**Ethernet e Protocolo ARP**

Ficha TP3

**Alberto Faria, César Augusto e Diogo Nogueira (Grupo 47)**

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal

e-mail: {a79077, a79014, a78957}@alunos.uminho.pt

------------------------------------

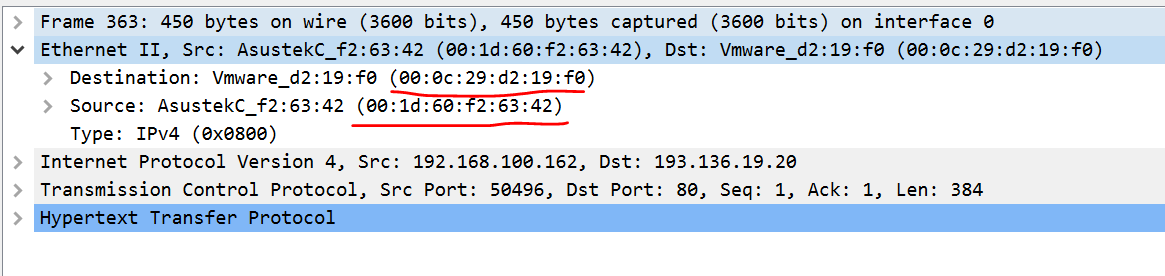
**Questões e Respostas**

Parte I

Exercício 3.

**1.** Os endereços MAC de origem e de destino da trama capturada são, respetivamente:

* **Endereço MAC origem:** 00:1d:60:f2:63:42
* **Endereço MAC destino:** 00:0c:29:d2:19:f0

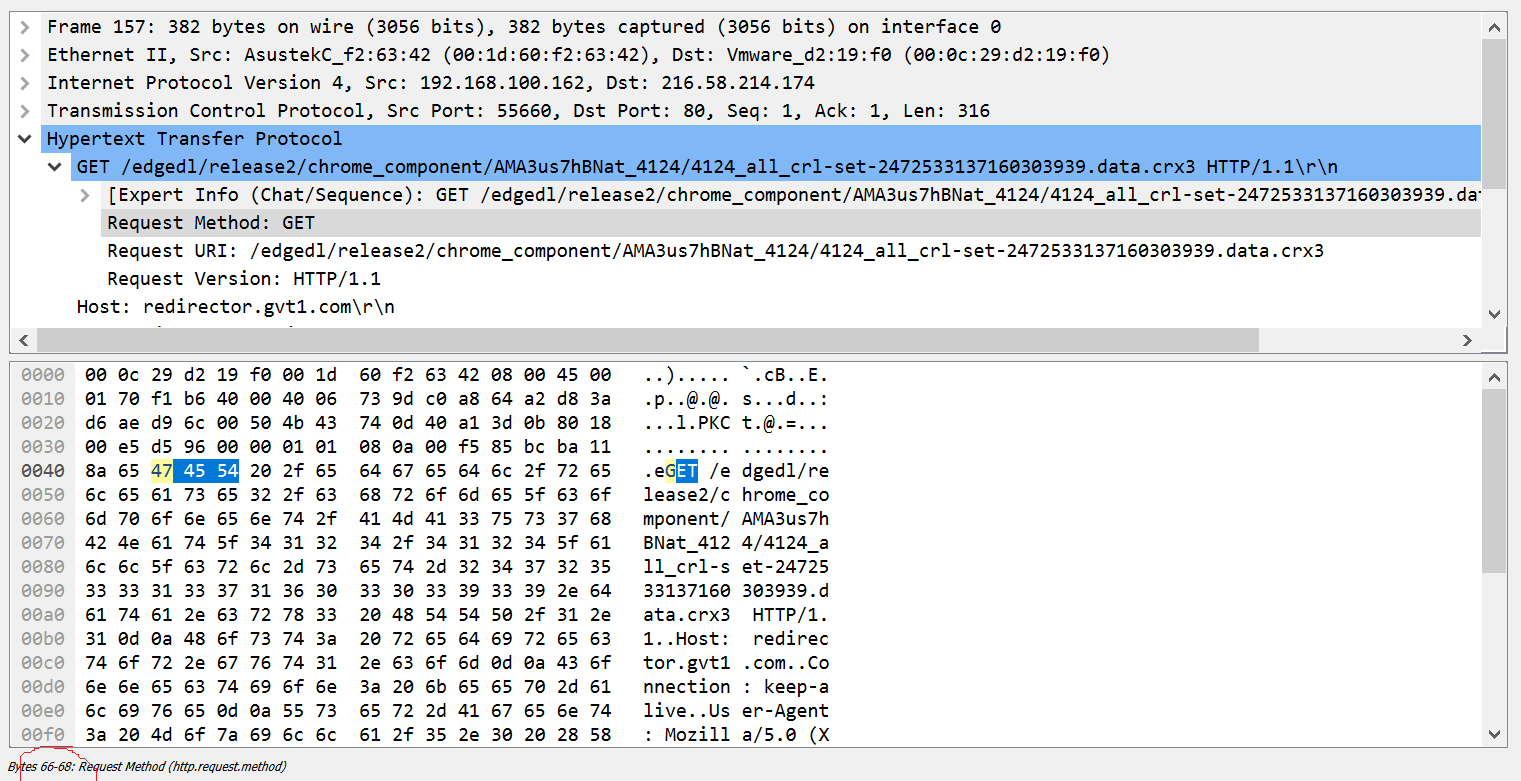


**2.** Os sistemas a que cada endereço acima se referem são, respetivamente, o nosso computador e o servidor web. O nome *“AsustekC”* é portanto referente ao computador que o grupo utilizou e o nome *“Vmware”* corresponde ao servidor, uma vez que, este está a ser migrado para uma Virtual Machine.

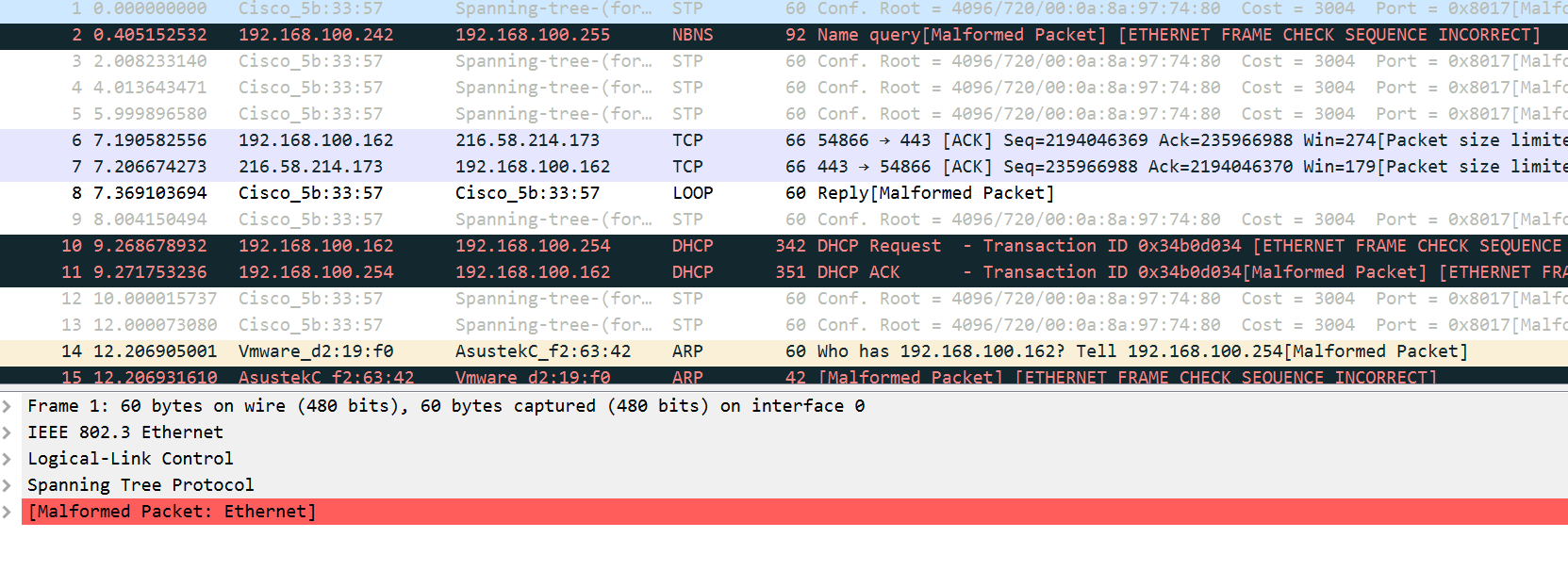
**3.** O valor hexadecimal do campo *Type* da trama *Ethernet* é 0x0800 (conforme percetível na imagem acima) e significa que o campo de dados da trama em questão é do tipo IPv4.

**4.** Uma vez existem 450 bytes de informação na primeira camada, antes de desencapsular, e efetuando os respetivos cálculos, conseguimos chegar à conclusão que, são usados 66 bytes desde o início da trama até ao caractere ASCII “G” do método HTTP GET. Note-se que, mesmo sem efetuar quaisquer tipos de cálculos, conseguiríamos chegar a esta exata conclusão através da identificação no número do byte a que corresponde este caractere. Pelo próprio Wireshark, selecionando o caractere “G” obtemos a informação que corresponde ao byte 66.

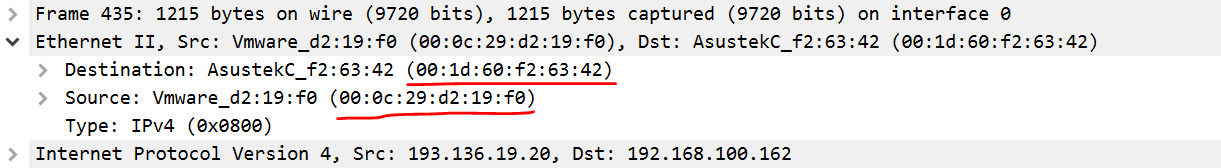
**Assim sendo, a percentagem de sobrecarga introduzida pela pilha protocolar no envio do HTTP Get é de:**

****

**5.** Através da imagem abaixo introduzida, podemos verificar que, não é visível o valor hexadecimal do campo FCS da trama capturada.

 Uma vez que não foi utlizado FCS na fonte, obtém-se um erro na comparação dos valores deste campo.

**6,7.** O endereço Ethernet da fonte corresponde ao servidor web em si. Isto é de esperar uma vez que, inicialmente, existiu uma mensagem HTTP GET por parte do nosso computador para o servidor web em questão. Sendo assim, o endereço MAC de destino corresponde ao nosso computador já que está a existir uma resposta por parte do servidor em consequência de um pedido nosso.

* **Endereço MAC origem:** 00:0c:29:d2:19:f0
* **Endereço MAC destino:** 00:1d:60:f2:63:42

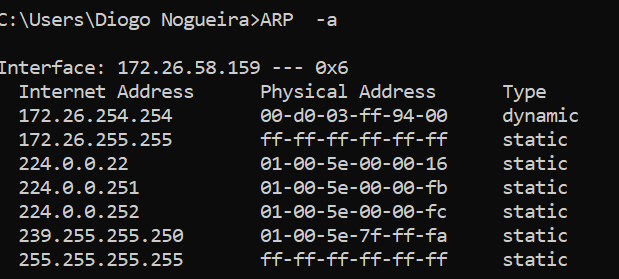
**8.** Tem de se ter em mente que a mensagem HTTP é transportada por um segmento TCP, que é carregado num datagrama IP, que é levada num quadro Ethernet. Isto é percetível se pensarmos nas 4 camadas da pilha protocolar TCP/IP.

* **Camada de Dados:** Ethernet
* **Camada de Rede:** IP
* **Camada de Transporte:** TCP
* **Camada de Aplicação:** HTTP

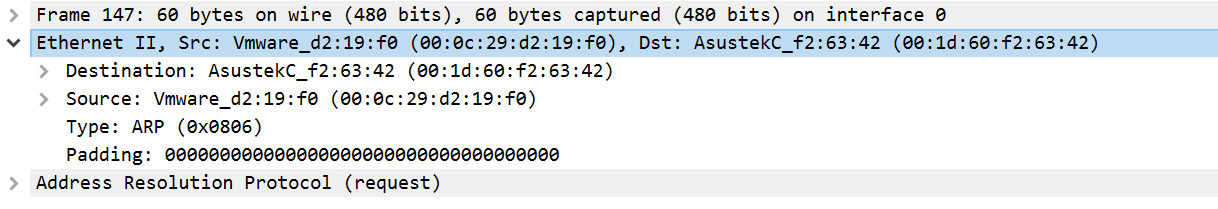
**O Wireshark exibe precisamente as informações sobre o quadro Ethernet, IP, TCP e HTTP, sendo por isso estes os protocolos contidos nesta trama.**

Exercício 4.

**9.** A tabela ARP mostra, numa primeira coluna, os vários endereços IP da nossa rede. Numa segunda coluna, o endereço MAC correspondente aos mesmos e, numa terceira coluna o seu tipo. Podemos por exemplo constatar o endereço de gateway/router e o seu endereço MAC da interface Ethernet.



**10.** O valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP são:

* **Endereço origem:** 00:0c:29:d2:19:f0
* **Endereço destino:** 00:1d:60:f2:63:42

**11.** O valor é 0x0806 e indica, segundo o RFC 7042, que o protocolo que foi encapsulado no *payload*, corresponde ao ARP.

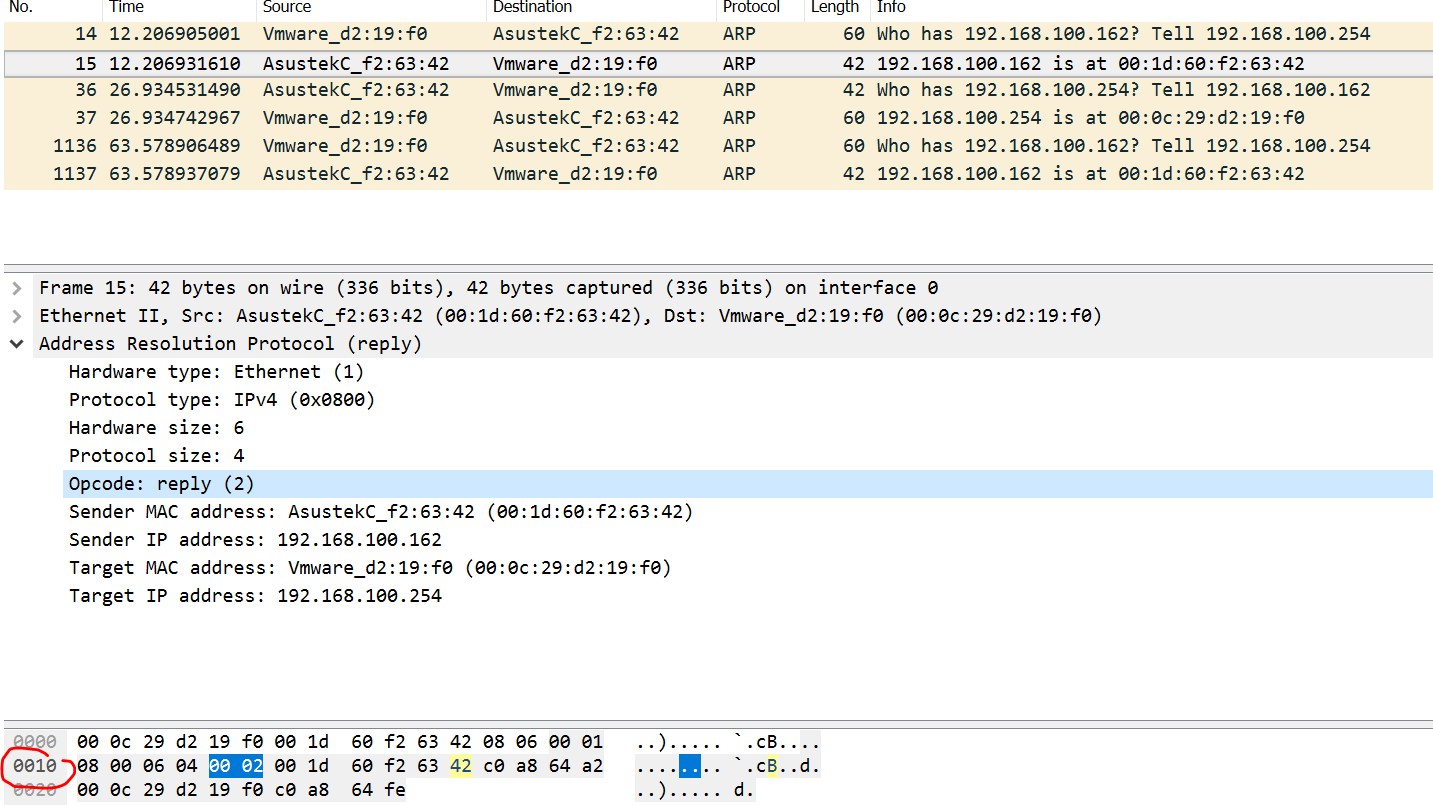
**12.** O campo ARP *opcode* tem o valor de 1 que equivale, segundo o RFC 826, a um pedido (*request)* de ARP.

**13.** Na mensagem ARP estão contidos os endereços IP e MAC, tanto de origem como de destino. O de origem é o que envia a mensagem e, que por isso, pretende saber qual o endereço físico correspondente ao endereço IP do destino.

**14.** O tipo de pergunta que é feita pelo host de origem é qual o endereço MAC correspondente a um dado endereço IP.

**É aqui que o protocolo ARP funciona, permitindo que se obtenha o endereço MAC através do endereço IP.**

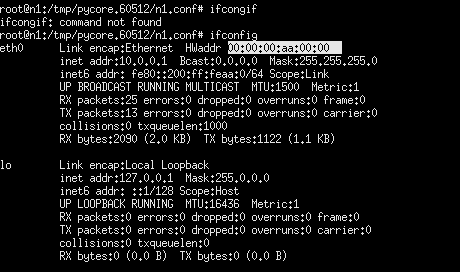
**15**. O valor do campo ARP opcode é 2 que equivale, segundo o RFC 826, a uma resposta *(reply)* de ARP.

 A posição da mensagem ARP em que está a resposta ao pedido ARP é 0x0010, identificada a vermelho na figura seguinte.

Exercício 5.

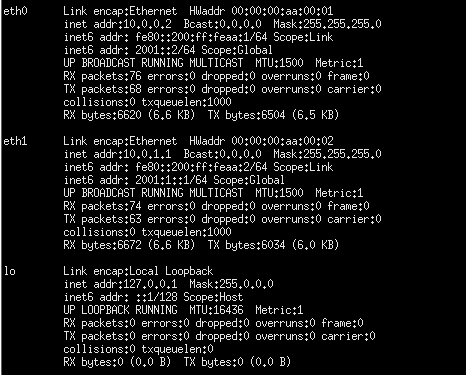
**16.**

**Aplicando o comando ipconfig ao primeiro router (n1) obtemos as seguintes informações:**



Assim, o endereço MAC da interface Ethernet é 00:00:00:aa:00:00.

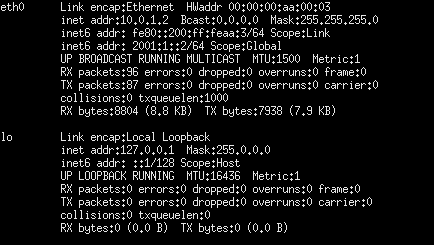
**Aplicando o comando ipconfig ao primeiro router (n2) obtemos as seguintes informações:**



Assim, o endereço Ethernet da interface eth0 é 00:00:00:aa:00:00.

Já o endereço Ethernet da interface eth1 é 00:00:00:aa:00:02.

**Aplicando o comando ipconfig ao primeiro router (n3) obtemos as seguintes informações:**



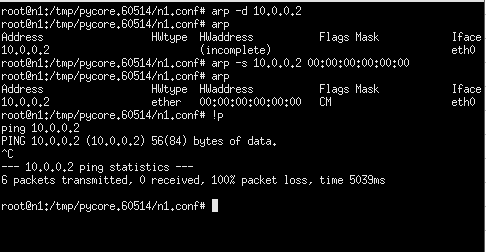
Assim, o endereço Ethernet da interface eth0 é 00:00:00:aa:00:03.

**17.** Utilizando o comando ARP aos diversos sistemas conseguimos perceber que todas as caches ARP se encontram vazias, uma vez que não existiu nenhum ARP Request/Reply. Isso confirma-se figura abaixo apresentada.



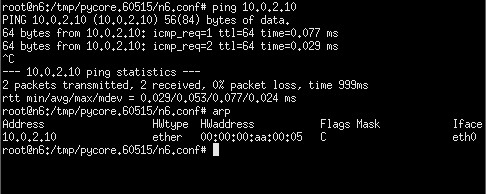
**18.** Como visto na caches ARP, cada router tem a interligação entre endereços IP e MAC das interfaces que estão presentes na sua rede apenas. Dessa forma o n1 tem as correspondências de endereços para n2. O n2 tem as correspondências de endereços para os routers n1 e n3. O n3 tem as correspondências para o router n2.

**19.** Ao mudar para um endereço MAC aleatório, o ping não consegue enviar os pacotes **(100% packet loss)** dado que a informação do endereço Ethernet está errada ao nível 2 (data layer).



**20.** Espera-se que a tabela ARP do n6 tenha uma entrada que correlacione o endereço IP do n5 e o seu respetivo endereço Ethernet.

Como visto no screenshot podemos comprovar o que foi dito acima.



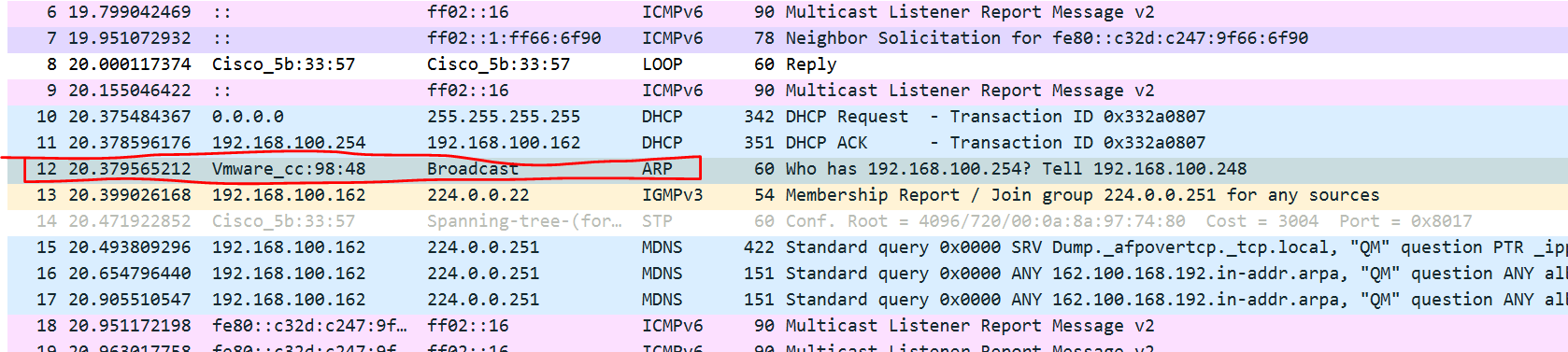
------------------------------------

**Questões e Respostas**

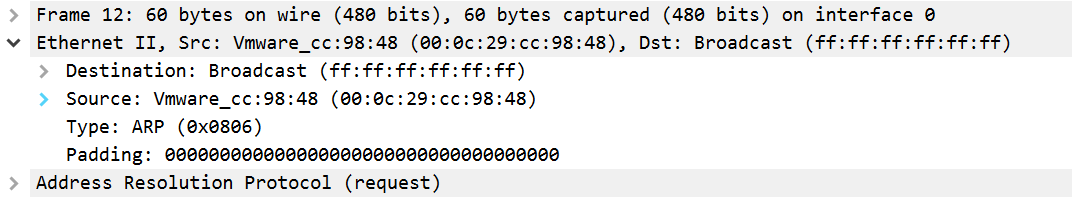
Parte II

Exercício 2.

**1.** Um pacote ARP Gratuito é um pacote de solicitação onde o IP de origem e de destino são ambos definidos para o IP da máquina que emite o pacote. Assim sendo, o endereço MAC de destino é o endereço de transmissão ff: ff: ff: ff: ff: ff, ou seja, *Broadcast*. Conseguimos identificar logo de início um pacote deste tipo.

Além disso, conseguimos verificar pela captura realizada pelo Wireshark que foram enviados apenas 2 pacotes ARP Gratuitos, com um intervalo temporal de aproximadamente 1s.

**2.** Conforme abordado acima, podemos identificar facilmente um pedido ARP Gratuito, distinguindo-o dos demais. Basta notar o facto de o endereço MAC de destino ser o do *Broadcast.*

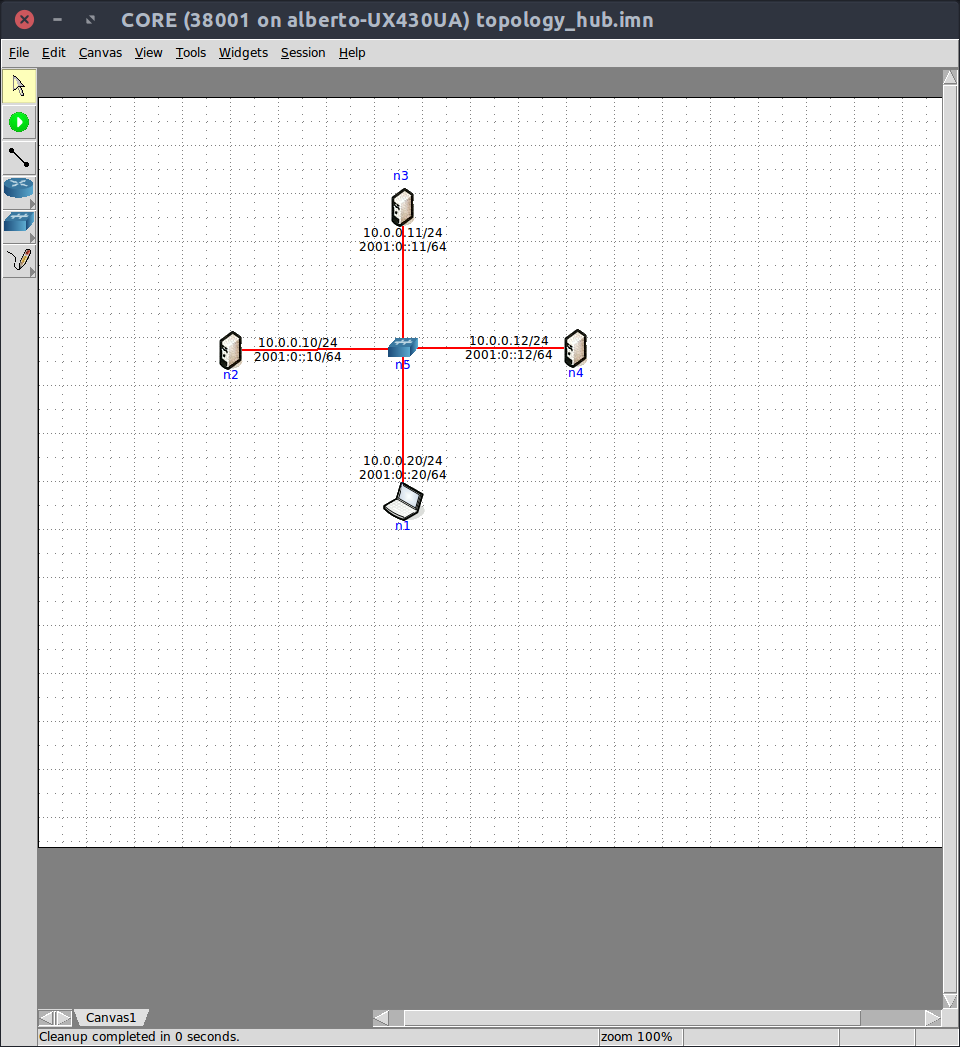
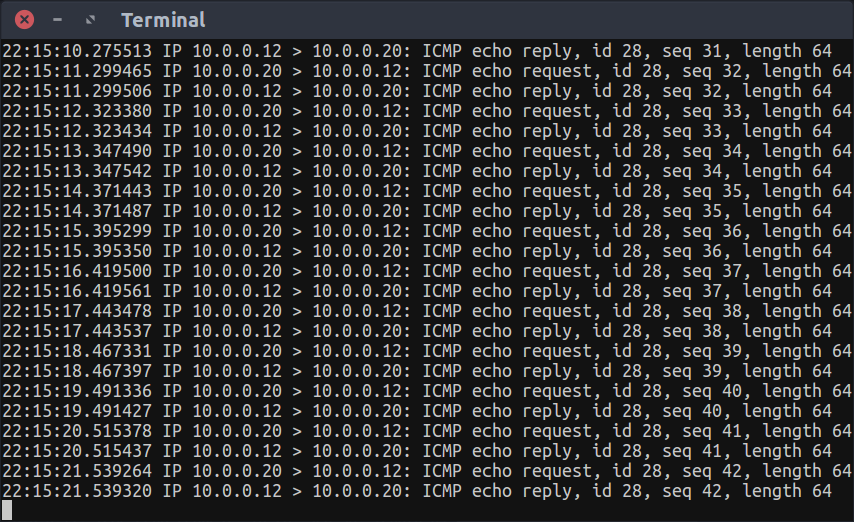
Na imagem abaixo podemos ainda verificar toda a trama Ethernet correspondente a este pacote.

O que se espera face ao pedido ARP Gratuito enviado é que não exista nenhum pacote de resposta já que o objetivo do uso deste tipo de pacotes não passa pela determinação do endereço MAC de um respetivo endereço.

Exercício 3.

**1.** O tráfego nas diversas interfaces dos vários dispositivos é semelhante. Isto seria de esperar uma vez que, estamos perante um hub e, o que acontece é que não há qualquer seleção por parte do tráfego de dados. Com isto, queremos dizer que, os vários pacotes, quando chegam ao hub, são propagados para todas as redes que se encontram ligados a este mesmo.

Assim, decidimos apenas incluir apenas o print do tráfego de um dispositivo já que os outros apresentam informação semelhante.



**2.** Ao efetuarmos a substituição do hub pelo switch observamos, logo à partida, aquando da execução dos vários procedimentos, que, existe um maior controlo sobre o tráfego que circula na rede. Isto acontece porque o switch, ao contrário do hub, possui a capacidade de apenas encaminhar o tráfego recebido para a interface ao qual efetivamente se destina.

Com isto, conseguimos reduzir a possibilidade da existência de colisões.

**Conclusões**

Após concluirmos a realização desta ficha prática que teve como objetivo base fortificar os nossos conhecimentos acerca de toda a camada de ligação lógica, focando para isso no uso da tecnologia Ethernet e no protocolo ARP, podemos tecer alguns comentários que nos parecem ser importantes.

Relativamente à primeira parte, o grupo não sentiu grande dificuldade. Consideramos assim que, a compreensão da análise das várias tramas Ethernet bem como todo o protocolo ARP ficou bem consistente e compreendido.

Onde sentimos alguma dificuldade foi na compreensão do funcionamento do ARP Gratuito. Nesse ponto, sentimos a necessidade de pesquisa e recorrência ao RFC de modo a perceber o porquê de realmente ser necessário o seu uso. Já no que diz respeito aos domínios de colisão não obtivemos grandes questões uma vez que, com toda a interligação desse mesmo assunto com os diferentes equipamentos de interligação de redes (hub e switch), o assunto ficou desde logo percetível.

Achamos ainda importante referenciar que a realização desta ficha prática foi suportada pela bibliografia (o referido RFC) que consideramos ter sido uma mais valia não só para a correta confirmação dos nossos palpites de resposta, mas também para uma aperfeiçoada consolidação da matéria.