TP3: Nível de Ligação Lógica: Ethernet e Protocolo ARP

Henrique Neto, Sara Marques e Tiago Gomes

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a89618,a89477,a78141}@alunos.uminho.pt

Resumo O objetivo deste trabalho é explorar a camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP (Address Resolution Protocol).
O protocolo ARP é usado pelos equipamentos em rede para efetuar o mapeamento entre os endereços de rede e os endereços de uma tecnologia de ligação de dados, vulgarmente designados por endereços MAC (Medium Access Control). Desta forma, o protocolo ARP permite determinar, por exemplo, qual o endereço Ethernet que corresponde a um endereço IP particular.

1 Captura e análise de Tramas Ethernet

Nesta fase foi nos pedido o estudo do conteúdo de tramas Ethernet proveniente de uma comunicação *HTTP* realizada entre o URL http://elearning.uminho.pt/. Com isto foram capturadas duas mensagens *HTTP*.

Nos exercícios 1 a 5 estudamos a mensagem *HTTP GET* originada nesta comunicação. O pacote capturado tinha as seguintes descrições:

```
No. Time      Source        Destination   Protocol Length Info
121 3.646841  172.26.27.39  193.137.9.150 HTTP     678    GET / HTTP/1.1

Frame 121: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface en0, id 0
Ethernet II, Src: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Source: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.27.39, Dst: 193.137.9.150
Transmission Control Protocol, Src Port: 54563, Dst Port: 80, Seq: 1, Ack: 1, Len: 612
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
            [GET / HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /
        Request Version: HTTP/1.1
    Host: elearning.uminho.pt\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://elearning.uminho.pt/]
    [HTTP request 1/1]
    [Response in frame: 125]
```

1. **Anote os endereços MAC de origem e de destino da trama capturada.**
   - *MAC* origem: `ac:bc:32:d2:3a:1d`
   - *MAC* destino: `00:d0:03:ff:94:00`
2. **Identifique a que sistemas se referem. Justifique.**
   - O *MAC* origem refere-se à interface da nossa máquina nativa e o *MAC* destino refere-se à interface do próximo nó da rede, que neste caso corresponderá ao router que nos dá acesso à rede da *eduroam*.
3. **Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?**

- O valor hexadecimal é `0x0800` que indica que a trama *ethernet* está a encapsular um pacote *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.**
   - Como o caractere "G"encontra-se no índice 66 (ou seja no byte 67), podemos concluir que foram usados 66 bytes nos *headers*. Assim, tendo em conta que a mensagem tem 678 bytes de tamanho, o overhead será de $\frac{66}{678} \approx 0,097$, ou seja, o overhead é de $9,7\%$
5. **Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)).**
   - Não foram detetatas tramas com erros a partir do *FCS*.

Nos exercicios 6 a 7 estudamos a mensagem *HTTP* dada como resposta à mensagem referida anteriormente. O pacote capturado tinha as seguintes descrições:

```
No. Time       Source          Destination   Protocol Length Info
125 3.650520 193.137.9.150 172.26.27.39 HTTP      198    HTTP/1.1 301

Frame 125: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface en0, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
    Destination: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
    Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.27.39
Transmission Control Protocol, Src Port: 80, Dst Port: 54563, Seq: 1, Ack: 613,
Hypertext Transfer Protocol
    HTTP/1.1 301 \r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 301 \r\n]
            [HTTP/1.1 301 \r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 301
        [Status Code Description: Moved Permanently]
    Location: https://elearning.uminho.pt/\r\n
    Content-Length: 0\r\n
    [Content length: 0]
    Date: Wed, 02 Dec 2020 10:05:11 GMT\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003679000 seconds]
    [Request in frame: 121]
    [Request URI: http://elearning.uminho.pt/]
```

6. **Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.**
   - O endereço da fonte é `00:d0:03:ff:94:00`, que corresponde ao último nó de rede que a mensagem precisa de percorrer antes de chegar à nossa máquina. Neste caso, provavelmente corresponderá ao *router* que nos permite o acesso à internet.
7. **Qual é o endereço MAC do destino? A que sistema corresponde?**
   - O endereço destino é `ac:bc:32:d2:3a:1d`, que corresponde à nossa máquina nativa.
8. **Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.**
   - Na trama recebida, podemos identificar os protocolos IP, TCP e HTTP.

2 Protocolo ARP

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

```
? (172.26.27.39)     at ac:bc:32:d2:3a:1d on en0 ifscope permanent [ethernet]
? (172.26.254.254)   at 00:d0:03:ff:94:00 on en0 ifscope           [ethernet]
? (224.0.0.251)      at 01:00:5e:00:00:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 01:00:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

- A primeira coluna indica o nome do *Host* referido. Neste caso como os nomes são desconhecidos, estão representados pelo caractere ? . Na segunda coluna aparece o endereço *IP* destino, seguido pelo seu *MAC Adress* na terceira coluna e pela interface que permite o acesso na quarta coluna. A quinta coluna indica, pelo parâmetro *ifscope*, que cada *IP* corresponde de facto à interface especificada. A sexta coluna indica o estado da linha na tabela, sendo as linhas identificadas como *permanent*, linhas sem tempo de vida. Por fim, a última coluna indica o tipo de tecnologia que está a ser usada em cada parâmetro.

Nos exercícios 10 a 13 estudamos a seguinte mensagem de *ARP request* :

```
No. Time      Source          Destination Protocol Length Info
23  1.585482  Apple_d2:3a:1d Broadcast   ARP      42     Who has 172.26.254.254? Tell 172.26.27.39

Frame 23: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
    Sender IP address: 172.26.27.39
    Target MAC address: 00:00:00:00:00:00
```

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 endereço origem, que possui o valor `ac:bc:32:d2:3a:1d`, corresponde à nossa máquina nativa. O endereço destino possui o valor `ff:ff:ff:ff:ff:ff`. Isto significa que esta mensagem irá ser distribuída a todos os endereços da rede Ethernet. Através disto, a mensagem *ARP Request* transmite um endereço *IP* a todos os elementos na sua rede local, de maneira a que a interface correspondente responda de volta com o seu *MAC adress*.

11. **Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?**
    - O campo tipo possui o valor `0x0806` que indica que este encapsula um pacote de *Address Resolution Protocol* (ARP).
12. **Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?**
    - O parâmetro de *opcode* da mensagem ARP tem o valor 1 que identifica um *request*. Estão presentes os endereços *MAC* e *IP* da interface de origem, que eventualmente serão usados para responder ao pedido. Adicionalmente está contido o endereço *IP* para o qual se planeia achar o endereço *MAC* destino, que apresenta um valor nulo nesta trama (`00:00:00:00:00:00`). Desta forma, concluímos que, tal como esperado, ao efetuar um pedido ARP a interface origem está a comunicar a sua identificação e o endereço *IP* para o qual pretende comunicar.
13. **Explicite que tipo de pedido ou pergunta é feita pelo host de origem?**
    - O *host* de origem, ou seja a nossa maquina nativa faz o pedido "Who has `172.26.254.254`? Tell `172.26.27.39`"ao *Broadcast*, ou seja, envia uma mensagem a todas as interfaces de redes locais a perguntar quem possui o endereço *MAC* correspondente ao endereço que pretende comunicar (neste caso é o endereço `172.26.254.254`). Isto ocorre normalmente por esta estar a tentar

enviar uma mensagem a um endereço *IP* que não possui correspondência na sua respetiva tabela ARP. Posteriormente ao receberam a mensagem, as interfaces da rede irão processar este pedido. Se forem identificadas pelo *IP* destino especificado, estas enviam uma mensagem com a resposta, ou seja, com o seu endereço *MAC*. Por outro lado, se a interface receber o pedido e o seu *IP* não corresponder ao IP pedido, esta simplesmente descarta o pacote.

14. **Localize a mensagem ARP que é a resposta ao pedido ARP efetuado**

```
No. Time      Source            Destination       Protocol Length Info
24  1.588994  ComdaEnt_ff:94:00 Apple_d2:3a:1d    ARP      60     172.26.254.254 is at 00:d0:03:ff:94:00

    Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0
    Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
    Address Resolution Protocol (reply)
        Hardware type: Ethernet (1)
        Protocol type: IPv4 (0x0800)
        Hardware size: 6
        Protocol size: 4
        Opcode: reply (2)
        Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
        Sender IP address: 172.26.254.254
        Target MAC address: Apple_d2:3a:1d (ac:bc:32:d2:3a:1d)
        Target IP address: 172.26.27.39
```

a) **Qual o valor do campo ARP opcode? O que especifica?**
   - O campo ARP *opcode* possui o valor 2 e identifica a mensagem como um *reply*.

b) **Em que posição da mensagem ARP está a resposta ao pedido ARP?**
   - A resposta ao *ARP request* é o endereço *MAC* origem contido nesta mensagem *ARP reply*. Neste caso corresponde ao endereço `00:d0:03:ff:94:00`.

2.1 ARP Gratuito

15. **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?**

```
No. Time      Source            Destination Protocol Length Info
103 3.032163  IntelCor_95:14:8d Broadcast   ARP      42     ARP Announcement for 172.26.20.50

Frame 103: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
          \Device\NPF_{051F8744-B812-4FFB-A8C0-388FCC79C18D}, id 0
Ethernet II, Src: IntelCor_95:14:8d (d8:f2:ca:95:14:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: IntelCor_95:14:8d (d8:f2:ca:95:14:8d)
    Sender IP address: 172.26.20.50
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.20.50
```

- Após uma série de mensagens ARP a confirmar que o endereço *MAC* da nossa máquina nativa é único na rede local, a mensagem anterior foi enviada. Esta mensagem trata-se de uma mensagem de *ARP* gratuito, pois o seu destino é o *Broadcast*, ou seja, todas as interfaces da rede local e o *IP* destino coincide com o *IP* de origem, logo não é esperada nenhuma resposta por parte das outras interfaces. Tendo em conta que esta mensagem ocorreu na mesma altura em que foi atribuído um *IP* à nossa interface, podemos concluir que o seu objetivo é atualizar as tabelas *ARP* das interfaces locais. Isto levará a um maior nível de eficiência nas eventuais comunicações futuras com a nossa interface, visto que já não será necessário o trabalho adicional de perguntar a todas as interfaces qual é o endereço *MAC* que corresponde ao *IP* da nossa maquina.

3 Domínios de colisão

Para estudar os domínios de colisão foi estabelecida a seguinte *Topologia Core*.

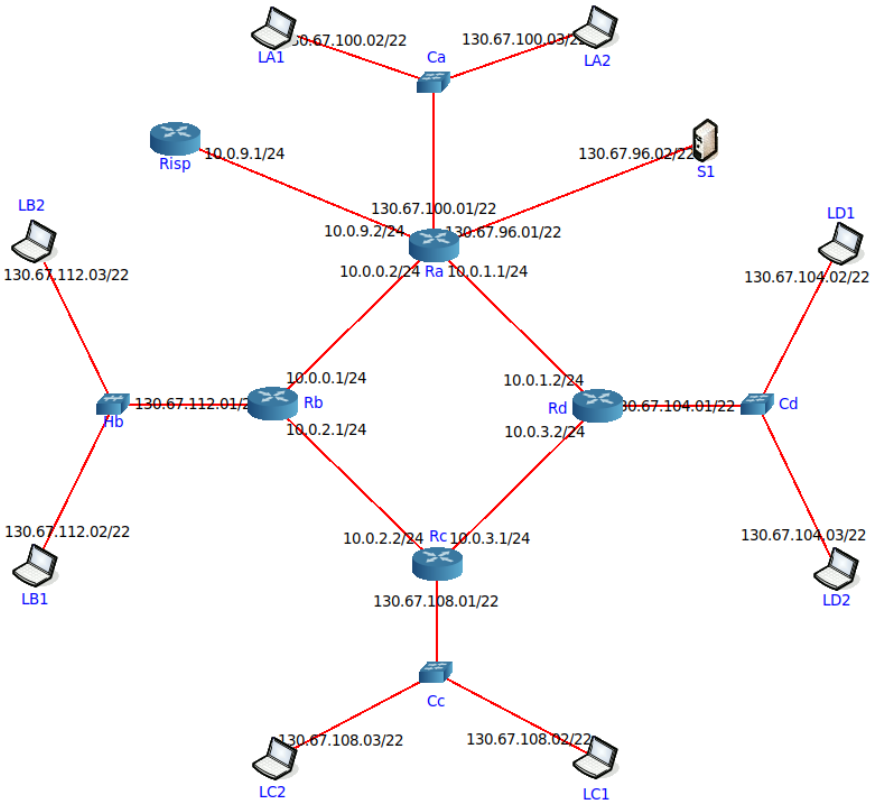

Figura 1. Topologia em estudo

16. **Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando ping). Que conclui? 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.**

   – Para estudo pretendido foram feitos pings do *Servidor1* a todas as interfaces do departamentamento B identificados na figura 2. Posteriormente o mesmo foi feito para as interfaces do departamento A identificados na figura 3.

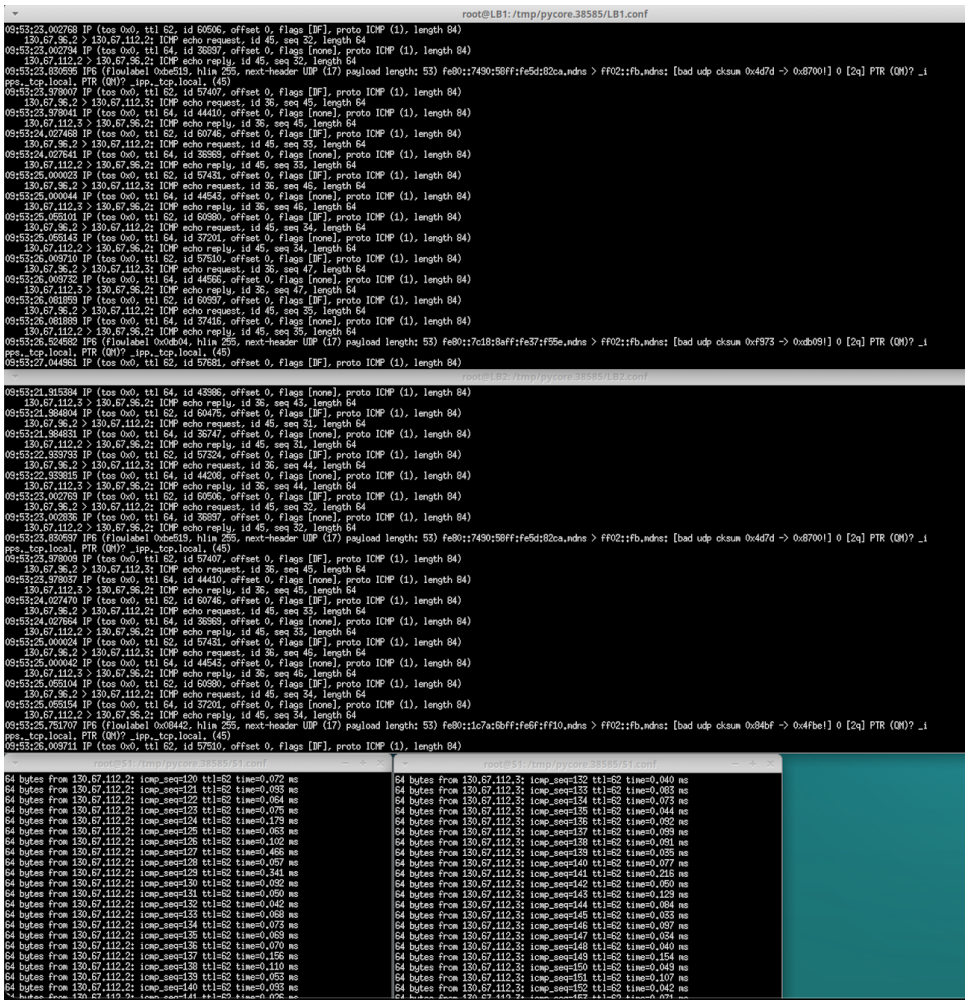

Figura 2. Tráfego no meio de difusão do departamento B.

– Como esperado, no departamento B o tráfego destinado a qualquer um dos laptops é partilhado por ambas as interfaces, visto que ambos partilham o mesmo meio de difusão como é possível ver na imagem 2. Consequentemente, à medida que o tráfego aumentasse (quer pelo surgimento de novas interfaces, quer pelo aumento do tráfego nas interfaces existentes) poderiam surgir situações de colisões quando duas ou mais tramas percorrem o mesmo meio, sobrepondo-se e destruindo a informação contida nelas. As interfaces iriam rejeitar estas tramas e, daí, estas teriam de ser reenviadas, ficando novamente sujeitas à mesma situação. Na imagem 2 é possível ver dois pacotes que foram rejeitados que tendo em conta que estamos perante uma rede virtual, podemos assumir que foram vítimas destas situações.

  Ora isto já não é um problema no departamento A visto que sendo um ambiente comutado, cada interface teria o seu próprio ambiente com o comutador e desta forma cada ligação só estaria sujeita a um único pacote em cada instante de tempo. Consequentemente, as interfaces da rede deixariam de receber pacotes destinadas a outras interfaces visto que, assim que fosse estabelecida uma correspondência no comutador, o tráfego já não seria encaminhado para as interfaces erradas. Isto é visível na imagem na imagem 3, em que cada *Laptop* só deteta tráfego destinado ou proveniente de si mesmo.

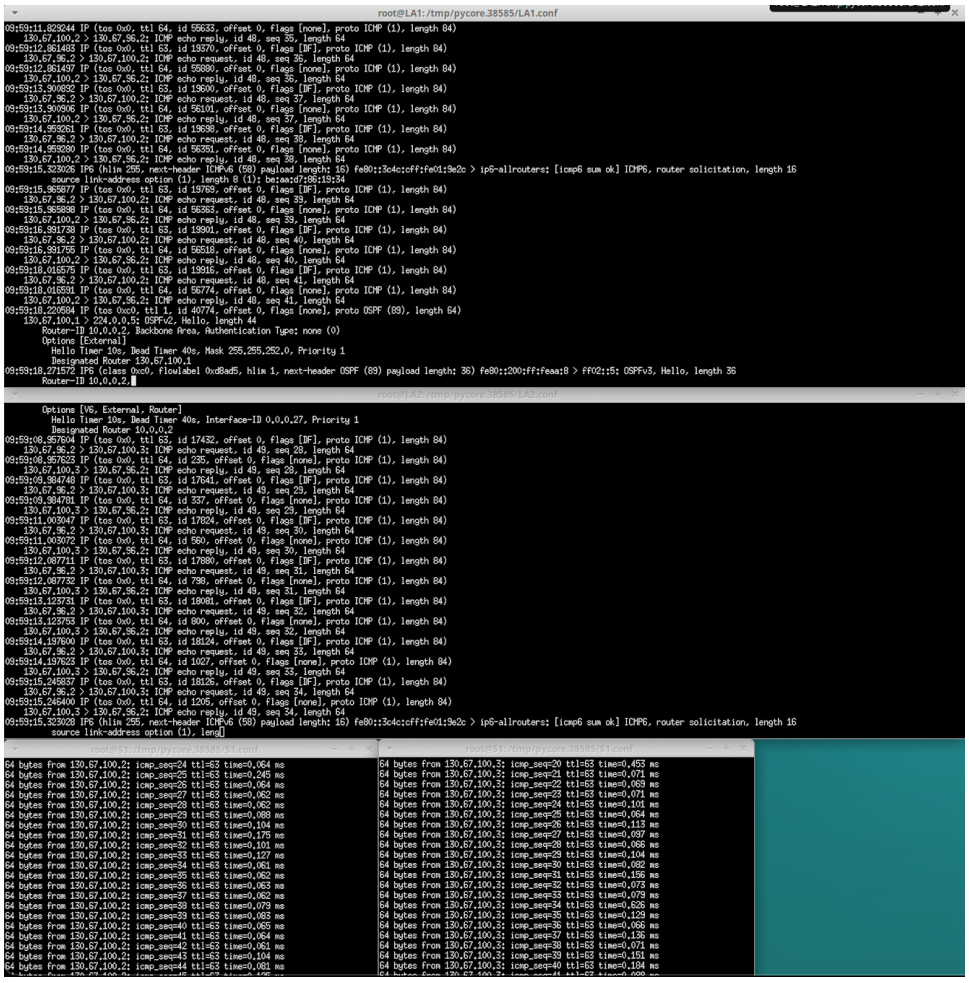

Figura 3. Tráfego no meio comutado do departamento A.

4 Conclusão

Em suma, este relatório apresenta as nossas respostas e estratégias utilizadas na observação e análise de tramas Ethernet e protocolos ARP. Para além disto, analisamos as particularidades dos protocolos ARP gratuitos, e as caraterísticas dos domínios de colisão em redes Ethernet de difusão.

Ao longo deste trabalho foi possível estudar e identificar os conteúdos e informações relevantes em cada trama Ethernet e entre pedidos e respostas ARP, aplicando assim os nossos conhecimentos deste conceitos de um modo prático. Adicionalmente, analisamos também o modo de funcionamento dos domínios de colisão em redes Ethernet de difusão e, consequentemente, o tráfego e as dificuldades a que estes são sujeitos. Para estes fins foram utilizadas as ferramentas propostas pela equipa docente, já utilizadas na fase anterior deste trabalho.

Consideramos, em geral, que o desenvolvimento deste trabalho contribuiu para o aprofundamento da nossa compreensão destes conceitos e da sua relevância no contexto da UC de Redes de Computadores, para além de ter desenvolvido a nossa capacidade de análise deste tipo de dados.