**eTP3: Camada de Ligação Lógica: Ethernet e Protocolo ARP**

Filipa Correia Parente, José André Martins Pereira, Ricardo André Gomes Petronilho

University of Minho, Department of Informatics, 4710-057 Braga, Portugal e-mail: [{a82145,a82880,a81744}@alunos.uminho.pt](mailto:%7ba82145,a82880,a81744%7d@alunos.uminho.pt)

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



Figura 1 - Endereços MAC origem e destino.

**Resposta:**

O endereço MAC de origem é o **a0:8c:fd:fc:6b:36** como se pode observar na região a vermelho e o endereço MAC de destino é o **00:0c:29:d2:19:f0** como de pode observar na região a azul.

**2)** Identifique a que sistemas se referem. Justifique.

**Resposta:**

Os MAC address referidos acima referem-se à placa de rede (NIC), do nosso computador **(HewlettP)** e a do servidor **(Vmware)**.

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

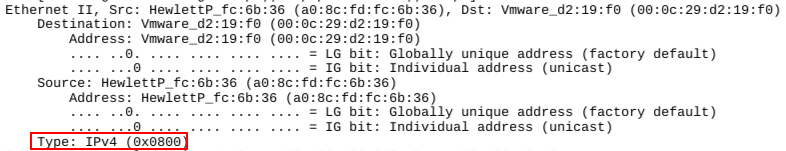


Figura 2 - Campo Type.

**Reposta:**

Identifica o tipo de encapsulamento usado para transportar os dados. Neste caso tem o valor **0x0800** o que significa que é um pacote do tipo **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.

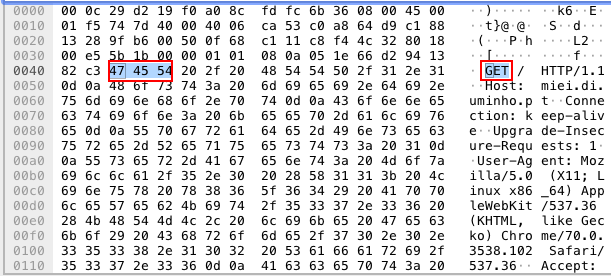


Figura 3 – Pacote.

**Reposta:**

Desde o início da trama até ao caracter ASCII “G” são usados **66 B**. O tamanho total do pacote são **515 B** sendo que o tamanho da sobrecarga introduzida pela pilha protocolar são **66 B**, desta forma a percentagem de sobrecarga é dada por 66 / 515 = 0.1282 logo existe **12.82 %** de “overhead”.

**5)** Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para deteção de erros não está a ser usado. Em sua opinião, porque será?

**Resposta:**

Verificamos que o campo FCS não está a ser usado, visto que a rede é composta por cabos, logo é bastante robusta garantindo transmissões de boa qualidade, não necessitando de deteção de erros.

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



Figura 4 – Pacote HTTP enviado pelo servidor.

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

**Resposta:**

O endereço Ethernet ou endereço MAC da fonte é o **00:0c:29:d2:19:f0** como se pode observar na região a vermelho (Figura 4), e corresponde ao servidor.

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

**Resposta:**

O endereço MAC do destino é o **a0:8c:fd:fc:6b:36** como se pode observar na região a azul (Figura 4) , e corresponde ao nosso computador.

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

**Resposta:**

De acordo com análise da captura identificou-se o protocolo **Ethernet II, IPv4, TCP, HTTP**.

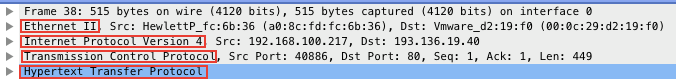


Figura 5 – Protocolos contidos na trama recebida.

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

**Resposta:**



Figura 6 – Output do comando arp -a

A primeira coluna corresponde ao DNS - Domain Name System **(gw.sa.di.uminho.pt)** do endereço IP da segunda coluna **(192.168.100.254)**, a terceira coluna corresponde ao endereço **MAC (0:c:29:d2:19:f0)**, e a quarta coluna identifica a interface rede que a máquina está a usar **(en3)** , e a última coluna identificao protocolo **Ethernet** .

**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?

**Resposta:**



Figura 7 – Pacotes ARP capturados.

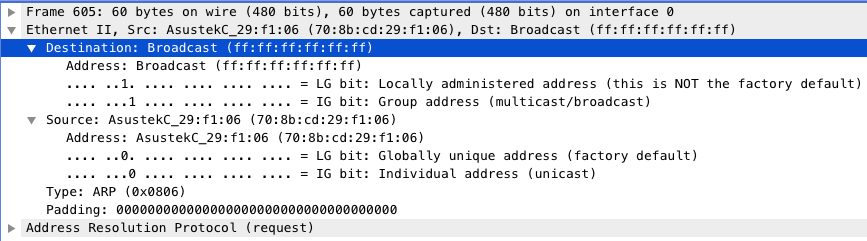


Figura 8 – ARP Request.

O valor do endereço origem é **(70:8b:cd:29:f1:06)** e o destino é **(ff:ff:ff:ff:ff:ff)**. O endereço destino usado é o broadcast, uma vez que o pedido **ARP Request** é enviado a todos endereços da rede, com o objetivo do recetor identificar-se através de um **ARP Reply**, caso esse tenha o IP procurado.

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

**Resposta:**

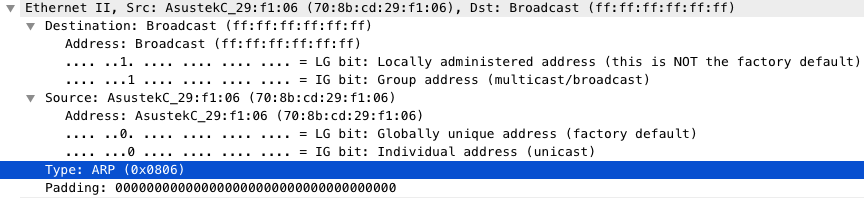


Figura 9 – O campo do Type.

O valor do campo Type é 0x0806 e indica o tipo de dados encapsulado, que neste caso corresponde ao protocolo ARP (Address Resolution Protocol).

1. Qual o valor do campo ARP *opcode*? O que especifica? Se necessário, consulte a RFC do protocolo ARP http://tools.ietf.org/html/rfc826.html.

**Resposta:**

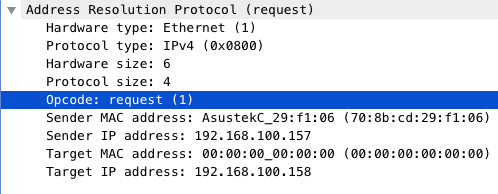
****

Figura 10 – Campo Opcode.

O valor do campo Opcode é 1 e especifica o tipo mensagem **ARP**, que pode ser **REQUEST** ou **REPLY**. Como se pode observar na Figura 10, o tipo neste caso **é REQUEST**(1).

1. Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

**Resposta:**

Os endereços contidos na mensagem **ARP** são: **Sender MAC address (70:8b:cd:29:f1:06)**, **Sender IP address (192.168.100.157)**, **Target MAC address (00:00:00:00:00:00)**, **Target IP address (192.168.100.158)**. Conclui-se que o campo **Target MAC address** está a zeros, pois ainda não foi encontrado o seu **MAC address**, pois isto é a mensagem **REQUEST(1)**.

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

**Resposta:**

O host de origem “questiona” todos os dispositivos (broadcast) conectados à rede, qual o dispositivo com o endereço IP procurado, que neste caso é o da nossa máquina **(192.168.100.158)**.

1. Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.
   1. Qual o valor do campo ARP *opcode*? O que especifica?

**Resposta:**

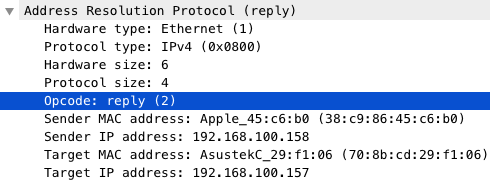
****

Figura 11 – Campo Opcode

* 1. Em que posição da mensagem ARP está a resposta ao pedido ARP ?

**Resposta:**

A resposta do ARP está no campo Target **MAC address (70:8b:cd:29:f1:06)**, como se pode observar na Figura 11

1. 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?

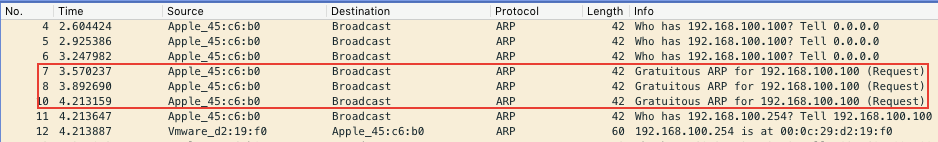
**Resposta:**

Figura 12 – Pacotes ARP Gratuitos.

O campo **Sender IP address** e **Target IP address** têm o mesmo valor, uma vez que, o endereço procurado pelo pedido **ARP** é igual ao endereço da própria máquina.

O resultado esperado é não ter resposta, uma vez que, se houver significa que o **endereço IP** que sugerimos está a ser ocupado por outro dispositivo, o que origina conflitos.

Através do **ARP Gratuito** é esperado que os dispositivos de nível 2, que tenham tabelas de endereçamento **MAC,** como por exemplo **switchs**, ou mesmo **hosts** sejam atualizadas

1. Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

**Resposta:**

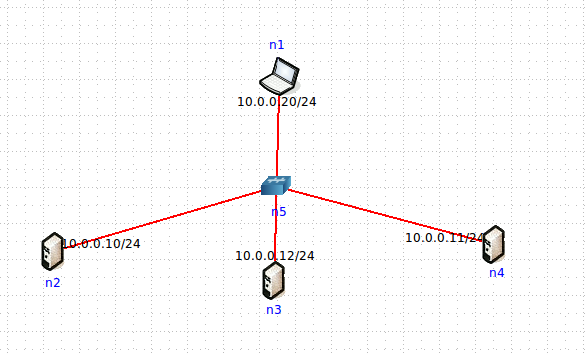


Figura 12 – Comando ping no

Figura 13 – Topologia Core com Hub.

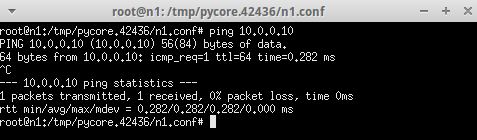


Figura 14 – Comando ping através da Shell de n1.

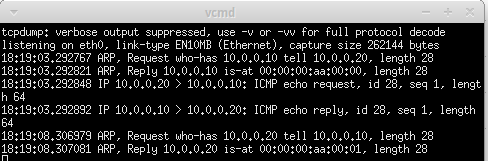


Figura 15 – Tráfego capturado em n3.

Assim, conclui-se que com a utilização de um Hub, qualquer envio de mensagem entre dispositivos irá ser enviado para todos os dispositivos conectados à rede. Isto pode ser observado com as **Figuras 13 e 14**, onde se fez um **ping** do **laptop n1** para o **servidor n2** **(10.0.0.10)**, e ao analisar o tráfego no **servidor n3**, verificou-se que este captura os pacotes enviados, de **n1** para **n2**, e o mesmo se verifica no servidor n4.

1. 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. Documente as suas observações e conclusões com base no tráfego observado/capturado.

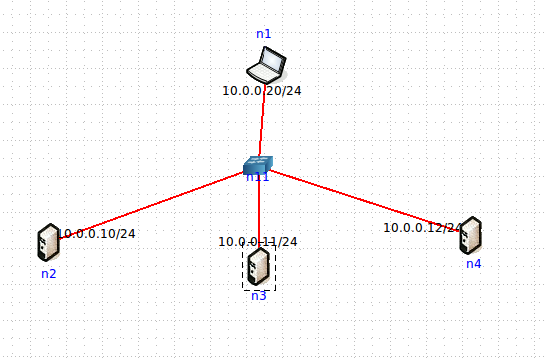
**Resposta:**

Figura 16 – Topologia Core com switch.

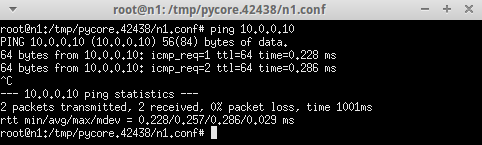


Figura 17 – Comando ping de n1 para n2 (10.0.0.10).

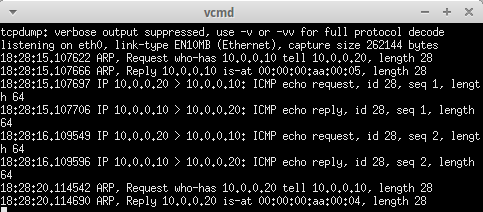


Figura 18 – Tráfego em n2.

Como se pode observar na **Figura 16** executou-se um **ping** do **laptop n1** para **servidor n2**. Deste modo, em **n2** foi capturado o tráfego que se pode observar na **Figura 17**, onde está incluído pacotes de **ARP request** e **reply**, responsáveis pela identificação dos MAC address dos dispositivos envolvidos e também os pacotes ICMP que retornam a informação do comando ping.

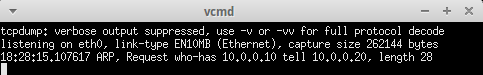


Figura 19 – Tráfego em n3.

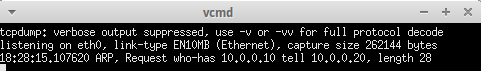


Figura 20 – Tráfego em n4.

Ao contrário do aconteceu no exercício 17, como se está a utilizar um switch, significa que envios realizados entre dispositivos, apenas são capturados nestes.

Isto verifica-se nas **Figuras 18** e **19**, onde se pode observar que apenas se capturou o pacote **ARP Request**, pois este foi enviado para **broadcast**, no entanto, não receberam os **ARP Reply** e **ICMP** enviados pelo **servidor n2**, sendo que este respondeu ao **laptop n1** para informar que é o dispositivo com o **endereço IP** que ele procura.

Isto acontece, visto que o **switch** reserva uma porta única para cada dispositivo, evitando assim o envio de dados para dispositivos, que não são o destino pretendido e reduzir as colisões.

**Conclusões:**

A realização do trabalho prático três permitiu uma melhor perceção dos conceitos **Ethernet** e do protocolo **ARP**. A nível de **Ethernet** aprendeu-se que todos os dispositivos são identificados por endereço único, associado à placa de rede **(NIC)** denominado por **MAC address**.

Compreendeu-se que a utilização do protocolo **ARP**, para identificação de **MAC address** numa rede, com mensagens de **ARP Request** e **Reply**, permite descobrir **os MAC address** dos dispositivos de modo que se consiga comunicar entre estes sem a necessidade da utilização do **endereço IP**.

O uso de **ARP Gratuitos**, permite aos dispositivos verificar a disponibilidade de um **endereço IP** numa rede, e também evitar a colisões entre mensagens dos mesmos.

Do mesmo modo, o **ARP Gratuito**, informa todos os dispositivos (**hosts e switchs**) de um novo endereço, com objetivo destes atualizarem as suas tabelas.

Verificou-se também no último exercício, as técnicas utilizadas para o controlo de colisões, tais como a utilização de **switchs**, e as suas diferenças em relação aos **hubs**.