**Questões e Respostas**

* **Parte I**

**HTTP**

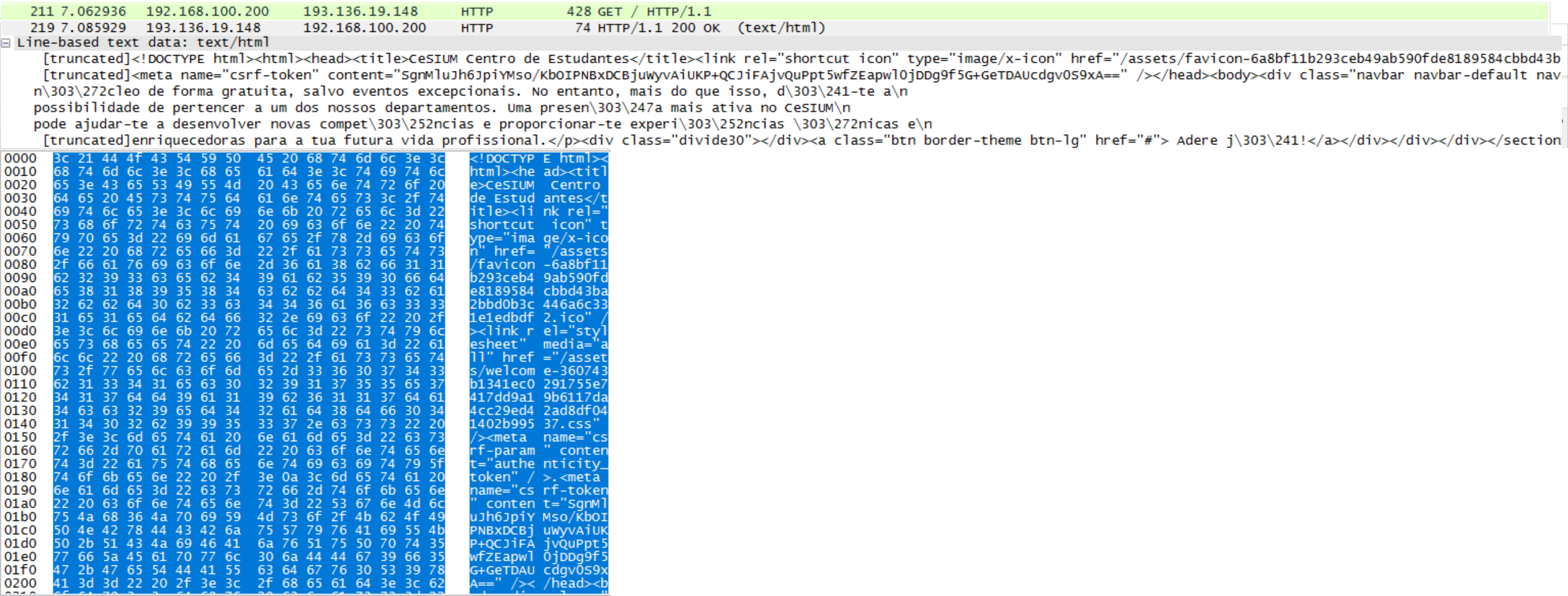


Imagem 0 – Número de ordem da sequência da mensagem HTTP GET é 211

1. 00:e0:4c:60:3d:d0

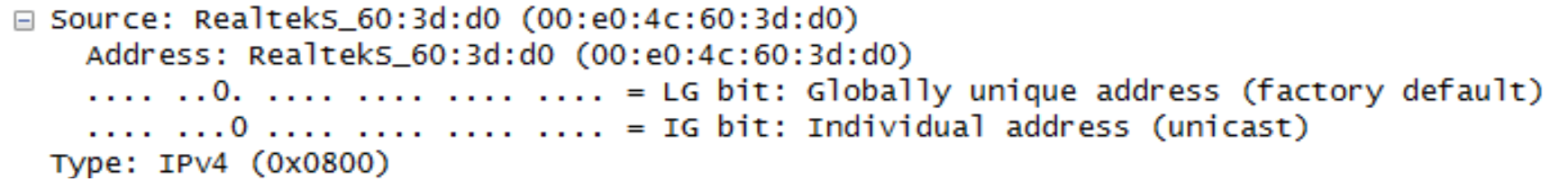


Imagem 1 – Endereço MAC da origem

1. 00:0c:29:d2:19:f0. Não, a trama Ethernet é destinada ao router da rede local do sala de aula. Isto porque como as redes locais do nosso computador e do servidor onde está alojado o servidor do Cesium estão separadas por um ou mais routers, ao estabelecermos uma conexão, o nosso computador não comunica diretamente com o site mas sim com o router da sua rede local que depois se encarregará de comunicar com o servidor.

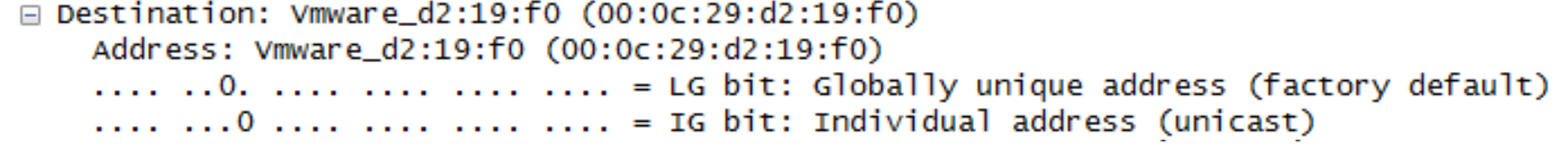


Imagem 2 – Endereço MAC do destino

1. 0x0800. Diz-nos que o protocolo utilizado ao nível da rede é o IPv4.

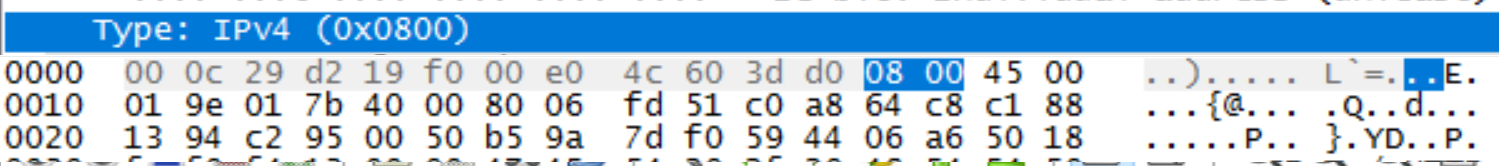


Imagem 3 - Campo Type da trama Ethernet

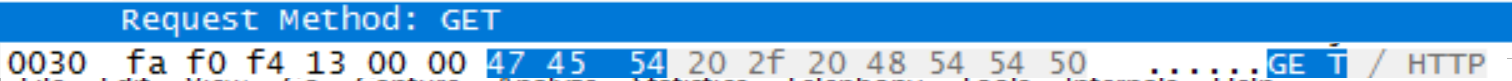


Imagem 4 - Localização do caractere "G" na trama Ethernet

* 1. São utilizados 54 bytes antes do caratere “G” (47 é o código ASCII da letra “G” em hexadecimal).
  2. 428 - 6 - 6 - 2 - 4 = 410 bytes (dados ou payload)

Overhead = 18/428 = 4,2%

1. (imagem 5) O valor hexadecimal do campo FCS da trama capturada 0x0d0a0d0a mas deveria ser 0x2e11ec44. Assim, podemos concluir que houve erros na transmissão da trama (i.e. os dados/payload que chegaram ao destino diferem dos dados que foram transmitidos originalmente).
2. 00:0c:29:d2:19:f0. Corresponde ao Vmware\_d2:19:f0, o servidor onde está alojado o site do Cesium.

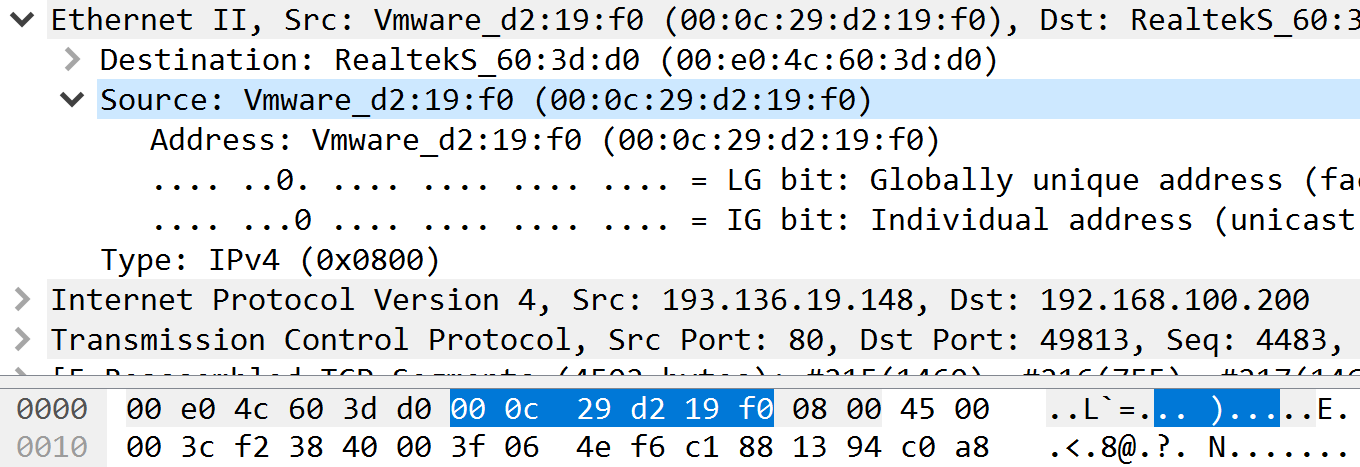


Imagem 5 - Endereço MAC da origem

1. 00:e0:4c:60:3d:d0. Corresponde à placa de rede da nossa máquina (RealtekS\_60:3d:d0 - fabricante da placa de rede).

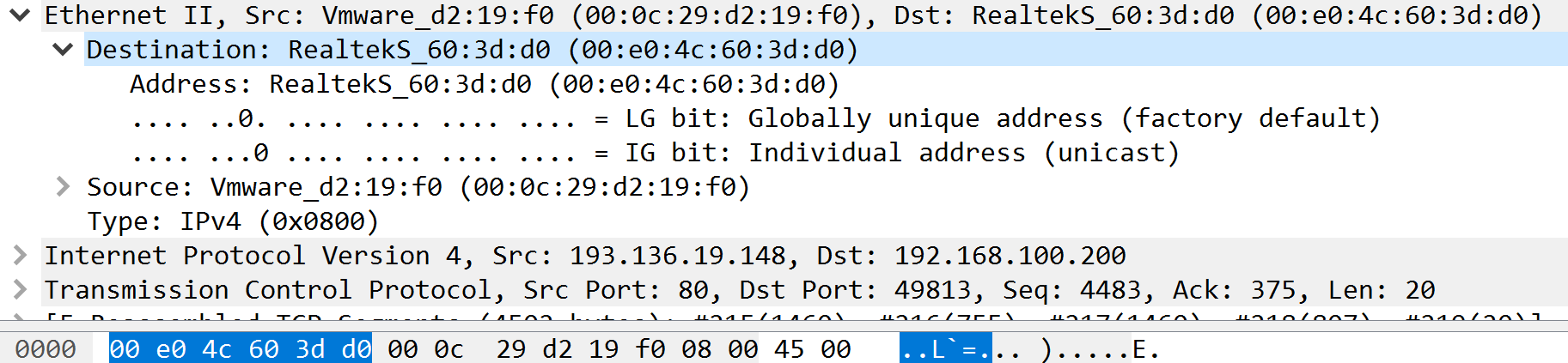


Imagem 6 - Endereço MAC do destino

1. 0x0800. Diz-nos que o protocolo utilizado ao nível da rede é o IPv4.

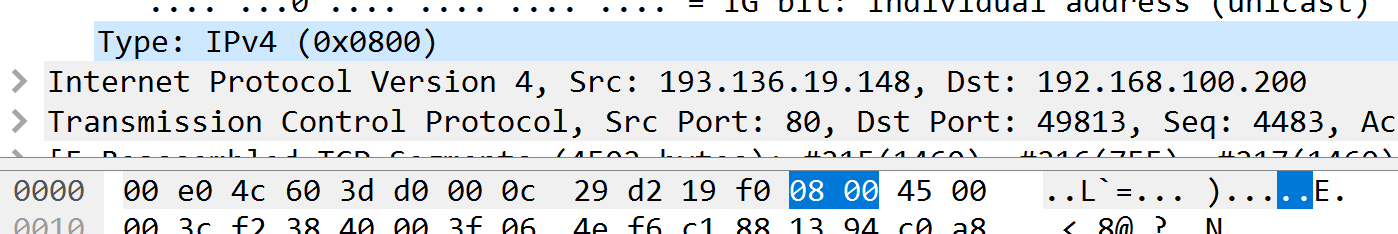


Imagem 7 - Campo Type da trama Ethernet

1. Foi um *text/html* (código da página inicial do site do *Cesium*).

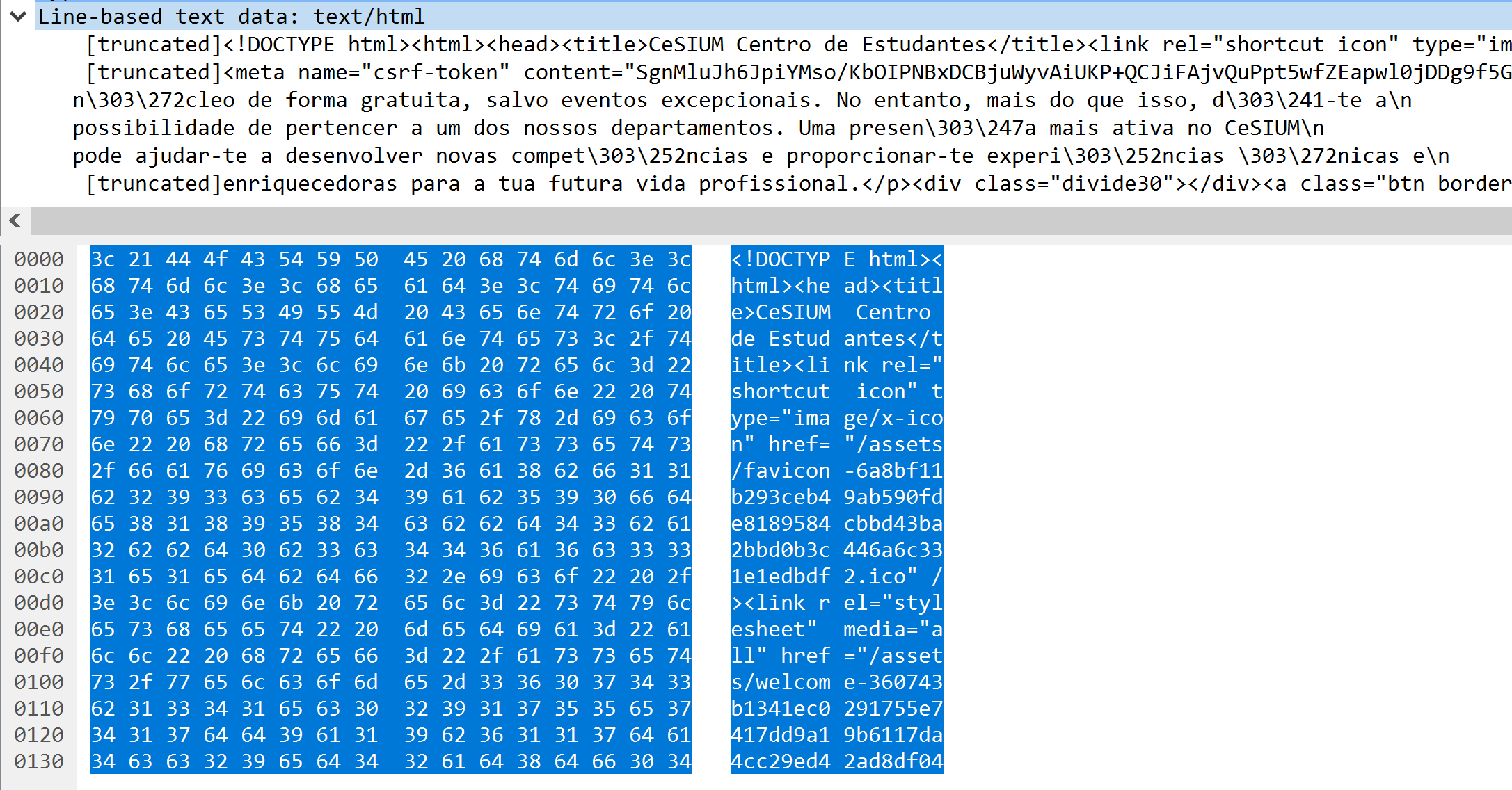


Imagem 8 - Resposta do servidor

**ARP**

1. A primeira coluna faz referência ao endereço IP que é um endereço lógico e corresponde ao nível de rede. A segunda coluna faz referência ao endereço MAC que é um endereço físico e corresponde ao nível da ligação de dados. A terceira coluna corresponde ao tipo ***ACABAMOS DEPOIS***

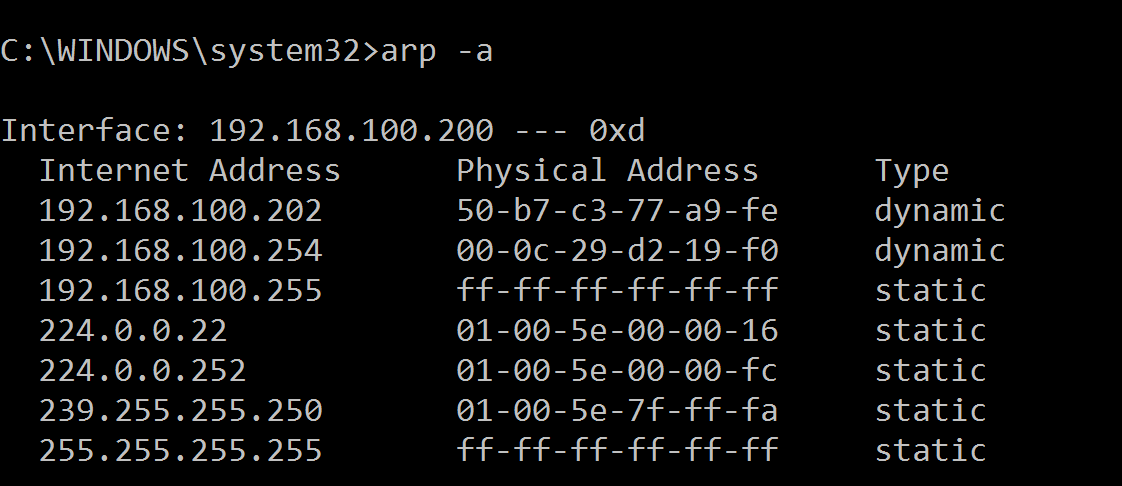


Imagem 9 - Tabela ARP da máquina

1. Origem: 0x00 e0 4c 60 3d d0. Destino: 0xff ff ff ff ff ff. O nosso computador quer aceder ao site miei.di.uminho.pt e conhece o endereço IP do servidor onde o site está alojado através da resolução de nomes providenciada pelo DNS. No entanto, ainda necessita de saber o endereço MAC para efetuar a comunicação com o servidor. Para isso, em primeiro lugar, tenta ver se existe na sua tabela ARP uma correspondência entre o endereço IP conhecido e um endereço MAC. Como tal não aconteceu (porque foi limpa a cache da tabela ARP), o nosso computador teve de efetuar um broadcast (i.e. enviar um ARP request) utilizando como endereço MAC de destino o endereço ff:ff:ff:ff:ff:ff (que denota o broadcast), pedindo às restantes máquinas da rede local que forneçam o endereço MAC associado ao IP. Como o servidor ao qual estamos a tentar aceder não se encontra na rede local ao nosso computador, é o router da rede que se encarrega de fornecer o endereço MAC pedido.

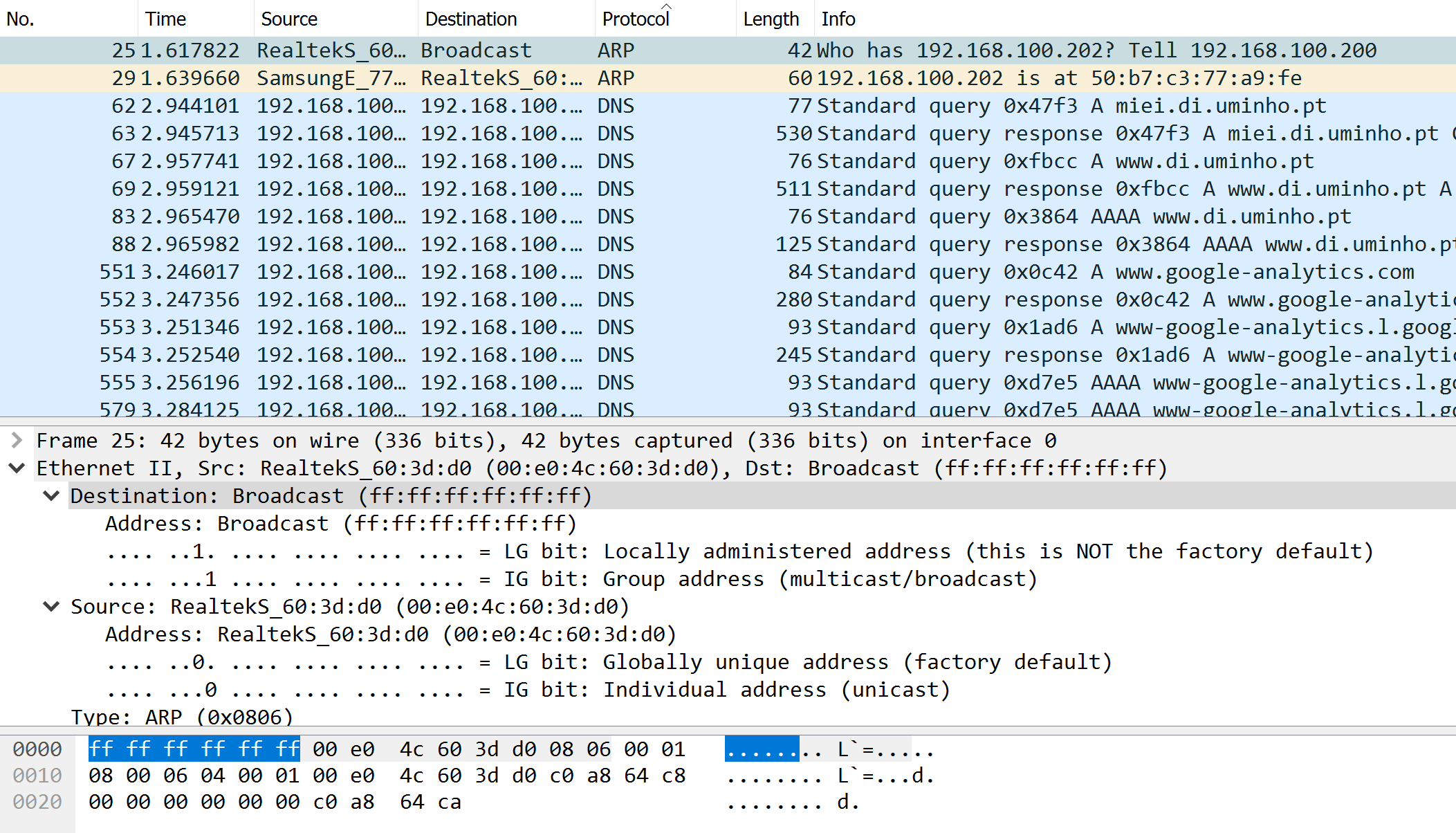


Imagem 10 - Endereços origem e destino da trama Ethernet

1. 0x0806. Indica que a trama Ethernet corresponde ao protocolo ARP.

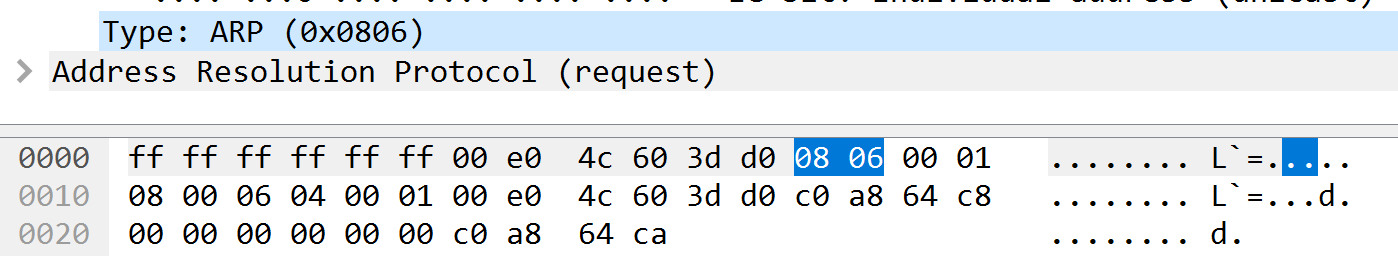


Imagem 11 - Campo Type da trama Ethernet

1. O ARP opcode é “request (1)”. Especifica que o conteúdo que é do tipo relativo ao protocolo ARP é, mais concretamente, um ARP request (pedido para conhecer o endereço MAC a partir de um endereço IP conhecido).

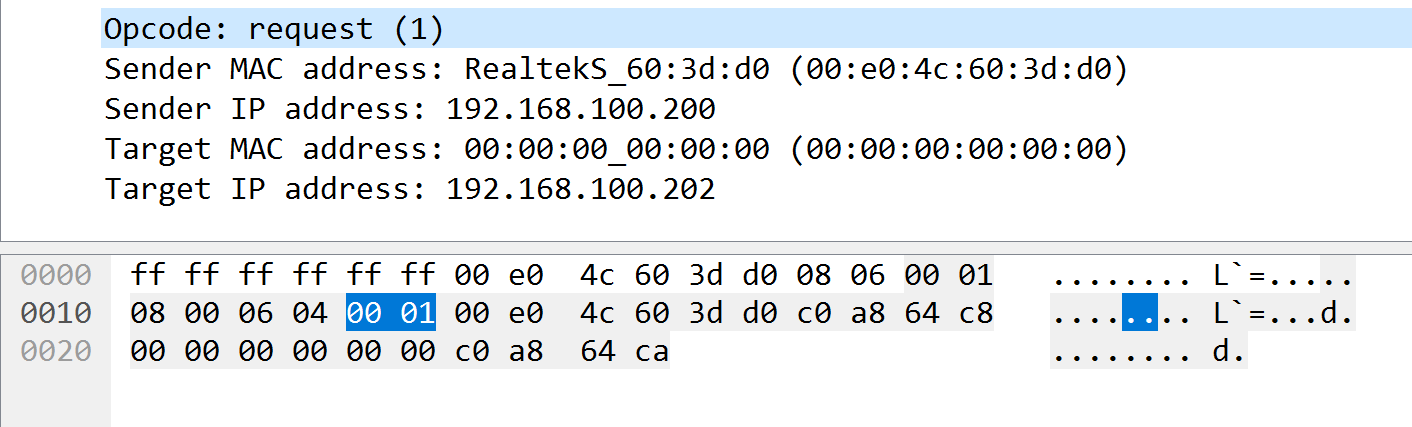


Imagem 12 - Campo ARP opcode

1. Sim, a mensagem ARP contém o endereço IP de origem (192.168.100.200). É feito um pedido para conhecer o endereço MAC a partir de um endereço IP conhecido.

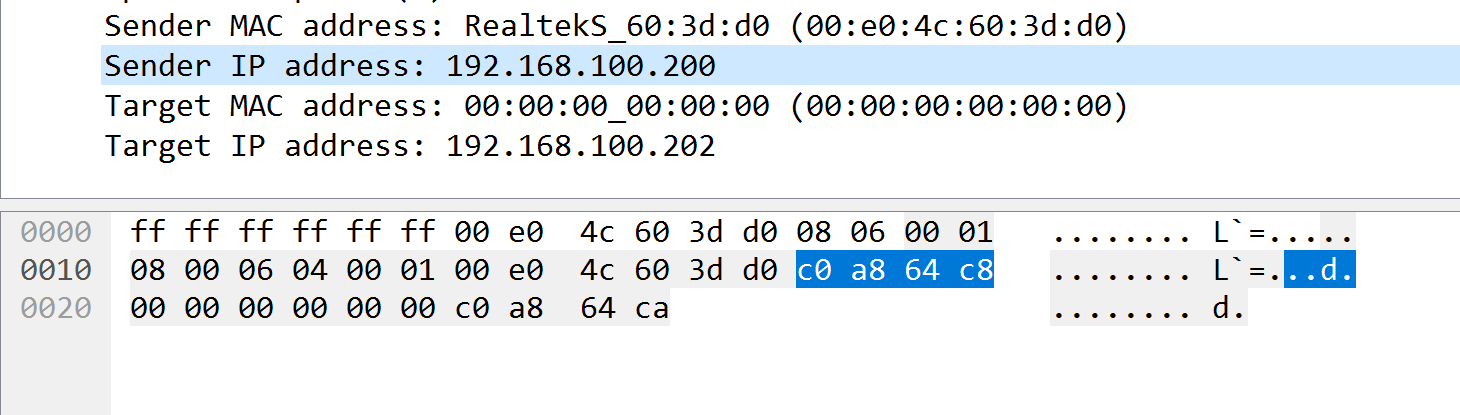


Imagem 13 - Endereço IP de origem

1. (imagem 15)
   1. O valor do ARP opcode é “reply (2)”. Indica que é a resposta ao ARP request, contendo a associação entre o endereço IP que lhe foi enviado e o endereço MAC que lhe era pedido.

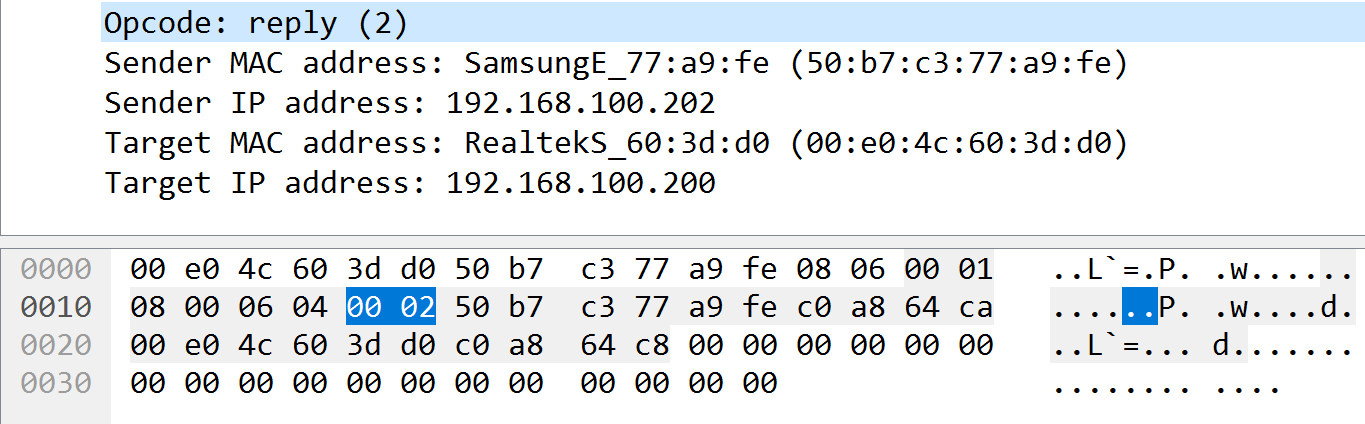


Imagem 14 - Campo ARP opcode

* 1. A resposta (endereço MAC 50:b7:c3:77:a9:fe) encontra-se …

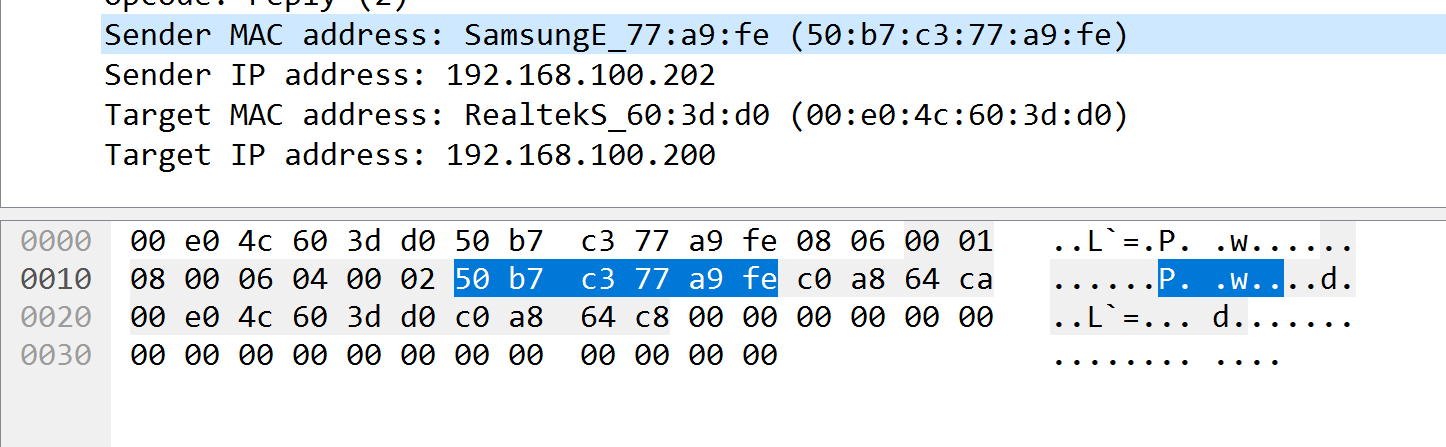


Imagem 15 - Resposta ao pedido ARP

1. Origem: 0x50 b7 c3 77 a9 fe (endereço MAC). Destino: 0x00 e0 4c 60 3d d0 (endereço MAC). Em primeiro lugar, podemos notar que o endereço de destino do ARP reply é o endereço de origem do ARP request e corresponde ao nosso computador. Em segundo lugar, podemos verificar que foi recebido o endereço MAC que era pedido.

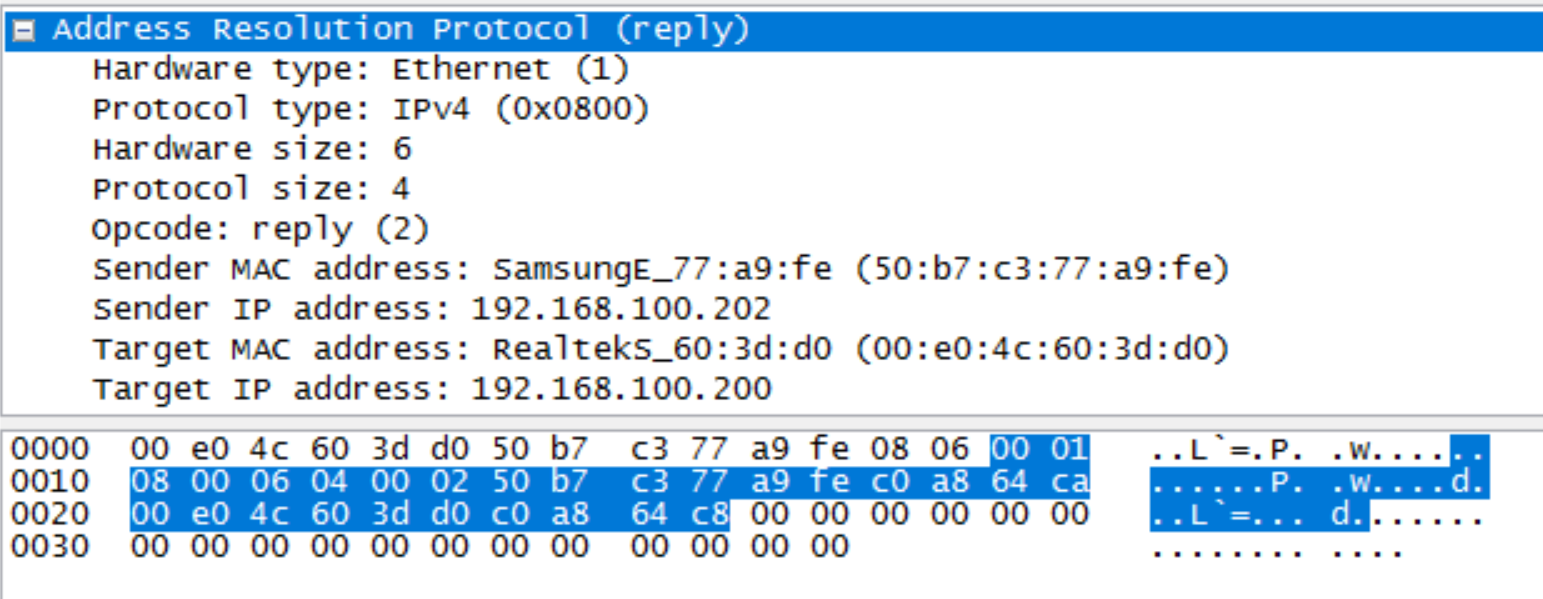
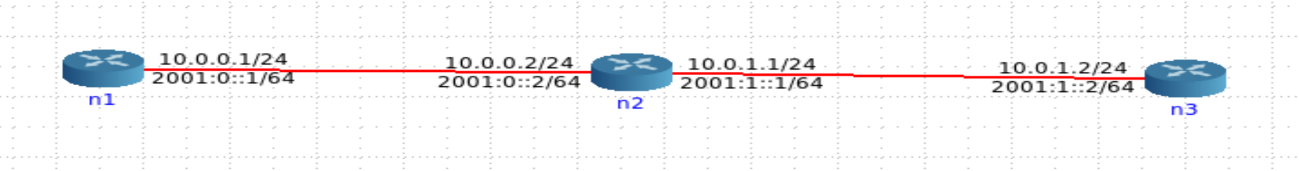


Imagem 16 - Endereços origem e destino do ARP

**ARP numa topologia CORE**



**Topologia com 3 *routers***

1. (inserir imagem 17-system e 17-ifconfig)
2. (inserir imagem 18)
3. Ao fazer um ping de N1 para N2, como já existia uma entrada na tabela ARP de N1 para os endereços de N2, não acontece nada. O mesmo ocorre para N3 pois o tráfego passa por N2 cujos endereços já eram conhecidos por N1.
4. Desaparecem a entrada dos endereços de N2 da tabela ARP de N1 e a entrada dos endereços de N1 da tabela ARP de N2.
5. (inserir imagem 21-system e 21-arp) Na nossa opinião, como o que liga N5 a N6 é um switch que apenas se encarrega de reenviar os dados que recebe numa entrada (a de N5) para a saída correspondente (a de N6), a entrada que deve ser adicionada à tabela ARP de N5 é a entrada correspondente aos endereços de N6. No caso anterior, quando N1 faz ping a N3, tal já não acontece pois o que liga N1 a N2 é um outro router (e não um switch); assim, N1 fica com a entrada correspondente aos endereços de N2 (e não de N3). Numa abordagem mais concreta, se um computador fizer ping a um qualquer servidor da Google, por exemplo, a entrada na tabela ARP que vai ser adicionada ao computador não será a dos endereços (Ethernet e MAC) do servidor, mas sim a dos endereços do primeiro router que liga a rede local do computador à rede local do servidor.

* **PARTE II**

**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.**

Foram enviados dois ARP gratuitos, um aos 9.57s e outro aos 68.67s. Registou- -se, então, um intervalo temporal de 59.1s.

1. **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?**

**++**

No primeiro ARP gratuito, os endereços IP de origem e de destino são iguais (e correspondem ao do nosso computador), sendo o endereço MAC de destino do tipo ff:ff:ff:ff:ff:ff que denota o *broadcast*.

Se alguém responder

**Domínios de colisão**

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