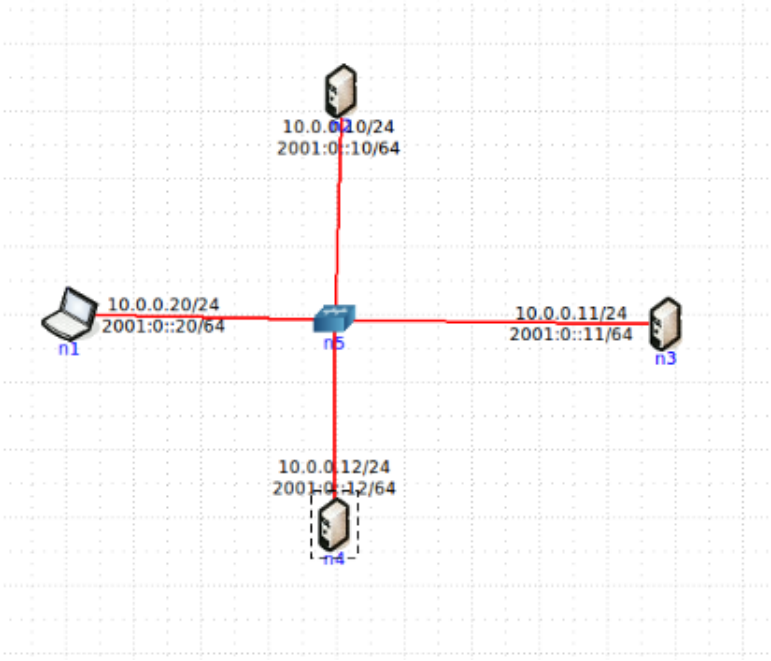

Figura 24. Rede com Hub

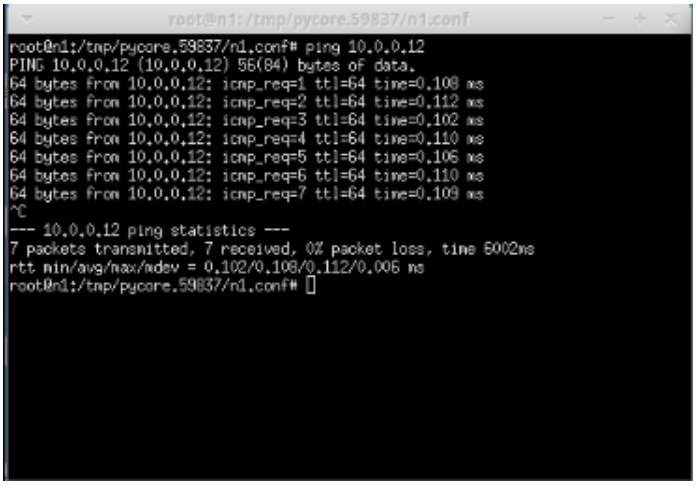

Figura 25. *ping* de n1 para n4.

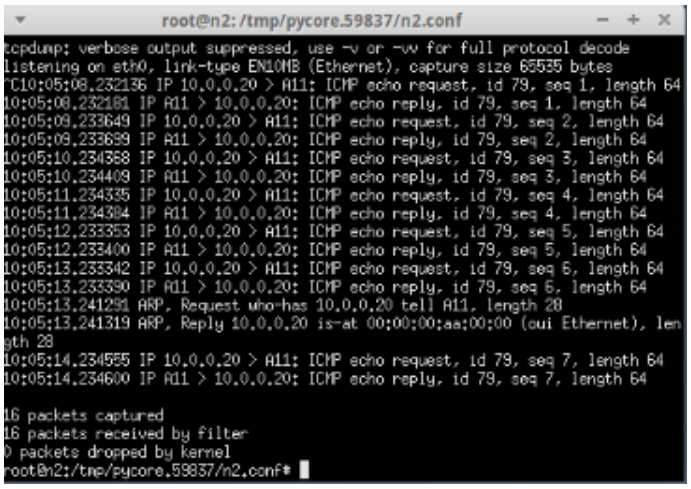

Figura 26. Tcpdump em n2

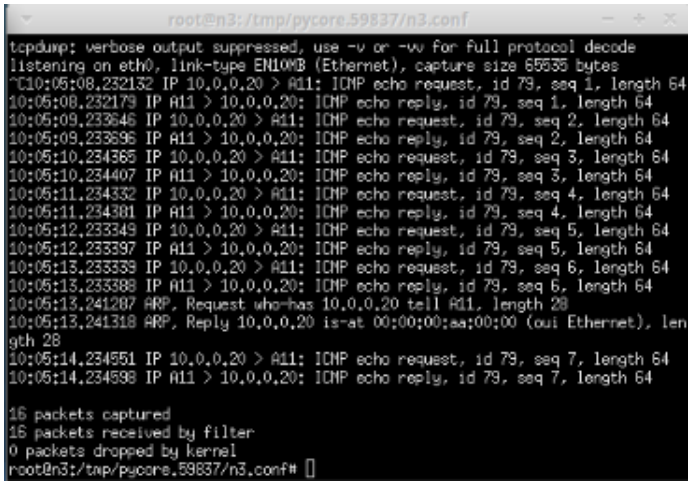

Figura 27. Tcpdump em n3

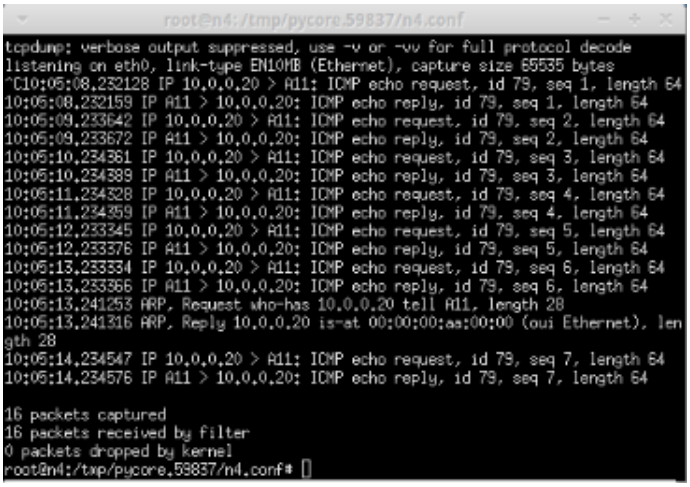

Figura 28. Tcpdump em n4

Um hub ao receber um pacote de dados, reencaminha-o para todos os dispositivos que fazem parte da rede a que ele pertence, fazendo também a deteção de colisões. Através da análise do output resultante do comando tcpdump em cada um dos hosts da rede conclui-se o que foi dito anteriormente. Apesar de ser realizada uma transferência de dados entre os hosts n1 e n4, a informação também é enviada como tráfego nos restantes hosts.

2) 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.

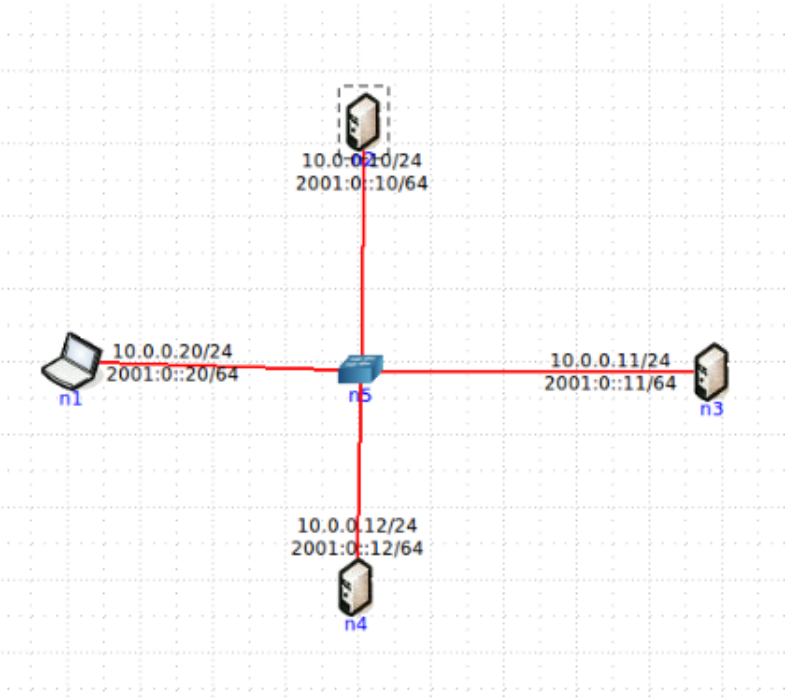

Figura 29. Rede com Switch

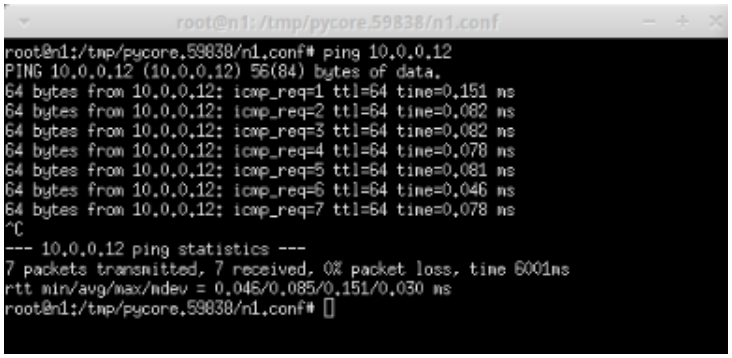

Figura 30. *ping* de n1 para n4.

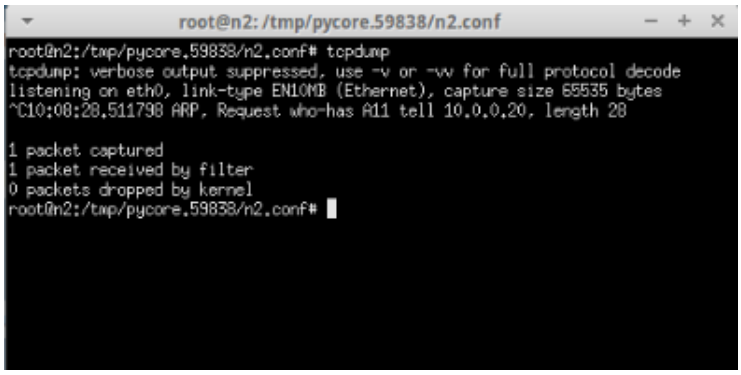

Figura 31. Tcpdump em n2

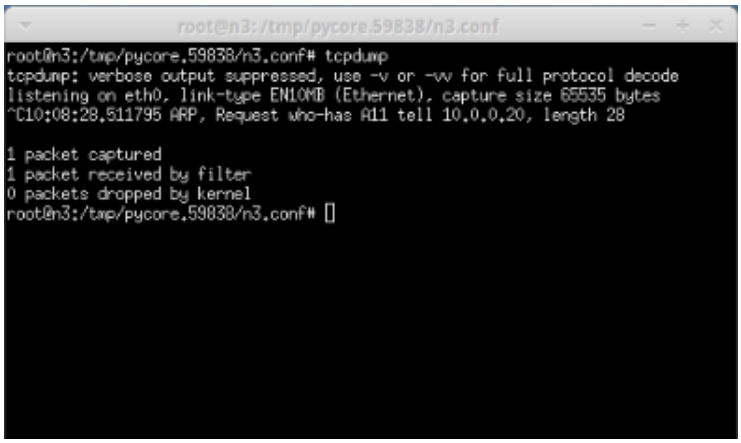

Figura 32. Tcpdump em n3

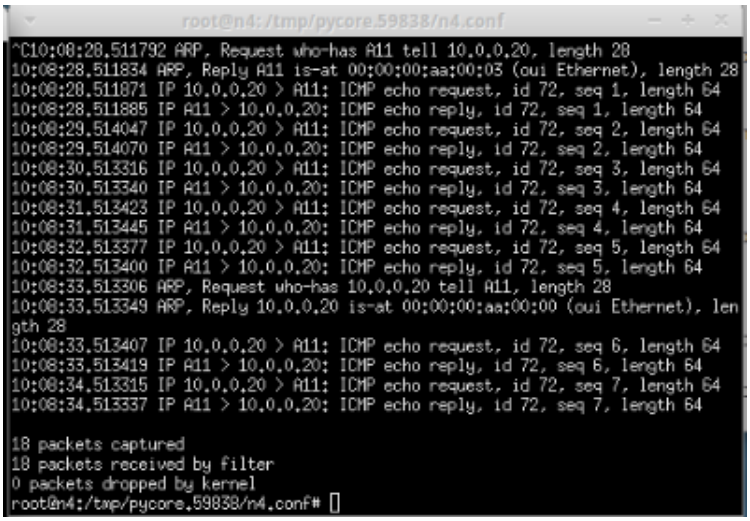

Figura 33. Tcpdump em n4

O hub permite detetar, se acontecer, uma colisão 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 neste dominio, permitem evitar colisões de tramas ao enviar dados que são relevantes a certos dispositivos na rede.
Ao analisarmos o tráfego nos dispositivos podemos concluir que nos hosts n1 e n4 se verificou a captura de dados, e no n2 e n3 não se observa qualquer tráfego. Ou seja, como o comando ping foi executado apenas entre n1 e n4, a transferência de dados apenas é relevante para eles próprios, não realizando qualquer tráfego nos restantes. Com isto podemos concluir que o switch é um dispositivo que atenua melhor os conflitos.

4 Conclusão

Executada a II podemos concluir que houve um aumento da compreensão sobre a execução dos processos e objetivo predefinido, (relacionar e fornecer informação entre a camada L2 e L3), do protocolo ARP que contribuiu também para uma melhor assimilação dos conceitos da abordados na parte I, Ethernet e ARP. Este trabalho prático permitiu-nos ainda aprofundar o nosso conhecimento sobre as ferramentas utilizadas, ferramenta de simulação de redes (CORE) e de captura e análise de tramas (Wireshark). A utilização do Wireshark foi fundamental para este trabalho pois permitiu-nos verificar quais os protocolos envolvidos, qual o encapsulamento correto no processo de transferência e verificar outras propriedades importantes, que nos permitem saber informações como quais os endereços envolvidos, tipo da mensagem ARP e a análise de um pedido ARP.