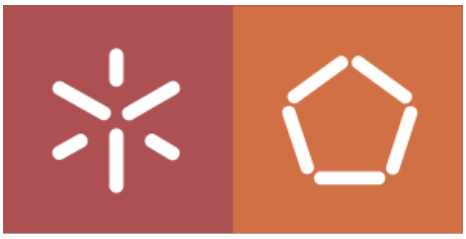

Universidade do Minho
Escola de Engenharia

Redes de Computadores TP3

Novembro de 2019


Ana Margarida Campos


Ana Catarina Gil


Tânia Rocha

1 Captura e análise de tramas Ethernet

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

Origem: 3c:52:82:e5:bc:4c
Destino: 00:0c:29:d2:19:f0

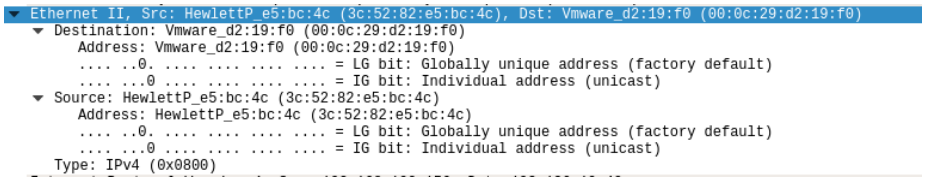

Figure 1: Endereços MAC de origem e destino

1.2 Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem corresponde ao nosso computador e o de destino corresponde ao router.

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

O valor hexadecimal do campo Type é 0x0800 e indica o tipo de encapsulamento (IPv4 neste caso).

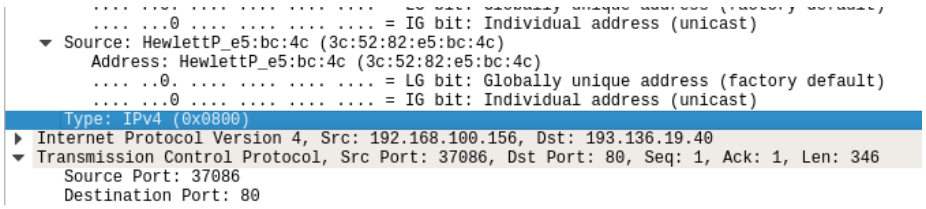

Figure 2: Valor hexadecimal do campo Type

1.4 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.

Até ao carater "G" (ascii:0x47) são usados 66 bytes. No total são usados 412 bytes, logo a percentagem de sobrecarga é de (66/412)*100 = 16,02

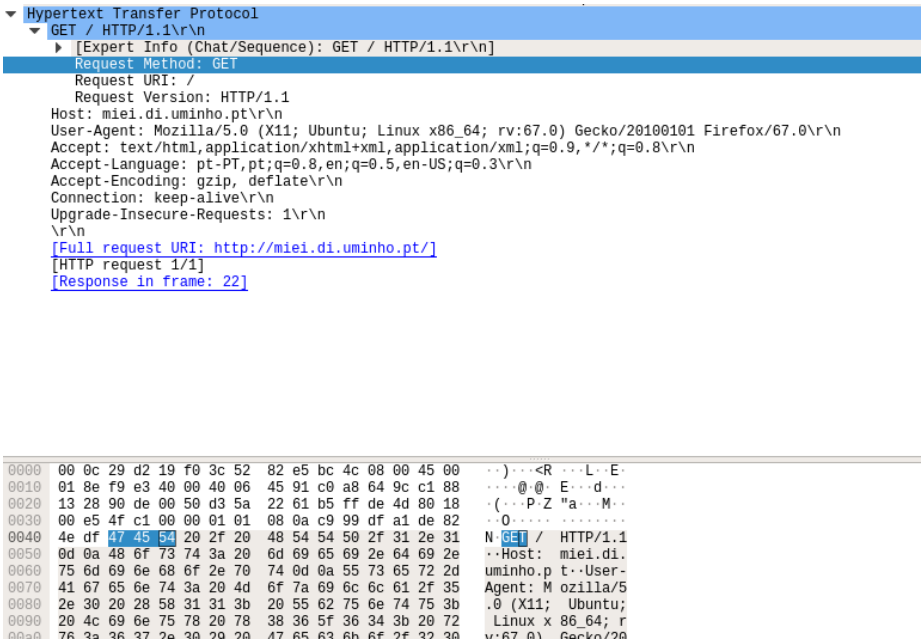

Figure 3: Pilha protocolar no envio HTTP GET

1.5 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?

Não aparece porque estamos numa ligação Ethernet um quadro danificado deve ser descartado.

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

Endereço Ethernet da fonte = 00:0c:29:d2:19:f0
Corresponde ao router da rede local.

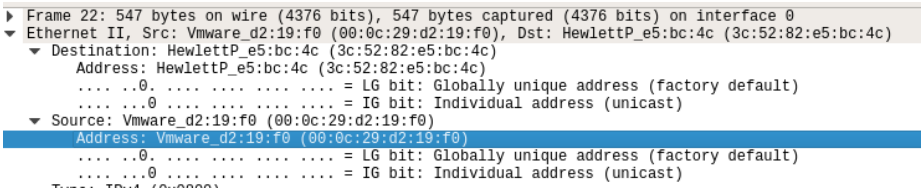

Figure 4: Endereço Ethernet

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

O endereço MAC do destino = 3c:52:82:e5:bc:4c
Este mesmo corresponde ao IP do nosso computador.

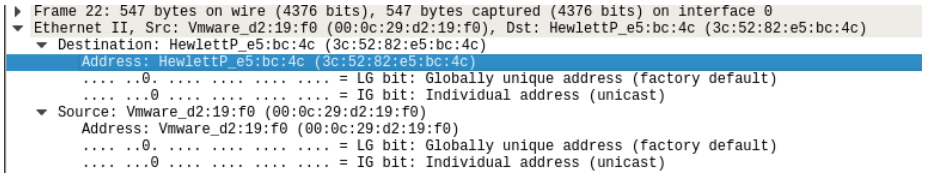

Figure 5: Endereço Mac do destino.

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

Os vários protocolos contidos na trama recebida são IPv4 ,TCP e HTTP.

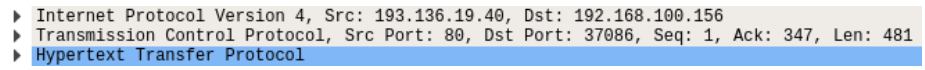

Figure 6: Protocolos contidos na trama.

2 Protocolo ARP

2.1 Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.

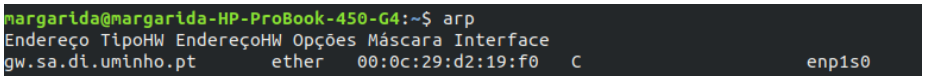

Figure 7: Comando arp.

Nota : Conforme confirmado na aula prática, o nosso computador não estava a executar o comando arp corretamente. Tal se verifica na fig.7. Mesmo assim, através de pesquisa conseguimos responder à questão.

Coluna Endereço : Representa o endereço IP do destino.

Coluna tipoWH : Representa o meio de ligação até ao destino.

Coluna EndereçoHW : Representa o MAC adress do destino.

Coluna Mascara : Representa o tipo de entrada.

Coluna Interface : Representa o tipo de interface.

2.2 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?

Como observado na figura o valor hexadecimal do destino é 0c:9d:92:35:f2:fb e o da origem é 3c:52:82:e5:bc:4c. Estes valores representam os endereços MAC. O endereço do destino Mac é para onde estamos a testar o ping.

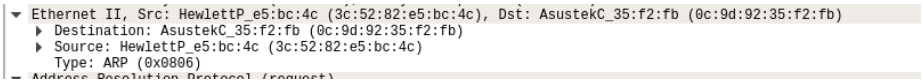

Figure 8: Valores Hexadécimais dos endereços de origem e de destino.

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

Como observado na figura anterior, o valor do campo tipo da trama Ethernet é ARP(0x0806). Isto indica qual o protocolo utilizado.

2.4 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)

O valor do campo ARP opcode é Request(1). Isto significa que, neste caso, a trama tem como objetivo o pedido do endereço MAC destino da trama em questão. RFC é um método de conversão de endereços IP em endereços Ethernet.

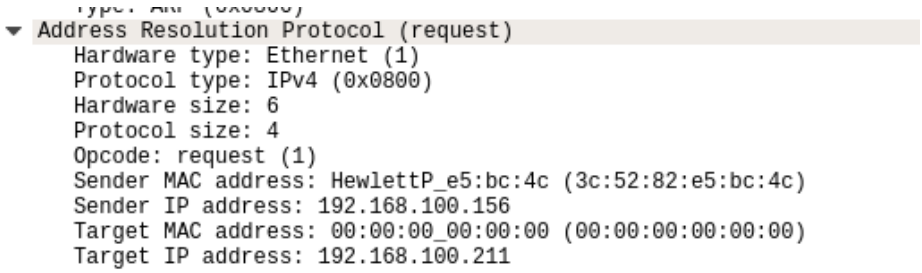

Figure 9: Valor do campo ARP code.

2.5 Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

Os endereços contidos na mensagem ARP são o IP e o MAC da origem e do destino. Ou seja os endereços que permitem a troca de tramas entre estes.

2.6 Explicite que tipo de pedido ou pergunta é feito pelo host de origem?

O host de origem pede o endereço MAC para o qual pretende enviar a trama.

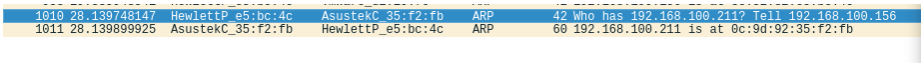

Figure 10: Host de origem.

2.7 Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.

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

Neste caso, o valor do campo ARP opcode é Reply(2).

Figure 11: Mensagem ARP.

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

A posição da mensagem ARP encontra-se desde os 23 aos 28 bytes.

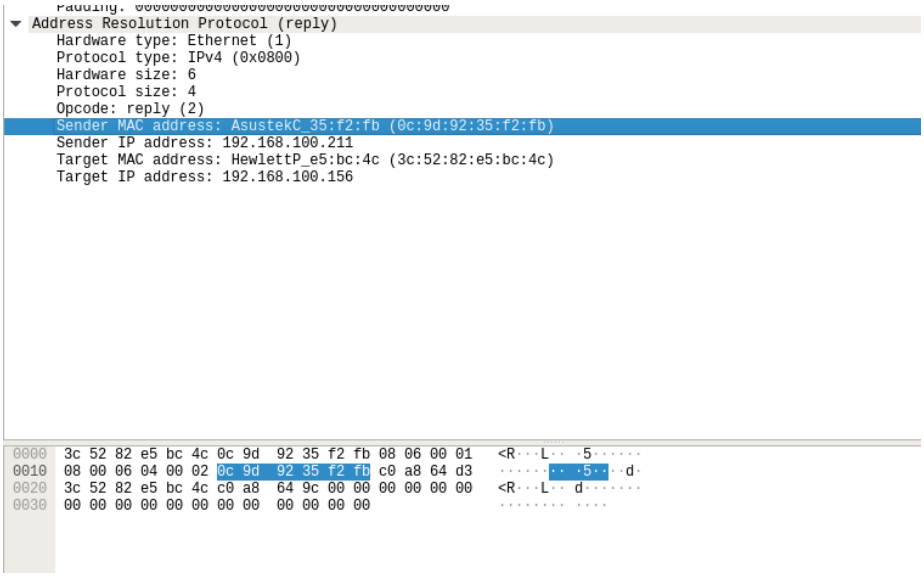

Figure 12: Mensagem ARP.

2.8 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?

Com a utilização do comando arping -U 192.168.100.156 (o IP da nossa maquina), obtivemos ARP's gratuitos. O que diferencia o pedido ARP gratuito dos restantes pedidos é que no pedido ARP gratuito existe uma flag Is gratuitouss: True e apresenta endereço de destino igual ao de origem. Prevê-se que não exista resposta por parte deste ARP gratuito, pois isso significaria que existe algo na rede com um IP igual ao da nossa máquina.

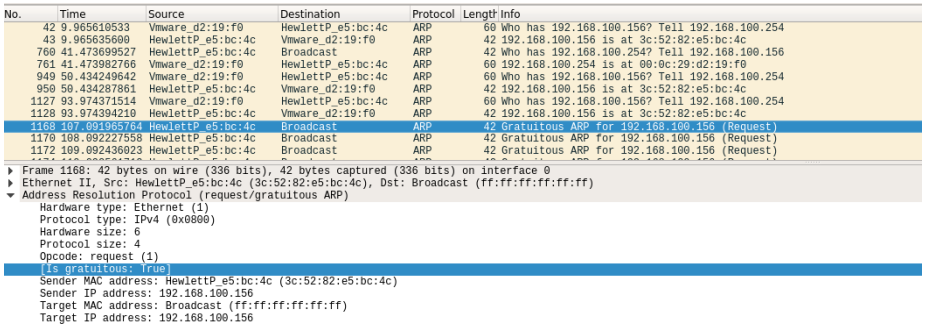

Figure 13: ARP Gratuito.

3 Domínios de colisão

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

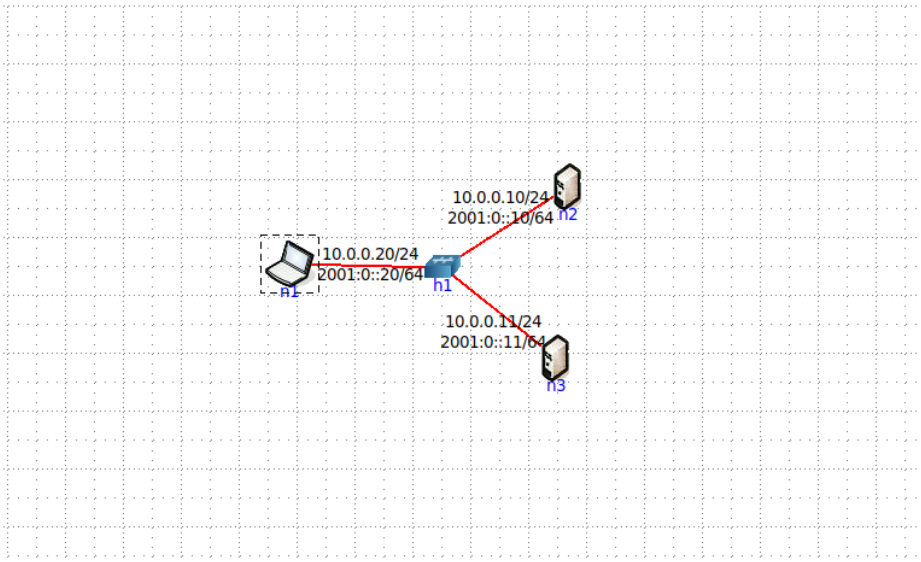

Figure 14: Mensagem ARP.

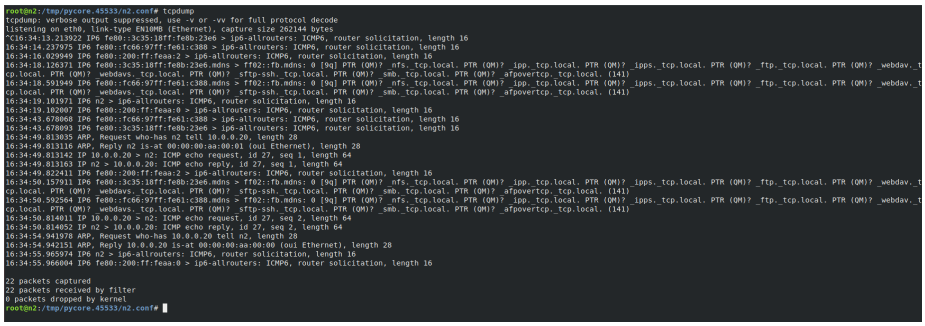

Figure 15: tcpdump no servidor n2.

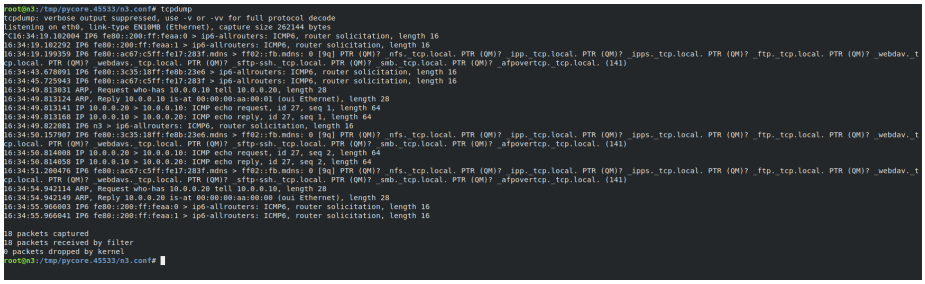

Figure 16: tcpdump no servidor n3.

Como se pode observar nas figuras, notamos que todos os servidores recebem pacotes quando é efetuado ping do laptop n1 para o servidor n2 com recorrencia ao comando tcpdump.

Isto deve-se ao facto de que quando o hub recebe um pacote de dados, este reencaminha os mesmos para todos os diapositivos que se encontram na mesma rede.

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

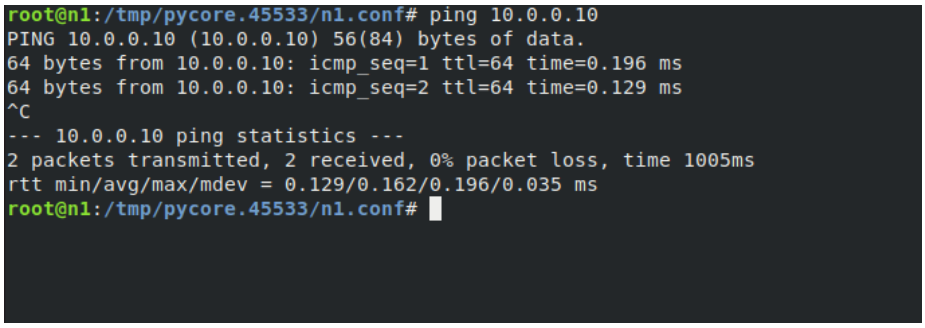

Figure 17: ping de n1 para n2

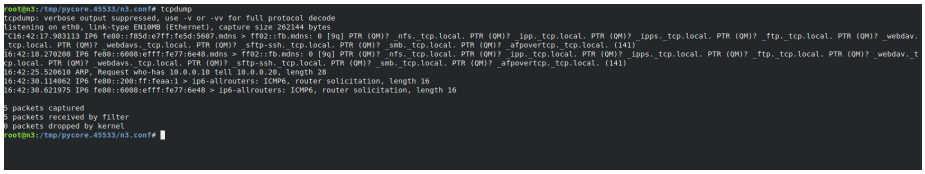

Figure 18: tcpdump no servidor n3.

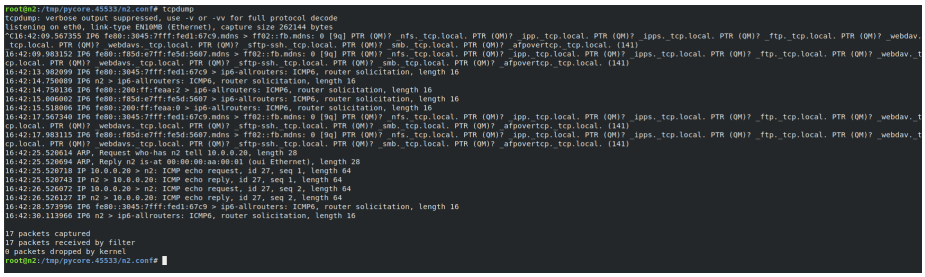

Figure 19: tcpdump no servidor n2.

Nas figuras apresentadas anteriormente, é possível observar que ao fazer ping do laptop n1 para o servidor n2, os pacotes são todos entregues ao destino pretendido, que neste caso é o n2.Reparamos que, o n3, apenas recebe os protocolos que ele necessita. Tal é possível, pois a mensagem é enviada para o switch que a envia diretamente para o host. Os switches ao limitar o envio da mensagem apenas para o destino pretendido, reduzem a possibilidade de colisão. Assim, podemos concluir que os switches são mais viáveis do que os hubs.

4 Conclusão

Com a realização deste trabalho conseguimos aprofundar conhecimentos acerca dos endereços MAC, ARP, Ethernet e interligações de redes locais. Isto deve-se, ao facto de para a resposta às questões do enunciado termos de efetuar capturas e as fazer as respetivas análises de tramas Ethernet com auxilio do software wireshark.

Utilizamos também a ferramenta CORE para podermos comparara eficácia da utilização dos switchs e hubs na diminuíção de colisões de tramas Ethernet.