Camada de Ligação Lógica: Ethernet e Protocolo ARP

Etienne Costa(A76089) Joana Cruz(A76270)
Rafael Alves(A72629)

Resumo

O objectivo deste trabalho é estudar, de uma forma genérica,a camada de ligação lógica. focando o uso da tecnologia Ethernet e o protocolo ARP.

1 Captura e análise de Tramas Ethernet

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

Solution:

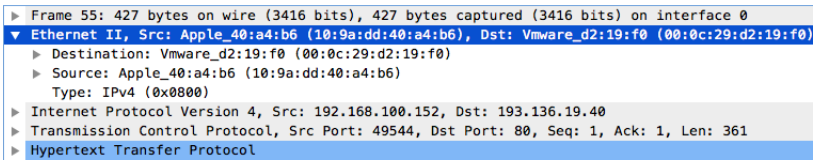

Figura 1: Endereços de origem e destino.

2. Identifique a que sistemas se referem.Justifique.

Solution: Source (10:9a:dd:40:a4:b6) : Corresponde ao endereço físico da nossa máquina nativa. Destination (00:0c:29:d2:19:f0) : Corresponde ao servidor aonde está alocado o site: http://miei.di.uminho.pt.

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

Solution:

$$Type = Ox0800. \tag{1}$$

Significa que está a ser transportado num datagrama Ip, que por sua vez está encapsulado no campo de dados de uma trama ethernet.

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.

Solution: Até ao caractere "G"temos 66 bytes.

$$Overhead = \frac{66}{427} = 15,46. \tag{2}$$

5. Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS(Frame Check Sequence) usado para detecção de erros não está a ser usado. Em sua opinião,porque será?

Solution:

- As redes com vários nós foram substituídas por redes com switches, que geralmente não encaminham pacotes com checksums errados.
- O hardware Ethernet tornou-se muito mais integrado e confiável, tornando-se mais raro precisar de soluções para problemas de baixo nível.
- As codificações da camada física tornaram-se mais complexas, tornando a NIC uma ferramenta menos útil para solucionar problemas nesse nível.

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

Solution: O endereço ethernet da fonte é :

$$Source : 00 : 0c : 29 : d2 : 19 : f0 \tag{3}$$

Corresponde ao servidor aonde está alocado o site: http://miei.di.uminho.pt.

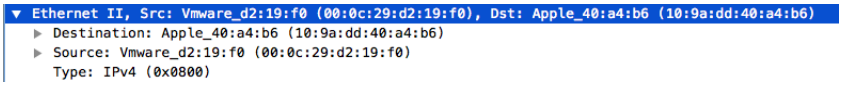

Figura 2: Reply.

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

Solution: O endereço ethernet do destino é :

$$Destination : 10 : 9a : dd : 40 : a4 : b6 \tag{4}$$

Corresponde ao endereço físico da nossa máquina nativa.

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

Solution: Os protocolos contidos na trama recebida são:

- **Ethernet**.
- **Internet Protocol**.
- **Transmission Control Protocol**.
- **Hypertext Transfer Protocol**.

2 Protocolo ARP

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

Solution: Tirando partido do comando arp -a obtemos o seguinte:

- **Primeira Coluna:** Corresponde aos endereços Ip.
- **Segunda Coluna:** Corresponde aos endereços físicos associados ao IP da primeira coluna.
- **Quinta Coluna:** Corresponde a interface que estamos a usar que neste caso é ethernet.

```
└[:)] % arp -all
Neighbor               Linklayer Address Expire(O) Expire(I)    Netif Refs Prbs
server6.sa.di.uminho.pt 0:c:29:98:ac:62   2m40s     2m40s          en7    1
gw.sa.di.uminho.pt      0:c:29:d2:19:f0   2m7s      2m7s           en7    1
192.168.100.255         ff:ff:ff:ff:ff:ff (none)    (none)         en7
broadcasthost           ff:ff:ff:ff:ff:ff (none)    (none)         en7
 ┌[~/Desktop/Universidade/RC/Resoluções/Ethernet e Protocolo ARP/Relatório]-[etiennec
osta@MacBook-Air-de-Etienne]-[0]-[7629]
└[:)] %
```

Figura 3: Arp -all

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?

Solution: O endereço destino é o broadcast visto que inicialmente ele não sabe o endereço MAC associado ao IP 192.168.100.227, sendo assim manda para todos que estão ligados a rede de modo a obter o endereço MAC do 192.168.100.227.

```
247 12.579498    Apple_40:a4:b6    Broadcast    ARP    42 Who has 192.168.100.227? Tell 192.168.100.186
▶ Frame 247: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: Apple_40:a4:b6 (10:9a:dd:40:a4:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Apple_40:a4:b6 (10:9a:dd:40:a4:b6)
    Type: ARP (0x0806)
▶ Address Resolution Protocol (request)
```

Figura 4: Arp Request

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

Solution:

$$Type = Ox0806. \tag{5}$$

Indica que o protocolo utilizado na trama em questão é o ARP.

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

Solution:

$$Opcode = request(1). \tag{6}$$

O opcode indica que tipo de pacote ARP é. Sendo que existem apenas dois valores possíveis para esse opcode, quando o mesmo é igual a 1 indica que é um Request.

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

Solution: Na mensagem ARP encontramos dois tipos de endereços que são:

- **IP:**
  - **Sender IP Adress:**192.168.100.186
  - **Target IP Adress:**192.168.100.227
- **MAC:**
  - **Sender MAC Adress:**10:9a:dd:40:a4:b6
  - **Target MAC Adress:**:00:00:00:00:00:00

Sendo que o ARP faz o mapeamento do endereço IP para o endereço MAC podemos, concluir que o Sender MAC Adress e o Target MAC Adress são resultados desse mapeamento dos respectivos valores do Sender IP Adress e Target IP Adress, embora o Target MAC Adress ainda seja tudo a zeros visto que ainda não se sabe o seu verdadeiro valor.

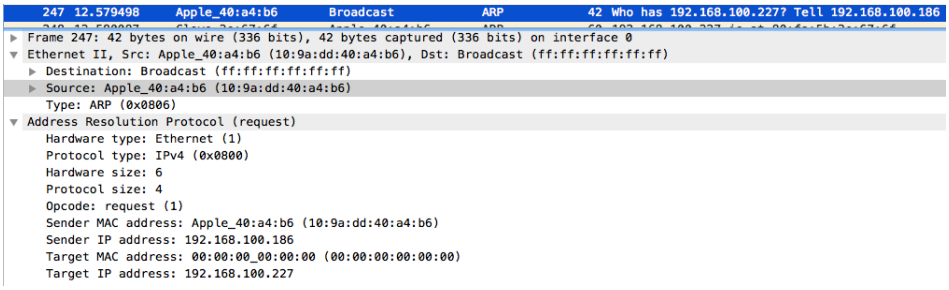

Figura 5: Arp Request

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

Solution: "Who has 192.168.100.227? Tell 192.168.100.186"O host envia uma pergunta ARP para descobrir qual o endereço MAC cujo endereço IP é 192.168.100.227, sendo que essa pergunta na rede é feita em broadcast.

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

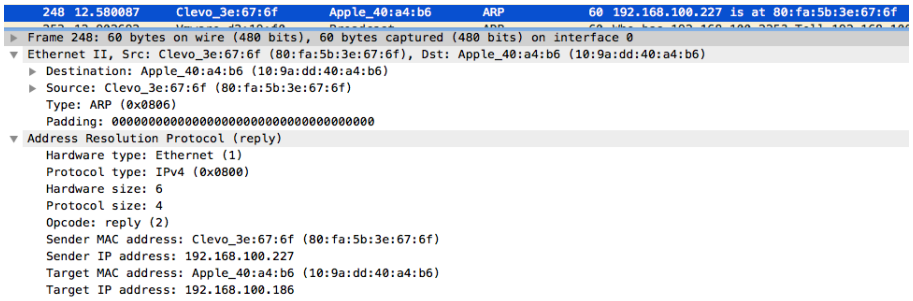

Figura 6: Arp Reply

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

Solution:

$$Opcode = reply(2). \tag{7}$$

O opcode indica que tipo de pacote ARP é. Sendo que existem apenas dois valores possíveis para esse opcode, quando o mesmo é igual a 2 indica que é um Reply.

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

Solution: A resposta ao pedido arp tem início no byte 14 sendo que o Mac Adress do IP em questão se encontra no byte 23.

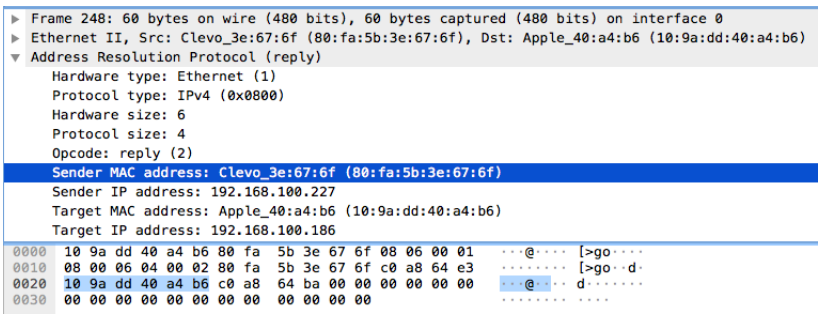

Figura 7: Posição da resposta ao pedido Arp.

3 ARP Gratuito

18. 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?

Solution: A primeira grande diferença que podemos constatar é que existe uma flag [Is gratuitous:True] que indica que se trata de um pedido Arp gratuito e o arp gratuito distingue-se dos outros pois possuí o mesmo IP no campo Sender IP Adress e Target Ip Adress. O resultado esperado face ao pedido Arp gratuito é não haver mais replies porque , caso houvesse , haveria endereços Ip's duplicados. Saber se o Ip está ou não a ser utilizado nesta rede.

```
139 18.686399    Apple_40:a4:b6    Broadcast    ARP    42 Gratuitous ARP for 192.168.100.186 (Request)
▶ Frame 139: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▶ Ethernet II, Src: Apple_40:a4:b6 (10:9a:dd:40:a4:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: Apple_40:a4:b6 (10:9a:dd:40:a4:b6)
    Sender IP address: 192.168.100.186
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.100.186
```

Figura 8: Arp Gratuitous.

sectionDomínios de colisão

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

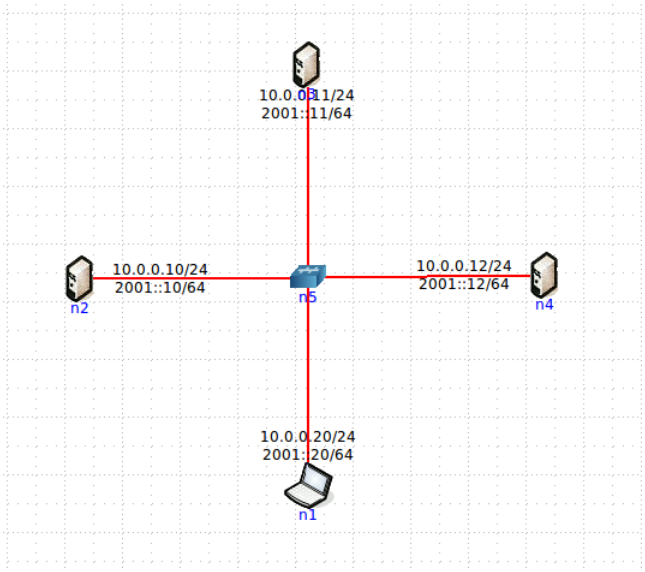

Figura 9: Topologia Core Hub.

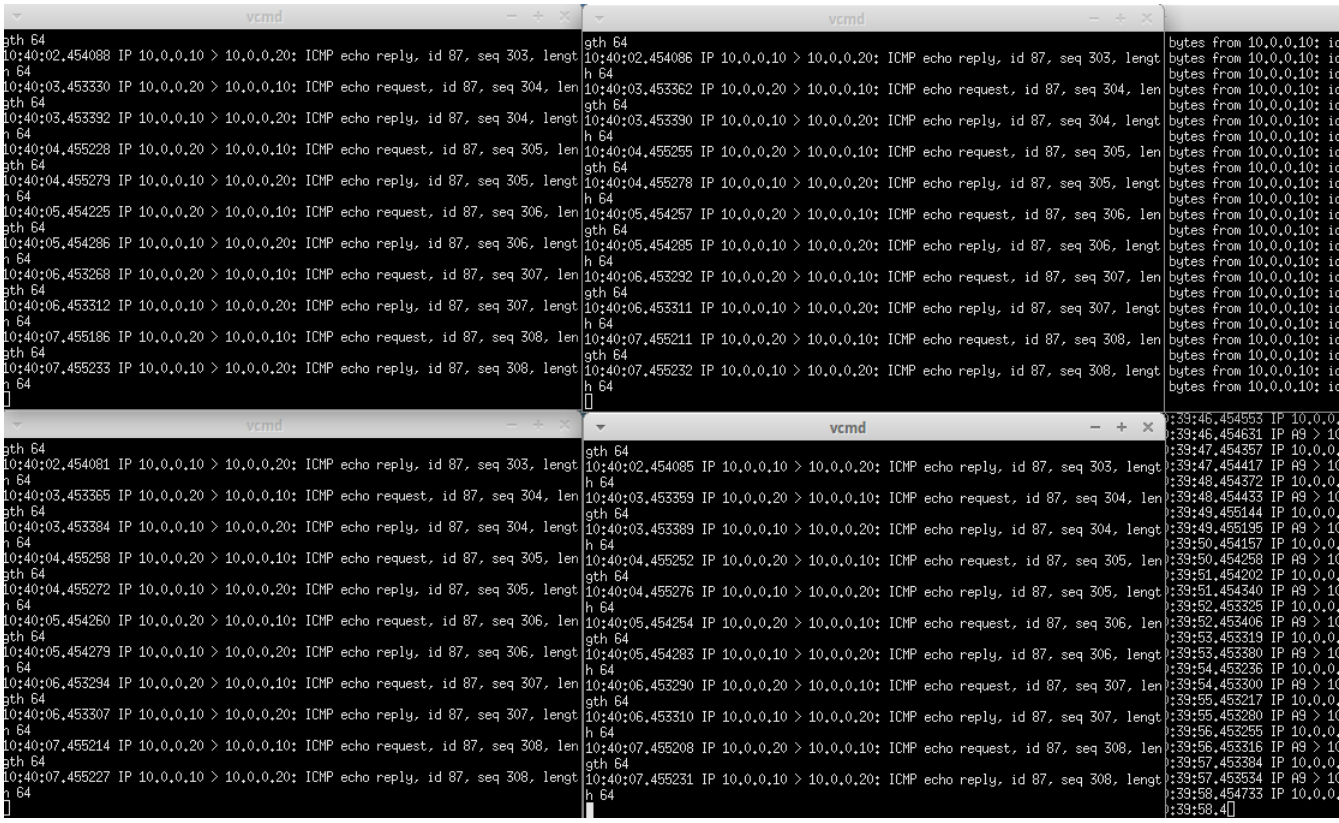

Figura 10: Trafego com um hub de interligação.

Solution: Visto que o equipamento de interligação se trata um hub(repetidor), este irá encaminhar os datagramas para todas as suas interfaces de saída e, portanto, o output do tcpdump será o mesmo em todas as interfaces dos dispositivos ligados ao hub, apesar da troca de mensagens ser entre o host n1 e o host n2.

20. Na topologia de rede substitua o hub por um switch. Repita os procedimentos que realizou na pergunta anterior . Comente os resultados obtidos quantos 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.

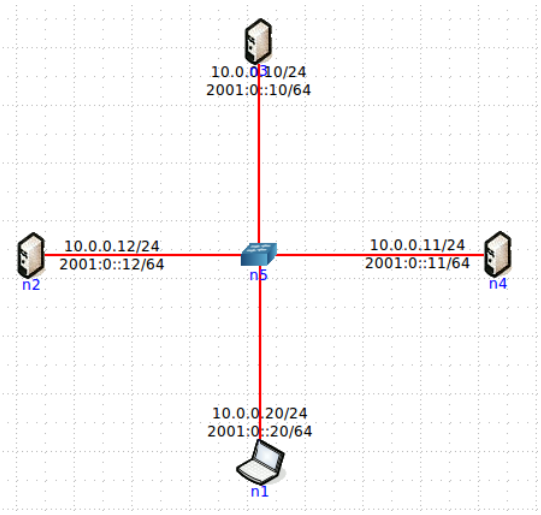

Figura 11: Topologia Core Switch.

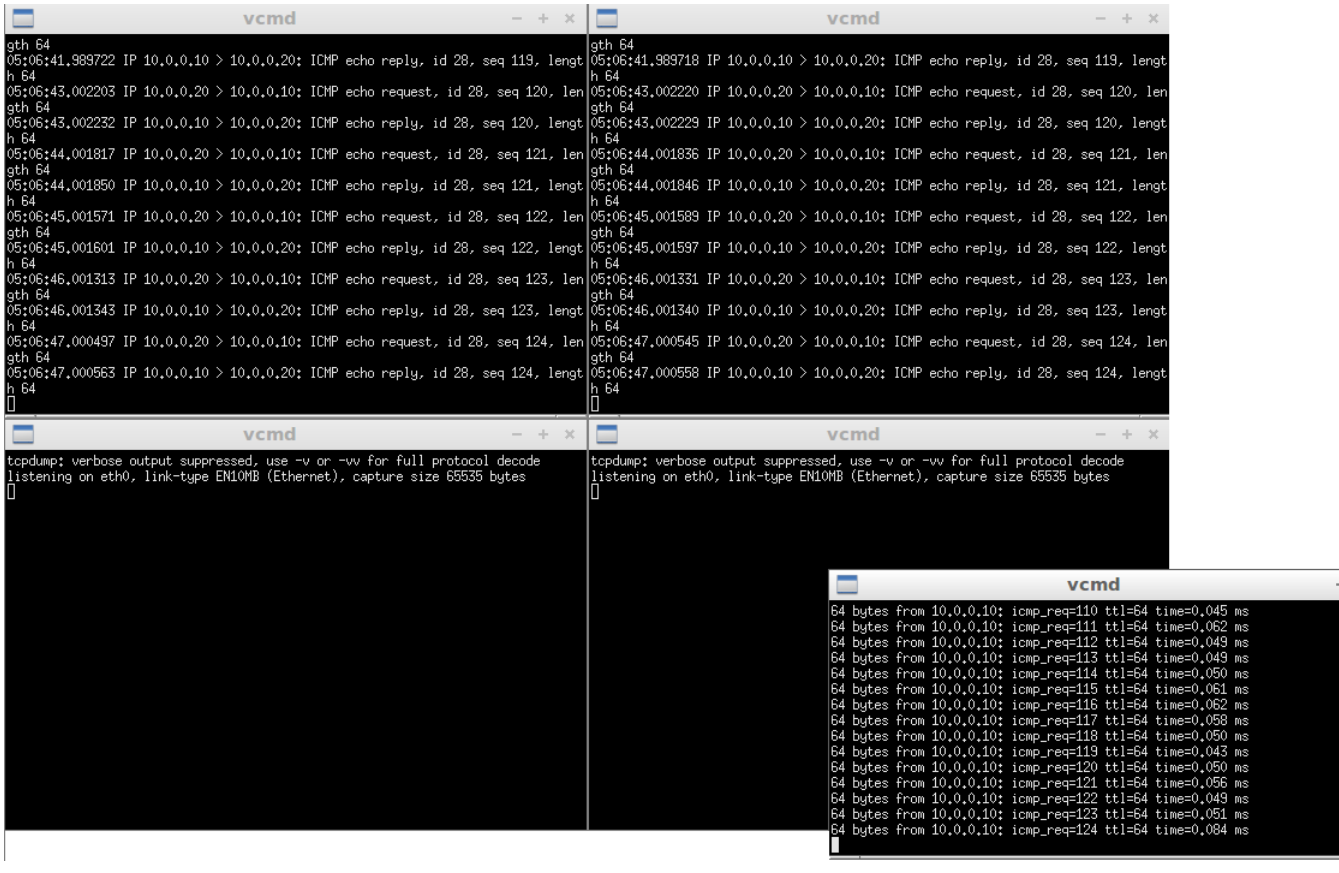

Figura 12: Trafego com um switch de interligação.

Solution: Visto agora o equipamento de interligação ser um switch, o encaminhamento é feito para a interface associada ao MAC adress destino de cada datagrama, como tal o tcpdump apenas apresentará output nos hosts envolvidos na operação ping, respetivamente os hosts n1 e n2.

4 Conclusão

O MAC Address tem um papel central na camada de ligação de dados permitindo identificar, de forma unívoca, uma NIC estando na base de protocolos como Ethernet que definem formas de acesso ao meio. Por outro lado, visto tratar-se de um endereço físico, surgiram protocolos como o ARP(Address Resolution Protocol) que mapeiam estes endereços em endereços IP permitindo assim a entrega de dados entre nós adjacentes (i.e. na mesma rede local). Este protocolo (ARP) pode ainda ser usado para deteção de endereços IP repetidos na mesma rede (local), tendo a desginação de ARP Gratuito quando é usado para este fim. Por fim, a ligação de equipamentos numa rede local implica a ocorrência (ocasional) de colisões derivado do facto de haver um meio partilhado de transmissão de dados entre hosts. A ocorrência de colisões pode ser evitada através do recurso a protocolos de acesso ao meio (nomeadamente CSMA/CD implementado pelo protocolo Ethernet) ou através do uso de aparelhos de ligação denominados switches.