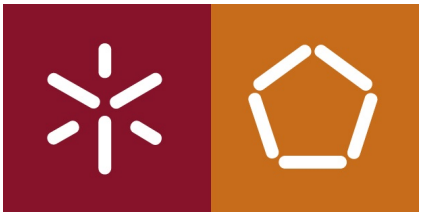

Universidade do Minho
Mestrado Integrado em Engenharia Informática
3ºano - 1º Semestre

Redes de Computadores

TP3: Camada de Ligação Lógica

Grupo 1 - PL1



a83732 – Gonçalo Rodrigues Pinto
a84197 – João Pedro Araújo Parente
a84829 – José Nuno Martins da Costa

28 de Novembro de 2019

Conteúdo

Lista de Figuras

1 Introdução

O objectivo deste trabalho foi estudar, de uma forma genérica, a camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP (Address Resolution Protocol).

O protocolo ARP, descrito na RFC 826, é usado pelos equipamentos em rede para efectuar o mapeamento entre os endereços de rede e os endereços de uma tecnologia de ligação de dados. Desta forma, o protocolo ARP permite determinar, por exemplo, qual o endereço Ethernet que corresponde a um endereço IP particular.

2 Questões e Respostas

2.1 Captura e análise de tramas Ethernet

Utilizando uma ligação com fios, i.e., a ligação à rede Ethernet da sala de aula, que a cache do nosso browser estava vazia e garantindo que estavamos conectados em rede através da interface Ethernet. Ativámos o software Wireshark na nossa máquina, acedemos ao URL http://miei.di.uminho.pt e paramos a captura de tráfego. Após identificar a mensagem HTTP GET enviada pelo nosso computador para o servidor Web, bem como o começo da respectiva mensagem HTTP Response proveniente do servidor. Podemos responder as questões abaixo apresentadas.

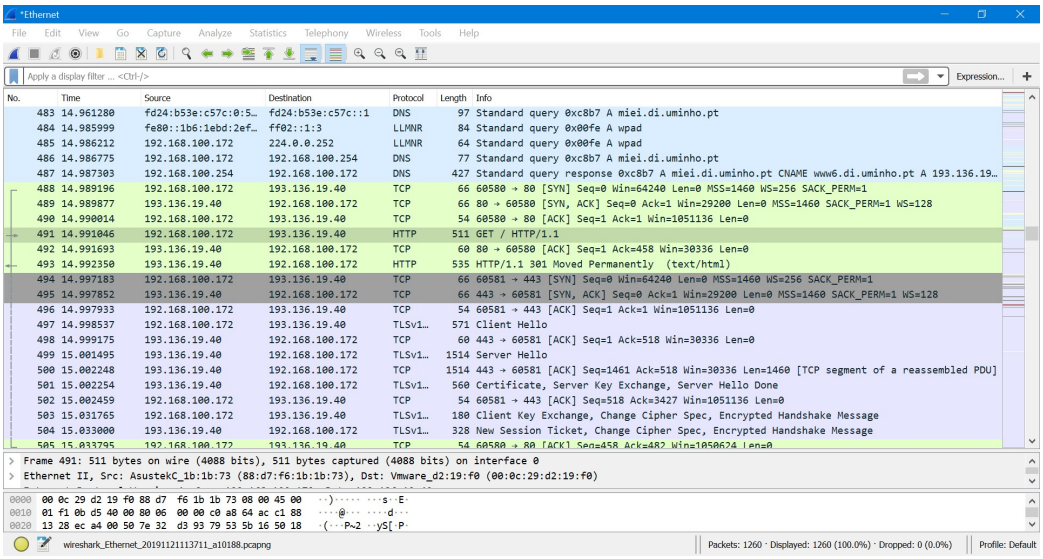

Figura 1: Tráfego capturado.

```
No.     Time           Source                Destination           Protocol Length Info
    491 14.991046      192.168.100.172       193.136.19.40         HTTP     511    GET / HTTP/1.1
Frame 491: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits) on interface 0
Ethernet II, Src: AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Destination: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Source: AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.100.172, Dst: 193.136.19.40
Transmission Control Protocol, Src Port: 60580, Dst Port: 80, Seq: 1, Ack: 1, Len: 457
    Source Port: 60580
    Destination Port: 80
    [Stream index: 10]
    [TCP Segment Len: 457]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 458    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 4106
    [Calculated window size: 1051136]
    [Window size scaling factor: 256]
    Checksum: 0xfbe8 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (457 bytes)
Hypertext Transfer Protocol
```

Figura 2: Mensagem HTTP GET enviada pelo nosso computador para o servidor Web.

```
No.     Time           Source                Destination           Protocol Length Info
    493 14.992350      193.136.19.40         192.168.100.172       HTTP     535    HTTP/1.1 301 Moved Permanently  (text/html)
Frame 493: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73)
    Destination: AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73)
    Source: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.172
Transmission Control Protocol, Src Port: 80, Dst Port: 60580, Seq: 1, Ack: 458, Len: 481
Hypertext Transfer Protocol
    HTTP/1.1 301 Moved Permanently\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        Response Version: HTTP/1.1
        Status Code: 301
        [Status Code Description: Moved Permanently]
        Response Phrase: Moved Permanently
    Date: Thu, 21 Nov 2019 11:37:25 GMT\r\n
    Server: Apache\r\n
    Location: https://miei.di.uminho.pt/\r\n
    Content-Length: 234\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.001304000 seconds]
    [Request in frame: 491]
    [Request URI: http://miei.di.uminho.pt/]
    File Data: 234 bytes
Line-based text data: text/html (7 lines)
```

Figura 3: Mensagem HTTP Response proveniente do servidor.

1. **Anote os endereços MAC de origem e de destino da trama capturada.**
   O endereço MAC de origem da trama capturada foi AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73). E o endereço MAC de destino foi Vmware_d2:19:f0 (00:0c:29:d2:19:f0).

2. **Identifique a que sistemas se referem. Justifique.**
   O endereço MAC de origem refere-se ao nosso computador utilizado para enviar mensagem ao servidor Web. E o endereço MAC de destino refere-se ao servidor Web que envia a mensagem ao nosso computador.

3. **Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?**
   O campo Type da trama Ethernet foi registado com valor hexadecimal de 0x0800 e significa o tipo de dados que a trama encapsula, neste caso o tipo é IPv4.

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 inicio da trama até ao caractere ASCII "G" do método HTTP GET foram utilizados 54 bytes dos 511 bytes totais. A percentagem de sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET foi de aproximadamente 10,57% ((54/511)*100).

5. **Através de visualização directa 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?**
   O campo FCS (Frame Check Sequence) é usado ao nível da camada de ligação sendo que apenas deteta a ocorrência de erros e não os corrige. Como foi feita uma ligação por cabo é raro acontecerem erros daí o campo não estar a ser usado, além de ligações entre nós adjacentes serem menos sujeita a erros.

6. **Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.**
   O endereço Ethernet da fonte da trama Ethernet que contém o primeiro byte da resposta HTTP foi Vmware_d2:19:f0 (00:0c:29:d2:19:f0) e corresponde ao servidor Web.

7. **Qual é o endereço MAC do destino? A que sistema corresponde?**
   O endereço MAC do destino da trama Ethernet que contém o primeiro byte da resposta HTTP foi AsustekC_1b:1b:73 (88:d7:f6:1b:1b:73) e corresponde ao nosso computador.

8. **Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.**
   Os protocolos contidos na trama recebida foram o protocolo de ligação de dados Ethernet, protocolo de rede IP, protocolo de transporte TCP e o protocolo de aplicação HTTP.

2.2 Protocolo ARP

```
nuno@toze:/$ arp
Endereço TipoHW EndereçoHW Opções Máscara Interface
gw.sa.di.uminho.pt       ether   00:0c:29:d2:19:f0   C                     enp2s0
```

Figura 4: Conteúdo da cache ARP do nosso computador.

9. **Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.**
   Após verificar o conteúdo da cache ARP do nosso computador. Neste conteúdo podemos observar uma tabela onde a primeira coluna indica o endereço IP dos dispositivos de rede, a segunda coluna a interface do nosso computador e a terceira coluna o endereço MAC para onde se pretende enviar a mensagem.

Para observar o protocolo ARP em operação, apagamos a cache ARP e asseguramos que a cache do browser está vazia. Após iniciar a captura de tráfego com o software Wireshark, acedemos a a http://miei.di.uminho.pt. Posteriormente efectuamos ping para o computador ativo do grupo ao nosso lado (192.168.100.193). Parámos a captura e localizamos o tráfego ARP desta forma podemos responder as questões abaixo apresentados.

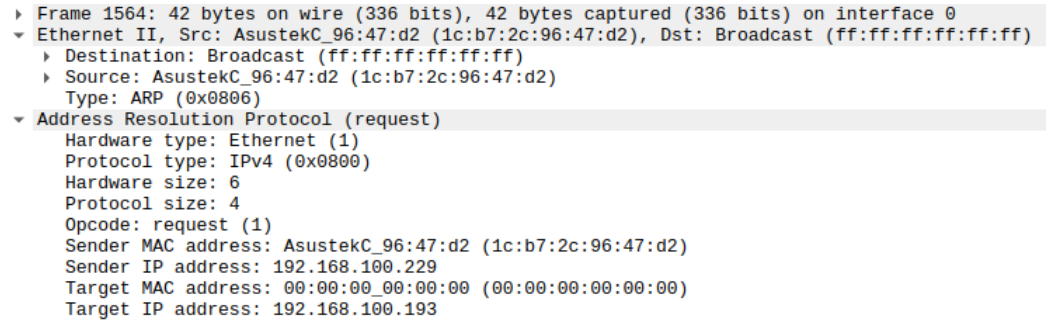

Figura 5: Mensagem com o pedido ARP (ARP Request).

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?**
    O valor do endereço origem e destino na trama Ethernet que contém a mensagem com o pedido ARP é em valor hexadecimal respetivamente, 1c:b7:2c:96:47:d2 e ff:ff:ff:ff:ff:ff. O endereço destino usado possui este valor para fazer um broadcast porque não sabe o endereço MAC correspondente de quem quer comunicar.

11. **Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?**
    O valor hexadecimal registado do campo tipo da trama Ethernet é 0x0806 e indica que a informação dentro da trama Ethernet capturada é ARP.

12. **Qual o valor do campo ARP opcode? O que especifica?**
    O valor do campo opcode registado foi de 1 e identifica que a trama Ethernet foi um pedido.

13. **Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?**
    Na mensagem ARP está contido o endereço MAC e IP do nosso computador que quer efetuar o pedido, o endereço MAC do destino que neste momento é desconhecido e o endereço IP a quem tentamos comunicar. Neste pedido é enviado o nosso endereço MAC para o destino já souber a quem tem que enviar a mensagem.

14. **Explicite que tipo de pedido ou pergunta é feito pelo host de origem?**
    O host de origem pergunta qual é o endereço MAC do endereço IP a quem faz o pedido.

15. **Localizado a mensagem ARP que é a resposta ao pedido ARP efectuado.**

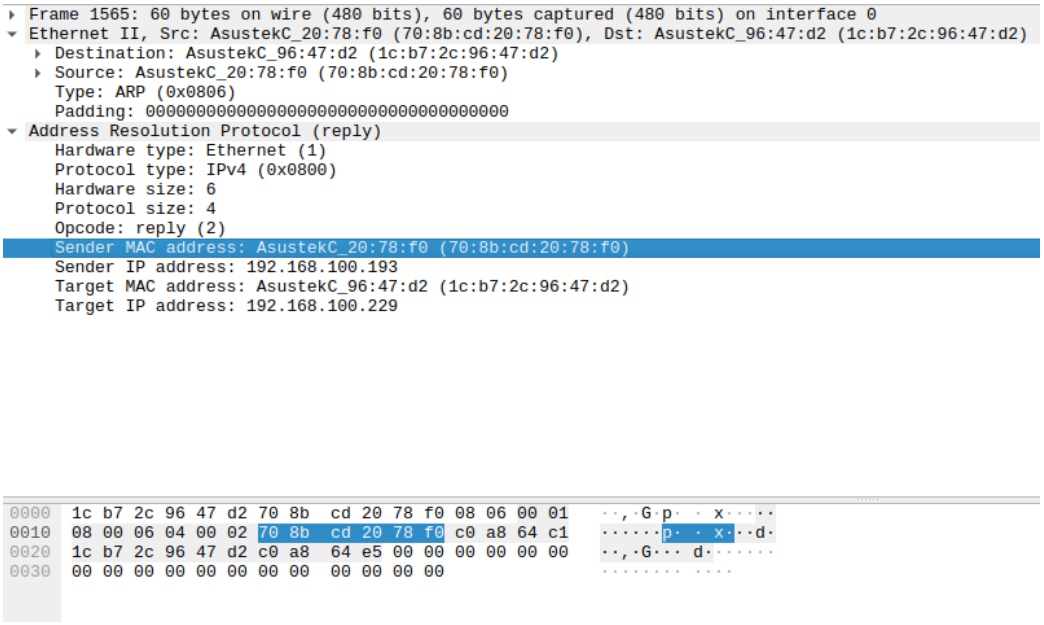

Figura 6: Mensagem com o pedido ARP (ARP Reply).

15.1. **Qual o valor do campo ARP opcode? O que especifica?**
O valor do ARP opcode é 2 e especifica a resposta ao pedido que foi efectuado.

15.2. **Em que posição da mensagem ARP está a resposta ao pedido ARP?**
No pedido ARP a resposta encontra-se no "Sender MAC address"onde indica o endereço MAC.

Após termos arrancado o Wireshark na nossa máquina nativa e iniciado a captura de dados. Desligado e voltado a ligar a ligação à rede local Ethernet. Paramos a captura de tráfego. Utilizando o filtro de visualização ARP para facilitar a identificação dos pacotes respectivos, podemos responder a seguinte 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?**
    O pacote de pedido ARP gratuito originado pelo sistema distingue-se dos restantes pedidos na maneira que a origem e o destino são iguais. Desta forma face ao pedido ARP gratuito enviado não se espera obter nenhuma resposta, o que mostra que não existe conflito entre este endereço MAC.

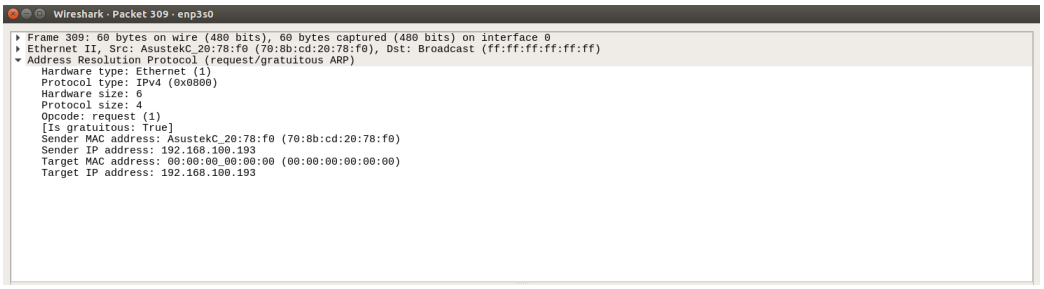

Figura 7: request/gratuitous ARP.

2.3 Domínios de colisão

Após temos contruído uma tpologia no emulador CORE com um host (n1) e dois servidores (n2, n3) interligados através de um hub.

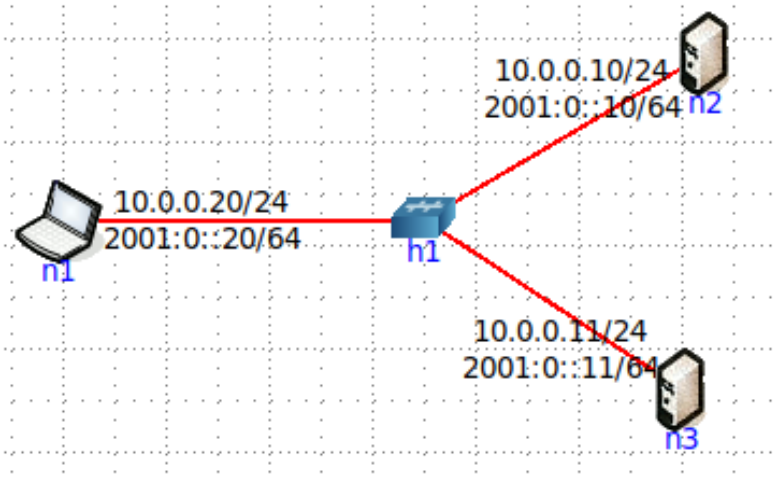

Figura 8: Topologia Core com um Hub.

17. **Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?**
    Existe tráfego de n1 para h1 ,de h1 para n2 e de h1 para n3.

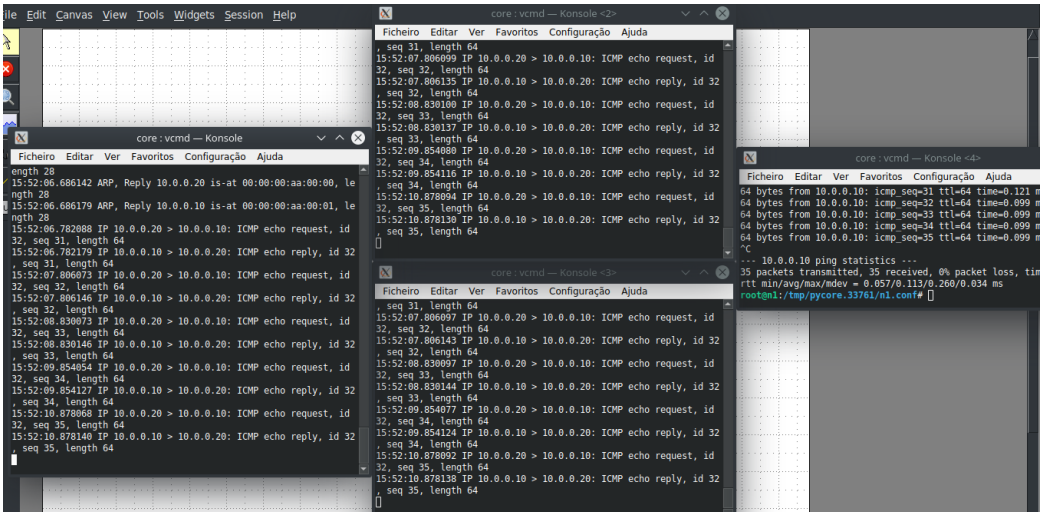

Figura 9: Shell tcpdump representando a máquina n1 à esquerda, n2 em cima e n3 em baixo.

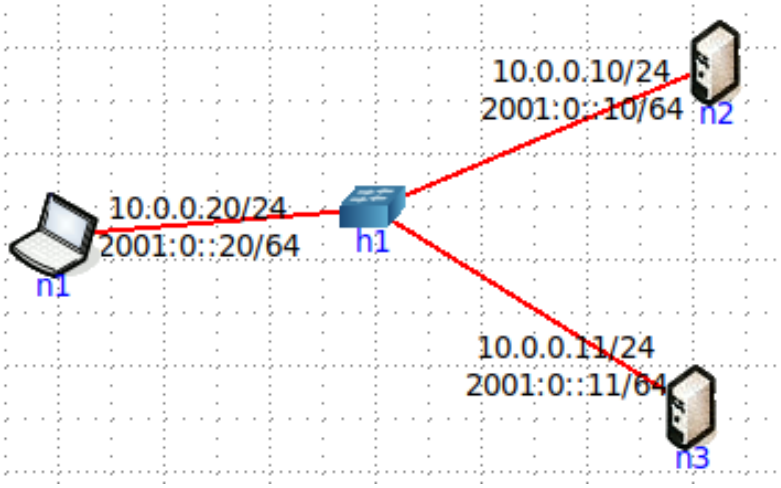

Figura 10: Topologia Core com um Switch.

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.**
Existe tráfego de n1 para h1 e de h1 para n2.

Domínio de colisão hub: n1-h1, h1-n2, h1-n3;
Domínio de colisão switch: n1-h1, h1-n2;

Ou seja, com um switch em vez de um hub temos menos domínio de colisões, o que implica menos colisões.

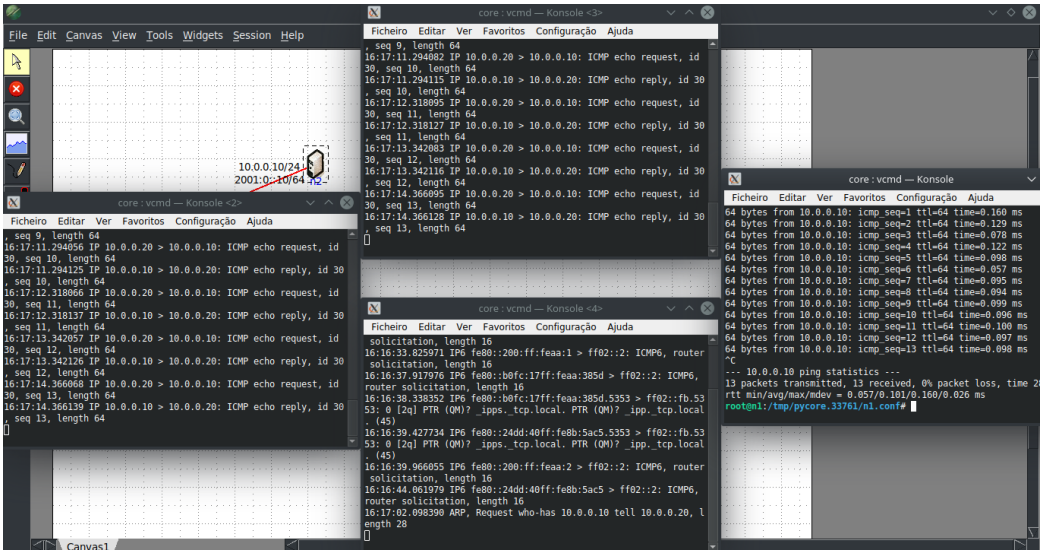

Figura 11: Shell tcpdump representando a máquina n1 à esquerda, n2 em cima e n3 em baixo.

3 Conclusão

O presente relatório descreveu, de forma sucinta, a resolução das questões propostas utilizando os softwares disponibilizados pelos docentes.

Após a realização deste trabalho, ficamos conscientes da camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP.

Consideramos que os principais objectivos foram compridos, no entanto, há que ter em conta que na questão do ARP gratuito não conseguimos registar a trama por questões técnicas contudo utilizámos um ARP gratuito que apareceu.

Sentimos que a realização deste trabalho prático consolidou os nossos conhecimentos do protocolo ARP.