Universidade do Minho

Mestrado Integrado em Engenharia Informática

TP3: Camada de Ligação Lógica: Ethernet e Protocolo ARP

Redes de Computadores

Grupo 1 – PL4

Ana Pereira A81712

Ana Ribeiro A82474

Jéssica Lemos A82061

1 Questões e Respostas

3. Captura e análise de Tramas Ethernet

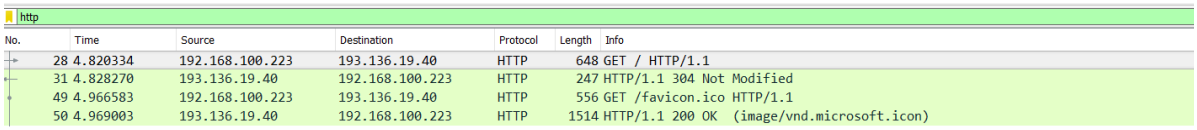

Figura 1 - Captura de Tramas Ethernet de mensagens HTTP

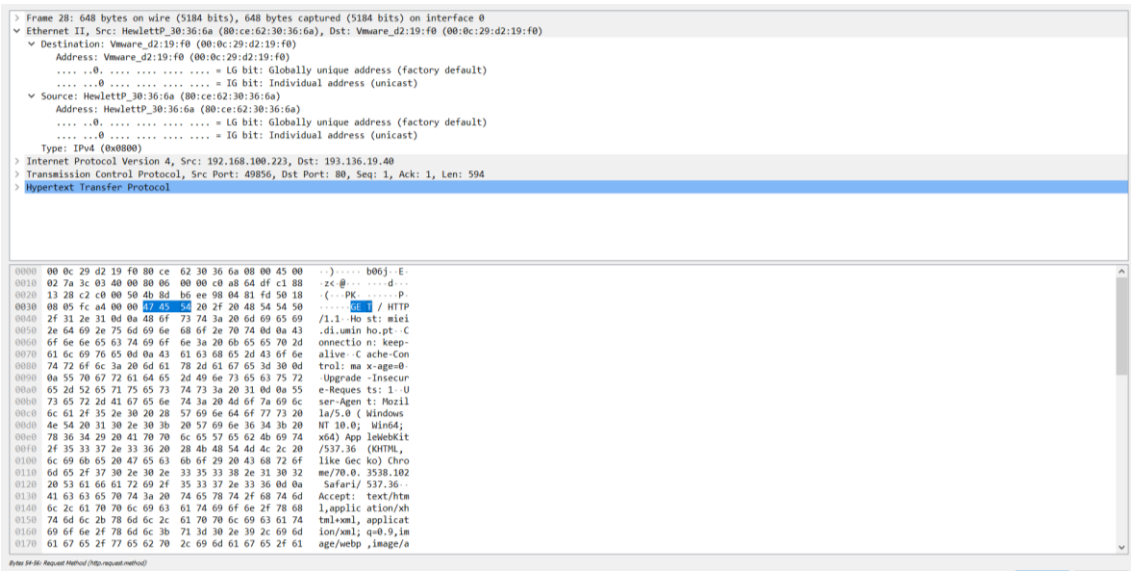

Figura 2 - Trama Ethernet que contém a mensagem HTTP GET

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

Como podemos observar na Figura 2, o endereço MAC de origem é 80:ce:62:30:36:6a e de destino 00:0c:29:d2:19:f0.

2. Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem, que é indicado no campo *Source*, corresponde ao da interface da nossa máquina nativa. Enquanto que o de destino, referente ao campo *Destination*, é o router da rede local à qual estamos ligados.

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

O valor do campo Type da trama Ethernet é 0x0800 e indica qual o protocolo utilizado ao nível de rede, ou seja, 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.

Desde o início da trama até ao caractere ASCII “G” são usados 54 bytes. Como no total, são utilizados 648 bytes, podemos verificar que a sobrecarga introduzida pela pilha é: (54/648) * 100 ≈ 8.333 %

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?

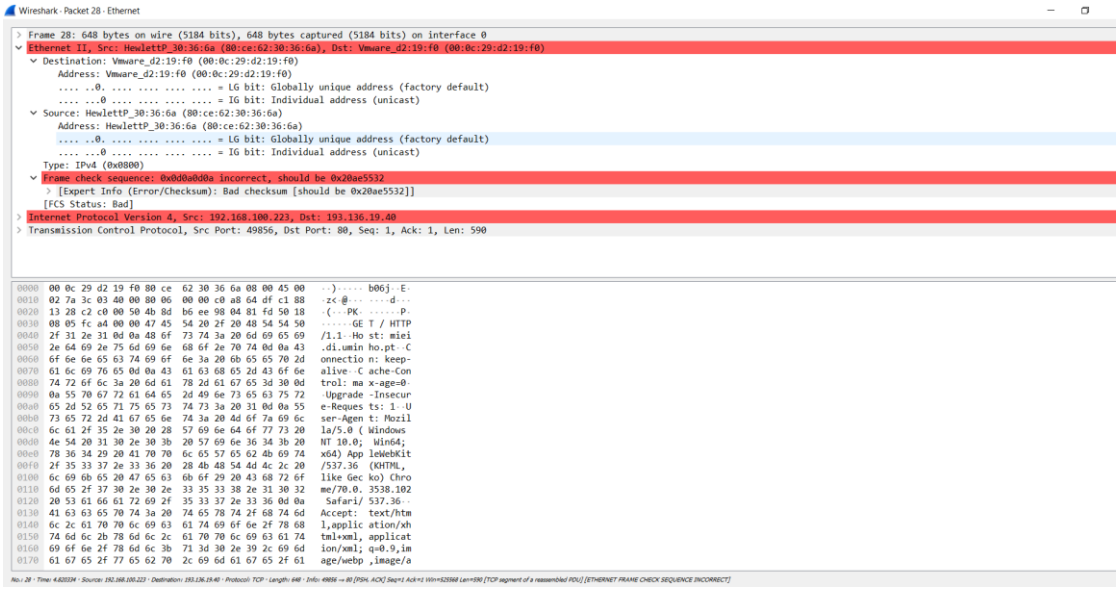

Figura 3 - Visualização da trama em análise

Como podemos verificar na Figura 3, o valor do campo FCS é 0x0d0a0d0a. Desta forma, o Wireshark indica que existe um erro na trama quando estipulamos que este deve interpretar os últimos bytes da trama como FCS. Assim, este campo não está a ser utilizado para controlo de erros. É raro existirem erros no meio cabelado, pelo que não compensa a utilização deste campo.

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

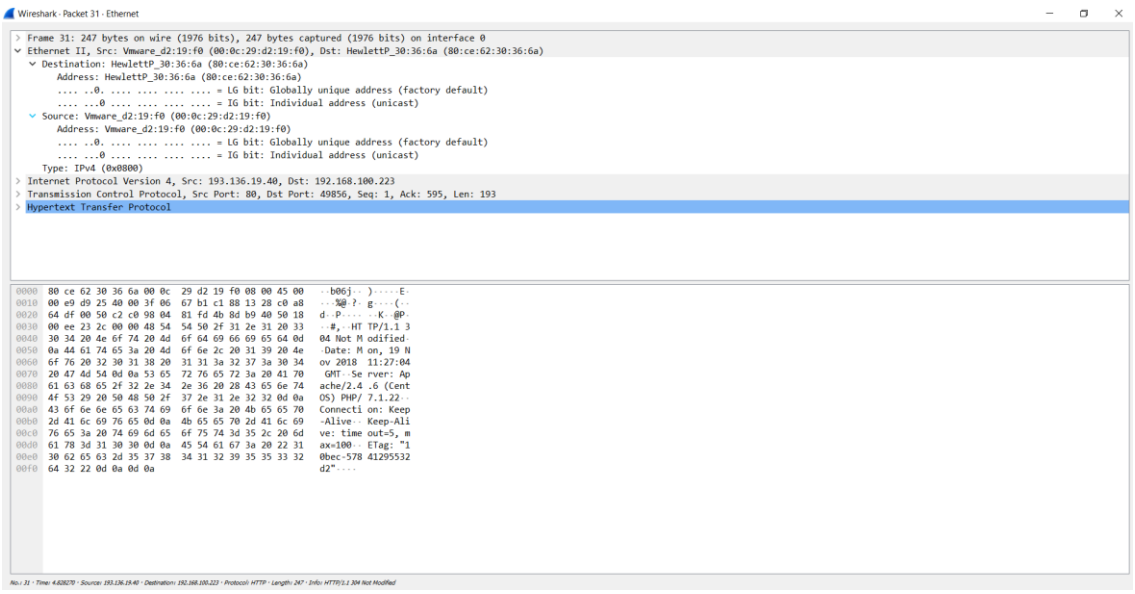

Figura 4 - Trama Ethernet que contém o primeiro byte da resposta HTTP

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

O endereço Ethernet da fonte, que é indicado no campo *Source*, é 00:0c:29:d2:19:f0, que corresponde ao router da rede local à qual estamos ligados.

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

O endereço de destino é 80:ce:62:30:36:6a, que representa a interface ativa da nossa máquina nativa.

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

Como podemos observar na Figura 4, os protocolos contidos na trama recebida são: Ethernet II, IPv4 (Internet Protocol Version 4), TCP (Transmission Control Protocol) e HTTP (Hypertext Transfer Protocol).

4. Protocolo ARP

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

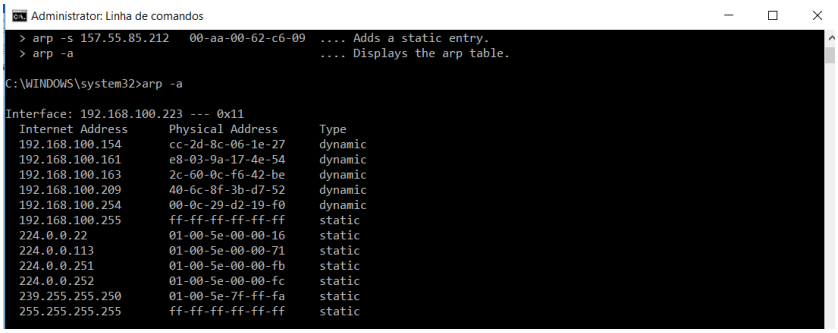

Figura 5 - Tabela ARP

A tabela ARP mapeia o endereço IP para o endereço MAC dos sistemas que comunicaram recentemente. Assim, a primeira coluna representa o endereço IP, a segunda o endereço MAC e a terceira o tipo de endereçamento que está a ser utilizado.

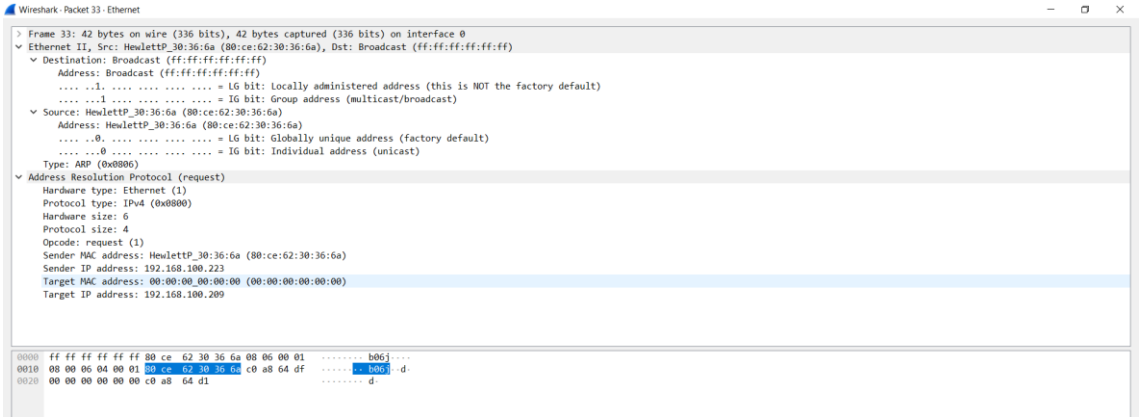

Figura 6 - Trama Ethernet que contém a mensagem com o pedido ARP (ARP Request)

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?

O valor do endereço de origem é 80:ce:62:30:36:6a e o de destino é ff:ff:ff:ff:ff:ff como podemos verificar na Figura 6. Este endereço de destino leva a que todos os endereços conectados à rede recebam a mensagem com o pedido, contudo só o endereço pretendido responde com o seu endereço MAC.

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

O valor do campo tipo da trama é 0x0806, como podemos verificar na Figura 6, sugerindo que o campo de dados pertence ao ARP.

12. 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.

Como podemos observar na Figura 6, o valor do campo ARP opcode é 0x0001, que indica se é um pedido ou uma resposta. Neste caso, corresponde a um pedido.

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

A mensagem ARP contém os endereços IP do destino e da origem, no entanto apenas é conhecido o endereço MAC correspondente do endereço IP da origem, dado que é um ARP request.

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

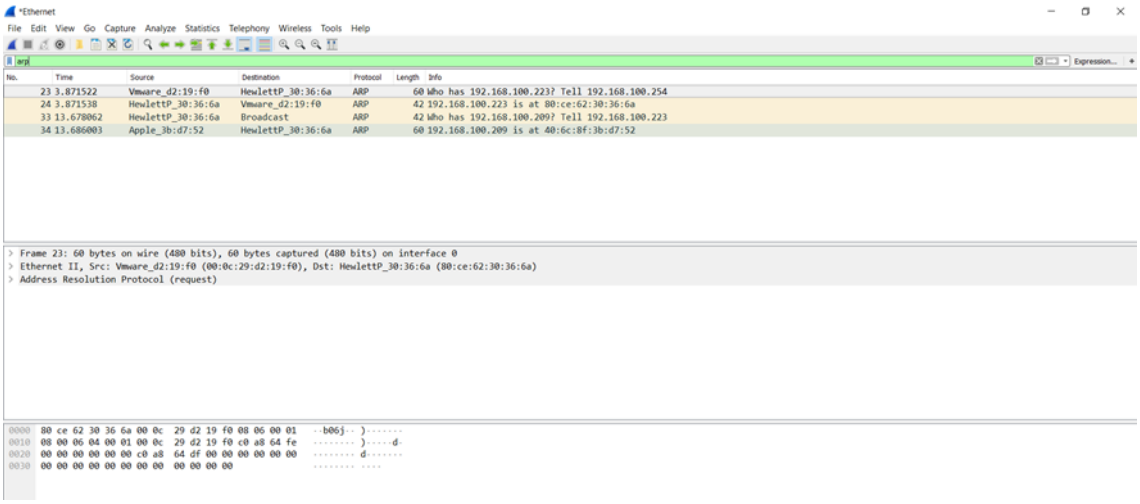

Figura 7 - Tráfego ARP

A nossa máquina pergunta “Quem tem o endereço 192.168.100.209? Diga 192.168.100.223”. Em resposta iremos obter o endereço MAC do equipamento com o endereço indicado.

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

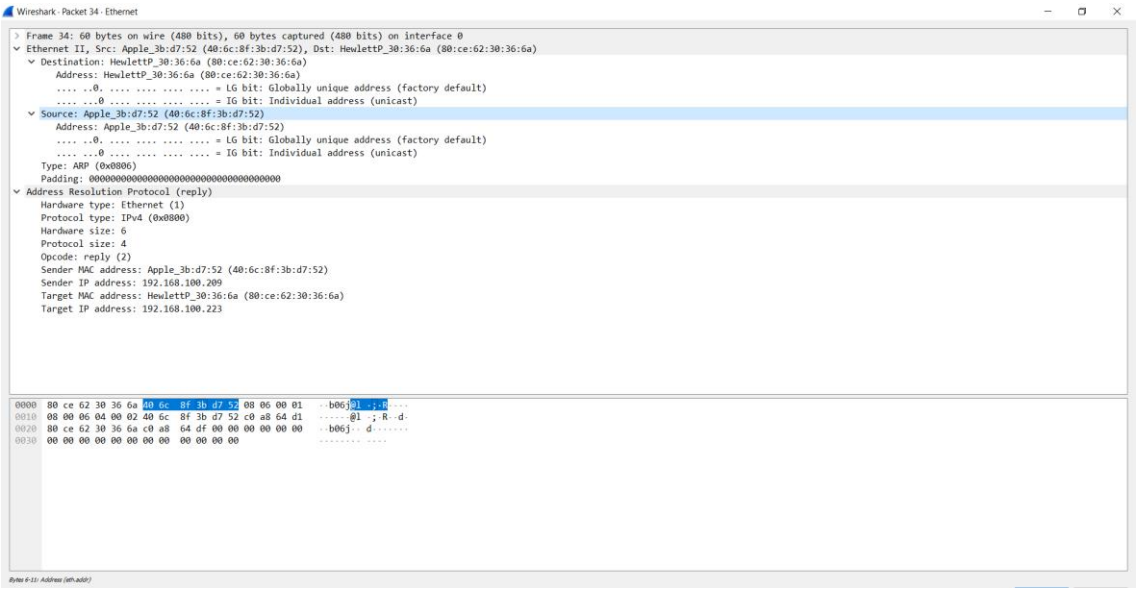

Figura 8 - Mensagem ARP que é a resposta ao pedido ARP efectuado

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

O valor do campo ARP opcode é 0x0002, indicando que se trata de uma resposta ao pedido ARP realizado.

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

Como podemos observar na Figura 8, a resposta ao pedido ARP está compreendido dos bytes 6 a 11.

5. ARP Gratuito

16. 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?

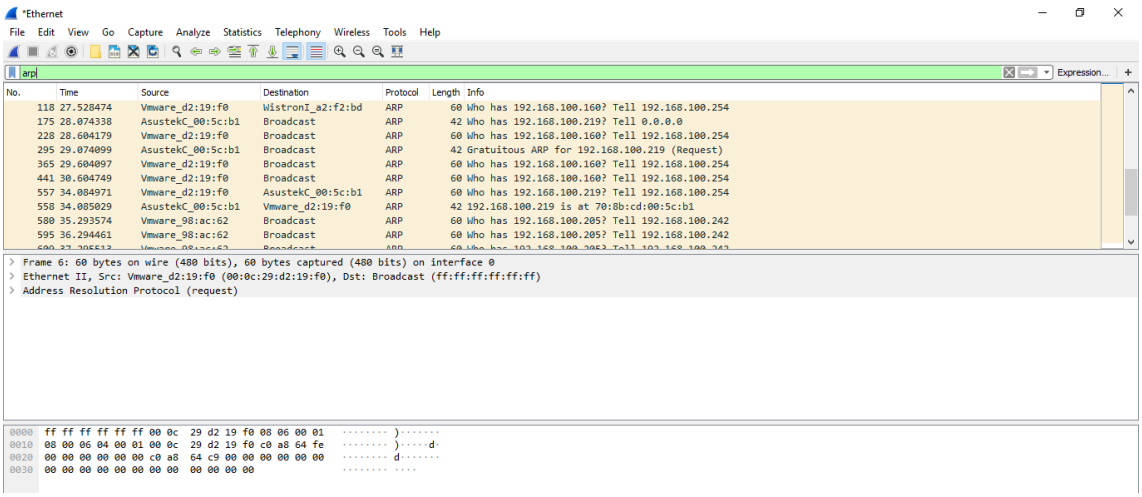

Figura 9 - Captura de tráfego

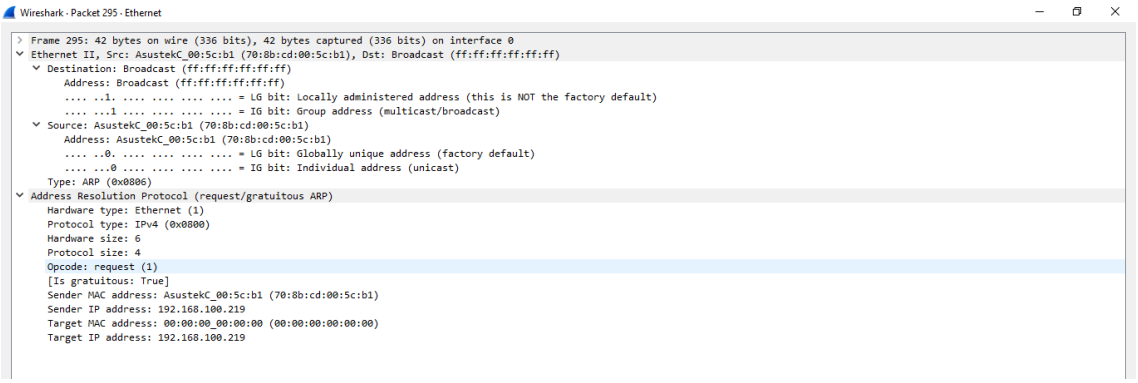

Figura 10 - Pedido ARP gratuito

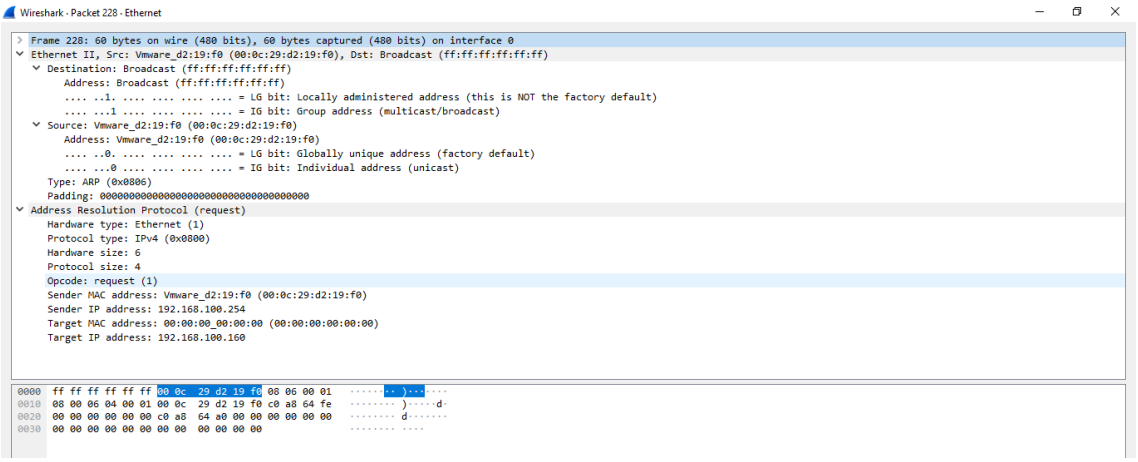

Figura 11 - Pedido ARP

Como podemos verificar nas Figuras 10 e 11, o que diferencia o pedido ARP gratuito dos restantes pedidos é que no pedido ARP gratuito existe uma flag *Is gratuitous: True* e apresenta endereço de destino igual ao de origem. É esperado que não exista resposta ao pedido ARP gratuito uma vez que se tal acontecesse significaria que há um sistema na rede com o endereço IP igual ao nosso, que indicaria um conflito na rede local.

6. Domínios de colisão

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

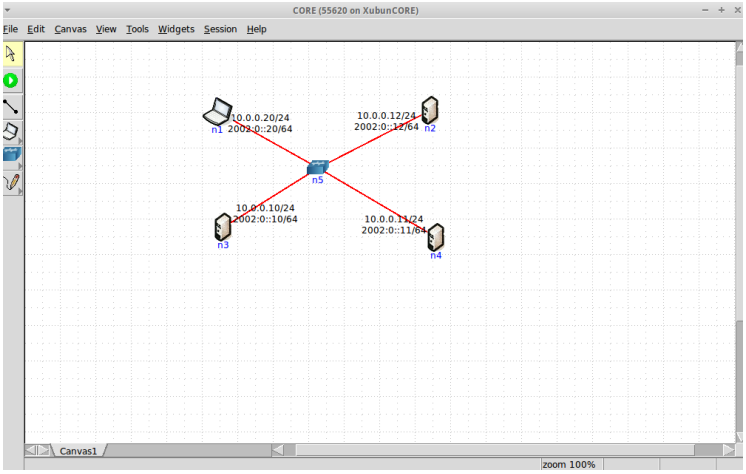

Figura 12 - Topologia CORE

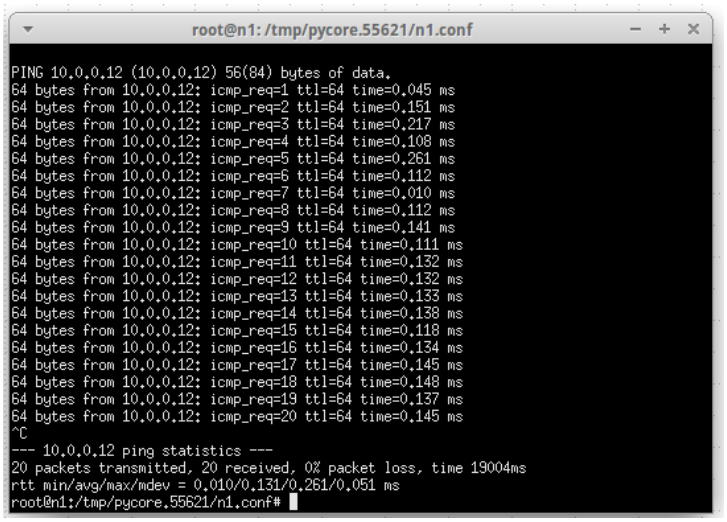

Figura 13 - Ping do laptop n1 para o servidor n2

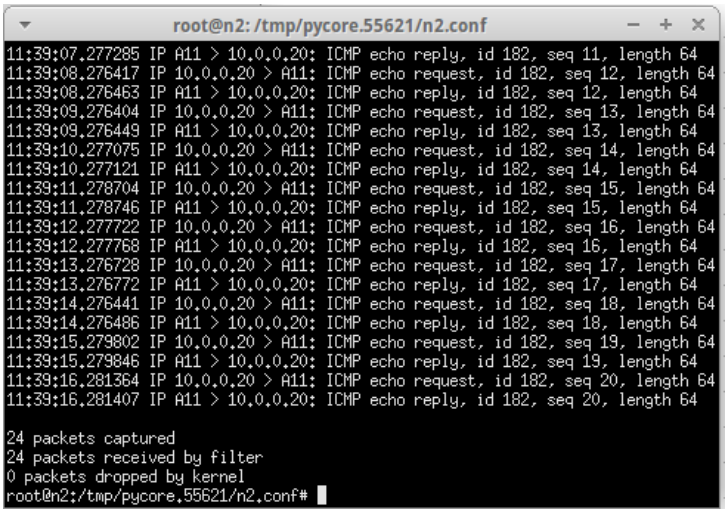

Figura 14 - tcpdump no servidor n2

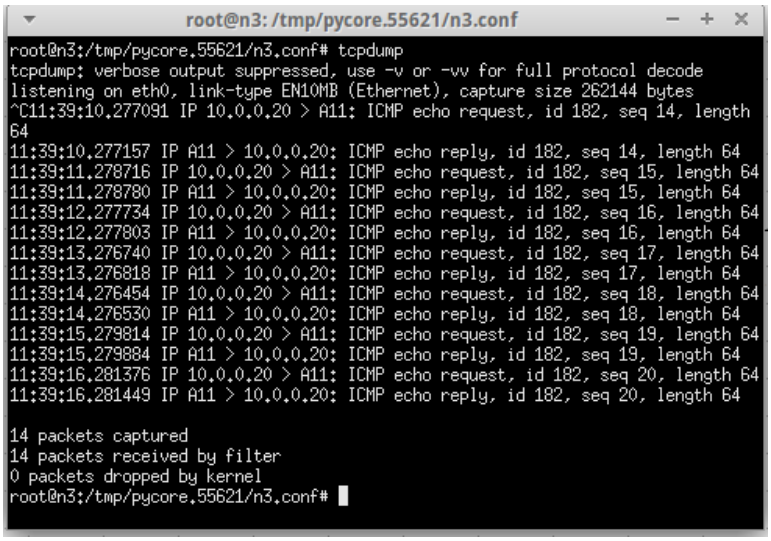

Figura 15 - tcpdum no servidor n3

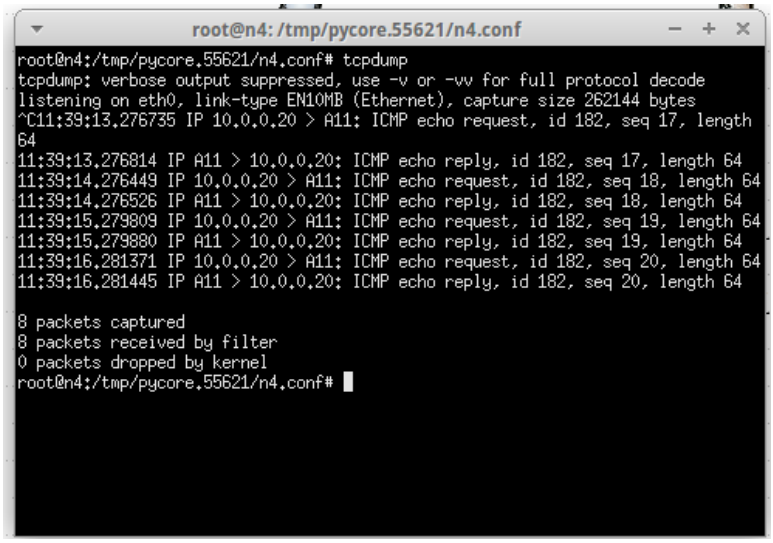

Figura 16 - tcpdump no servidor s4

Como podemos verificar nas figuras anteriormente apresentadas, ao fazer *ping* do laptop n1 para o servidor n2 e recorrendo ao comando *tcpdump*, constatamos que todos os servidores recebem os pacotes. Tal deve-se ao facto de o *hub* ao receber um pacote de dados reencaminha-os para todos os dispositivos que se encontram na rede.

18. 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.

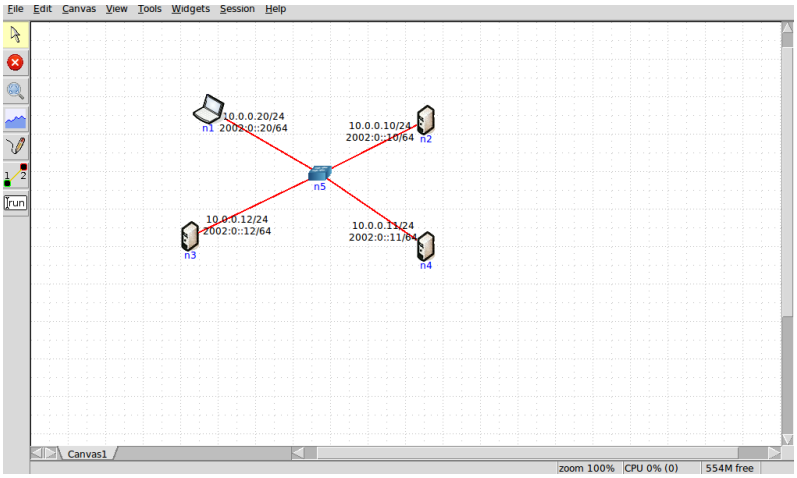

Figura 17 - Topologia CORE

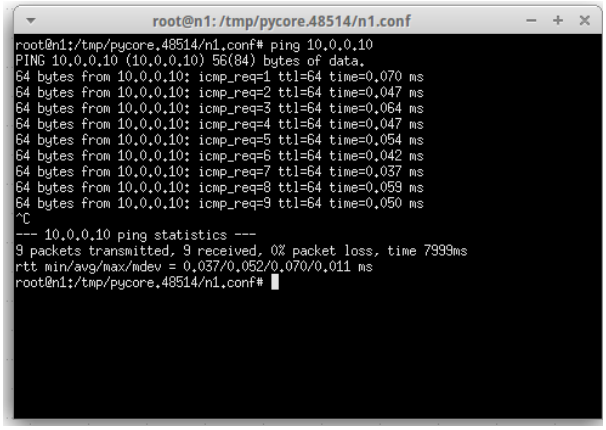

Figura 18 - Ping no laptop n1 para o servidor n2

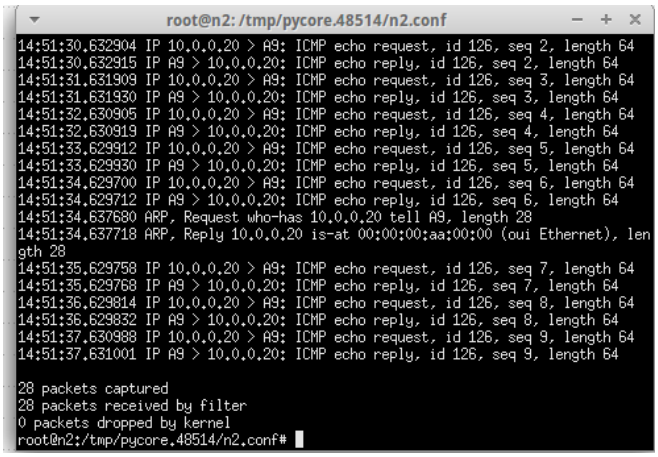

Figura 19 - tcpdump no servidor n2

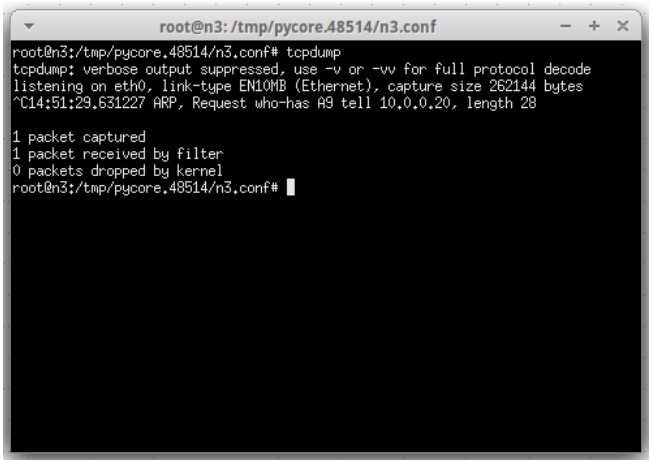

Figura 20 - tcpdump no servidor n3

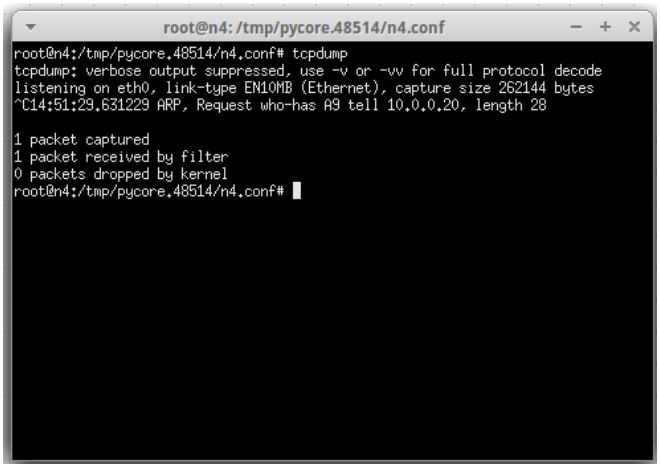

Figura 21 - tcpdump no servidor n4

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. Tal é possível, pois a mensagem é enviada para o *switch* que a envia diretamente para o *host*. Assim nas imagens referentes ao *tcpdump* dos servidores n3 e n4, verificamos que apenas capturam um pacote que corresponde a um pacote *arp-broadcast* enviado pelo switch para todas as interfaces da rede, de modo a conhecer o endereço MAC do *host* destino para o qual a mensagem deve ser enviada. Este procedimento apenas ocorre, quando este endereço ainda não se encontra na tabela de comutação do *switch*. Como os *hubs* transmitem a mensagem recebida por todas os nodos da rede, por apenas um canal de comunicação, as colisões são bastantes frequentes. Para além disto a quantidade de informação desnecessária a circular na rede é considerável. Enquanto que, 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*.

2 Conclusões

A realização deste relatório permitiu aprofundar os conhecimentos acerca dos Endereços MAC, Address Resolution Protocol (ARP), Ethernet e Interligação de Redes Locais. Tal deve-se ao facto de termos efetuado capturas e as respetivas análises de tramas Ethernet recorrendo à ferramenta Wireshark, que foi essencial para obter todas as informações relativas às tramas, desde os protocolos utilizados até ao código de deteção de erros. Para uma melhor compreensão do mapeamento entre endereços do nível de rede e endereços do nível de ligação lógica foi fundamental o estudo do protocolo ARP.

A utilização da ferramenta de simulação de redes (CORE) proporcionou a criação de topologias que permitiram comparar a eficácia da utilização dos *switches* e *hubs* na diminuição de colisões em tramas Ethernet. Através do trabalho realizado conseguimos verificar que os *switches* são mais viáveis que os *hubs*.