Universidade do Minho
Mestrado Integrado em Engenharia Informática

REDES DE COMPUTADORES
TP3
PL 110

Gonçalo de Sá Quental Rosa Medeiros A89514
José Pedro Castro Ferreira A89572
Rui Emanuel Gomes Vieira A89564

25 de novembro de 2020


A89514


A89572


A89564

Captura e Análise de Tramas 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 da esquerda 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 de uma trama Ethernet. Expanda a informação do nível da ligação de dados e 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.

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

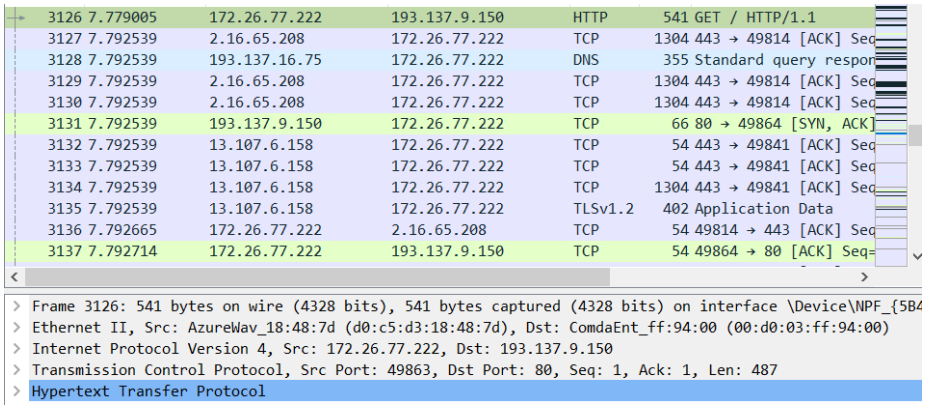

Figura 1: Pacote TCP enviados ao aceder ao site

src: 00:c5:d3:18:48:7d
dst: 00:d0:03:ff:94:00

2 Identifique a que sistemas se referem. Justifique

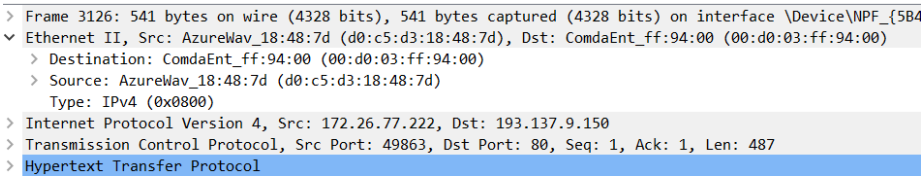

Figura 2: Campo Ethernet II da trama selecionada

O endereço *MAC* refere-se ao endereço físico da interface ativa de uma máquina.
Neste caso, a origem refere-se ao endereço físico do nosso computador e o destino refere-se ao endereço físico do router com que se está a comunicar.

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

O campo *Type* tem valor 0x800, que significa que a camada superior está a utilizar o protocolo 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.

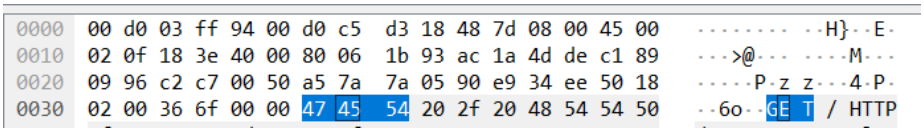

Figura 3: Valor dos bytes da trama

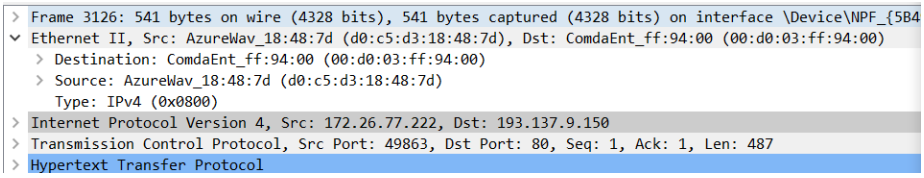

Figura 4: Descrição da trama

Até ao GET temos $3 * 2 * 8 + 6$ bytes, ou seja, 54 bytes. Pela figura, vemos que a trama tem 541 bytes, ficando assim com uma percentagem de 9.98%

$$\frac{51}{541} * 100 = 9.98$$

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)).

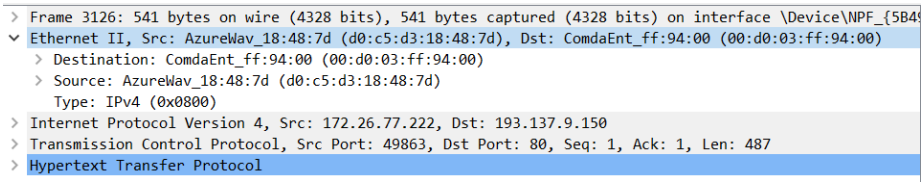

Figura 5: Campo Ethernet II da trama capturada

Ao analisar a imagem, podemos concluir que o campo FCS não foi utilizado, uma vez que não aparece na parte da ethernet. Do nosso ponto de vista, deve-se ao facto de as ligaçãoes por cabo serem ligações muito estáveis e pouco suscetíveis a acumularem erros.

A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP.

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

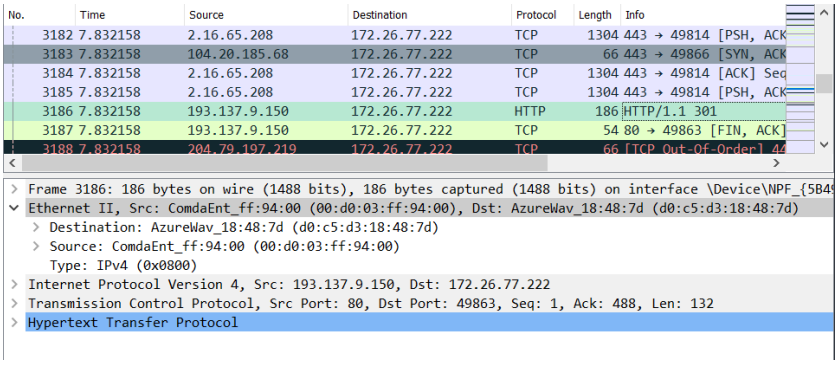

Figura 6: Pacote TCP selcionado e Campo Ethernet II da resposta HTTP

O endereço da fonte é 00:d0:03:ff:94:00 e corresponde ao endereço físico do router com que estamos a comunicar.

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

O endereço do destino é d0:c5:d3:18:48:7d e corresponde ao endereço físico da interface ativa do nosso computador

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), Ethernet e TCP (Transmission Control Protocol).

Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP. Verifique o conteúdo da cache ARP do seu computador.
No sentido de observar o envio e recepção de mensagens ARP, é conveniente apagar o conteúdo da cache ARP. Caso contrario, é provável que a associação entre endereços IP e MAC já exista em cache.

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.

Responda às seguintes perguntas:

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

A primeira coluna apresenta os endereços IP, a segunda coluna apresenta os respectivos endereços MAC para os nodos conhecidos em LAN e a terceira indica o tipo de endereço (estático/dinâmico).

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?

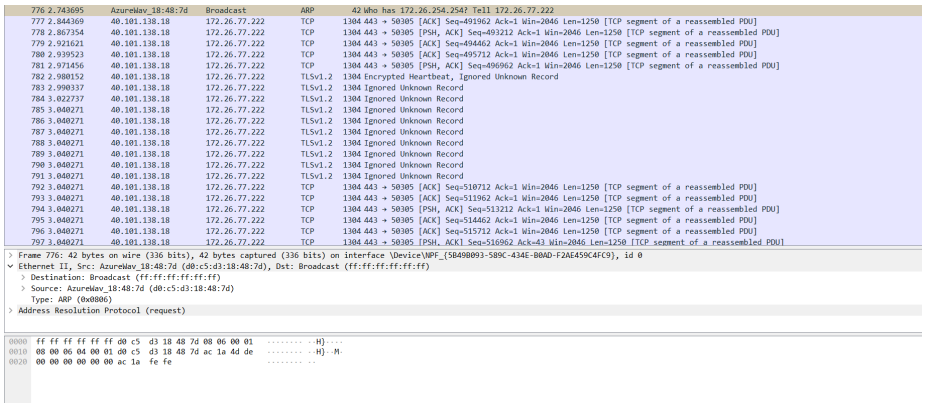

Figura 7: Tabela ARP

A origem tem o valor d0:c5:d3:18:48:7d. O destino tem o valor ff:ff:ff:ff:ff:ff. Este valor deve-se ao facto de a nossa tabela ARP não ter o valor do endereço MAC associado ao endereço ip para o qual mandamos o *ping*. Assim sendo, é preciso enviar para todos os dispositivos na rede para que o destino possa responder e assim guardar o valor do endereço MAC. Para isso, usamos o endereço de broadcast. (ff:ff:ff:ff:ff:ff)

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

O campo *Type* tem o valor 0x0806 e indica que a camada acima está a usar o protocolo ARP (Address Resolution Protocol)

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 *opcode* tem valor 1, que representa um request. Isto diz-nos que a nossa máquina está a pedir aos dispositivos na rede para responderem caso o seu ip seja o pretendido. Numa mensagem ARP temos endereços MAC e IP. Assim, concluimos que o protocolo ARP serve para converter um endereço IP no endereço MAC da interface ativa respectiva.

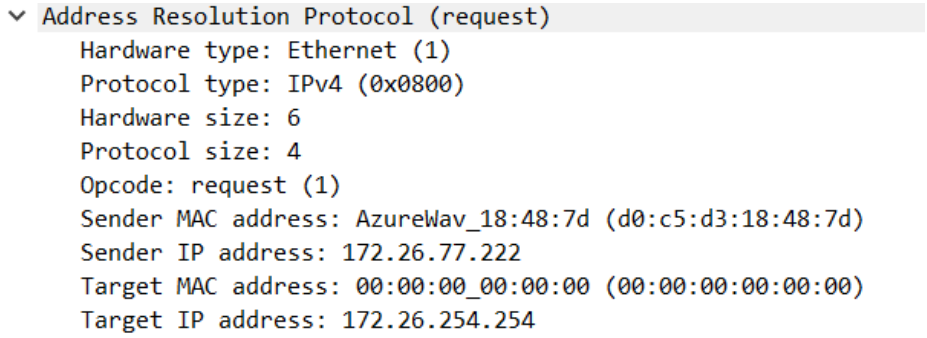

Figura 8: Mensagem ARP

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

Quando fizemos o *ping*, a nossa tabela ARP não tem uma associação entre o IP para o qual enviamos o *ping* e o respetivo endereço MAC. Assim, é enviado uma mensagem ARP para todos os dispositivos na rede para que o endereço IP pretendido, caso receba a mensagem, responda com o seu endereço MAC.

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

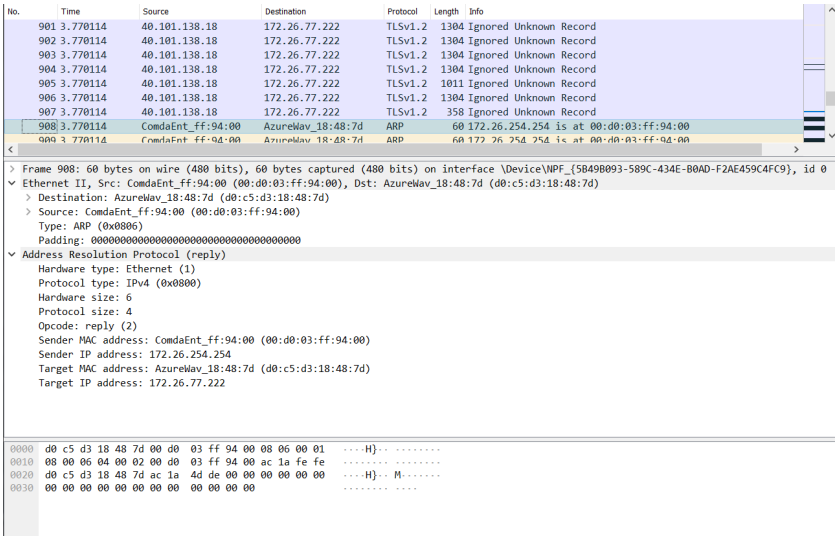

Figura 9: Pedido ARP

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

O *opcode* tem valor 2, que representa uma *reply*. Isto significa que a nossa máquina está a receber o endereço MAC correspondente ao endereço IP para o qual mandou o *ping*

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

A resposta entá entre o bytes 23 e 28 da trama, ou seja, é o *sender MAC Address* da *source* na mensagem de resposta

ARP Gratuito

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.

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?

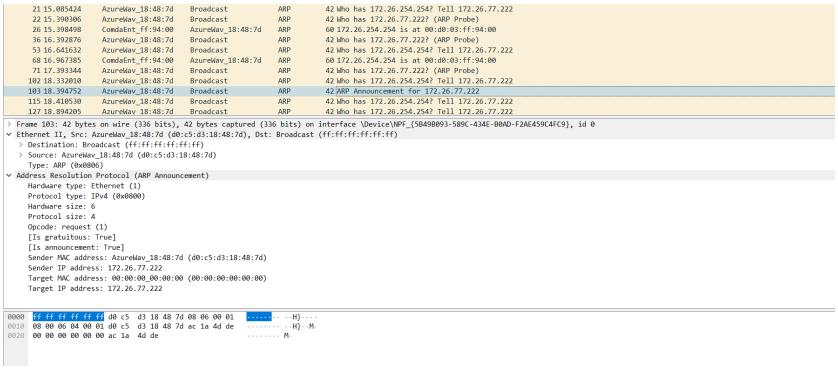

Figura 10: Pedido ARP Gratuito

A grande diferença entre valores do ARP gratuito e os outros é o valor do *Target IP address* que aqui tem o mesmo valor que o *Sender IP address*. Como

não temos um *target IP* não é suposto outros dispositivos, para além do router, responderem aos ARP. Como podemos ver na figura, apenas o router a que estamos ligados respondeu

Domínios de Colisão

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

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 melhor comparar os resultados obtidos nos departamentos A e B, adicionamos um host ao departamento B para que os tenham o mesmo número de interfaces ativas (2 PCs, 1 host e 1 router). A diferença entre os dois será então no equipamento de interligação entre os dispositivos de cada departamento. No Departamento A será então um switch e no Departamento B será um hub.

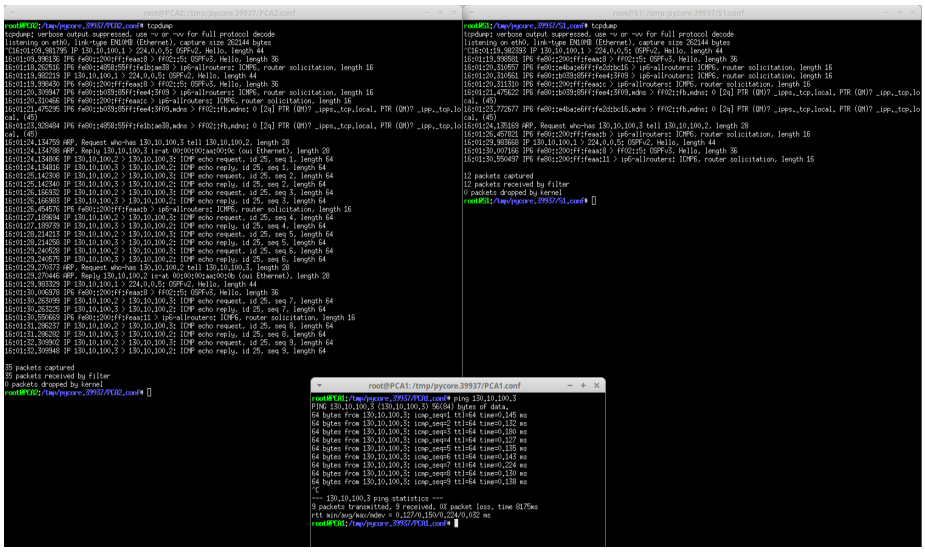

Figura 11: Departamento A

Na topologia do Departamento A (com switch) o tráfego apenas é direcionado para o PCA2 (destino do ping enviado). O outro dispositivo (s1), possui apenas uma captura que é a resultante do envio ARP Broadcast como podemos ver pela figura.

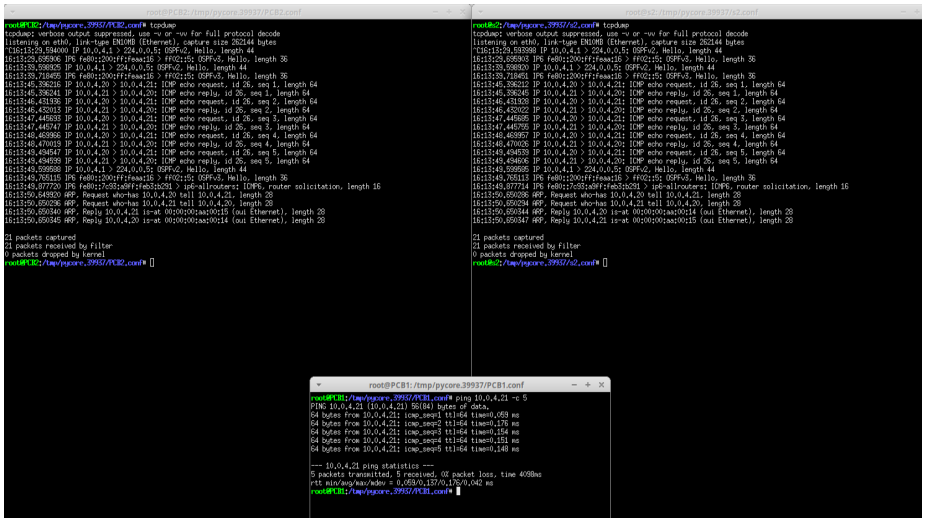

Figura 12: Departamento B

Um hub é um dispositivo que trabalha a nível físico juntando várias portas num único segmento de rede. Quando algo é enviado entre duas portas, o hub

envia o input que recebeu para todas as portas ligadas (exceto para a porta que enviou o input). Como podemos ver pelas imagens, o tráfego captado em PCB2 (destino do ping), é o mesmo captuado em S2, visto que o hub redireciona o tráfego para todas as portas. Com isto, concluímos que acabam por chegar mensagens que não são supostas a outros dispositivos.

Assim sendo, concluímos que os switches, ao evitarem enviar a informalão para todos os hosts fazem com que o risco de haver colisões seja menor. Em contra partida, o hub como junta tudo num canal de transmissão e repede muita da informação está mais propício a colisões. Um switch possui uma tabela de endereçamento que permite fazer o redirecionamento apenas para o nó pretendido, o que não é possível fazer com o hub.

Conclusão

Neste trabalho prático foi-nos possível aprofundar o conhecimento acerca das tramas de Ethernet, perceber que estão organizadas em bytes, bem como conhecer o protocolo ARP. Para a realização deste trabalho utilizamos o simulador de redes (CORE) e ainda um software de captura e análise de tramas (Wireshark).

A utilização desta segunda ferramenta foi essencial pois permitiu a observação dos protocolos envolvidos, qual o encapsulamento a ter aquando a transferência de processos e verificar outras propriedades importantes, que permitem ter conhecimento e informações sobre os endereços envolvidos, o tipo da mensagem ARP, assim como a análise de um pedido ARP.

Outro ponto abordado foi a análise de um ARP Gratuito, verificando assim que apesar de ser algo que acontece sem que se tenha pedido para o fazer este torna-se útil na verificação de um host ter o mesmo endereço IP que o originador do pedido, assim como permite informar hosts e/ou switches novos endereços MAC para que todos os sistemas da rede possam atualizar as suas tabela ARP.

Desta forma pudemos consolidar conceitos, protocolos e comportamento dos dados transmitidos em Ethernet.