Redes de Computadores

Uma imagem com ClipArt

Descrição gerada automaticamente

Trabalho prático 3

28 de novembro de 2019

**Grupo nº 6**

Filipa Alves dos Santos (A83631)

Hugo André Coelho Cardoso (A85006)

João da Cunha e Costa (A84775)

Uma imagem com pessoa, parede, homem, interior

Descrição gerada automaticamenteUma imagem com pessoa, céu, homem, parede

Descrição gerada automaticamenteUma imagem com pessoa, parede, vestuário, sorriso

Descrição gerada automaticamente

Mestrado Integrado em Engenharia Informática

Universidade do Minho

**Índice de conteúdos**

**1. Questões e Repostas 3**

1.1. Captura e análise de tramas Ethernet 3

1.2. Protocolo ARP 5

1.3. Domínios de colisão 8

**2. Conclusões 10**

1. **Questões e Respostas**

**1.1.** **Captura e análise de tramas Ethernet**

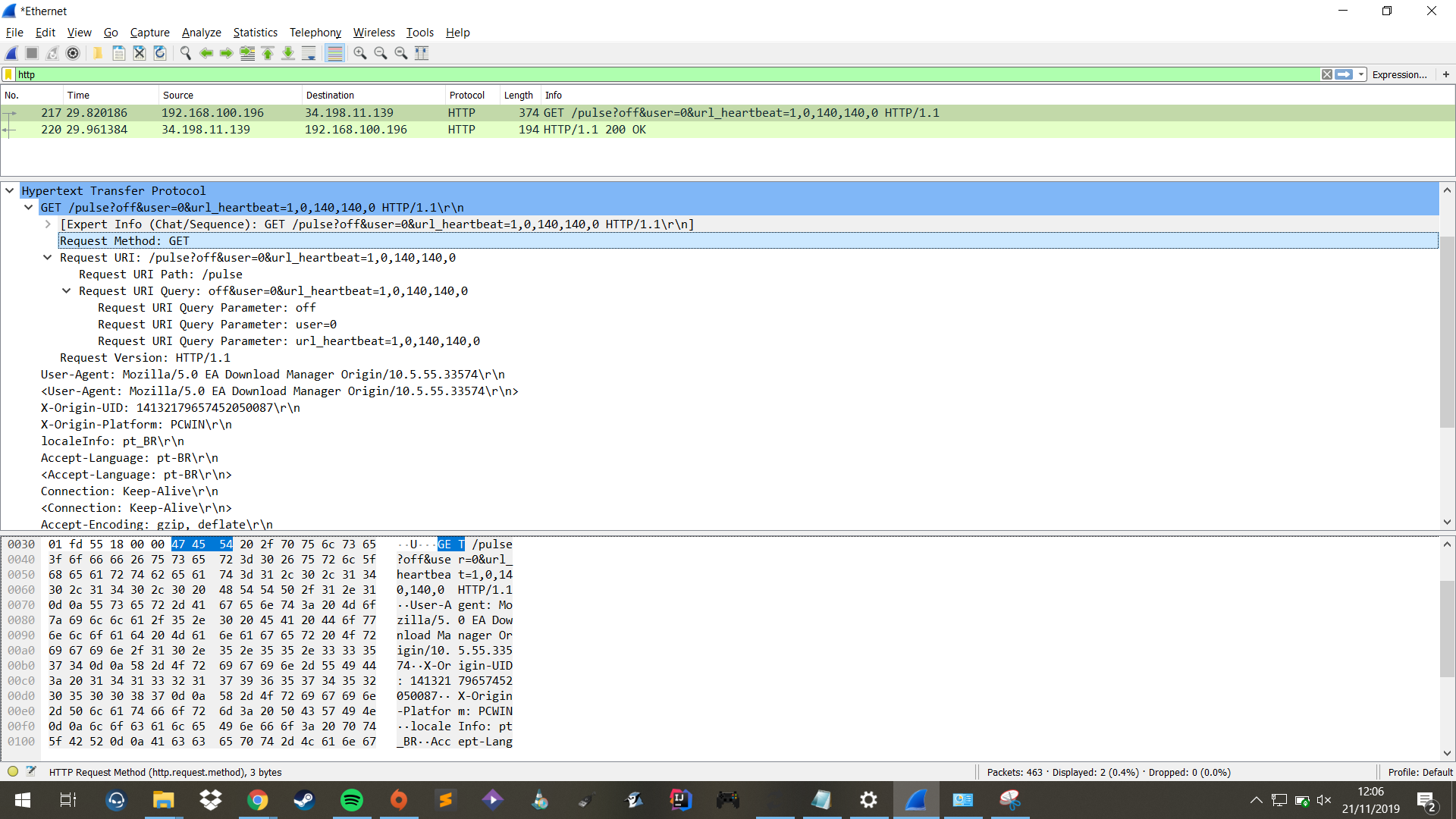
**3)** A captura e análise de tramas Ethernet será efetuada usando a aplicação Wireshark. Assegure-se que utiliza a ligação com fios, i.e., a ligação à rede Ethernet da sala de aula e que a cache do seu browser está vazia e está conetado em rede através da interface Ethernet.

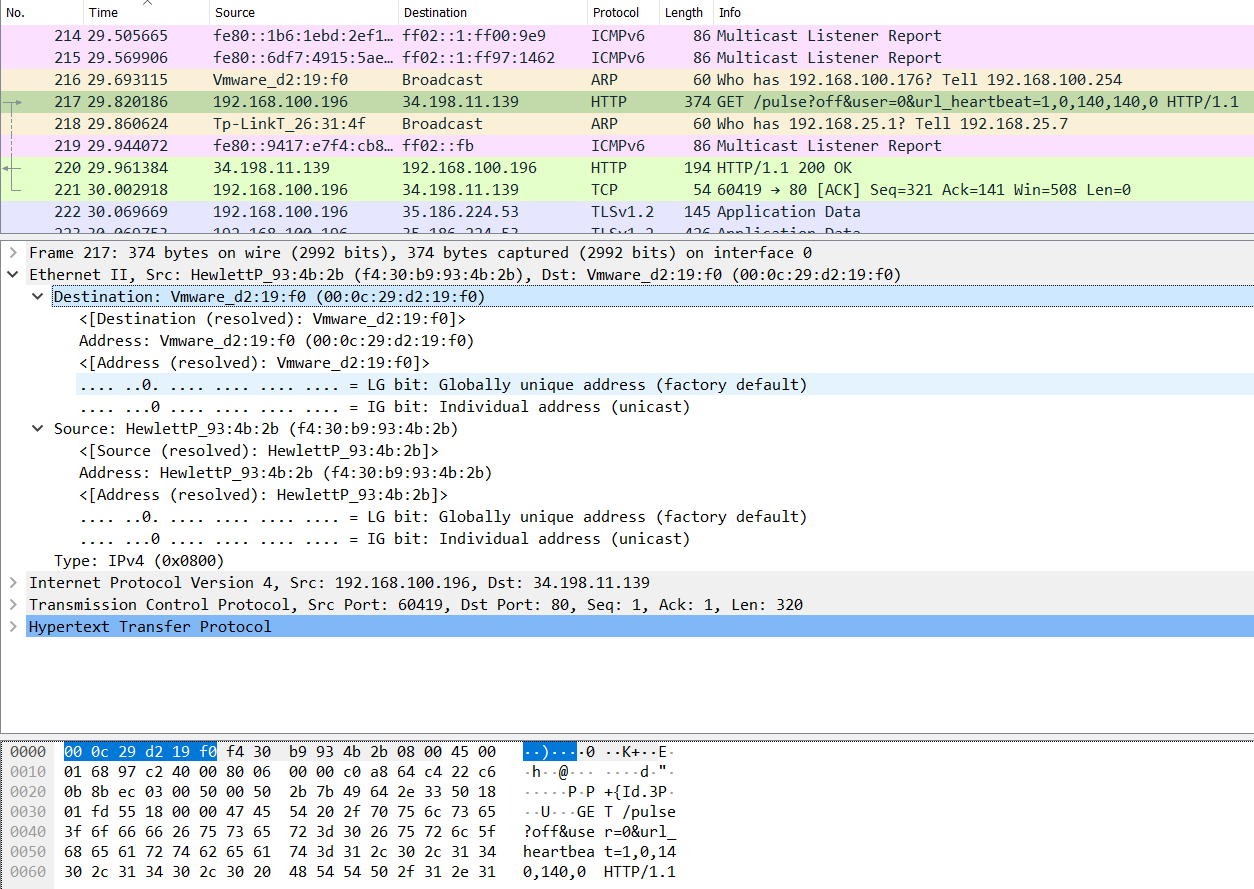
(...)

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.

(…)

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem HTTP GET (sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada.





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

Endereço de origem: f4:30:b9:93:4b:2b

Endereço de destino: 00:0c:29:d2:19:f0

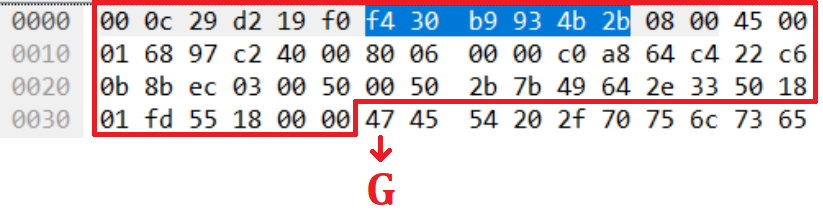
**3.2)** Identifique a que sistemas se referem. Justifique.

O source é o nosso computador ("HewlettP") e o destino corresponde à placa de rede "virtual" da sala de aula.

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

O valor hexadecimal do campo Type é 0x0800 que significa que encapsula um pacote IpV4.

**3.4)** 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.



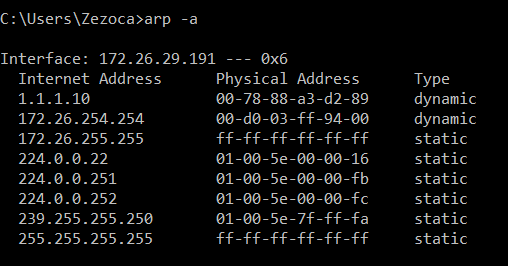
São usados 54 bytes até ao caractere “G” . Como a quantidade total de bytes da trama é de 374 bytes, a percentagem de sobrecarga é 54/374 = 14,44%.

**3.5)** 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?

O campo FCS não está a ser presente nesta trama porque pacotes em que se verificam erros são descartados (mau checksums) enquanto nos que não apresentam erros, como é o caso desta trama, não existe tal campo. A nível de redes por cabo, os erros raramente ocorrem.

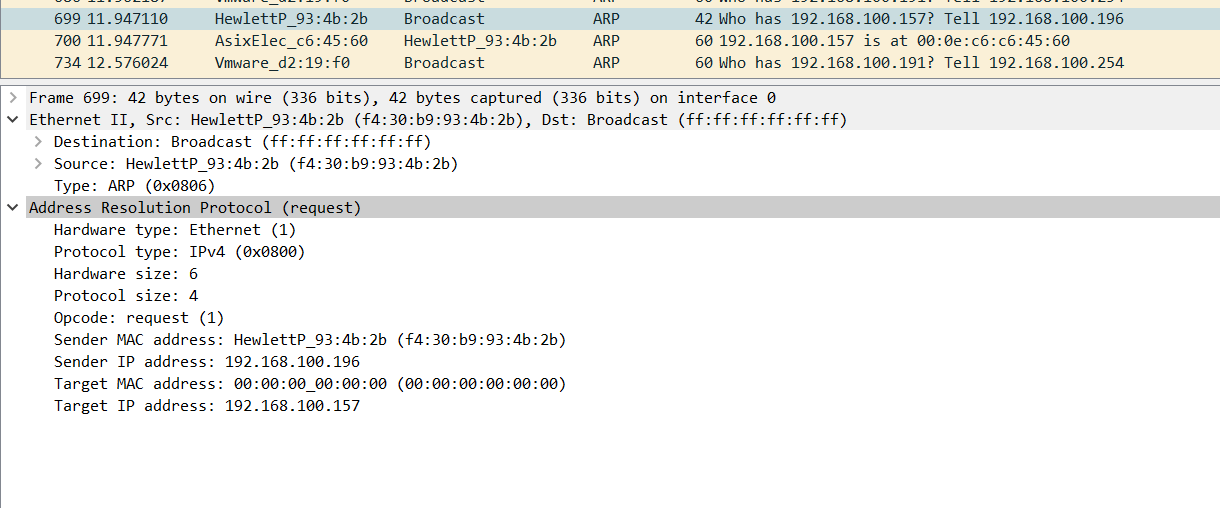
**1.3.** **Protocolo ARP**

**4)** Inicie a captura de tráfego com o Wireshark, e aceda a http://miei.di.uminho.pt. Efetue também um ping para um host da sala de aula (e.g. ping 192.168.100.xxx) que esteja a ser usado por outro grupo. Pare a captura de tráfego e tente localizar o tráfego ARP. Se necessário limite os protocolos visíveis apenas a protocolos abaixo do nível IP. Para tal, seleccione Analyze->Enabled Protocols e remova a selecção da opção IPv4 e IPv6. Responda às seguintes perguntas:

**4.9)** Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.

A primeira coluna representa o endereço IP do host e a segunda coluna representa o endereço MAC, ou seja, o endereço da ethernet associado ao IP. Já a terceira coluna representa o tipo de ligação estabelecida.

**4.10)** 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 hexadecimal dos endereços origem e destino são, respetivamente, f4:30:b9:93:4b:2b e ff:ff:ff:ff:ff:ff. O endereço de destino usado significa que todos os nós da rede local vão receber esta trama Ethernet.

**4.11)** Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?

O valor hexadecimal do campo Type é 0x0806 que significa que encapsula um pacote ARP.

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

O valor do campo ARP opcode é “request(1)” e especifica que é uma mensagem de pedido (“Who has 192.168.100.157?”).

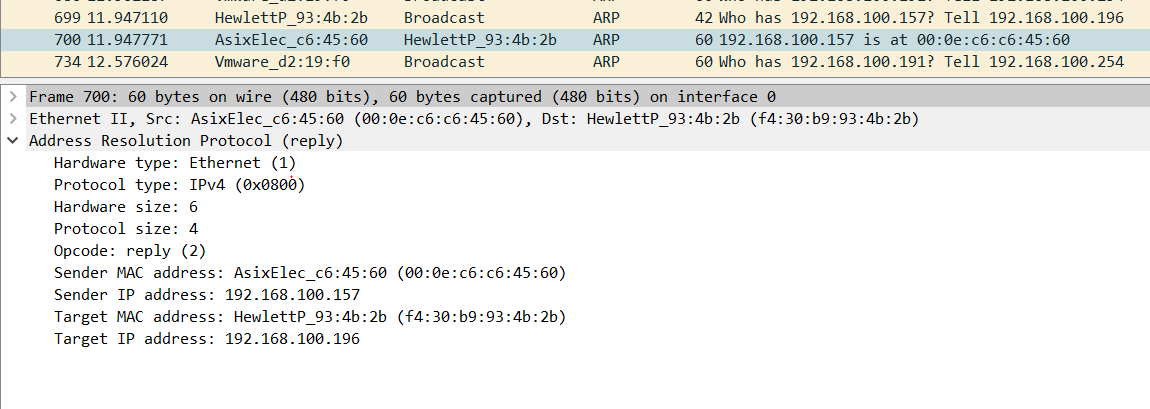
**4.13)** Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

Estão contidos endereços do tipo MAC e IP. Podemos concluir através disto que host de endereço IP “192.168.100.196” (Sender IP adress) e MAC “f4:30:b9:93:4b:2b” (Sender MAC adress) é a origem da mensagem, que pretende saber o endereço MAC do host de IP “192.168.100.157” (Target IP adress). Assim, vai-se mandar a mensagem como broadcast, explicando o Target Mac Adress “00:00:00:00:00:00”.

**4.14)** Explicite que tipo de pedido ou pergunta é feito pelo host de origem?

Perguntamos a todos os hosts da rede local quem tem o IP “192.168.100.157” e pedimos para enviarem o MAC correspondente para “192.168.100.196”.

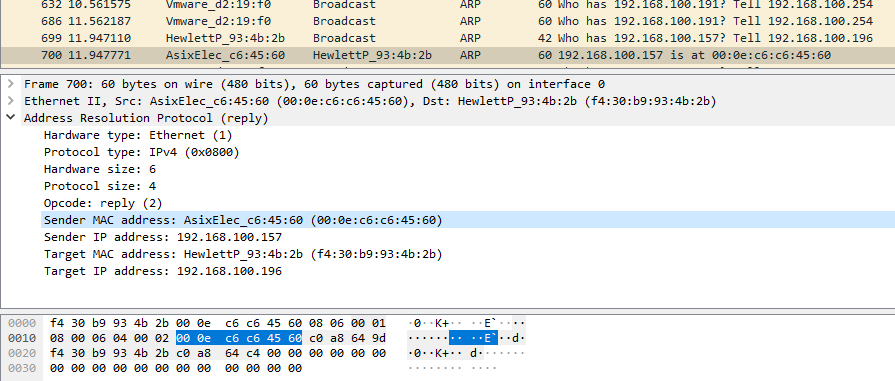
**4.15)** Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.

****

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

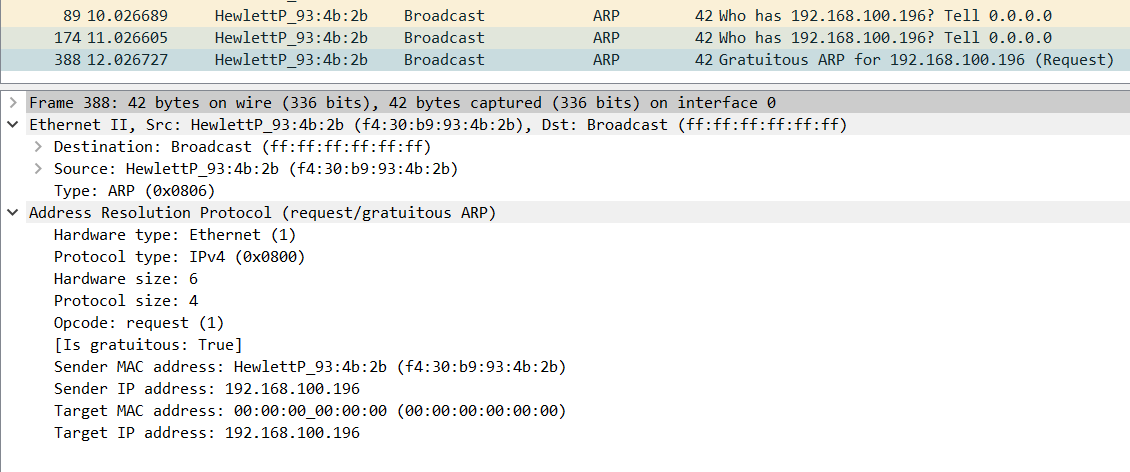
O valor do campo ARP opcode é “reply(2)” e especifica que é uma mensagem de resposta (“192.168.100.157 is at 00:0e:c6:c6:45:60”).

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



A mensagem está contida entre os bytes 23 e 28.

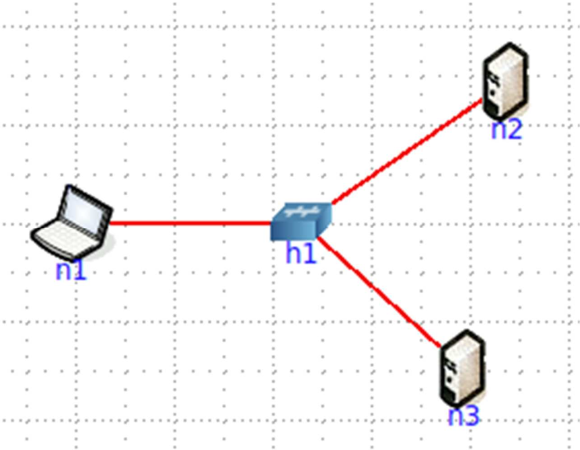
**4.16)** Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado?

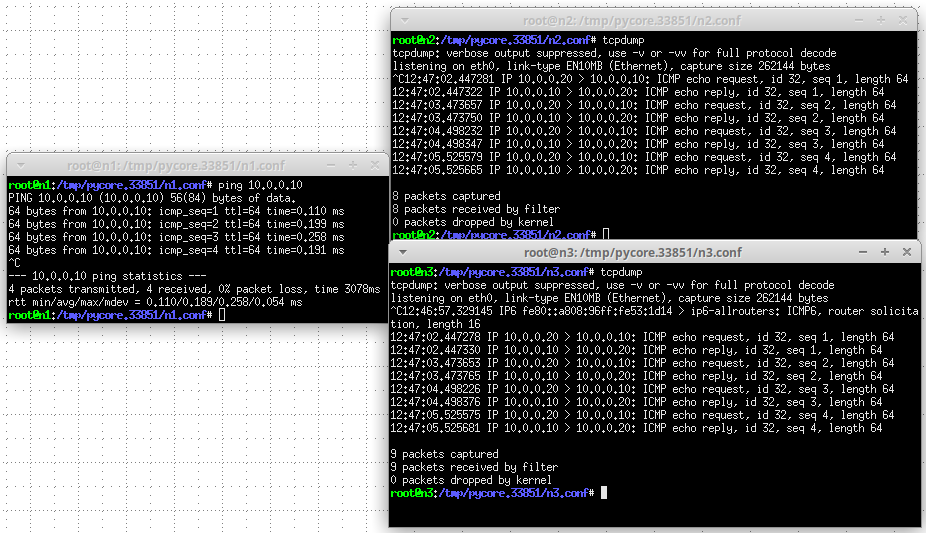


O que distingue o ARP gratuito dos restantes pedidos é a flag “[Is gratuitous: True]”, que indica que o pedido é de facto, gratuito. O host envia um ARP gratuito ao ligar-se de novo à rede, quando lhe é atribuído um endereço IP. Este envio permite informar os dispositivos da rede local do seu novo endereço MAC, para poderem atualizar as suas tabelas ARP.

**1.3.** **Domínios de colisão**

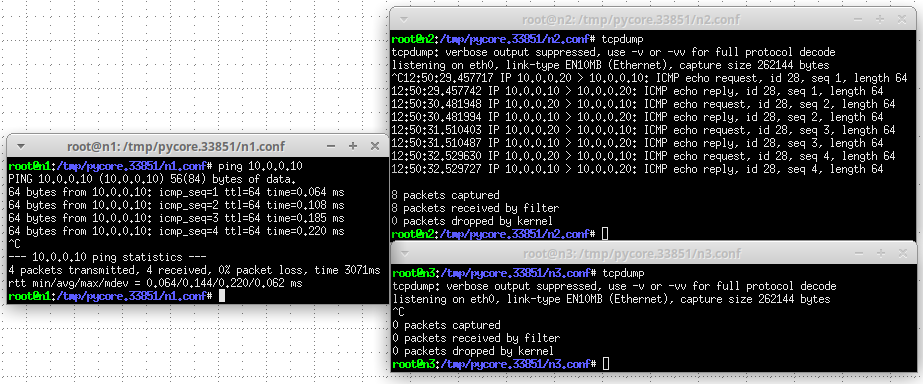
**5)** Construa uma topologia no emulador CORE com um host (n1) e dois servidores (n2, n3) interligados através de um hub.



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

Ao correr a opção tcpdump nos dois servidores (n2 e n3), podemos concluir que ambos capturam o mesmo tráfego, embora a comunicação seja feita apenas entre n1 e n2. O servidor n3 recebe na mesma os pacotes enviados pelo host dado que os dispositivos da rede estão ligados por um hub, que funciona como um repetidor de múltiplas portas, redistribuindo qualquer sinal enviado na porta de input por todas as outras portas.

**5.18)** Fa 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.



Um switch mantém para cada endereço MAC a indicação da interface de saída, com a ajuda de uma tabela de comutação, direcionando qualquer trama Ethernet que chegue para a interface apropriada.

Ao substituir o hub da arquitetura por um switch, paramos de ter a redistribuição de dados observada na pergunta anterior. Assim, neste caso, n3 não recebe tráfego nenhum, sendo a comunicação exclusivamente entre n1 e n2.

1. **Conclusões**

Este trabalho prático permitiu aprofundar e consolidar a matéria dada nas aulas teóricas, em particular a Camada de Ligação Lógica: Ethernet e Protocolo ARP.

Estudamos a partilha de endereços MAC em redes de computadores, através da análise de tráfego capturado com recurso ao Wireshark, e as vantagens e implicações do uso do protocolo ARP, que serve para efetuar o mapeamento de endereços de redes e endereços de uma tecnologia de ligação de dados, bem como o funcionamento dos domínios de colisão nestas últimas. Para tal efeito, recorremos também ao uso da ferramenta CORE fornecida pelos docentes, tal como já tínhamos feito no trabalho prático anterior.

Concluindo, este trabalho serviu como um bom meio de estudar a camada de ligação de redes de computadores e avaliar os conhecimentos da mesma.