

Universidade do Minho

Departamento de Informática

TP3 - Nível de Ligação Lógica: Ethernet e Protocolo ARP

Redes de Computadores

Grupo 37

Catarina Pais Vieira (a89524)

José Duarte Pereira de Castro Alves (a89563)

Leonardo de Freitas Marreiros (a89537)

**Conteúdo**

[**Questões e Respostas** 3](#_Toc58439692)

[**3. Captura e análise de Tramas Ethernet** 3](#_Toc58439693)

[**Exercício 1** 3](#_Toc58439694)

[**Exercício 2** 3](#_Toc58439695)

[**Exercício 3** 3](#_Toc58439696)

[**Exercício 4** 3](#_Toc58439697)

[**Exercício 5** 4](#_Toc58439698)

[**Exercício 6** 4](#_Toc58439699)

[**Exercício 7** 4](#_Toc58439700)

[**Exercício 8** 4](#_Toc58439701)

[**4. Protocolo ARP** 5](#_Toc58439702)

[**Exercício 9** 5](#_Toc58439703)

[**Exercício 10** 5](#_Toc58439704)

[**Exercício 11** 6](#_Toc58439705)

[**Exercício 12** 6](#_Toc58439706)

[**Exercício 13** 6](#_Toc58439707)

[**Exercício 14** 7](#_Toc58439708)

[**5. ARP Gratuito** 8](#_Toc58439709)

[**Exercício 15** 8](#_Toc58439710)

[**6. Domínios de colisão** 8](#_Toc58439711)

[**Exercício 16** 8](#_Toc58439712)

[**Conclusão** 11](#_Toc58439713)

# **Questões e Respostas**

## **3. Captura e análise de Tramas Ethernet**

### **Exercício 1**

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

Figura - endereço MAC

Pela Figura 1 observamos que o endereço MAC de destino é 00:d0:03:ff:94:00 e o endereço MAC de origem é 88:e9:fe:62:de:d1.

### **Exercício 2**

Identifique a que sistemas se referem. Justifique.

Sistema destino de endereço 00:d0:03:ff:94:00, que corresponde à interface da rede local do router, pois trata-se de um endereço MAC e o *request* tem como destino final um sistema fora da rede local.

Sistema origem de endereço 88:e9:fe:62:de:d1, que corresponde ao *host*, pois este fez o *request*.

### **Exercício 3**

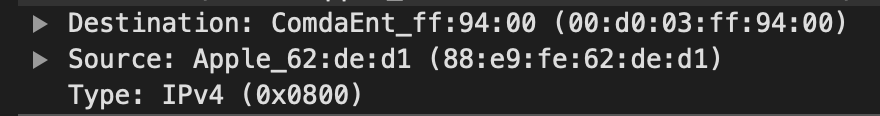
Qual o valor hexadecimal do campo *Type* da trama Ethernet? O que significa?

Figura - trama Ethernet

Como se pode ver pela Figura 2, o campo *type* tem o valor 0x0800. Indica que o protocolo IP utilizado ao nível da rede é IPv4.

### **Exercício 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.

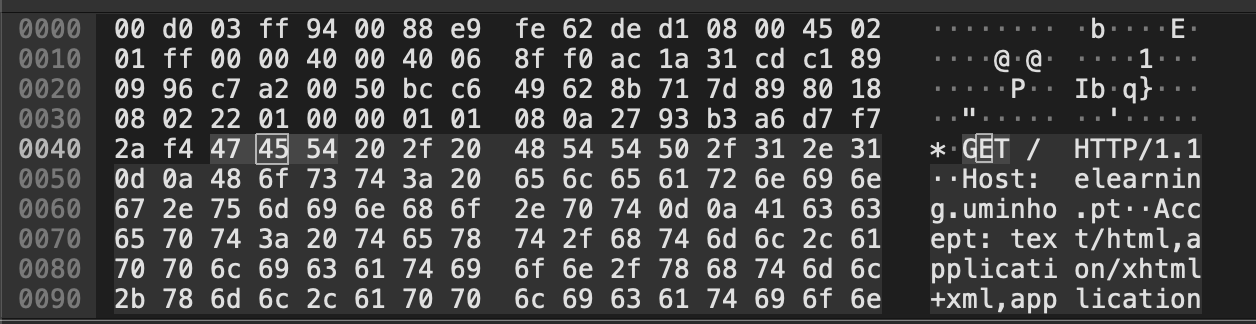
Pela Figura 3, vemos que até ao caractere ASCII “G” são utilizados 66 bytes. No total são usados 525 bytes, logo, a percentagem da sobrecarga é: 66/525 \* 100 = 12.57%.

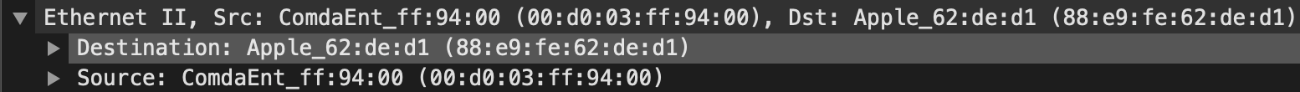
Figura - bytes até ao G

### **Exercício 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*)).

Segundo a documentação do Whireshark a maior parte dos sistemas operativos não suportam a captura do FCS em Ethernet, logo o Whireshark não deteta os FCS das tramas, o que não permite verificar se foram detetadas tramas com erros.

### **Exercício 6**

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

Endereço de origem: 00:d0:03:ff:94:00, como se trata de um endereço MAC e de uma resposta que vem de fora da rede local, este endereço corresponde ao router dessa rede.

Figura - trama Ethernet

### **Exercício 7**

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

Endereço destino: 88:e9:fe:62:de:d1, que corresponde à interface Ethernet da máquina nativa.

### **Exercício 8**

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



Figura - protocolos da trama recebida

Os protocolos contidos na trama da Figura 4 são: Ethernet, IPv4, TCP e HTTP

## **4. Protocolo ARP**

### **Exercício 9**

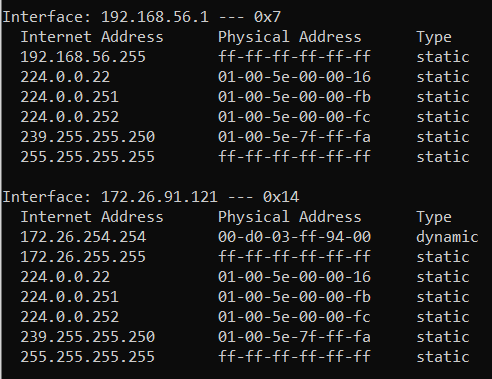
Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.

Figura - tabela ARP

A tabela ARP mapeia o endereço IP para o endereço MAC dos sistemas que comunicaram recentemente. A primeira coluna representa o endereço IP do *host*, a segunda coluna representa o MAC *address* e a terceira o tipo do endereço usado.

### **Exercício 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?

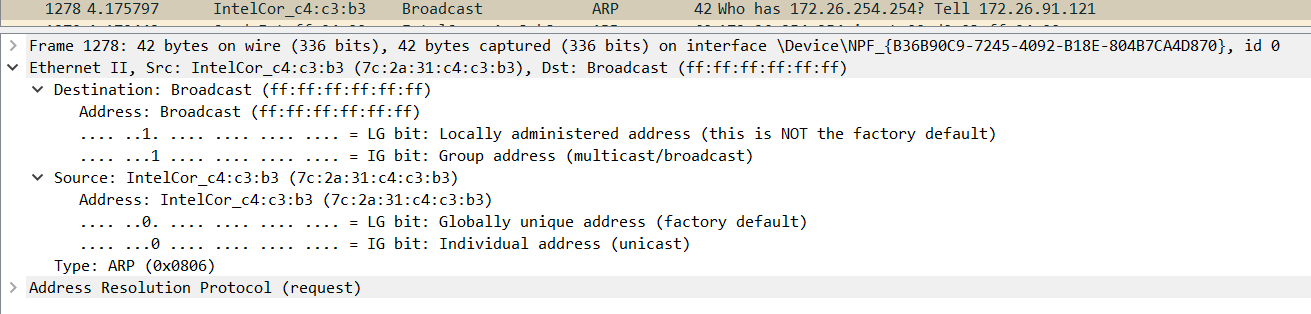


Figura - pedido ARP

O valor hexadecimal dos endereços de origem é 7c:2a:31:c4:c3:b3 e o valor hexadecimal dos endereços destino é ff:ff:ff:ff:ff:ff.

É usado o endereço ethernet do *broadcast* (da camada 2) para poder ser recebido por todos os *hosts* da rede.

### **Exercício 11**

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

O valor hexadecimal do campo tipo da trama Ethernet pode-se ver na Figura 7. Tem o valor 0x0806. Isto indica que o campo de dados pertence ao ARP.

### **Exercício 12**

Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

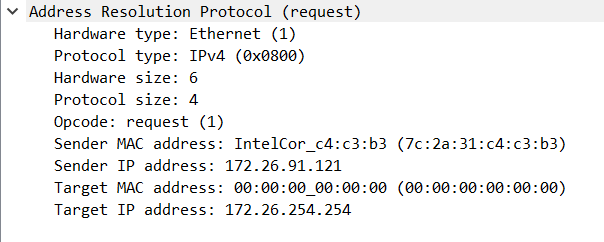


Figura - pedido ARP

Pela observação da Figura 8 verificamos que o *opcode* tem o valor 1 pelo que se trata de um pedido ARP (RFC 826, RFC 5227). Nesta mensagem estão contidos endereços MAC e IP do remetente e do alvo. Se um *host* está a comunicar com outro *host* na mesma rede IP, o destino do pedido ARP é o endereço IP do outro *host*. Se um *host* estiver a comunicar com outro *host* numa rede IP diferente, o destino do pedido ARP será o endereço IP do *gateway* padrão. Neste caso, o *host* com IP 172.26.91.121 e MAC 7c:2a:31:c4:c3:b3 pretende saber qual o MAC do *host* com IP 172.26.254.254 pelo que o MAC alvo é o endereço de *broadcast*.

### **Exercício 13**

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

A pergunta feita pelo *host* de origem é do tipo “Who has 172.26.254.254? Tell 172.26.92.121”. Isto significa que perguntamos ao *host* da rede qual o MAC e quem tem o IP 192.26.92.254, e pedimos para enviar a resposta para 172.26.92.121.

### **Exercício 14**

Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. **a.** Qual o valor do campo ARP *opcode*? O que especifica? **b.** Em que posição da mensagem ARP está a resposta ao pedido ARP?

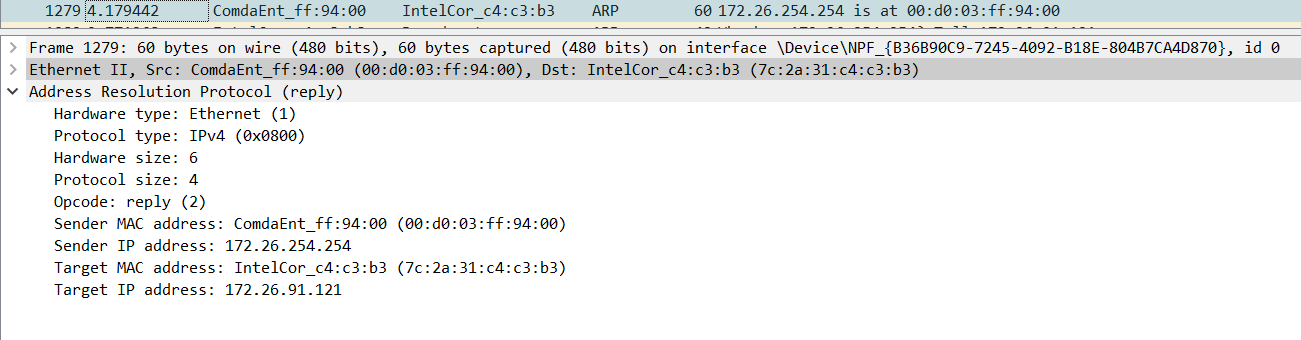


Figura - campo ARP opcode

**a.** O valor do campo *opcode* é reply(2), o que significa que se trata de uma resposta a um “request” anterior.

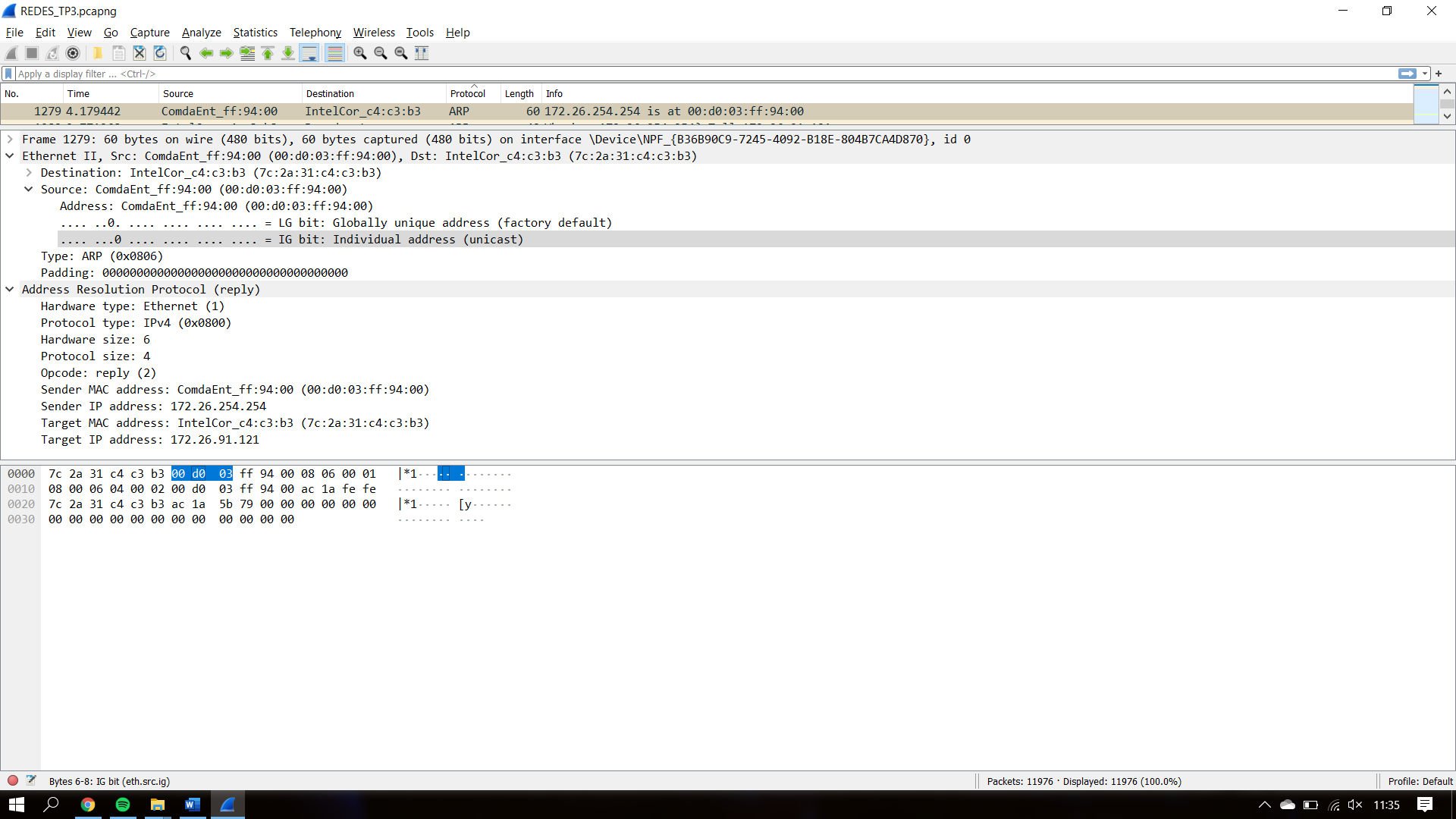
**b.** A resposta (*reply*) é fornecida de forma direta (*unicast*) pela máquina com o endereço lógico requisitado, contendo então o endereço físico da mesma. Pela observação da Figura 10 verificamos que se encontra nos bytes 6 a 8.

Figura - pedido ARP

## **5. ARP Gratuito**

### **Exercício 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?

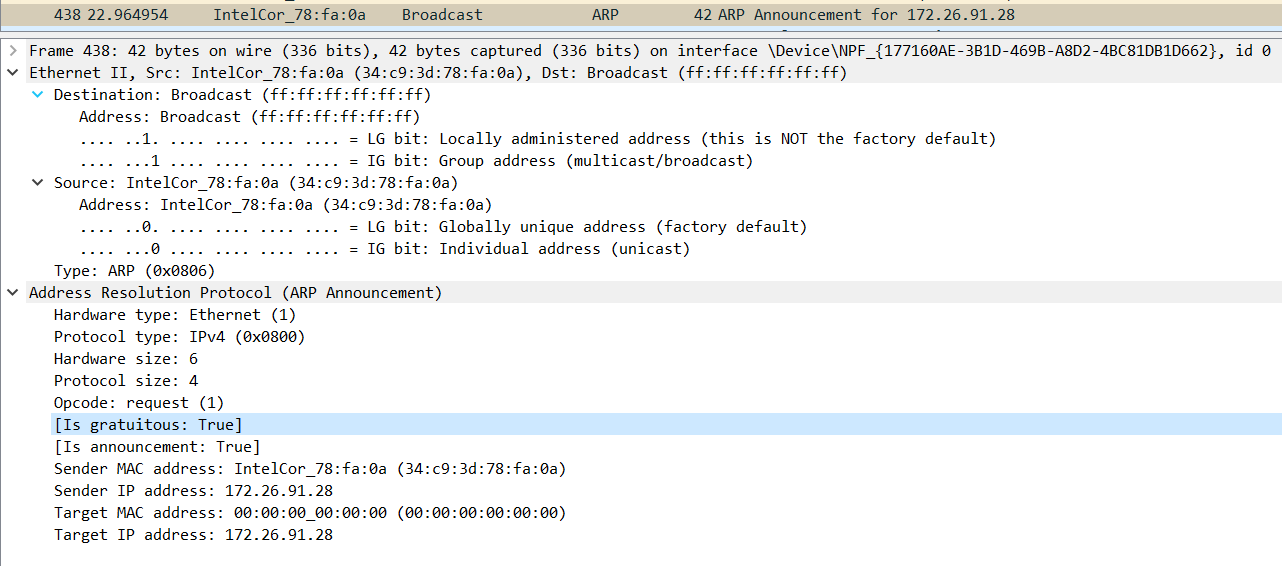


Figura - pedido ARP gratuito

Analisando a Figura 11 verificamos que este pedido ARP diferencia dos anteriores pela presença da *flag* – “Is gratitous”, que apresenta o valor True, o que significa que se trata de um pedido ARP gratuito. Além disso, os endereços IP alvo e remetente são iguais. O ARP gratuito é enviado como um *broadcast*, como forma de um nó anunciar ou atualizar seu mapeamento IP para MAC para toda a rede. **Nota:** Foram também enviados 3 pedidos ARP de sonda (*Probe*) antes do pedido ARP de anúncio (*Announcement*).

## **6. Domínios de colisão**

### **Exercício 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.

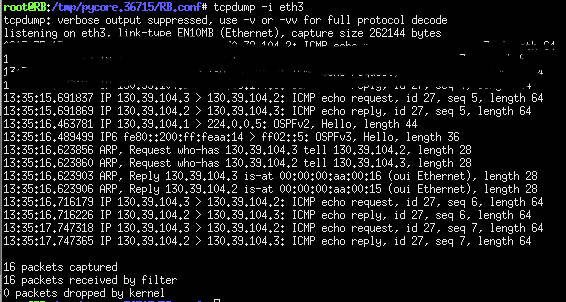


Figura 13 - Router departamento B com Hub

Figura 12 - Host departamento B com Hub

Foram feitos pings de um *host* do departamento B para um outro *host* do mesmo departamento (Figura 12 - tcpdump host recetor, Figura 13 - tcpdump da interface da rede B do respetivo router). Assim, como se pode ver pelas imagens, no departamento B (com *hub* em vez de *switch*), tudo passa no router (tanto o ping, como a resposta, como até tramas ARP), o que suporta o facto de existir um domínio de colisão entre o *hub* e a interface do router neste tipo de redes.

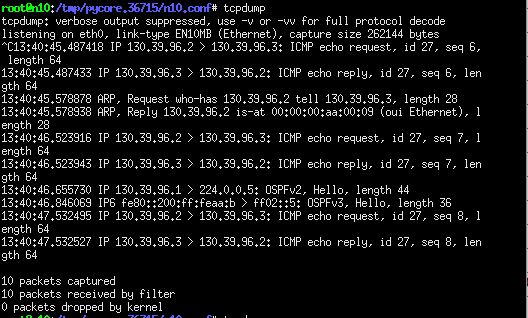
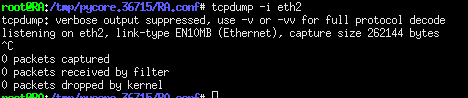


Figura 15 - Router departamento A com switch

Figura 14 - Host departamento A com switch

O mesmo método foi utilizado para a observação da rede do departamento A que tem um *switch* em vez de um *hub* (Figura 14 - tcpdump do host recetor, Figura 15 - tcpdump da interface da rede A do respetivo router). Como é observável nas imagens, ao router não chega qualquer informação, o que mostra que é o *switch* que está a controlar o fluxo da rede local e que suporta o facto de que apenas as portas do *switch* são potencialmente domínios de colisão (dado que, em oposição a “half-duplex”, se a comunicação for “full-duplex” não existe domínio de colisão).

# **Conclusão**

Com este trabalho, foram colocados em prática conhecimentos referentes ao capítulo *Link Layer* adquiridos durante as aulas teóricas anteriores, o que nos levou a consolidar melhor a matéria. Podemos dividir este trabalho em três partes: análise de tramas Ethernet, protocolo ARP e domínios de colisão.

Com a ajuda do Wireshark e o Core conseguimos capturar e analisar tramas de Ethernet, esta informação foi essencial para a realização deste trabalho, e ajudou-nos a aprimorar os conhecimentos referidos anteriormente.

A primeira parte foi baseada na utilização de uma conexão por Ethernet. Na segunda parte focamo-nos nos pacotes ARP e na terceira parte o nosso foco virou para a comparação entre *Hubs* e *Switches*.

Com este trabalho prático abordamos melhor a camada de ligação lógica, percebendo melhor como funciona a interconexão de redes locais baseado no envio de pacotes.

Utilizando a ferramenta anteriormente referida, Core, simulamos um ambiente que nos permitiu analisar a maneira de funcionamento dos domínios de colisão e o modo como eles são corrigidos.

Com isto, basicamente todo este capítulo de *Link Layer* foi abrangido e consolidado.