TP3: Camada de Ligação Lógica: Ethernet e Protocolo ARP

Sérgio Jorge, João Freitas, and Alexandre Martins

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a77730,a74814,a77523}@alunos.uminho.pt

1 Introdução

O principal objetivo deste trabalho é o aprofundamento de conhecimentos em redes *Ethernet* e no Protocolo ARP através do estudo e análise de Tramas Ethernet, endereços MAC e tabelas ARP, utilizando ferramentas como *Wireshark* e *CORE*.

2 Captura e análise de Tramas Ethernet

2.1 Questão 1

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

Como se mostra na figura 1, os endereços são os seguintes:

- Origem: `HewlettPdc:ba:3d` com o MAC Address: b0:5a:da:dc:ba:3d
- Destino `Vmware_5e:69:ad` com o MAC Address: 00:0c:29:5e:69:ad

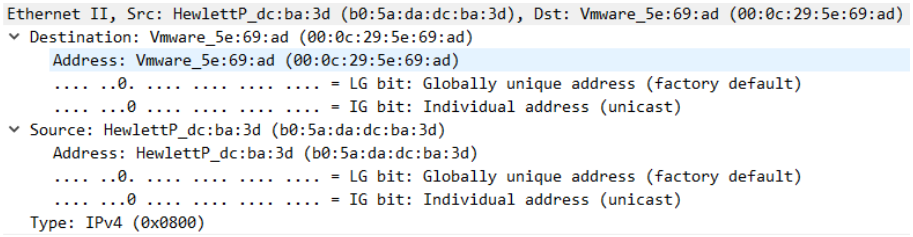

Figura 1: Endereços MAC envolvidos no HTTP GET

2.2 Questão 2

"Identifique a que sistemas se referem. Justifique."

O endereço MAC origem corresponde à máquina que fez o pedido. Neste caso, refere-se ao computador utilizado para realizar este exercício.

O endereço MAC destino corresponde ao comutador da rede local.

2.3 Questão 3

"Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?"

O valor do campo é 0x800 e indica o tipo, IPv4.

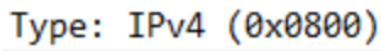

Figura 2: Campo *type*

2.4 Questão 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."

Desde o início da trama até ao caractere G, são utilizados 53 bytes. Uma vez que o total de bytes da trama é 422, então a percentagem de sobrecarga introduzida pela pilha protocolar é de 12%.

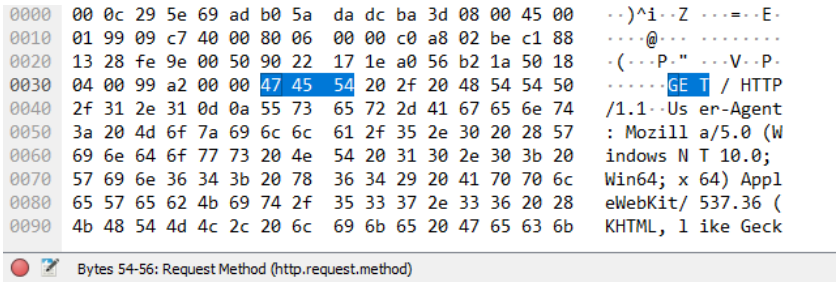

Figura 3: O caractere G aparece após 53 bytes

2.5 Questão 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?"

Nas redes *Ethernet* a utilização de FCS torna-se algo desnecessária por várias razões. Duas delas são a existência de comutadores na rede, que geralmente não enviam pacotes que tenham erros, e também o facto de as redes *Ethernet* se terem tornado muito mais fiáveis e estáveis, o que leva a um número muito reduzido de erros. Por estas e outras razões, não compensa estar a utilizar o campo FCS para cada pacote de informação.

2.6 Questão 6

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

O endereço Ethernet da fonte é `Vmware_5e:69:ad` (00:0c:29:5e:69:ad). Este endereço corresponde ao comutador da rede local já que, a este nível protocolar, os sistemas só comunicam com máquinas adjacentes a partir do ARP.

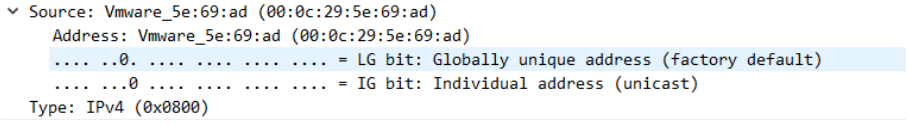

Figura 4: *Endereço Ethernet fonte de quem fez o HTTP Reply*

2.7 Questão 7

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

O endereço MAC do destino é `HewlettP_dc:ba:3d` (b0:5a:da:dc:ba:3d) e corresponde ao computador que foi utilizado para a realização deste exercício. Ou seja, o computador que inicialmente fez o HTTP GET.

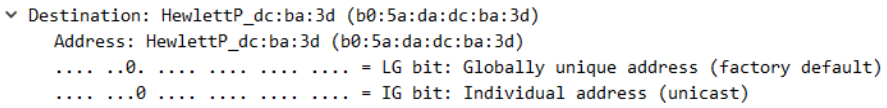

Figura 5: O endereço MAC do destino

2.8 Questão 8

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

A trama recebida transporta o protocolo *Ethernet 2* no qual está encapsulado o protocolo IPv4, que por sua vez transporta o protocolo TCP, onde está o protocolo HTTP.

3 Protocolo ARP

3.1 Questão 9

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

Como podemos ver na Figura 6, a tabela ARP é composta por três colunas.

- Internet Address - que indica o endereço IP de uma máquina.
- Physical Address - que indica o endereço MAC de uma máquina.
- Type - que indica se o tipo da ligação entre IP e MAC é estático ou dinâmico.

Esta tabela permite manter uma relação entre os endereços IP (*Internet Address*) e MAC (*Physical Address*). A coluna *Type* tem duas opções possíveis, estático ou dinâmico. Uma relação estática significa que esta foi definida manualmente e não se altera. Enquanto que, uma dinâmica é definida no momento em que é estabelecida e fica guardada em cache até que deixe de ser utilizada ou atinja o tempo máximo para ser guardada.

```
Interface: 192.168.2.190 --- 0xa
  Internet Address      Physical Address      Type
  192.168.2.1           00-0c-29-5e-69-ad     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.0.0.1 --- 0xf
  Internet Address      Physical Address      Type
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Figura 6: Tabela ARP

3.2 Questão 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?"

Como se verifica na figura 7, os endereços são:

- Origem: `HewlettPdc:ba:3d` com o MAC Address: b0:5a:da:dc:ba:3d
- Destino `Broadcast` com o MAC Address: ff:ff:ff:ff:ff:ff

Neste exercício, o grupo procurou fazer ping a uma máquina de um colega presente na sala de aula. Ou seja, uma vez que, relativamente à máquina destino, só se sabia o endereço IP, então a máquina origem usou o protocolo ARP de forma a descobrir o endereço MAC do destino.

Por isso, é feito o envio de um ARP request para todos os dispositivos na rede local e daí é que surge o *broadcast*. Na figura 8, mostra-se exatamente que o computador usado

para a realização do exercício, pergunta à rede quem é o 192.168.2.178 e, mais tarde, essa máquina responde anunciado o seu MAC Address.

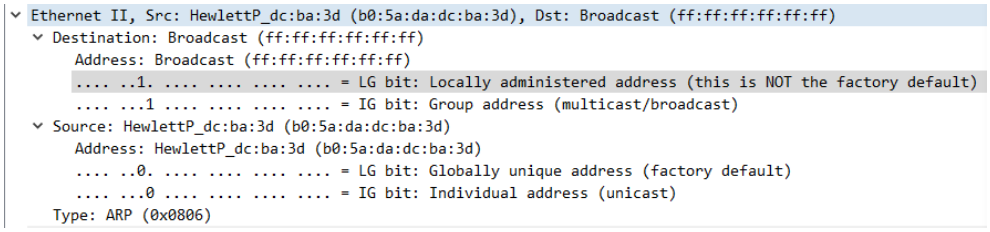

Figura 7: Endereços envolvidos no ARP Request

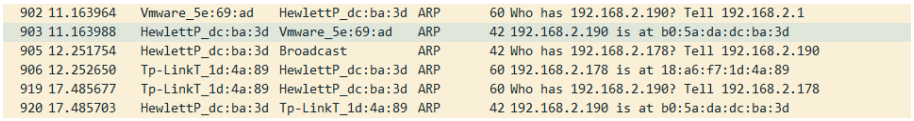

Figura 8: Tramas Ethernet com ARP

3.3 Questão 11

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

O valor do campo é 0x0806 e indica que a trama Ethernet leva ARP encapsulado.

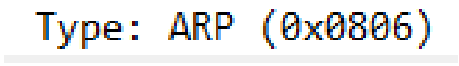

Figura 9: Tipo da trama Ethernet

3.4 Questão 12

"Qual o valor do campo ARP opcode? O que especifica?"

Como se mostra na figura 10, o valor do campo opcode é `request (1)`.

De acordo com a página sugerida, este campo mostra se o ARP é request, que por si só, pode provocar reply a seguir ou se é justamente reply.

Ou seja, prova-se que a trama é um ARP request.

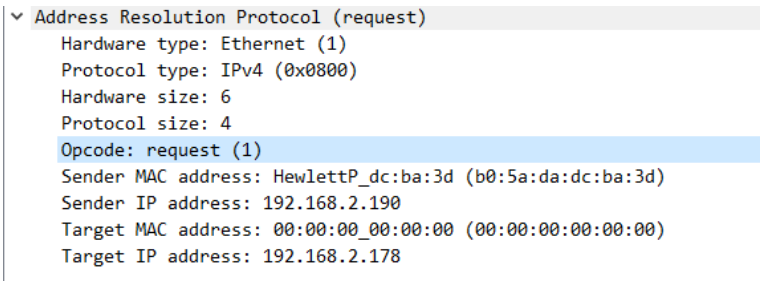

Figura 10: Protocolo ARP

3.5 Questão 13

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

Os endereços contidos na mensagem ARP são os seguintes:

- Sender MAC Address: `HewlettP_dc:ba:3d` (b0:5a:da:dc:ba:3d)
- Target MAC Address: `00:00:00_00:00:00` (00:00:00:00:00:00)

Verifica-se, então, que o endereço MAC de destino está a zeros. Significa, por isso, que o endereço destino é desconhecido e que está à espera de ser preenchido.

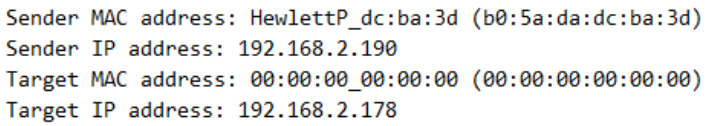

Figura 11: Endereços na mensagem ARP

3.6 Questão 14

"Explicite que tipo de pedido ou pergunta é feita pelo host de origem?"

Como se mostra na figura seguinte, o computador origem quer saber qual é o endereço MAC da máquina destino, que tem interface com IP 192.168.2.178.

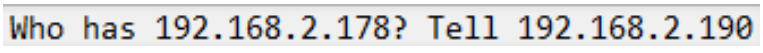

Figura 12: Descrição do ARP Request

3.7 Questão 15

"Localize a mensagem ARP que é a resposta ao pedido ARP efectuado."

15 - A *"Qual o valor do campo ARP opcode? O que especifica?"*

Como se mostra na figura 13, o valor do campo opcode é `reply (2)`.

De acordo com a página sugerida, este campo mostra se o ARP é request, que por si só, pode provocar reply a seguir ou se é justamente reply.

Ou seja, prova-se que a trama é um ARP reply e que é resposta a um ARP request recebido anteriormente.

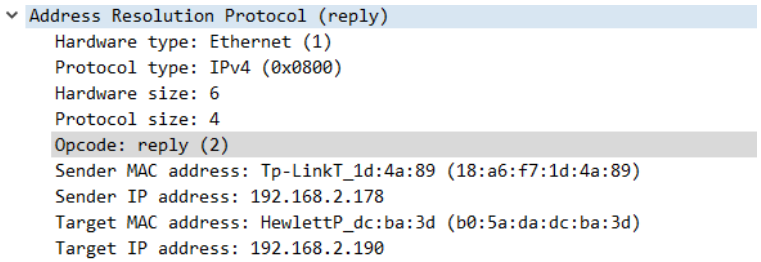

Figura 13: Protocolo ARP

15 - B *"Em que posição da mensagem ARP está a resposta ao pedido ARP?"*

A resposta ao pedido ARP está no campo `Sender MAC Address` onde se especifica que o MAC Address do 192.168.2.178 é o 18:a6:f7:1d:4a:89.

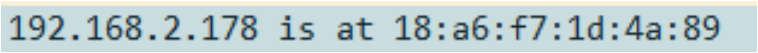

Figura 14: Descrição da resposta

4 ARP Gratuito

4.1 Questão 16

"Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. 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?"

A seguinte imagem, mostra um ARP request gratuito originado pelo sistema.

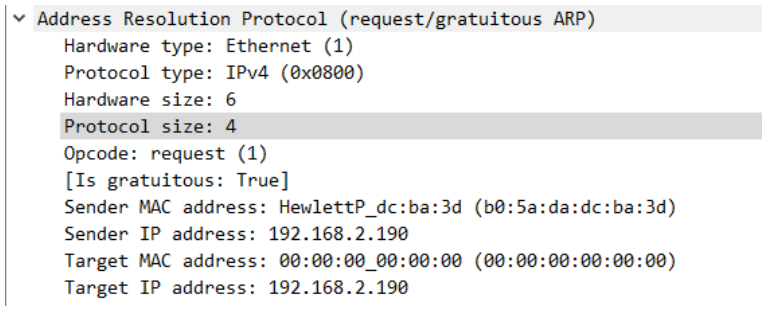

Figura 15: ARP gratuito

Este tipo de pacote difere dos outros, na medida em que, o IP origem é igual ao IP destino. O pacote irá ser enviado para todas as máquinas na rede local (*broadcast*) e estas vão recebê-lo, atualizando as suas tabelas ARP com o novo endereço IP, em relação aquele MAC.

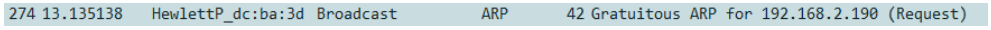

Figura 16: ARP gratuito

5 Domínios de colisão

5.1 Questão 17

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

Pela *Figura 17* podemos observar a principal desvantagem de um *Hub*, que é não saber o destino de uma frame e, por isso, manda para todas as interfaces a que está ligado. Isto e o facto de um *Hub* ser *Half-Duplex*, o que significa que só uma interface é que pode transmitir de cada vez, faz com que a rede possa ficar sobrelotada aumentando os tempos de resposta e possibilitando colisões.

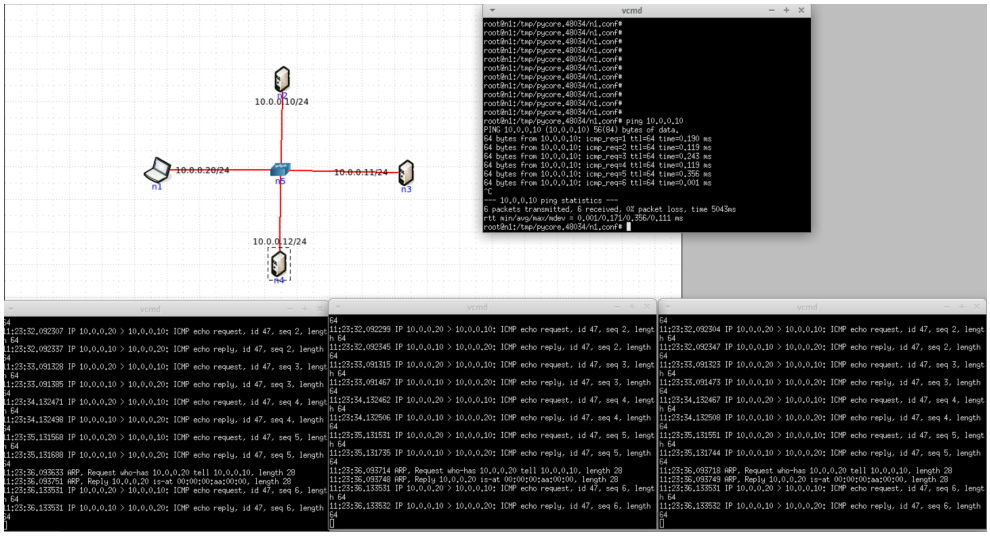

Figura 17: Comando ping do n1 para n2 com Hub

5.2 Questão 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."

Como se pode observar, com o *Switch*, é feito um "ARP Request"a n2, n3 e n4, sendo que só n2 responde com "ARP Reply". O *Switch* fica então a saber a interface do n2 logo o "ICMP request"é só feito para n2.

Os *Switches* têm capacidade de gerir paralelamente os pedidos, logo é impossível haver colisões. Como os *Hubs* não têm essa capacidade, existe sempre a possibilidade de haver colisões.

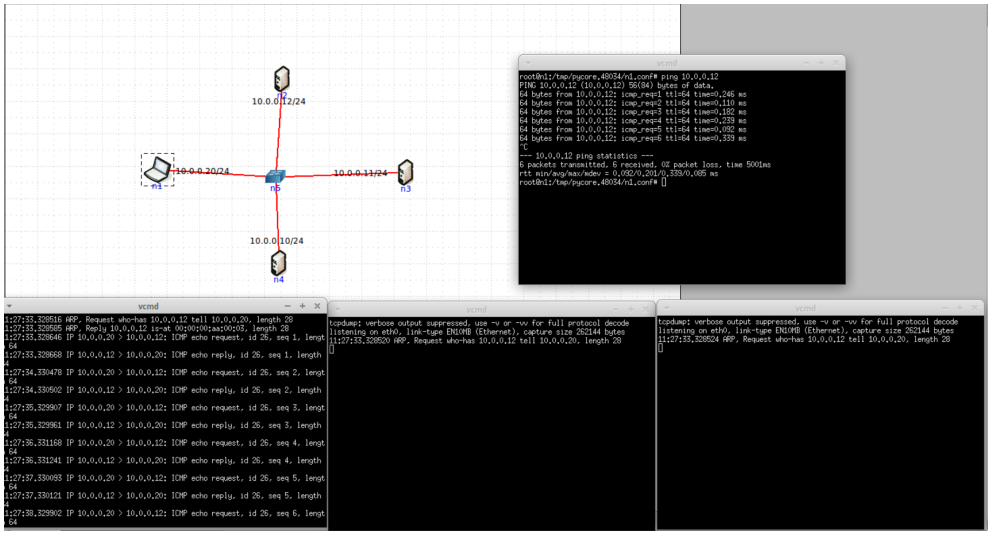

Figura 18: Comando ping do n1 para n2 com Switch

6 Conclusão

Neste trabalho, foram analisadas e compreendidas tramas de rede *Ethernet*, o que permitiu ter uma noção mais prática do que acontece na realidade numa rede deste tipo e consolidar bases para uma melhor análise do protocolo ARP.

Através de alguns teste e exemplos conseguiu-se também entender como é que funcionam os endereços MAC e como são atribuídos.

Surgiu, então, o protocolo ARP, e foram analisadas tabelas ARP assim como algumas tramas ARP. Aqui, ficou-se a saber como é feita a relação entre os endereços IP e MAC, utilizando ARP *requests* e *replies*.

Também se estudou as diferenças entre um *Hub* e *Switch* e suas diferenças. Ou seja, os sistemas podem, de facto, ter impacto na rede, principalmente ao nível das colisões e, esses dispositivos dão então perspetivas diferentes do que acontece (uso de diversos protocolos como o CSMA/CD para evitar colisões).