FUNDAÇÃO UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO
CAMPUS JUAZEIRO
CURSO DE ENGENHARIA DA COMPUTAÇÃO

Breno Gabriel de Souza Coelho

Prática Wireshark de Ethernet e ARP

Juazeiro, BA
2022

Breno Gabriel de Souza Coelho

Prática Wireshark de Ethernet e ARP

Relatório requerido pelo professor Fábio Nelson de Sousa Pereira, como parte das exigências de avaliação da disciplina Redes de Computadores I, do curso de Engenharia da Computação, da Universidade do Vale do São Francisco.

Juazeiro, BA
2022

SUMÁRIO

1 INTRODUÇÃO

O protocolo Ethernet é um dos elementos chave do funcionamento da internet moderna, sendo responsável pelo conjunto de regras e formato da grande maioria das transmissões de enlace atuais. O avanço da tecnologia ao longo dos anos exigiu um desempenho cada vez mais dos protocolos de enlace, pois a velocidade das transmissões, aumento dos acessos simultâneos e expansão das redes de internet para regiões cada vez maiores fez com que muitos dos problemas presentes nesse protocolos, especialmente o ethernet, se tornassem mais pronunciados e danosos, Em 2010, o artigo de WINZER, PETER J. já trazia uma discussão a respeito da popularização dos enlaces 100G (com capacidade de transmissão máxima - porém geralmente não alcançada, pelas várias razões discutidas no livro - de 100 GB/s). Nessa discussão ele já apresenta as redes 400G e 1 T como um futuro possível da tecnologia no período até 2020.

As aplicações do protocolo ethernet, no entanto, não se limitam a rede mundial de computadores. Na verdade esse protocolo estabelece o mecanismo de comunicação entre nós de qualquer tipo de rede, podendo ser usado em outros contextos de interesse também. SKEIE, TOR et al (2002) trata das aplicações e limitações desse aos sistemas de controle autônomo em sistemas distribuídos de energia. A utilização de dispositivos inteligentes e controlados por humanos é essencial nessa área, pois a complexidade de operação dos sistemas envolvidos faz com que não seja possível prever exatamente “o que está acontecendo agora ou ocorrerá pouco tempo no futuro”, exigindo que sistemas semiautomáticos tomem decisões de importância em algumas instâncias. Muitas vezes a comunicação entre esses sistemas, bem como a geração de relatórios e dados, é obtida por uma rede que utiliza o protocolo ethernet para as comunicações do enlace. O artigo discute sobre se o estado atual da tecnologia ethernet é capaz de obter resultados satisfatórios em sistemas de tempo real como esses.

Outra limitação da Ethernet que pode ser discutida é seu custo energético. REVIRIEGO, PEDRO et al (2009) esclarece que, à época, muito pouco era tratado a respeito desse assunto, mas que a chegada de novos padrões focados em economia de energia, como o EEE (*Energy-Efficient Ethernet* - Ethernet Eficiente Energeticamente), podem mudar esse cenário. A crítica principal diz respeito ao fato de que os sistemas de entrada e saída operam em voltagem máxima mesmo quando não há fluxo eficaz de quadros/sinal através de nós. Essas novas tecnologias propunham um sistema de redução de custo em potência para situações de ociosidade, que dependiam da intensidade do tráfego de quadros e tempo de chegada deles.

O autor apresenta com maiores detalhes essa tecnologia em seu artigo de 2011 (REVIRIEGO, PEDRO et al., 2011). Informando que em setembro de 2010, o IEEE 802.3az (Energy Efficient Ethernet) havia sido oficialmente aprovado e ratificado. No trabalho ele apresenta uma série de dados experimentais a fim de justificar os ganhos de custo energético comentados antes, mas destaca que a

intensidade de tráfego possui um papel decisivo no espaço de atuação dessa tecnologia.

Mudando de tema, um dos elementos centrais dos protocolos de enlace que operam em morfologias de broadcasting é o mecanismo de acesso ao meio. A transmissão de dois quadros de dados (ou mais) simultaneamente, pelo mesmo meio, induz a ocorrência de “colisões”, fenômeno no qual os sinais se superpõe nas entradas dos dispositivos da rede e o resultado é essencialmente ruído incompreensível aos sistemas. ZHENG, JUN et al (2009) trata dos protocolos de acesso ao meio em sistemas de fibra óptica operando com o protocolo ethernet, apresentando uma visual geral sobre o assunto e discutindo como os EPON (protocolos ethernet para acesso de redes ópticas passivas, em tradução livre) devem utilizar um mecanismo de acesso ao meio de modo a evitar colisões de dados e fornecer uma distribuição de banda adequada entre os dispositivos conectados. Os autores ressaltam os principais problemas envolvidos com esse tipo de meio de comunicação, apresentando um trabalho de descrição geral que almejam ser usado para futuras análises maiores do problema.

2 METODOLOGIA

1. What is the 48-bit Ethernet address of your computer?

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

c) Does the ARP message contain the IP address of the sender?

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

13. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

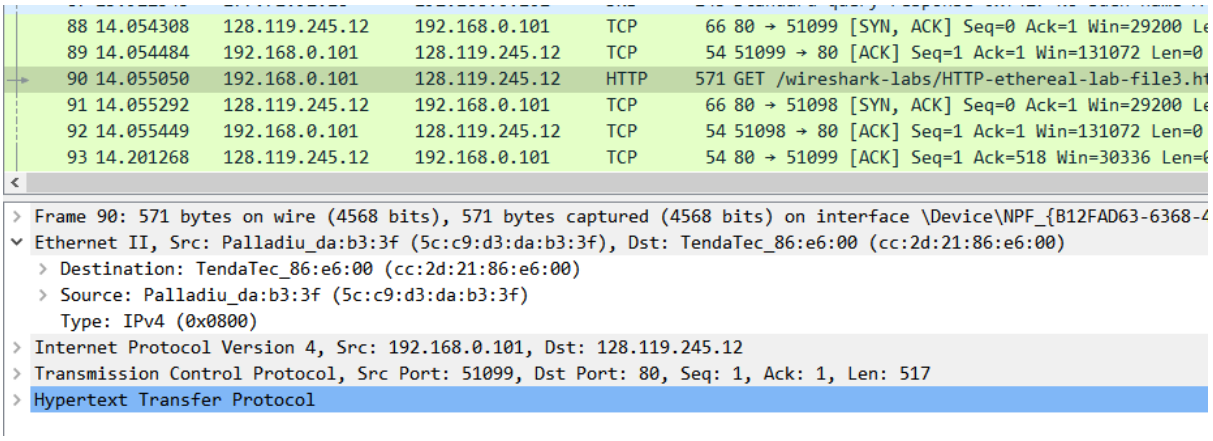
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

15. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

3 DISCUSSÃO



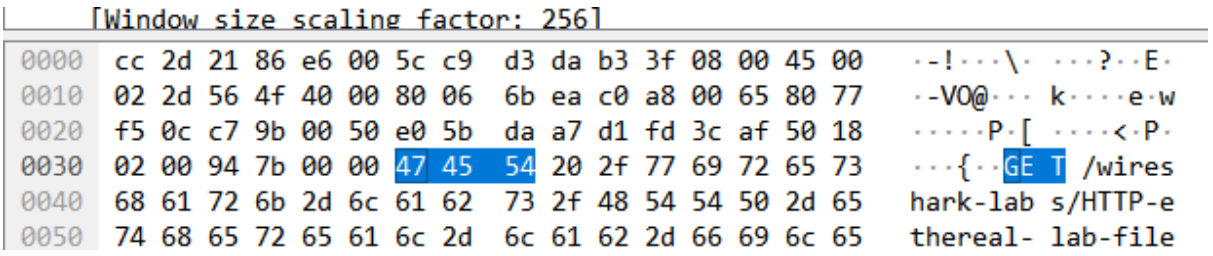
1 - Analisando o campo “source”, podemos ver que o endereço MAC do meu adaptador de rede é 5c:c9:d3:da:b3:3f.

2 - Pela mesma imagem, cc:2d:21:86:e6:00. Na verdade ele é apresentado como “TendaTec_86:e6:00”, “tenda tec” ocorre de ser o nome da empresa da qual comprei meu roteador. Isso mostra que a resposta é “não”, o endereço MAC de destino *não* é o endereço MAC do adaptador presente no servidor que possui o domínio buscado, na verdade é o do meu roteador* (*mais especificamente, do adaptador de rede nele presente). Isso acontece porque esses endereços discriminam nós conectados por um enlace, que no meu caso é o enlace não-físico do Wi-Fi. Essencialmente, esse valor apenas informa que o quadro produzido deve ser enviado para o roteador num primeiro momento.

3 - Ainda na mesma imagem, vemos que o valor do campo de tipo é 0x0800, que se refere a um datagrama IP. (contido no quadro de enlace)

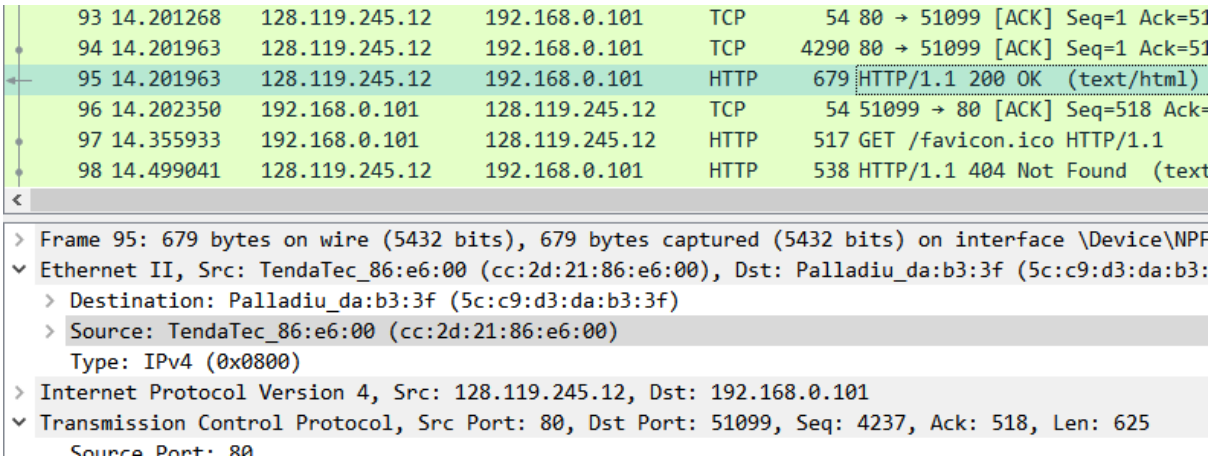
4 - O cabeçalho Ethernet possui 6 + 6 + 2 = 14 bytes. O cabeçalho IP possui um campo que diz seu tamanho, e ele tem 20 bytes nesse caso. O cabeçalho TCP também possui 20 bytes (um campo informa isso), portanto o primeiro dígito do dado HTTP deve ocorrer após 54 bytes do início dos dados do cabeçalho ethernet.

Outra forma de identificar isso é olhando no canto inferior,



A linha 3 começa com o byte de número 16*3 = 48 (esses estão sendo medidos do início do quadro ethernet). O “G”, como destacado, é o 7° dessa linha, ou seja, o 55° desde o começo. Portanto existem 54 bytes entre o ínicio do quadro e ele.

5 - A imagem referente a essa resposta é:



Como era de se esperar, a fonte tem o endereço MAC do adaptador de meu roteador, cc:2d:21:86:e6:00.

6 - Sim, é o endereço MAC do adaptador de rede do meu dispositivo, 5c:c9:d3:da:b3:3f.

7 - Novamente, o quadro carrega um datagrama IP (0x0800)

8 - Seguindo uma lógica análoga, existem 54 bytes do inicio até o “OK”

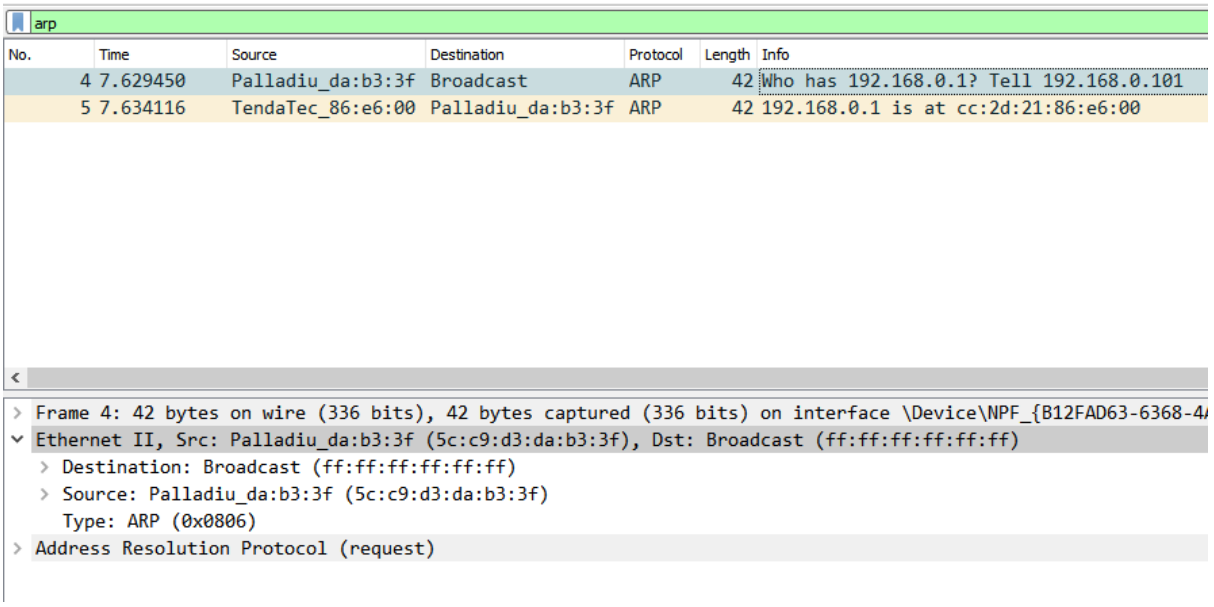
9 - Executando o comando “arp -a”, obtenho as seguintes informações:

```
C:\Users\Anduin110>arp -a

Interface: 192.168.0.101 --- 0xd
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           cc-2d-21-86-e6-00     dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

A primeira coluna é o endereço IP dos diferentes dispositivos para o qual a tabela de conversão do núcleo ARP possui o endereço MAC correspondente, e a segunda tabela é formada exatamente por esses endereços. A coluna de tipos especifica se os IP 's referidos são dinâmicos ou estáticos.

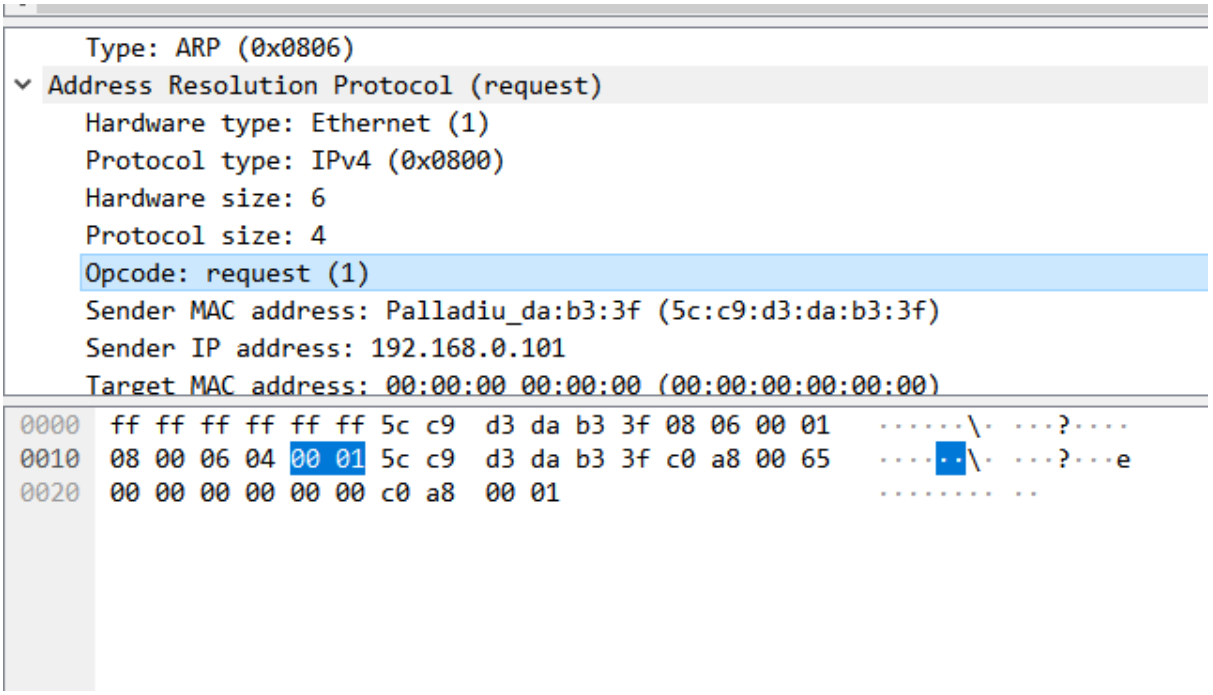
10 - Executando o pedido, esses são os quadros ARP trocados:



A mensagem de pedido é enviada para o endereço de *broadcast* FF:FF:FF:FF:FF:FF, e a fonte é o adaptador de rede do meu roteador, cujo endereço MAC vale 5c:c9:d3:da:b3:3f.

11 - Dessa vez corresponde ao protocolo ARP, com código 0x00000806.

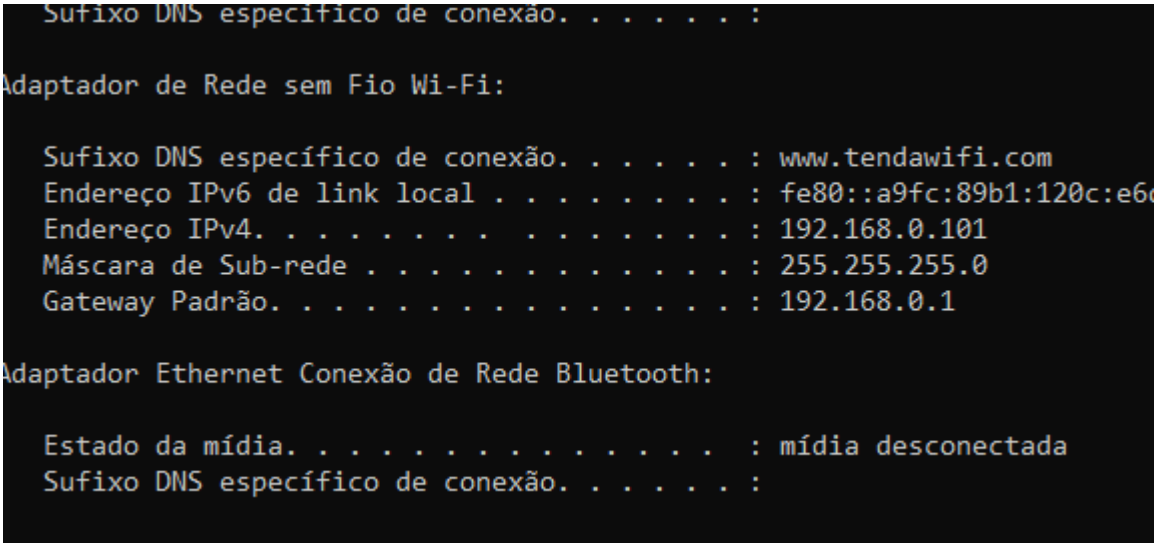
12 - (a) Pela imagem abaixo, 20 bytes depois (exclusive)



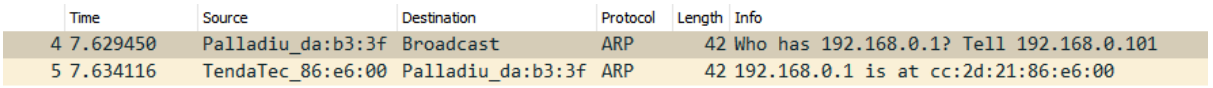
(b) Vale 1, código que representa a operação de “pedido” segundo o wireshark (vide imagem acima)

(c) Sim, isso inclusive pode ser visto na imagem. O dispositivo que enviou o pedido ARP tem IP 192.168.0.101. Usando o comando “ipconfig”, posso ver que esse é o IP que meu computador possui agora. O valor ali presente era apenas uma

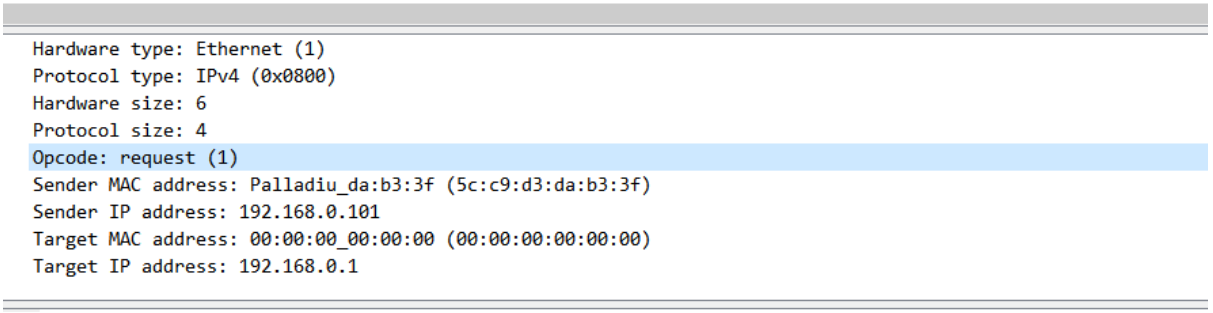
solicitação de um valor de IP para meu dispositivo, que foi aceita já que é esse meu IP de rede agora:



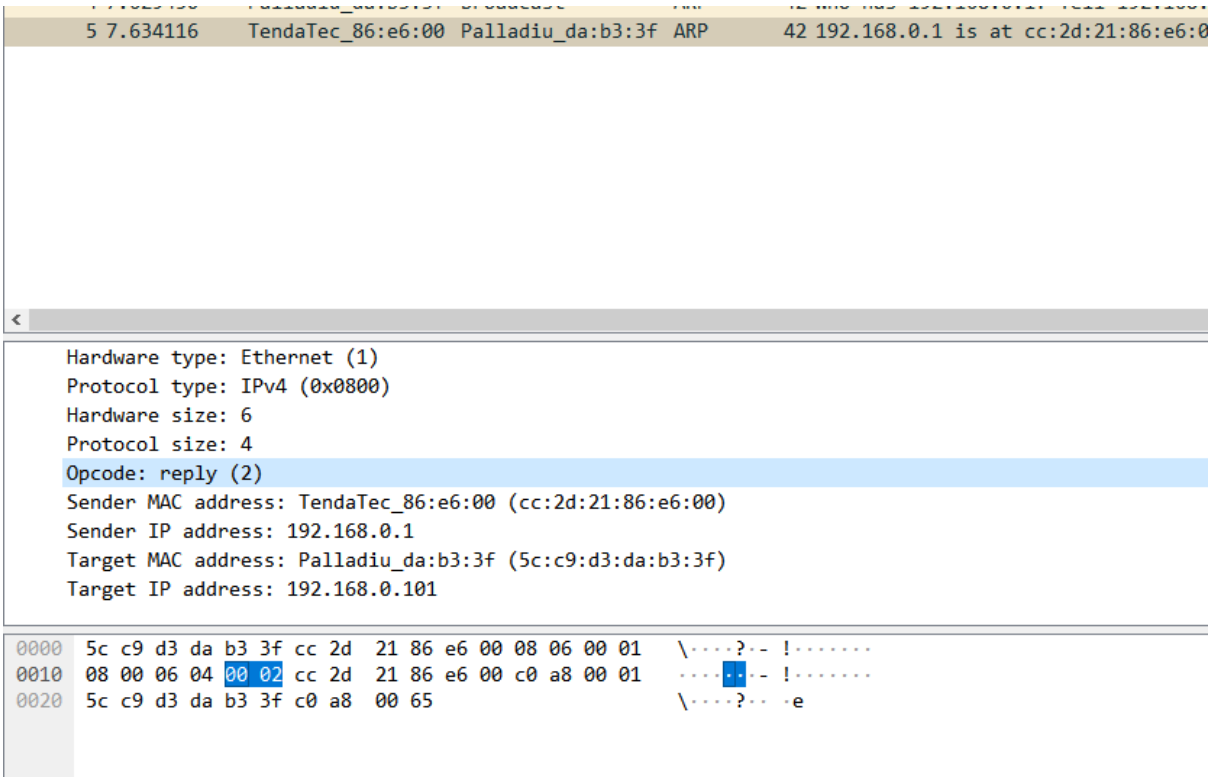
(d) Pode-se dizer que ela é formada por duas partes, primeiro pelo *opcode,* que especifica que esse é um pedido de endereço. Segundo pelo endereço IP alvo (target), que é 192.168.0.1, o IP do meu roteador



	Time	Source	Destination	Protocol	Length	Info
4	7.629450	Palladiu_da:b3:3f	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.101
5	7.634116	TendaTec_86:e6:00	Palladiu_da:b3:3f	ARP	42	192.168.0.1 is at cc:2d:21:86:e6:00



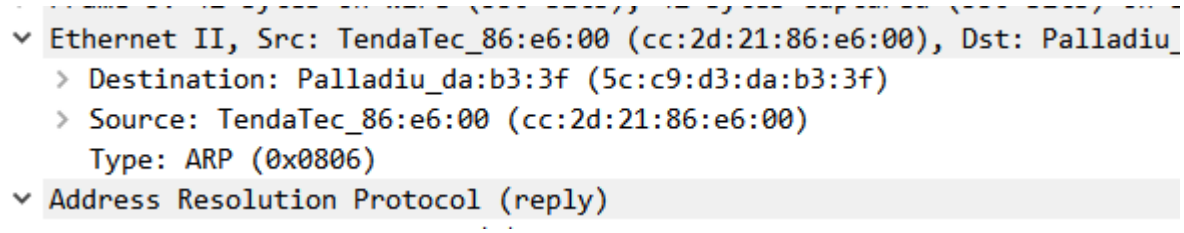
13 - (a) Da mesma maneira, após 20 bytes.



(b) Pela imagem, vemos que vale 2. Esse valor é referente às mensagens de resposta, como o wireshark indica.

(c) Aparece no campo “Sender MAC Adress”, pois a resposta foi enviada pelo dispositivo que recebeu o quadro ARP e reconheceu que era à ele que a pergunta estava adereçada. Daí enviou um outro pacote para a rede em resposta, e portanto o campo com o “endereço MAC do emissor” é exatamente a resposta buscada. Cujo valor é cc:2d:21:86:e6:00.

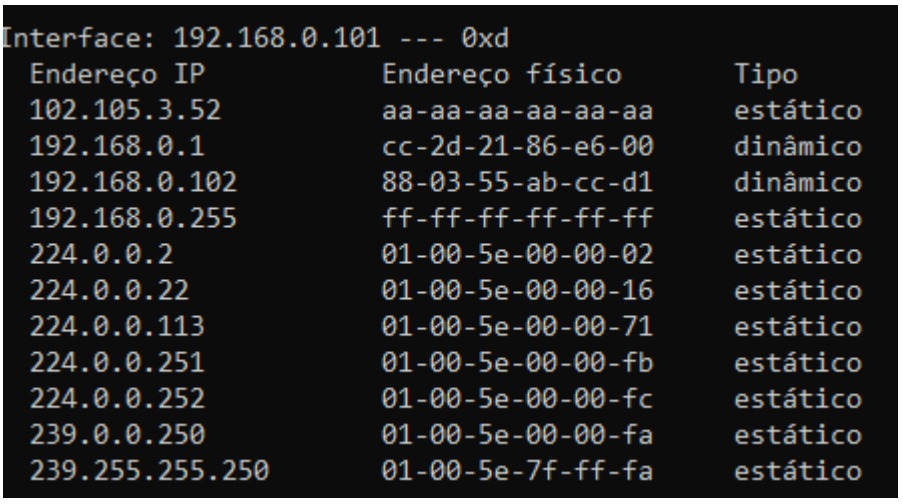
14 - Como pode ser visto abaixo, são cc:2d:21:86:e6:00 (emissor) e 5c:c9:d3:da:b3:3f (destino)



15 - Porque enquanto o pedido ARP é emitido em broadcast (para todos os dispositivos conectados ao enlace), a resposta é endereçada diretamente para aquele que emitiu o pedido. Dessa forma um sistema terceiro não consegue visualizá-la.

(EXTRA 1) Isso significa que meu núcleo analisador ARP irá enquadrar um datagrama destino àquele endereço IP com um valor MAC destino incorreto. Possivelmente esse pacote irá acabar se perdendo na rede (pois o cálculo de rota feito a nível da camada de rede se baseia no endereço IP, e faz o melhor esforço para entregar o datagrama ao IP pedido - no entanto quando esse chegar até o enlace que o levaria para o endereço pretendido, não vai encontrar o endereço MAC adequado e será descartado -), ou então, com menor chance, será entregue ao adaptador de enlace errado, e então o datagrama será percebido como incorreto na camada de rede e será descartado (mesmo que o descarte não ocorra nesse nível, em algum momento vai inevitavelmente acontecer - já que os dados de pacote TCP/UDP ou da camada de aplicação provavelmente serão alienígenas ao sistema destino -)

(EXTRA 2) Uma pesquisa rápida me indicou que ele dura entre 10 a 20 minutos. Vou testar isso empiricamente criando uma entrada falsa e registrando o tempo. Curiosamente já se passaram cerca de 40 minutos e o registro criado (com “aaaa”) continua no mesmo local. Tavez seja algum “bug”, ou então os registros criados diretamente pelo usuário não sejam excluídos da mesma forma que os demais.



```
Interface: 192.168.0.101 --- 0xd
  Endereço IP           Endereço físico       Tipo
  102.105.3.52          aa-aa-aa-aa-aa-aa     estático
  192.168.0.1           cc-2d-21-86-e6-00     dinâmico
  192.168.0.102         88-03-55-ab-cc-d1     dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.113           01-00-5e-00-00-71     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.0.0.250           01-00-5e-00-00-fa     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

4 CONCLUSÃO

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

5 REFERÊNCIA BIBLIOGRÁFICA

WINZER, PETER J. **BEYOND 100G ethernet.** IEEE Communications Magazine, v. 48, n. 7, p. 26-30 (2010)

SKEIE, TOR; JOHANNESSEN, SVEIN; BRUNNER, CHRISTOPH. **Ethernet in substation automation.** IEEE control systems magazine, v. 22, n. 3, p. 43-51, (2002).

REVIRIEGO, PEDRO ET AL. **Performance evaluation of energy efficient ethernet.** IEEE Communications Letters, v. 13, n. 9, p. 697-699 (2009)

REVIRIEGO, PEDRO ET AL. **An initial evaluation of energy efficient Ethernet.** IEEE Communications Letters, v. 15, n. 5, p. 578-580 (2011)

ZHENG, JUN; MOUFTAH, HUSSEIN T. **Media access control for Ethernet passive optical networks: an overview.** IEEE Communications Magazine, v. 43, n. 2, p. 145-150 (2005).