Rede de Computadores - Trabalho Prático nº 2
Camada de Ligação Lógica: Ethernet e Protocolo ARP

William Sousa, Manuel Maciel e Rui Santos

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a61029,a68410,a67656}@alunos.uminho.pt

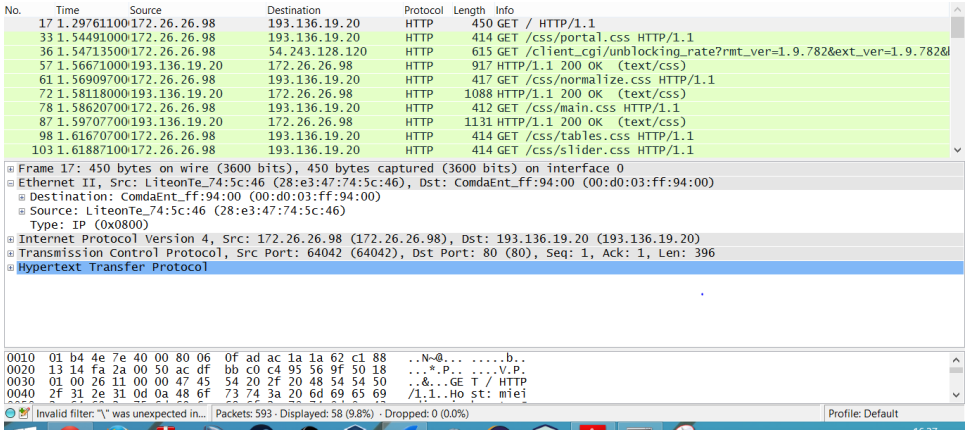
Resumo Neste relatório, iremos propor respostas para as perguntas da ficha de trabalho pratica nº 2 que foi realizada no âmbito da unidade curricular de Redes de Computadores, lecionada no ano lectivo 2015/2016 do Mestrado Integrado de Engenharia Informática, logo toda a estrutura de perguntas e respostas, presentes neste relatório, irão de encontro ao que foi fornecido e pedido nessa ficha prática. Acreditamos que as perguntas e respostas aqui apresentadas, de uma forma geral, ajudam a compreensão e análise de muitos conceitos relacionados com as redes de computadores, nomeadamente dos níveis mais baixo do modelo OSI (i.e. camada de ligação lógica e camada física) com especial atenção a tecnologia de rede local *Ethernet* e do dos endereços *IP (Internet Protocol)* e *MAC (Media Acess Control)*; e da implementação e normas seguida pelos protocolos *ARP (Adress Resolution Protocol)* e *HTTP (Hypertext Transfer Protocol)*.

1 Introdução

Numa primeira fase iremos tratar de analisar, com algum detalhe, uma serie de capturas de tramas feitas na rede eduroam, rede este responsável por fornecer acesso a Internet na Universidade do Minho, com o intuito de analisar e compreender o comportamento e pedidos/repostas que são gerados durante uma consulta ao portal do Departamento de Informática (http://www.di.uminho.pt). Para isso utilizamos como ferramenta de captura e analise de tramas o Wireshark, tal como sugerido e indicado na ficha. Depois iremos estudar o comportamento de uma rede fictícia, criada para o efeito, e animada através da aplicação CORE; o que vai permitir um estudo mais aprofundado de questões relacionadas com o domínio de colisão e pedidos/repostas associadas ao protocolo ARP. No entanto, temos que realçar que a captura das tramas que fizemos, embora não fosse o mais aconselhável, foi realizada através da rede Wi-Fi; felizmente o Wireshark é capaz de tratar devidamente a captura das tramas e permite, de uma forma eficiente, filtrar os pacotes por tipos, dessa forma, apesar do funcionamento da rede local sem fios ser "diferente" da rede local com fios, por exemplo nos pedidos ARP, os resultados apresentados conseguem, em certa medida, corresponder aquilo que é pretendido.

2 Captura e análise de Tramas *Ethernet*

Procedemos a utilização, tal como referido anteriormente, a ferramenta Wireshark para conseguir capturar e analisar as tramas associadas a Ethernet e com base nessas tramas, conseguir dar resposta as perguntas apresentadas mais abaixo. Vejamos, por exemplo, a seguinte captura de trafego, gerado durante uma pesquisa ao portal do Departamento Informático da Universidade do Minho (http://www.di.uminho.pt) e filtrando essa mesma captura apenas para o protocolo HTTP, temos então a seguinte captura:



2.1 Qual é o endereço *MAC* da interface activa do seu computador?

Com base na trama apresentada acima, especificamente no pacote relacionado com o HTTP GET, que contem a versão do HTTP utilizado pelo site, possivelmente numa tentativa de estabelecer o inicio da conexão entre o servidor que tem alojado os dados e o meu computador; podemos verificar, analisando o campo source do Ethernet II temos que o endereço MAC da minha interface de rede é o (28:e3:47:74:5c:46).

Poderíamos colocar aqui a questão em saber se de facto somos a fonte desse pacote, uma vez que estamos a efectuar a captura na rede Wi-Fi, mas felizmente o Wireshark filtra as tramas que não estão relacionadas com o nosso computador e dessa forma, consegue passar ilusão que "estamos conectados" por fios e que a captura corresponde a uma captura ponto a ponto entre o meu computador é o router. Portanto sabemos que os pacotes presentes nessa captura dizem respeito ao meu computador, ou seja, os endereços IP só estão associados ao meu computador ou a outro que envio e/ou recebeu os meus pacotes. E por exclusão de hipóteses, uma vez que eu sei a partida que o endereço IP do domínio associado ao site do departamento de informática é o 193.136.19.20, verifica-se trivialmente a partir da resolução de nomes do DNS, então como esse endereço IP no pacote está associado ao destino, tanto o endereço IP como MAC de origem têm necessariamente de serem os meus.

2.2 Qual é o endereço *MAC* destino da trama? Em sua opinião, a que sistema é destinada essa trama, ou dito de outra forma, será destinada ao endereço Ethernet do servidor HTTP para miei.di.uminho.pt?

Tal como referido anteriormente, sabemos que o endereço IP do servidor HTTP é o 193.136.19.20, por exemplo, através da resolução de nomes do DNS. E portanto poderíamos, erradamente, afirmar que o endereço MAC (00:d0:03:ff:94:00) presente no campo de destino no Ethernet II do pacote HTTP GET corresponderia ao do servidor. Porém, como sabemos que o servidor não se encontra na nossa rede local, esse endereço MAC de encaminhamento do pacote corresponde não ao do servidor, mas sim ao do router, que por sua vez é o responsável por encaminhar o pacote até ao destino pretendido através do protocolo TCP/IP e consequentemente da Internet.

2.3 Qual o valor hexadecimal presente no campo *Type* da trama *Ethenert*?

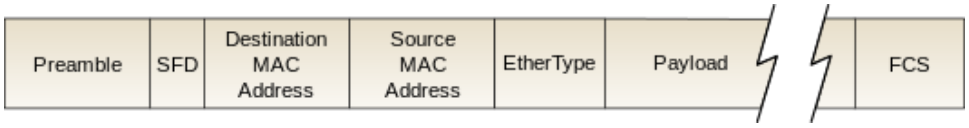
O valor desse campo é o (0x0800) que segundo o Wireshark wiki, a corresponde ao protocolo IPv4.

2.4 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*?

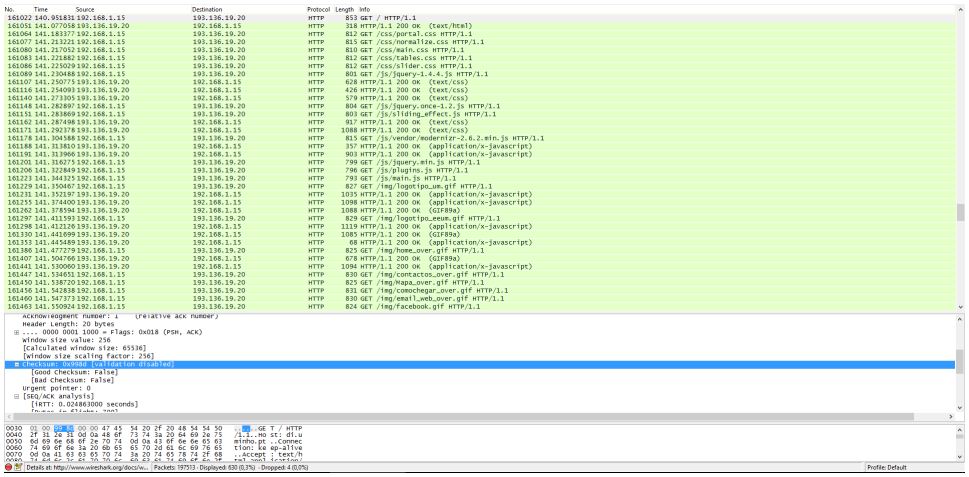
Sabemos que o caractere *ASCII* 'G' em hexadecimal tem o valor 47 é com base na informação detalhada do pacote e a respectiva correspondência *ASCII* e hexadecimal, parte inferior da captura do Wireshark, sabemos que ele ocorre na 4º linha é penúltima coluna e que cada linha tem 8 bytes, ou seja, na posição $(8 * 4) + 7 = 39$. Para além disso, sabemos que essa trama (frame 17) tem ao todo 450 bytes, informação essa também fornecida pelo Wireshark. Logo o overhead protocolar é igual $(39/450) * 100 = 8.(6)$, ou seja, cerca de aproximadamente $8,7\%$.

2.5 Em ligações com fios pouco susceptíveis a erros, nem sempre as NICs gero o código de detecção de erros. Verifique se o campo *FCS* está a ser utilizado?

Com base na seguinte imagem, podemos verificar que o *FCS (Frame Check Sequence)*, vem logo a seguir no *payload* do pacote:



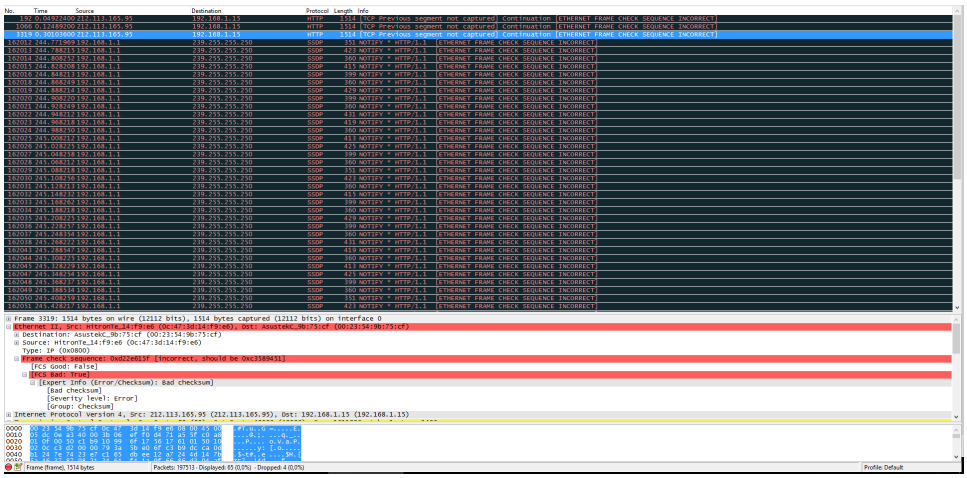
No entanto a indicação se o pacote utiliza ou não o campo *FCS* vem logo no preâmbulo, tal como indicado na figura abaixo:



Logo podemos afirmar, com certeza, que não estamos a utilizar o *FCS* nessa conexão.

2.6 Aceda à opção Edit/Preferences/Protocols/Ethernet e indique que é assumido o uso do campo FCS. Assumindo que o uso do campo *FCS*, verifique qual o valor hexadecimal desse campo? Que conlui?

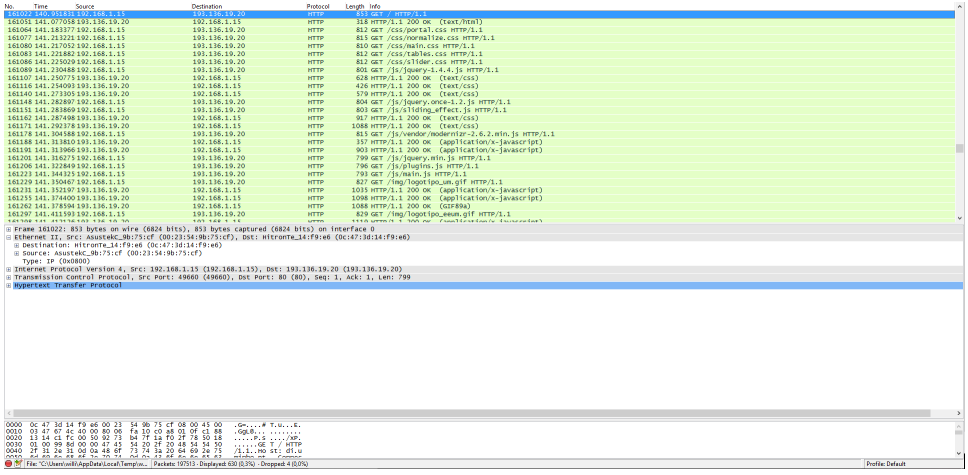
Procedendo a seguinte alteração temos a seguinte imagem:



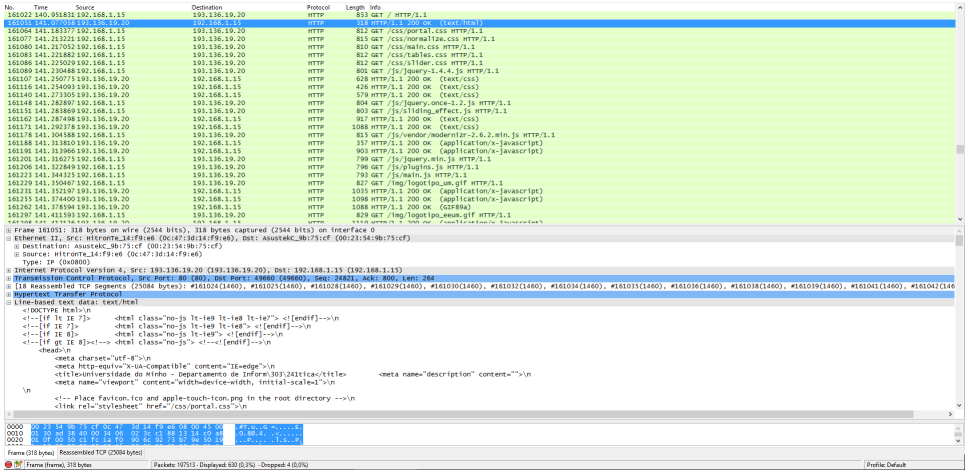
Como se pode verificar o valor hexadecimal desse campo é (0xd22e615f), no entanto, como essa alteração implica voltar a interpretar os pacotes como contendo o campo FCS quando na verdade eles não gerados pelos NICs essa valor, como se pode verificar também pelo Wireshark (0xd22e615f [incorrect, should be 0xc3589451]), logo este valor está incorrecto e trata-se de lixo uma vez que foi lido/interpretado mal todo o conteúdo das tramas, e consequentemente do pacote.

2.7 Qual é o endereço *Ethernet* da fonte? A que sistema de rede corresponde?

Para responder a essa questão e as seguintes, vamos proceder a duas novas capturas ao mesmo domínio, no entanto efecutado apenas em um computador diferente, apenas com o intuito de facilitar a análise. Temos então o primeiro HTTP GET efecutado pelo meu computador ao endereço IP 193.136.19.20, que como já referido anteriormente corresponde ao servidor HTTP do miei.di.uminho.pt, temos então a seguinte captura: -



Que tem como resposta, nesse caso logo a seguir mas podia não o ter sido assim, o seguinte pacote:



È fácil perceber que o endereço ethernet da fonte corresponde, nesse caso, ao endereço IP do servidor HTTP do miei.di.uminho.pt.

2.8 Qual é o endereço *MAC* do destino? Reconhece-o?

È o endereço de MAC do meu computador, que corresponderia ao endereço MAC da alínea anterior se tivesse sido feito a captura no mesmo computador. Infelizmente, devido a resolvermos essa alínea em aulas separadas e porventura num computador diferente, não nos é possível evidenciar tão bem o que é pretendido nessa alínea, i.e. a parte referente ao reconhecer que deveria ser o mesmo.

2.9 Qual é o valor hexadecimal do campo *Type* ?

Toma o valor (0x0800) que como já referido anteriormente corresponde a indicar que é do tipo IPv4.

2.10 Que tipo de resposta foi enviada pelo servidor?

Foi uma confirmação ao pedido efecutado pelo meu computador, ou seja, esta a indicar qual a versão do HTTP que o servidor utiliza e a enviar o inicio da informação HTML necessária para proceder a visualização da pagina web.

3 Protocolo ARP

3.1 O que significa cada uma das colunas?

3.2 Qual é o valor hexadecimal dos endereços origem e destino na trama *Ethernet* que contém a mensagem com o pedido *ARP (ARP Request)*?

3.3 Qual o valor hexadecimal do campo tipo da trama *Ethernet*?

3.4 Qual o valor do campo *ARP opcode*? O que especifica?

3.5 A mensagem *ARP* contém o endereço *IP* de origem?

3.6 Relativamente *ARP* que é a resposta ao pedido *ARP* efectuado:

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

Em que posição da mensagem *ARP* está a informação que responde ao pedido *ARP*?

3.7 Quais são os valores hexadecimais para os endereços origem e destino da trama que contém a resposta ARP?

4 ARP numa topologia CORE

4.1 Com auxílio do comando *ifconfig* obtenha os endereços *Ethernet* das interfaces dos diversos routers.

4.2 Usando o comando *arp* obtenha o contéudo das caches *arp* dos diversos sistemas.

4.3 Faça *ping* de n1 para n2. Que modificações observa nas caches *ARP* dos sistemas envolvidos.

4.4 Faça *ping* de n1 para n3. Consulte as caches *ARP*. Que conclui?

4.5 Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com o endereço *Ethernet* inexistente. O que acontece?

4.6 Faça *ping* de n5 para n6. Sem consultar a tabela *ARP* anote a entrada que, em sua opnião, é criada na tabela *ARP* de n5. Verifique se a sua interpretação sobre a operação da rede *Ethernet* e protocolo *ARP* estava correto.

5 ARP Gratuito

5.1 Identifique um pacote de pedido *ARP* gratuito originado pelo seu sistema. Verifique quantos pacotes *ARP* gratuito foram enviados e com que intervalo temporal?

5.2 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?

6 Domínios de colisão

6.1 Faça *ping* de n2 para n4. Verifique com a opção *tcpdump* como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

6.2 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.

7 Conclusão

According to Table 1...

(a) Delay and jiiter	(b) Delay and loss
(c) Delay and throughput	(d) Jitter and loss
(e) Jitter and throughput	(f) Loss and throughput

Figura 1. Tabela exemplo.

8 Conclusions

Neste trabalho...

Referências

1. Zadeh, L.: Fuzzy sets (1965)
2. Nguyen, H., Walker, E.: First course in fuzzy logic. Boca Raton: Chapman and Hall/CRC Press (1999)