# TP3 - Ethernet e ARP

## Redes de Computadores - Grupo 12

Ana Teresa Gião Gomes A89536
André Carvalho da Cunha Martins A89586
Pedro Miguel de Soveral Pacheco Barbosa A89529

**Fig. 1.** A89536

**Fig. 2.** A89586

**Fig. 3.** A89529

9 de dezembro de 2020

# Ethernet e ARP

André Martins, Ana Teresa Gomes, and Pedro Barbosa

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89586,a89536,a89529}@alunos.uminho.pt

A captura de tráfego deverá ser efetuada usando a aplicação Wireshark instalada na máquina nativa. Uma vez que as salas de aula atuais não disponibilizam uma ligação com fios a uma rede Ethernet, a captura será realizada na rede Eduroam. Este facto não impacta na realização do trabalho porque, por defeito, o Wireshark disponilibiliza o tráfego capturado ao utilizador como sendo (pseudo) Ethernet. Assegure-se que a cache do seu browser está vazia.

Ative o Wireshark na sua máquina nativa.

No seu browser, aceda ao URL http://elearning.uminho.pt.

Pare a captura do Wireshark.

Obtenha o número de ordem da sequência de bytes capturada (coluna daesquerda na janela do Wireshark) correspondente à mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o começo da respectiva mensagem HTTP Response proveniente do servidor.

No sentido de proceder à análise do tráfego, selecione a trama Ethernet que contém a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP está no interior de um segmento TCP que é transportado num datagrama IP que, por sua vez, está encapsulado no campo de dados deuma trama Ethernet. Expanda a informação do nível da ligação de dadose observe o conteúdo da trama Ethernet (cabeçalho e dados (payload)).

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem HTTP GET.

Sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada. Para imprimir um pacote, use File-Print, escolha Selected packet only e Packet summary line, ou use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o mínimo detalhe necessário para responder à pergunta.

# Captura e análise de Tramas Ethernet

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

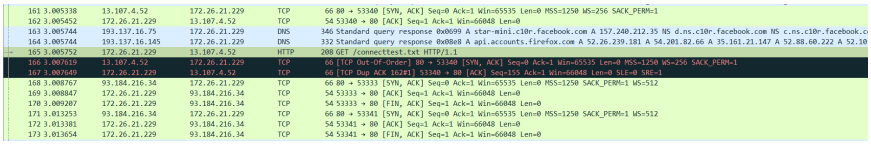



**Fig. 1.** Pacotes TCP enviados ao aceder ao elearning


**Fig. 2.** Campo Ethernet II da trama selecionada

Endereço MAC source: ac:ed:5c:8d:f2:61

Endereço MAC destination: 00:d0:03:ff:94:00

## 2 Pergunta 2: Identifique a que sistemas se referem. Justifique.

O endereço MAC refere-se ao endereço físico da interface ativa de uma máquina. Portanto, o endereço MAC source refere-se ao endereço físico do nosso computador e o endereço MAC destination refere-se ao endereço físico do router com o qual está a comunicar.

## 3 Pergunta 3: Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?


**Fig. 3.** Valor hexadecimal

Como é possível analisar na figura, o valor do campo Type é de 0x0800. Isto indica que a camada superior está a utilizar o protocolo IPv4.

## 4 Pergunta 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.

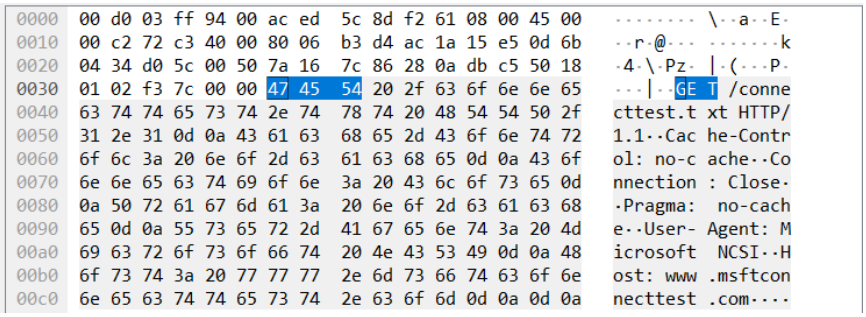
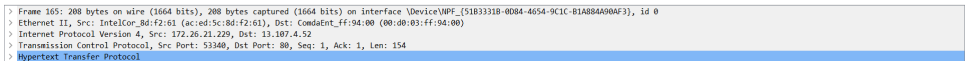



**Fig. 4.** Valor dos bytes da trama


**Fig. 5.** Descrição da trama

Como a figura 3 ilustra, até ao GET temos 54 bytes (8 * 2 * 3 + 6). Na figura 4, vemos que a trama tem 208 bytes. Ficamos, assim, com uma percentagem da sobrecarga introduzida pela pilha protocolar de 54/208 * 100 = 25,96 %

## 5 Pergunta 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)).




Como é possível observar na figura, o campo FCS não está a ser utilizado, uma vez que não aparece na trama, logo não foram detetadas tramas com erros.

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


**Fig. 6.** Pacote TCP

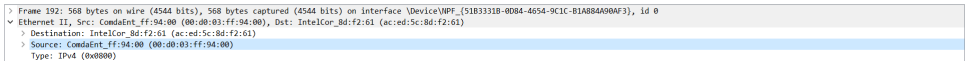



**Fig. 7.** Campo Ethernet II

O endereço Ethernet da fonte é 00:d0:03:ff:94:00 e corresponde ao endereço físico do router da rede à qual estamos ligados.

## 7 Pergunta 7: Qual é o endereço MAC do destino? A que sistema corresponde?

O endereço MAC do destino é ac:ed:5c:8d:f2:61 e diz respeito à interface ativa do computador.

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

Os protocolos HTTP (Hypertext Transfer Protocol), IPv4 (Internet Protocol Version 4), TCP (Transmission Control Protocol) e Ethernet.

# Protocolo ARP

**9 Pergunta 9: Observe o conteúdo da tabela ARP. Diga o que significa cada umadas colunas.**

```
PS C:\WINDOWS\system32> arp -a

Interface: 172.26.21.229 --- 0x9
  Internet Address      Physical Address      Type
  172.26.254.254        00-d0-03-ff-94-00     dynamic
  172.26.255.255        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: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.56.255        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
PS C:\WINDOWS\system32>
```

**Fig. 8.** Tabela ARP

Na primeira coluna da tabela é possível observar os Endereços IP e na segunda coluna temos os Endereços MAC correspondentes.

Para observar o protocolo ARP em operação, apague novamente a cache ARP e assegure-se que o cache do browser está vazia.

Inicie a captura de tráfego com o Wireshark, e aceda a http://alunos.uminho.pt. Efectue também um ping para um host da sala de aula que esteja a ser usado por outro grupo. Pare a captura de tráfego e tente localizar o tráfego ARP. Se necessário, limite os protocolos visíveis apenas a protocolos abaixo donível IP. Para tal, seleccione Analyze->Enabled Protocols e remova a selecção da opção IPv4 e IPv6.

```
PS C:\WINDOWS\system32> arp -d
PS C:\WINDOWS\system32> arp -a

Interface: 172.26.21.229 --- 0x9
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
PS C:\WINDOWS\system32>
```

**Fig. 9.** Delete da Tabela ARP

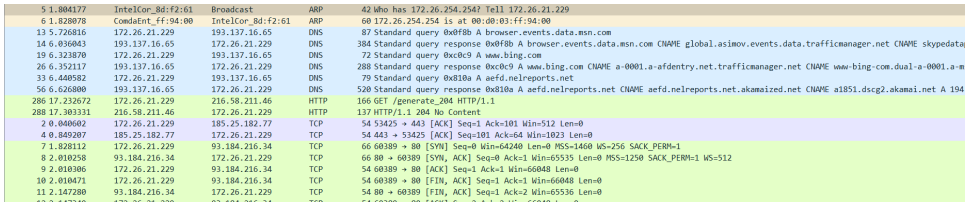



**Fig. 10.** Tráfego ARP

Como a rede Eduroam não estava a permitir realizar o comando ping, iremos responder às próximas perguntas recorrendo ao pedido ARP para o gateway.

## 10 Pergunta 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?

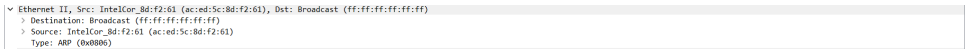



**Fig. 11.** Campo Ethernet

O valor do Source é igual a ac : ed : 5c: 8d : f2: 61 e o Destination tem valor igual a ff : ff : ff : ff : ff. Isto deve-se ao facto de, na nossa Tabela ARP, ainda não existir nenhum endereço MAC associado ao ao endereço IP para o qual fizemos ping. É necessário comunicar com todos os dispositivos da rede para que o destino possa responder de volta, daí utilizar o endereço de broadcast ff : ff : ff : ff : ff.

## 11 Pergunta 11: Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?


**Fig. 12.** Type: ARP (0x0806

O campo type tem valor 0x0806, indicando que a camada acima está a utilizar o protocolo ARP.

## 12 Pergunta 12: Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?


**Fig. 13.** Opcode

Como é possível observar, o opcode tem valor igual a 1, logo representa um request. Assim, concluímos que o nosso dispositivo está a pedir dispositivos em rede, correspondentes ao IP pedido.
Na mensagem ARP estão contidos endereços IP e MAC, portanto, o protocolo ARP serve para converter um endereço IP num endereço MAC.

## 13 Pergunta 13: Explicite que tipo de pedido ou pergunta é feita pelo host de origem.

No momento em que se realiza o ping, a nossa tabela ARP não tem definida a associação entre o IP para o qual foi feito o ping e o respetivo endereço MAC. Logo, é enviada uma mensagem ARP para todos os dispositivos de rede para, caso exista uma correspondência com o endereço IP, esse dispositivo envie o seu endereço MAC.

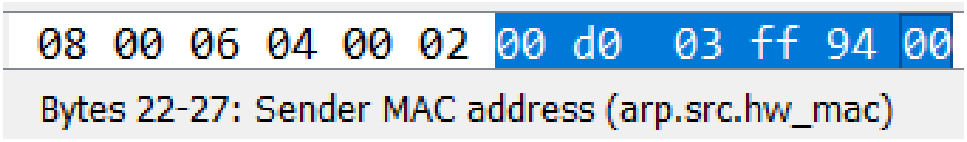
## 14 Pergunta 14: Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

### 14.1 a) Qual o valor do campo ARP opcode? O que especifica?


**Fig. 14.** Mensagem de Resposta

O valor do campo ARP opcode é igual a 2, mostrando, assim, que se trata de uma reply. Isto prova que o dispositivo com o endereço 172.26.254.254 recebeu o request e está a enviar o seu endereço MAC.

### 14.2 b) Em que posição da mensagem ARP está a resposta ao pedido ARP?




A resposta ao pedido ARP é o endereço MAC da origem, que se encontra na posição 22-27 bytes, que corresponde à secção Sender MAC Address.

Arranque o Wireshark na sua máquina nativa e inicie a captura de dados.

Desligue e volte a ligar a sua ligação à rede local, ou force o pedido de atribuição de um novo endereço IP à interface em uso. Pare a captura de tráfego. Utilize o filtro de visualização ARP para facilitar a identificação dos pacotes respetivos.

# ARP Gratuito

## 15 Pergunta 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?

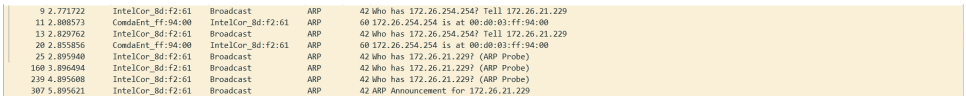



**Fig. 15.** ARP Gratuito


**Fig. 16.** ARP

Ao analisarmos as imagens acima, rapidamente percebemos que o pedido ARP Gratuito tem o mesmo IP de Origem e de Destino (neste caso é o endereço 172.26.21.229). Isto permite-nos concluir se existe algum equipamento na rede que possua o mesmo endereço IP que a máquina que envia a mensagem. Caso isso se verifique, seria obtida uma resposta,

uma vez que o pedido é feito a qualquer equipamento da rede que possua o IP que é solicitado.
Assim, o objetivo do ARP gratuito é evitar conflitos, verificando se mais algum equipamento possui o mesmo IP que a fonte. Uma vez que este pedido não obteve qualquer resposta, conclui-se que não existe mais nenhum equipamento com aquele IP.

# Domínios de Colisão

Ative o emulador CORE e carregue a topologia de rede com a solução desubnetting que construiu no âmbito do TP2. Substitua o switch do departamentos B por um hub (repetidor).

**16 Pergunta 16: Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces dos vários diapositivos 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.**

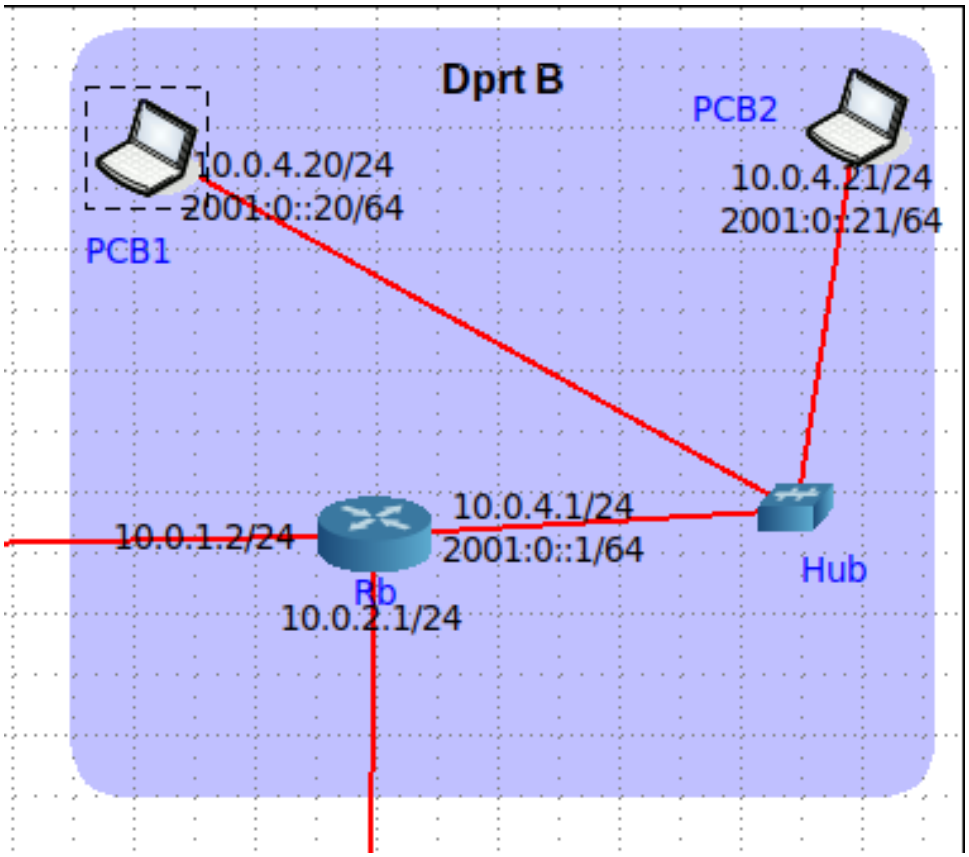
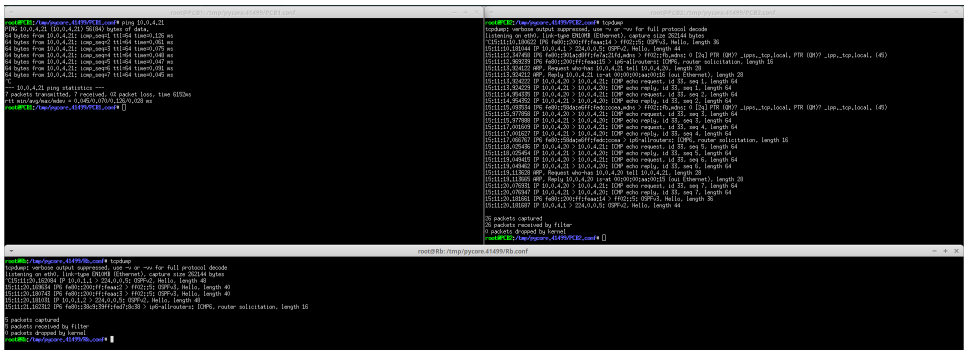
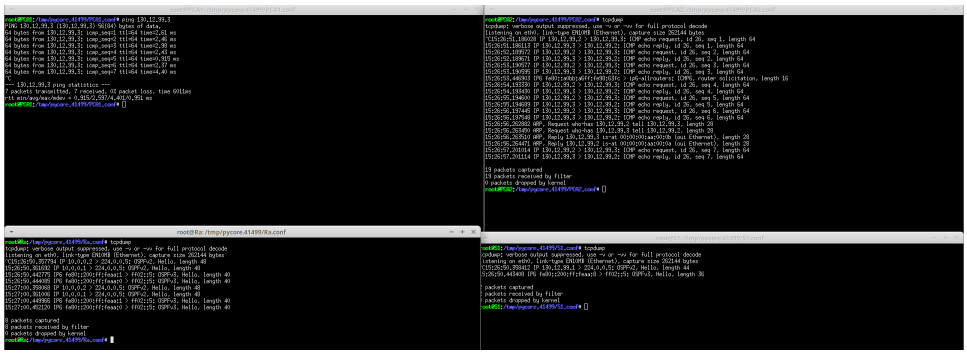



**Fig. 17.** Departamento B com HUB

Quando o PC PCB1 faz ping para o PCB2, podemos observar, através das imagens abaixo, que todos os equipamentos recebem várias mensagens ARP de pedido e de resposta, apesar do ping ter sido feito apenas para o PCB2. Isto explica-se pelo facto de um hub ser um dispositivo que atua a nível físico e que repete o sinal que lhe chega, através de uma porta de entrada, para todas as outras portas, fazendo, assim, com que todos os outros dispostivos recebam a mensagem.



Agora, ao analisar os vários dispositivos do Departamento A (LAN comutada), observamos várias diferenças. O switch, ao invés do hub, recebe a mensagem e transmite-a para o equipamento pretendido (neste caso, PCA2), em vez de enviar a mensagem a todos os equipamentos a si ligados. Assim sendo, observamos tráfego semelhante ao do departamento B em apenas um equipamento, e não em todos os equipamentos como se havia verificado anteriormente.
Os swicthes evitam colisões, uma vez que limitam o envio de mensagens apenas para o equipametno de destino. Ao ter várias portas para cada interface, um switch consegue ter vários domínios de colisão, diminuindo, assim, a probabilidade destas acontecerem.
Por outro lado, um hub repete a mensagem para todos os equipamentos que estão a ele ligados, o que aumenta bastante a probabilidade de existirem colisões. Quando uma colisão ocorre, é necessário reenviar a mensagem, o que acarreta vários custos para a nossa rede.



## 17 Conclusão

Ao desenvolver mais um trabalho prático, ficamos a compreender melhor o funcionamento da camada de ligação lógica, tendo analisado a tecnologia Ethernet. Analisamos, também, o protocolo ARP (Address Resolution Protocol), o que nos proporcionou um melhor entendimento dos mecanismos de mapeamento de endereços de rede e de endereços físicos, como os endereços IP e os endereços MAC.
Com a última questão, estudamos o funcionamentos de dispostivos que operam a nível físico, como é o caso do swicth e do hub, e analisamos os comportamentos característicos de cada um. Vimos que as propriedades de cada um destes equipamentos são bastante importantes e algo a ter em conta na nossa rede e, ao analisar o caso específico das colisões, vimos como um switch consegue ser mais eficiente nessa situação, contribuindo para a redução de colisões.