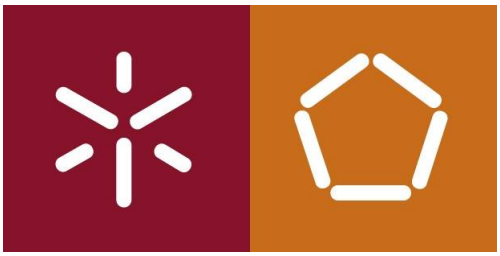
Universidade do Minho

Mestrado Integrado em Engenharia Informática



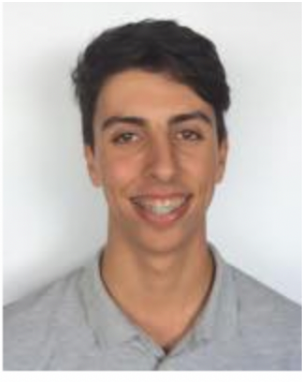
TP3 - Camada de Ligação Lógica: Ethernet e Protocolo ARP

Redes de Computadores

PL 4 Grupo 8

Carla Cruz
A80564

Diogo Sobral
A82523



Pedro Freitas
A80975

November 26, 2018

Captura e análise de Tramas Ethernet

Assegure-se que a cache do seu browser está vazia e está conectado em rede através da interface Ethernet.

Ative o Wireshark na sua máquina nativa.

No seu browser, aceda ao URL http://miei .di.uminho.pt.

Pare a captura do Wireshark.

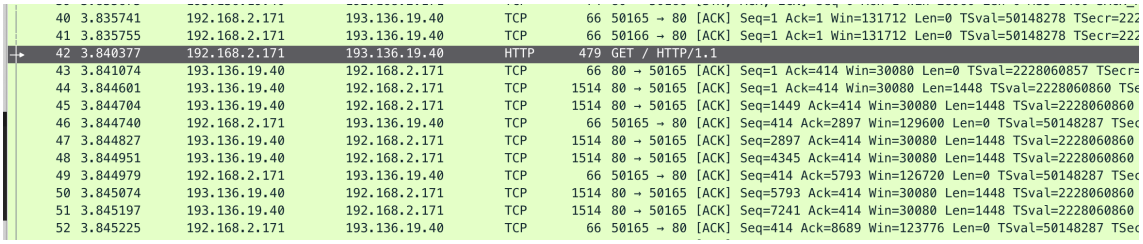
Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda da janela do Wireshark) correspondente à mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o começo da respetiva mensagem HTTP Response proveniente do servidor.

No sentido de proceder à análise do tráfego, selecione a trama Ethernet que contém a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP está no interior de um segmento TCP que é transportado num datagrama IP que, por sua vez, está encapsulado no campo de dados de uma trama Ethernet. Expanda a informação do nível da ligação de dados (Ethernet II) e observe o conteúdo da trama Ethernet (cabeçalho e dados (payload)).

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem HTTP GET.

Sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada. Para imprimir um pacote, use File-àPrint, escolha Selected packet only e Packet summary line, ou use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o mínimo detalhe necessário para responder à pergunta.

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



40	3.835741	192.168.2.171	193.136.19.40	TCP	66	50165 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=50148278 TSecr=222
41	3.835755	192.168.2.171	193.136.19.40	TCP	66	50166 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=50148278 TSecr=222
42	3.840377	192.168.2.171	193.136.19.40	HTTP	479	GET / HTTP/1.1
43	3.841074	193.136.19.40	192.168.2.171	TCP	66	80 → 50165 [ACK] Seq=1 Ack=414 Win=30080 Len=0 TSval=2228060857 TSecr=
44	3.844601	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=1 Ack=414 Win=30080 Len=1448 TSval=2228060860 TSe
45	3.844704	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=1449 Ack=414 Win=30080 Len=1448 TSval=2228060860
46	3.844740	192.168.2.171	193.136.19.40	TCP	66	50165 → 80 [ACK] Seq=414 Ack=2897 Win=129600 Len=0 TSval=50148287 TSec
47	3.844827	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=2897 Ack=414 Win=30080 Len=1448 TSval=2228060860
48	3.844951	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=4345 Ack=414 Win=30080 Len=1448 TSval=2228060860
49	3.844979	192.168.2.171	193.136.19.40	TCP	66	50165 → 80 [ACK] Seq=414 Ack=5793 Win=126720 Len=0 TSval=50148287 TSec
50	3.845074	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=5793 Ack=414 Win=30080 Len=1448 TSval=2228060860
51	3.845197	193.136.19.40	192.168.2.171	TCP	1514	80 → 50165 [ACK] Seq=7241 Ack=414 Win=30080 Len=1448 TSval=2228060860
52	3.845225	192.168.2.171	193.136.19.40	TCP	66	50165 → 80 [ACK] Seq=414 Ack=8689 Win=123776 Len=0 TSval=50148287 TSec

Figure 1: Pacote TCP enviados ao aceder ao site

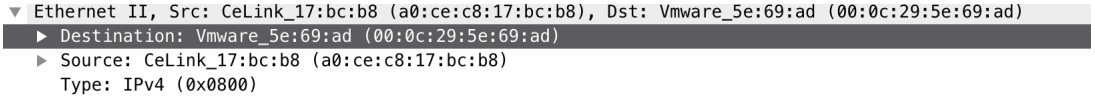


Figure 2: Campo Ethernet II da trama selecionado

Endereço MAC destino -> 00:0c:29:5e:69:ad

Endereço MAC origem -> a0:ce:c8:17:bc:b8

2. **Identifique a que sistemas se referem. Justifique.**

   O endereço mac refere-se ao endereço físico da interface ativa de uma máquina. Neste caso a origem refere-se ao endereço físico do nosso computador e o destino refere-se ao endereço físico do router com que se está a comunicar.

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

   Como podemos ver na figura 2, o campo do Type tem o valor 0x0800 que significa que a camada superior está a utilizar o protocolo IPv4.

4. **Quanto bytes são usados desde o início de trama de caractere ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.**

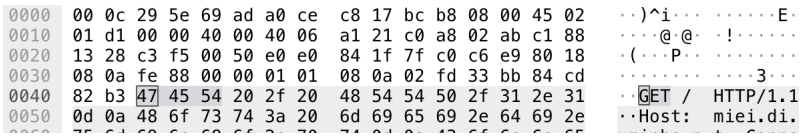


Figure 3: Valor dos bytes da trama

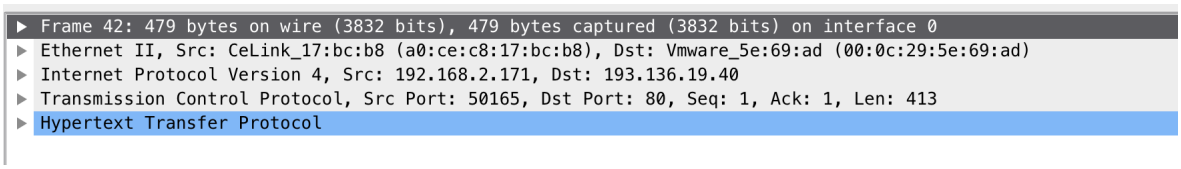
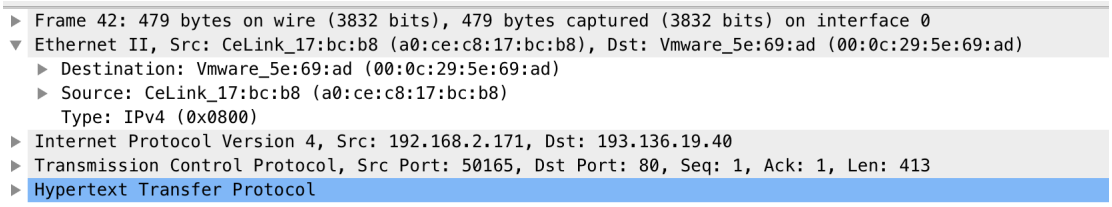


Figure 4: Descrição da trama

Como podemos ver na figura 3, até ao GET temos 8*2*4 +2 (66) bytes. Pela análise da figura 4 vemos que a trama tem 479 bytes ficando assim com uma percentagem com valor 13.78% ((66 * 100) / 479).

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?**



Ao análisar a imagem acima, podemos concluir que o campo FCS não foi utilizado, visto que este não aparece na parte da Ethernet. Do nosso ponto de vista deve-se ao facto de as ligações por cabo serem ligações muito estáveis e pouco suscetíveis a acumularem erros.

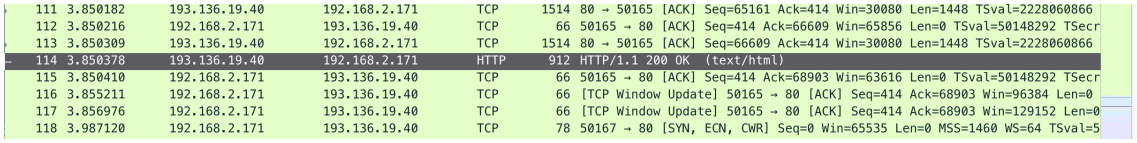


Figure 5: Pacote TCP selecionado

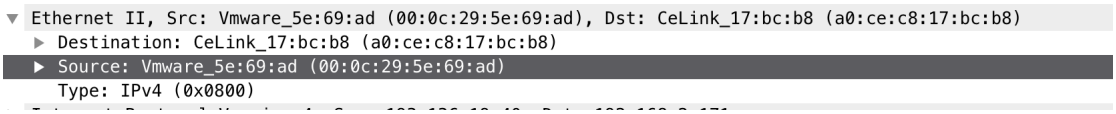


Figure 6: Campo Ethernet II da resposta HTTP

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

   Com a ajuda da figura 6, o endereço ethernet da fonte é 00:0c:29:5e:69:ad e corresponde ao endereço físico do router com que estamos a comunicar.

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

   A figura 6 mostra-nos que o endereço ethernet do destino é a0:ce:c8:17:bc:b8 e corresponde ao endereço físico da interface ativo do nosso computador.

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

   Os protocolos HTTP(Hypertext Transfer Protocol), IPv4(Internet Protocol Version 4), Ethernet e TCP (Transmition Control Protocol).

Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP.

Verifique o conteúdo da cache ARP do seu computador.

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

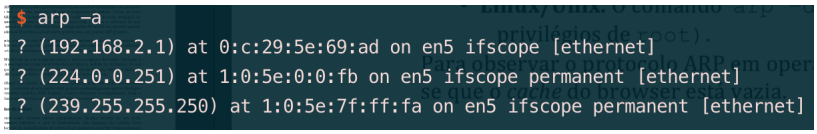


Figure 7: Tabela ARP

R: A primeira coluna tem os endereços IP e a segunda coluna tem os respetivos endereços MAC para os nodos conhecidos em LAN.

Para observar o protocolo ARP em operação, apague novamente a cache ARP e assegura-se que a cache do browser está vazia.

Inicie a captura de tráfego com o Wiresharke e aceda a http://miei.di.uminho.pt. Efetue também um ping para um host da sala de aula que esteja a ser usado por outro grupo. Pare a captura de tráfego e tente localizar o tráfego ARP. Se necessário limite os protocolos visíveis apenas a protocolos abaixo do nível IP. Para tal selecione Analyse->Enabled Protocols e remova a opção IPv4 e IPv6.

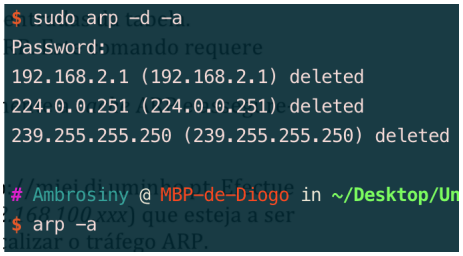


Figure 8: Delete da tabela ARP

No.	Time	Source	Destination	Protocol	Length	Info
5	2.333233	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
6	2.333596	Vmware_5e:69:ad	CeLink_17:bc:b8	ARP	60	192.168.2.1 is at 00:0c:29:5e:69:ad
30	7.377833	Vmware_5e:69:ad	CeLink_17:bc:b8	ARP	60	Who has 192.168.2.171? Tell 192.168.2.1
31	7.377884	CeLink_17:bc:b8	Vmware_5e:69:ad	ARP	42	192.168.2.171 is at a0:ce:c8:17:bc:b8
699	37.182334	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 192.168.2.161? Tell 192.168.2.171
700	37.182670	CompalIn_cc:91:76	CeLink_17:bc:b8	ARP	60	192.168.2.161 is at 20:89:84:cc:91:76
714	42.333281	CompalIn_cc:91:76	CeLink_17:bc:b8	ARP	60	Who has 192.168.2.171? Tell 192.168.2.161
715	42.333323	CeLink_17:bc:b8	CompalIn_cc:91:76	ARP	42	192.168.2.171 is at a0:ce:c8:17:bc:b8

Figure 9: Tráfego ARP

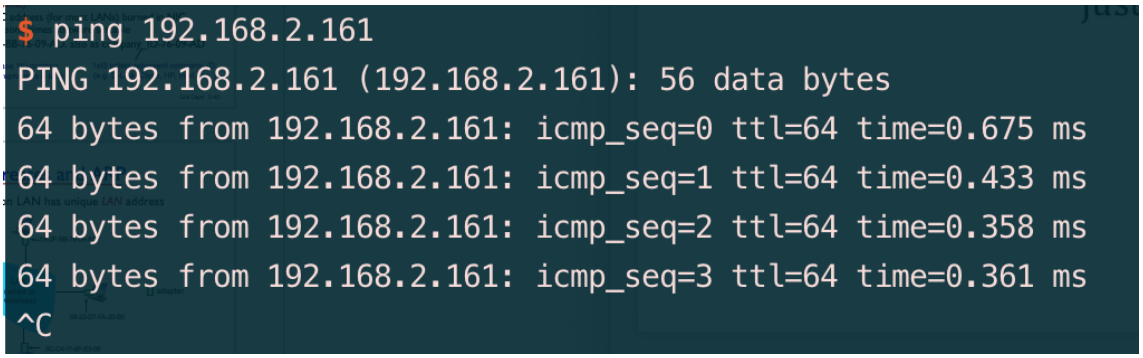


Figure 10: Ping para 192.168.2.161

10. **Qual é o valor hexadecimal dos endereços de origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (ARP Request)? Como interpreta e justifica o endereço destino usado?**

    A origem tem o valor a0:ce:c8:17:bc:b8. O destino tem o valor ff:ff:ff:ff:ff:ff. Este valor deve-se ao facto de a nossa tabela arp não ter o valor do endereço mac associado ao endereço ip para o qual mandamos o ping. Assim é preciso enviar para todos os dispositivos na rede para que o destino possa responder e assim guardar o valor do endereço mac. Para isto usamos o endereço de broadcast (ff:ff:ff:ff:ff:ff).

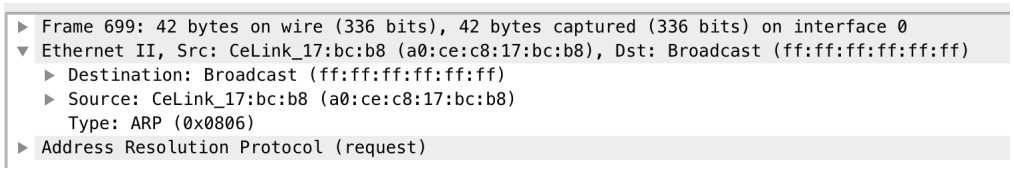


Figure 11: Campo Ethernet

11. **Qual o valor hexadecimal do campo tipo de trama Ethernet? O que indica?**

    Como mostra na figura 12, o campo type tem o valor 0x0806 e indica que a camada acima está a usar o protocolo ARP (Address Resolution Protocol).

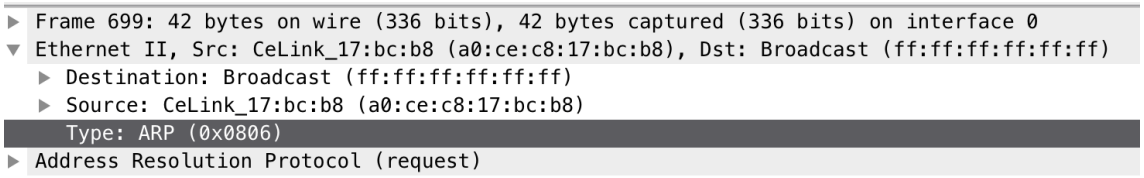


Figure 12: Type

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.**

    Na figura 13, podemos ver que o opcode tem o valor 1 que representa um request. Assim podemos concluir que a nossa máquina está a pedir aos dispositivos em rede para que respondam se o seu ip for o pretendio.

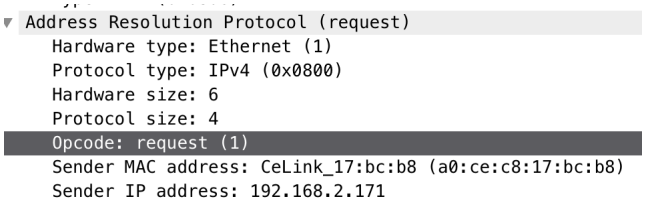


Figure 13: Opcode do ARP

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

    Uma mensagem ARP contém endereços MAC e IP. Com isto concluimos que o protocolo ARP serve para converter um endereço IP no endereço mac da interface ativa respetiva.

14. **Explicite que tipo de pedido ou pergunta é feita pelo host de origem?**

    Quando o ping é feito, a nossa tabela arp não tem uma associação entre o IP para o qual o ping foi executado e o respetivo endereço mac. Assim é enviado uma mensagem ARP para todos os dispositivos na rede para que o endereço IP pretendido, caso receba a mensagem, responda com o seu endereço mac.

15. **Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.**

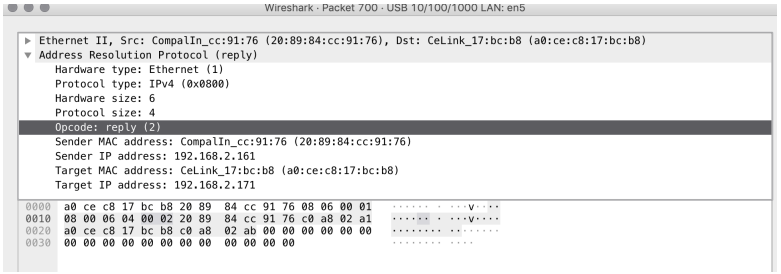


Figure 14: Mensagem de resposta

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

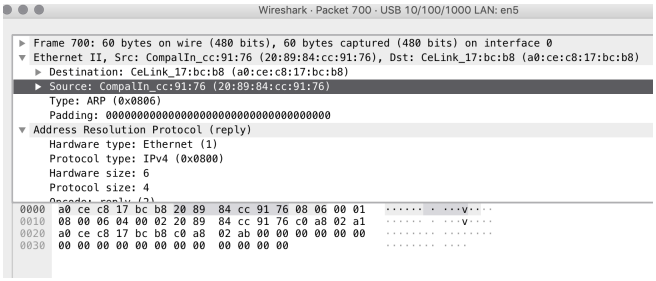


Figure 15: Opcode

O campo opcode tem o valor 2 e significa que o endereço 192.168.2.161 recebem a mensagem de request e está a comunicar o seu endereço mac de volta.

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

A resposta à mensagem está nos bytes entre 23 e 28 da trama, ou seja, é o sender mac address da source na mensagem de resposta.

ARP Gratuito

Arranque Wireshark na sua máquina nativa e inicie a captura de dados.

Desligue e volte a ligar a sua ligação à rede local Ethernet, ou force o pedido de atribuição de um novo endereço IP à interface em uso. Pare a captura de tráfego. Utilize o filtro de visualização ARP para facilitar a identificação dos pacotes respetivos.

16. **Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúde 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?**

91	14.856914	CeLink_17:bc:b8	Vmware_5e:69:ad	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
95	14.879460	CeLink_17:bc:b8	Vmware_5e:69:ad	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
96	14.924724	CeLink_17:bc:b8	Vmware_5e:69:ad	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
97	15.010003	CeLink_17:bc:b8	Vmware_5e:69:ad	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
98	15.010359	Vmware_5e:69:ad	CeLink_17:bc:b8	ARP	60	192.168.2.1 is at 00:0c:29:5e:69:ad
99	15.010803	CeLink_17:bc:b8	Broadcast	ARP	42	Gratuitous ARP for 192.168.2.171 (Request)
100	15.015431	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.171
101	15.041272	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.171
102	15.041548	Vmware_5e:69:ad	CeLink_17:bc:b8	ARP	60	192.168.2.1 is at 00:0c:29:5e:69:ad
109	15.340510	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.171
123	15.662060	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.171
152	15.983521	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.171
216	16.305604	CeLink_17:bc:b8	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.171

Figure 16: ARP Gratuito

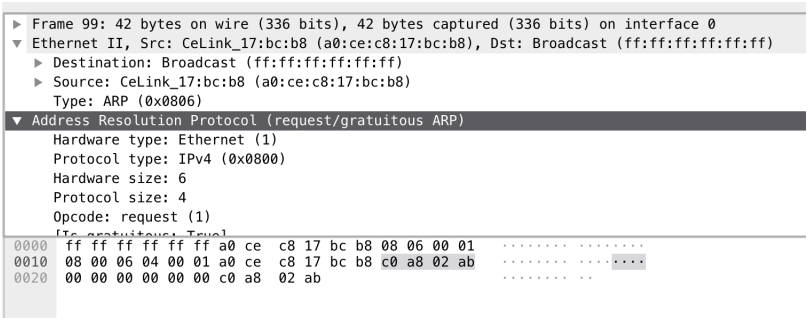


Figure 17: ARP valores

A grande diferença entre os valores do ARP gratuito e os outros é o valor do Target IP address que aqui tem o mesmo valor que o Target IP address e nos outros tem valor diferente. Como não temos um target IP não é suposto outros dispositivos, para além do router, responderem aos ARP. Como podemos ver na figura 16, apenas o router a que estamos ligados respondeu.

Domínios de colisão

Construa uma topologia no emulador CORE com um Laptop (n1) e três servidores (n2,n3,n4) interligados através de um hub(repetidor).

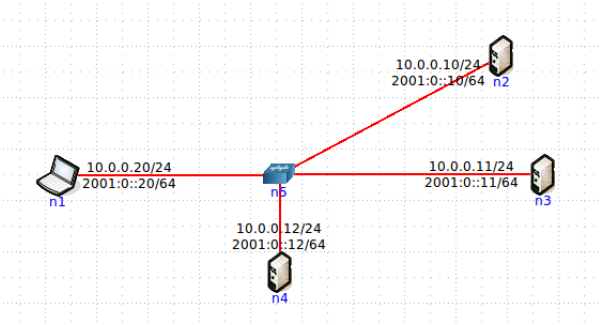


Figure 18: Topologia implementada

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

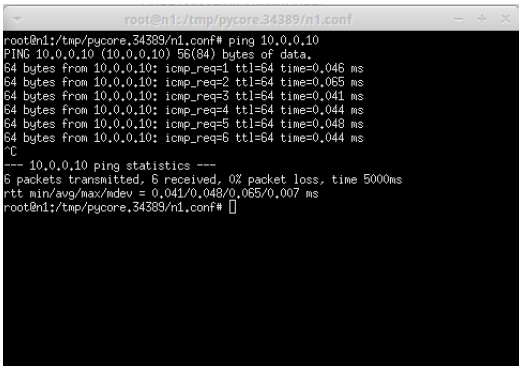


Figure 19: N1

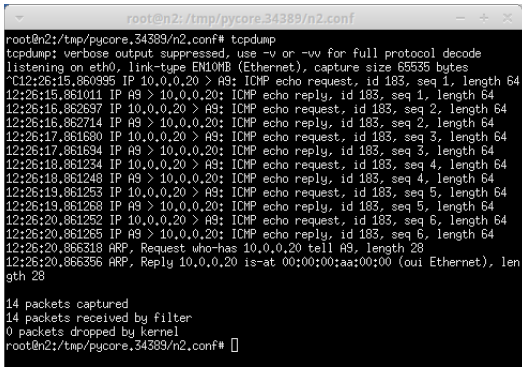


Figure 20: N2

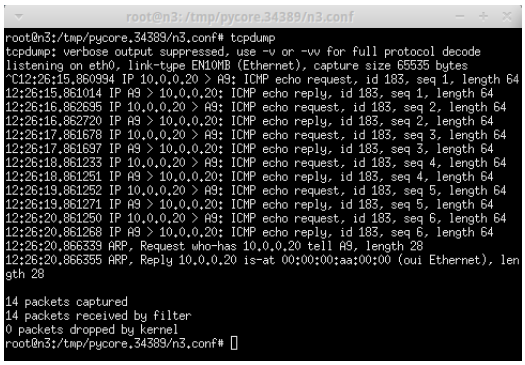


Figure 21: N3

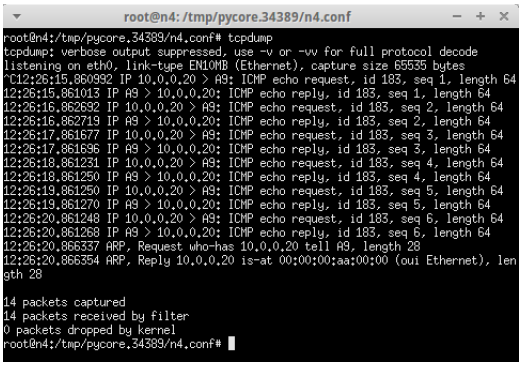


Figure 22: N4

Um hub é um dispositivo que trabalha a nível físico juntando várias portas num único segmento de rede. Quando é enviado algo entre duas portas, o hub envia o input que recebeu para todas as portas ligadas à exceção da porta que enviou o input. Como podemos ver pelas imagens, o tráfego que passa em n2,n3 e n4 é o mesmo, visto que o hub redireciona para todas as portas. Com isto concluimos que acabam por chegar mensagens que não são supostas a outros dispositivos.

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.**

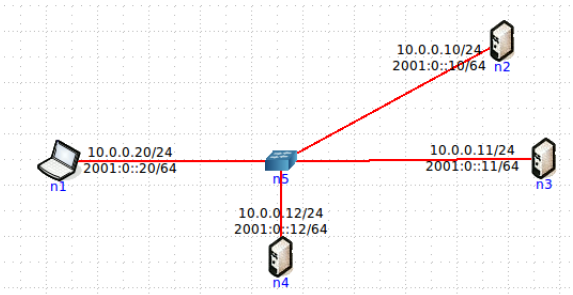


Figure 23: Topologia implementada

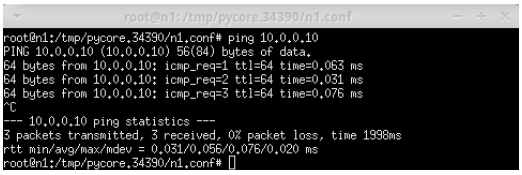


Figure 24: N1

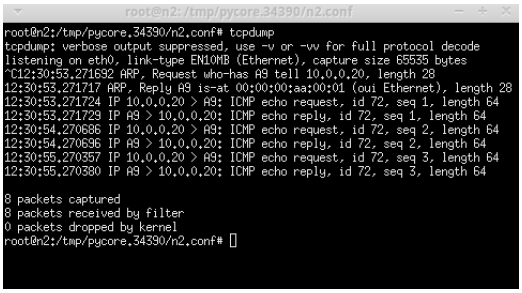


Figure 25: N2

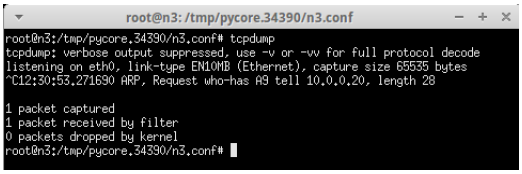


Figure 26: N3

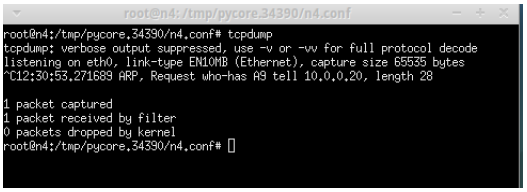


Figure 27: N4

Quando usamos a topologia com hub, o tráfego é enviado para todos os dispositivos. Ao mudar para switch, o tráfego capturado pelo tcpdump muda. Ao contrário da primeira topologia, agora o tráfego é apenas direcionado para o n2. Os outros dispositivos n3 e n4, possum apenas uma captura que é a resultante do envio ARP Broadcast como podemos ver nas figura 26 e 27. Com isto concluímos que os switchs ao evitarem enviar a informação para todos os hosts fazem com que o risco de haver colisões seja menor. Em contra partida, o hub como junta tudo num canal de transmissão único e repete muita da informação está mais propicio a colisões. Um switch possui um tabela de enderaçamento que permite fazer o redirecionamento apenas para o nó pretendido.

Conclusão

Neste trabalho prático realizado foi-nos possível aprofundar o conhecimento acerca as tramas de Ethernet e que estas estão organizadas em bytes, bem como, conhecer um melhor o protocolo ARP. Para realização deste utilizamos o simulador de redes (CORE) e ainda um de captura e análise de tramas (Wireshark).

A utilização desta segunda ferramenta foi essencial pois permitiu a observação dos protocolos envolvidos, qual o encapsulamento a ter aquando a transferência de processos e verificar outras propriedades importantes, que permitem ter conhecimento e informações sobre os endereços envolvidos, o tipo da mensagem ARP, assim como a análise de um pedido ARP.

Outro ponto abordado foi a análise de um ARP Gratuito, verificando assim que apesar de ser algo que acontece sem que se tenha pedido para o fazer este torna-se útil na verificação de um host ter o mesmo endereço IP que o originador do pedido, assim como permite informar hosts e/ou switches novos endereços MAC para que todos os sistemas da rede possam atualizar as suas tabela ARP.

Desta forma pudemos consolidar conceitos, protocolos e comportamento dos dados transmitidos em Ethernet.