Relatório Trabalho Prático nº3

João Pimentel (a80874) Rodolfo Silva (a81716) Pedro Gonçalves (a82313)

Novembro 2018

Universidade do Minho
Mestrado Integrado em Engenharia Informática
Redes de Computadores
Grupo 64

Conteúdo

1 Questões e Respostas

1.1 Captura e análise de tramas Ethernet

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

   Como é possível comprovar pela Figura 1, o endereço *MAC* de origem é **74:d0:2b:10:f3:b1** e o de destino corresponde a **00:0c:29:d2:19:f0**.

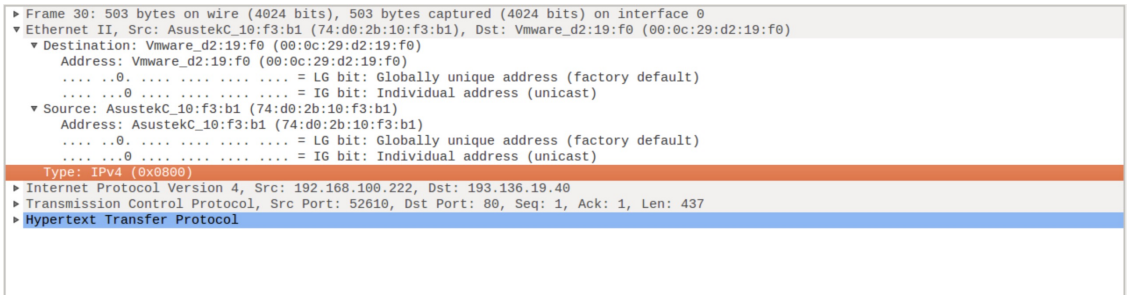

Figura 1 - Trama capturada.

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

   Os sistemas referidos são os adaptadores de rede *AsustekC* (origem), correspondendo ao nosso computador e *Vmware* (destino), correspondente ao servidor do *URL* `http://miei.di.uminho.pt`, como pode ser observado na Figura 1.

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

   O valor hexadecimal é **0x0800**, indicando que a trama possui um pacote *IPv4*, como se vê na Figura 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.**

   São usados 66 bytes como é possível observar no canto inferir direito da Figura 2. A sobrecarga introduzida pela pilha protocolar é 13.12%, que corresponde a 66/503*100, sendo 503 o tamanho da trama.

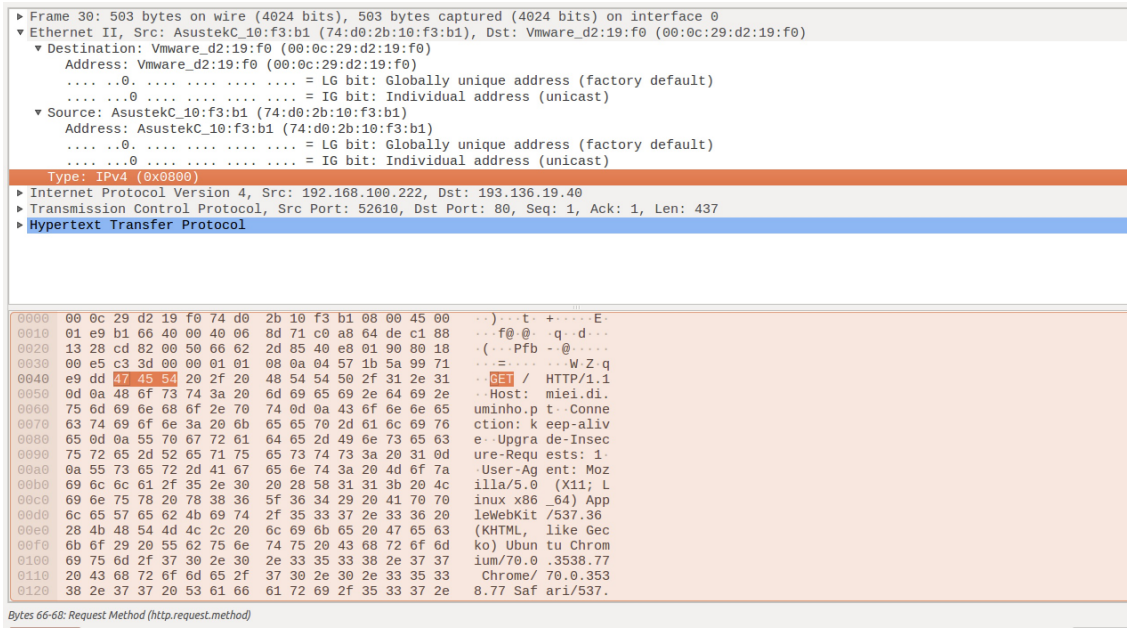

Figura 2 - Overhead introduzida pela pilha protocolar no envio do HTTP GET.

5. **Através da 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?**

   Visto que o FCS se encontra no fim da trama *Ethernet*, podemos observar que este não está a ser utilizado, pois a trama acaba na secção do overload. Isto deve-se ao facto de nas ligações *Ethernet* a taxa de ocorrência de erros ser demasiado baixa, não sendo justificável a utilização de *FCS*.

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

   Como se pode observar na Figura 3, o *MAC address* do endereço fonte é **00:0c:29:d2:19:f0**, correspondendo a um dispositivo de rede nível 2, do qual é feito o último salto até chegar à interface da nossa máquina. Isto deve-se ao facto de o endereço *Ethernet* da fonte se referir a um *switch*, *hub*, ou outro adaptador de rede.

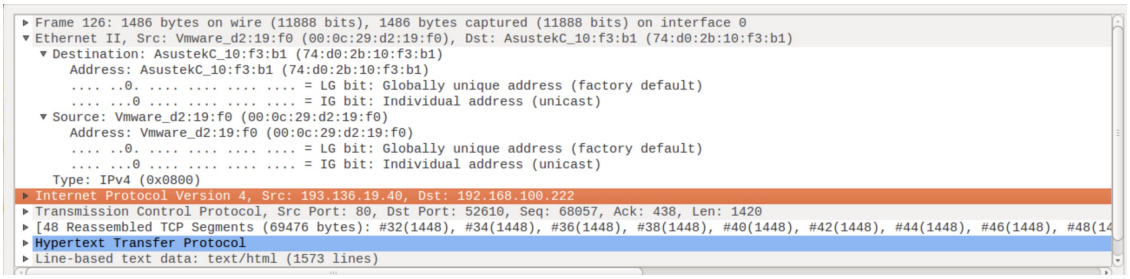

Figura 3 - Trama recebida.

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

   Como se pode observar na Figura 3, o endereço *MAC* do destino é **74:d0:2b:10:f3:b1** e corresponde ao adaptador de rede do computador onde foi realizada a atividade.

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

   Os protocolos contidos na trama recebida são *TCP*, *IPv4* e *Ethernet*, como se observa na Figura 3.

1.2 Protocolo ARP

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

   HWtype corresponde ao tipo de ligação efetuada, neste caso *ether*, indicando que é uma ligação por cabo.

   HWadress corresponde ao endereço *MAC* de origem.

   Flag Mask possuindo um *C*, indica que está completa.

   Iface representa a interface do equipamento.

```
thol@thol-K56CB:/usr/sbin$ ./arp
Address                  HWtype  HWaddress           Flags Mask            Iface
gw.sa.di.uminho.pt       ether   00:0c:29:d2:19:f0   C                     enp4s0f2
thol@thol-K56CB:/usr/sbin$ ./arp -a
gw.sa.di.uminho.pt (192.168.100.254) at 00:0c:29:d2:19:f0 [ether] on enp4s0f2
```

Figura 4 - Tabela ARP.

10. **Qual o valor hexadeciomal 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 endereço *MAC* de destino é **74:d0:2b:10:f3:b1** e o de origem é **00:0c:29:d2:19:f0**. O destino é a interface da nossa máquina, demonstrando que o protocolo *ARP* perguntou quem possuía o *IP* **192.168.100.222**, sendo que este pertencia à máquina em questão.

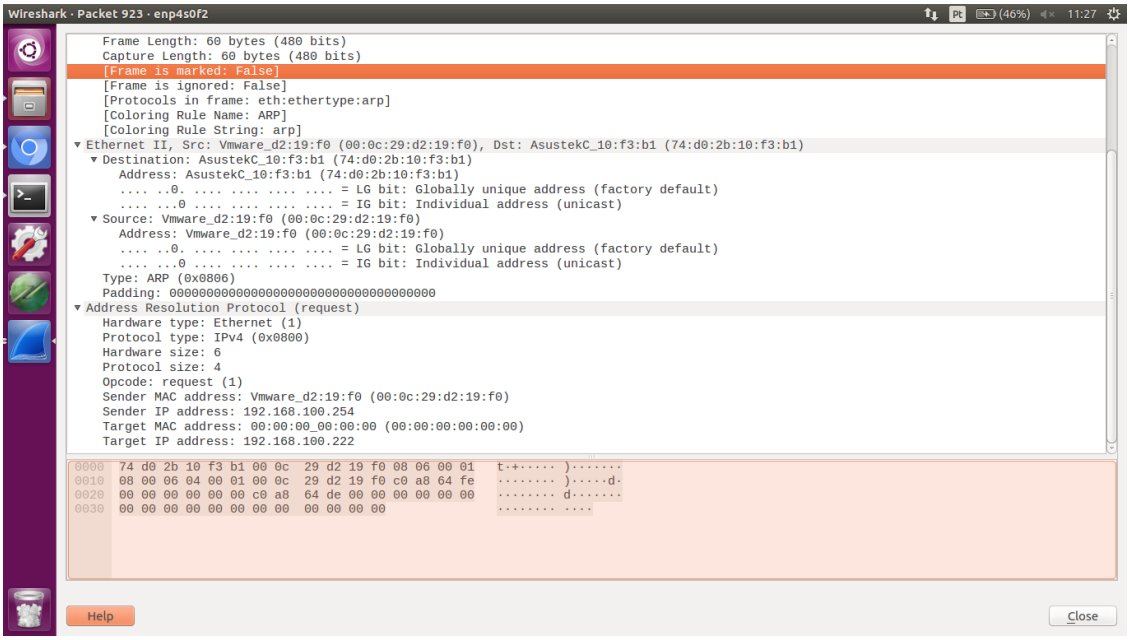

Figura 5 - Trama Ethernet que contém a mensagem de pedido ARP.

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

    Como é visível na Figura 11, o valor hexadecimal é **0x0806**, indicando que o tipo da trama é de protocolo *ARP*.

12. **Qual o valor do campo ARP *opcode*? O que especifica? Se necessário, consulte a RFC do protocolo ARP.**

    O valor do campo *Opcode* apenas adota dois valores. Caso o seu valor seja 1, indica que foi feito um pedido. Caso seja 2, retrata que foi dada uma resposta a um pedido (ver Figura 6). Como é visível na Figura 7, possui o valor 1, representando um pedido de resolução de endereço.

```
Ethernet transmission layer (not necessarily accessible to
     the user):
    48.bit: Ethernet address of destination
    48.bit: Ethernet address of sender
    16.bit: Protocol type = ether_type$ADDRESS_RESOLUTION
Ethernet packet data:
    16.bit: (ar$hrd) Hardware address space (e.g., Ethernet,
                     Packet Radio Net.)
    16.bit: (ar$pro) Protocol address space.  For Ethernet
                     hardware, this is from the set of type
                     fields ether_typ$<protocol>.
     8.bit: (ar$hln) byte length of each hardware address
     8.bit: (ar$pln) byte length of each protocol address
    16.bit: (ar$op)  opcode (ares_op$REQUEST | ares_op$REPLY)
    nbytes: (ar$sha) Hardware address of sender of this
                     packet, n from the ar$hln field.
    mbytes: (ar$spa) Protocol address of sender of this
                     packet, m from the ar$pln field.
    nbytes: (ar$tha) Hardware address of target of this
                     packet (if known).
    mbytes: (ar$tpa) Protocol address of target.
```

Figura 6 - Explicação dos valores do campo Opcode.

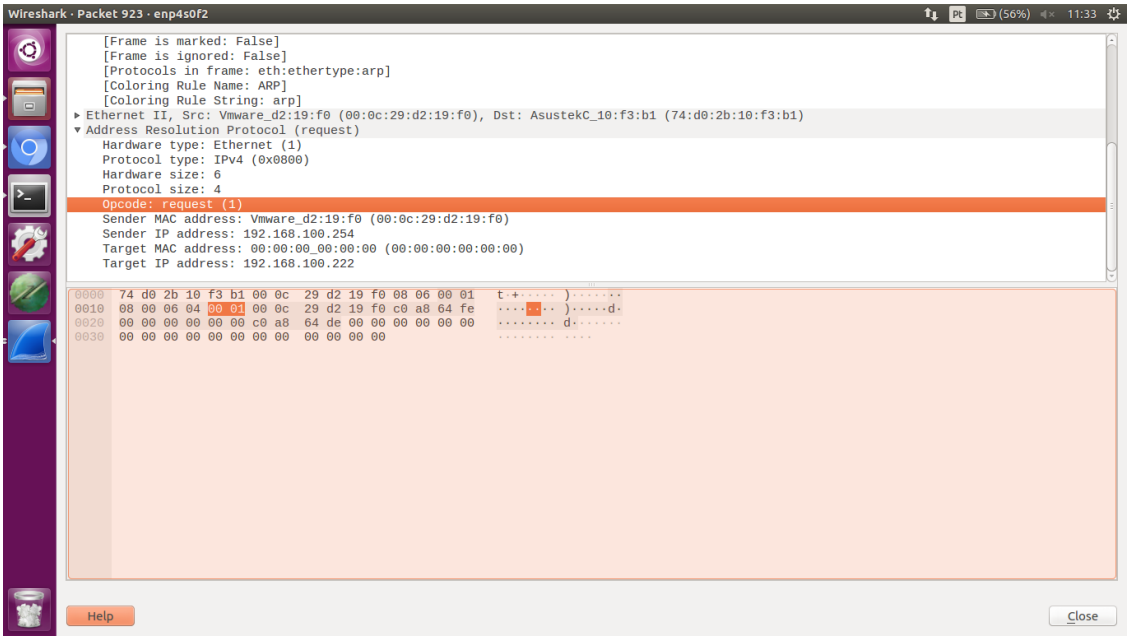

Figura 7 - Valor do campo Opcode da trama em análise.

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

    Como é visível na Figura 7, estão contidos os endereços *IP* da máquina que envia o pedido, bem como da que é pretendido atingir. Além disso, possui os endereços *MAC* dos dispositivos de rede nível 2 da nossa máquina e da máquina que está a comunicar com a mesma.

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

    O pedido feito representa uma resolução de endereçamento. Esta retrata uma situação em que se pergunta à máquina de destino se possui o endereço *IP* indicado como *Target*. A máquina de destino deverá responder com o seu endereço *MAC*.

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

    (a) **Qual o valor do campo ARP *opcode*? O que especifica?**
    Como se vê na Figura 8, o valor do campo *Opcode* é 2, indicando que está a ser dada uma resposta a um pedido anteriormente feito.

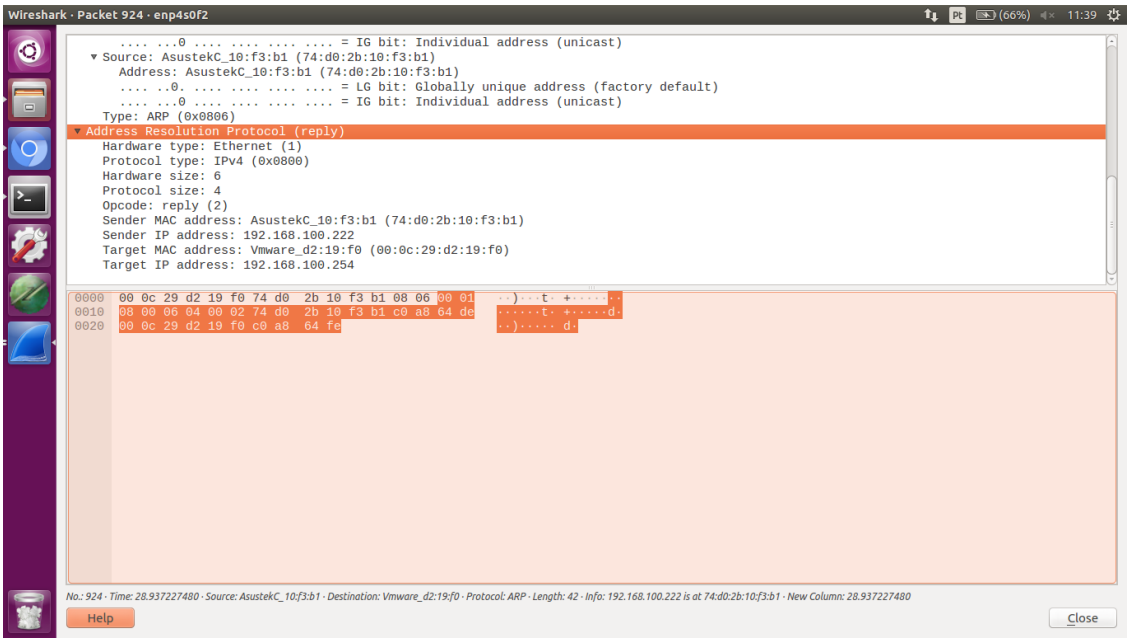

Figura 8 - Conteúdo da trama de resposta ao pedido ARP.

    (b) **Em que posição da mensagem ARP está a resposta ao pedido ARP?**
    A resposta ao pedido *ARP* encontra-se no *Sender MAC address* em análise, ou seja, em **74:d0:2b:10:f3:b1**.

1.3 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?**

    Um pedido *ARP* gratuito e um não gratuito diferenciam-se no facto de que um *ARP* gratuito pode ser enviado a qualquer altura por um *host* para o endereço de *Broadcast* da rede, com a finalidade de verificar que o seu endereço *IP* não está a ser utilizado e para que outros dispositivos da rede possam atualizar a sua tabela *ARP*, com a finalidade de conseguirem comunicar com o *host* que envia o pedido.

Assim, este pedido é diferente do *ARP* não gratuito, já que não espera uma resposta, mas sim atualiza o estado de rede. É semelhante a uma resposta *ARP*, não sendo necessário efetuar um pedido. Sendo assim, como era expectável, não foi registada nenhuma resposta ao pedido *ARP* gratuito efetuado.

Figura 9 - Trama ARP gratuita.

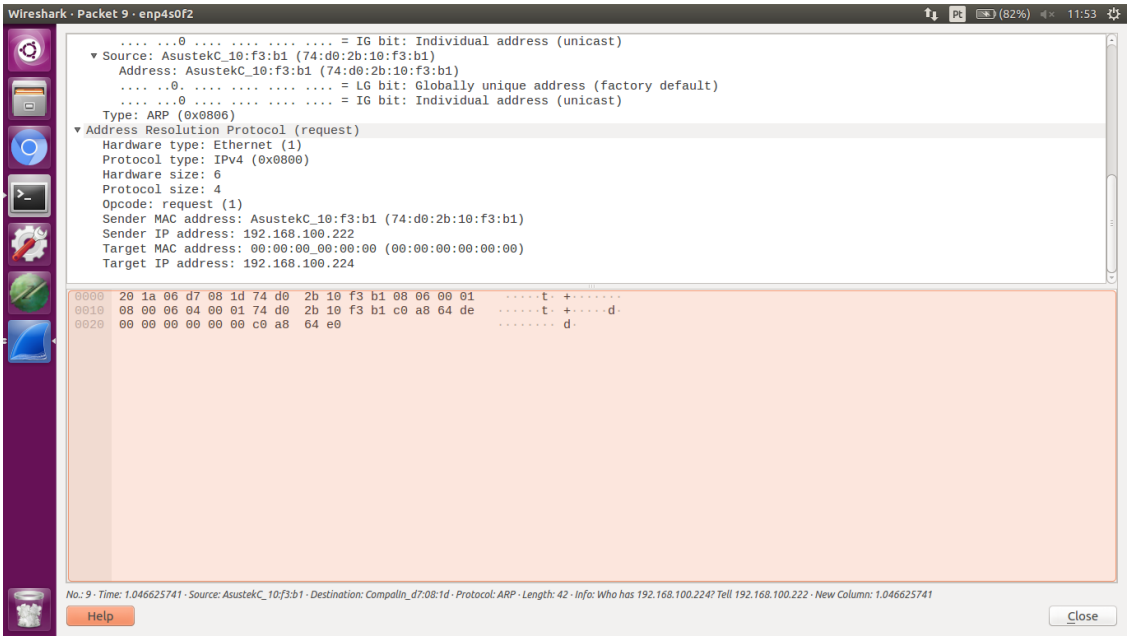

Figura 10 - Trama ARP não gratuita.

1.4 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?**

    Tendo em conta o tráfego registado pelas diferentes interfaces dos dispositivos, é fácil perceber que os dispositivos *n2* (em baixo e à esquerda), *n3* (em cima e à direita) e *n4* (em cima e à esquerda) receberam o tráfego que estava destinado a *n2*, como se vê na Figura 11. Esta situação ocorreu, pois existe um *hub* entre as diferentes interfaces dos dispositivos. Tal facto leva a que se gere apenas um domínio de colisão, comum a todos. Isto faz com que todos os dispositivos recebam todas as comunicações entre os dispositivos existentes na rede, impedindo a comunicação entre pares de máquinas.

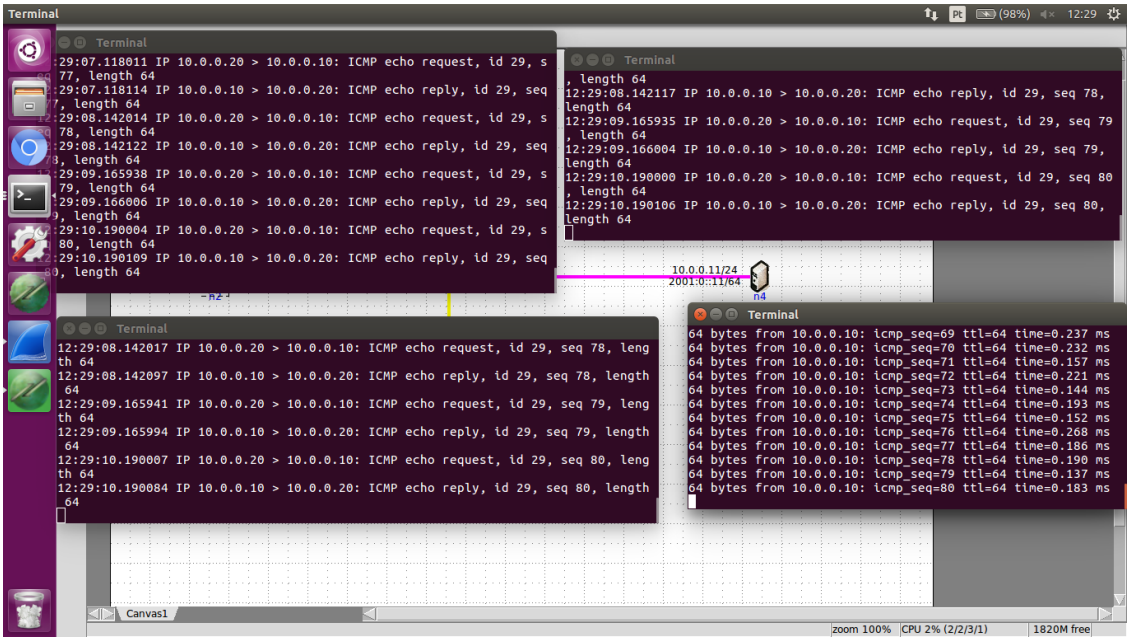

Figura 11 - Tráfego com *hub*.

18. **Na topologogia 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 conslusões com base no tráfego observado/capturado.**

    Como é visível na Figura 12, apenas *n2* recebeu o tráfego oriundo de *n1* (terminais na mesma ordem da questão anterior). Assim, podemos concluir que um *switch* assegura a existência de mais do que um domínio de colisão, permitindo várias comunicações diferentes simultaneamente, sem colisões entre os dispositivos da rede.

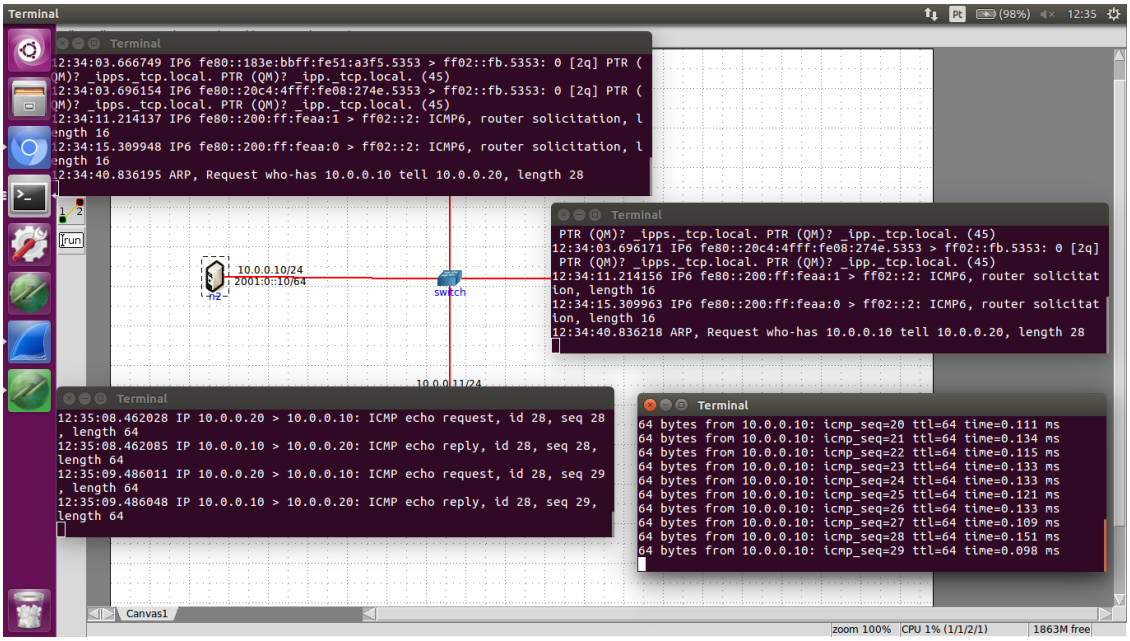

Figura 12 - Tráfego com *switch*.

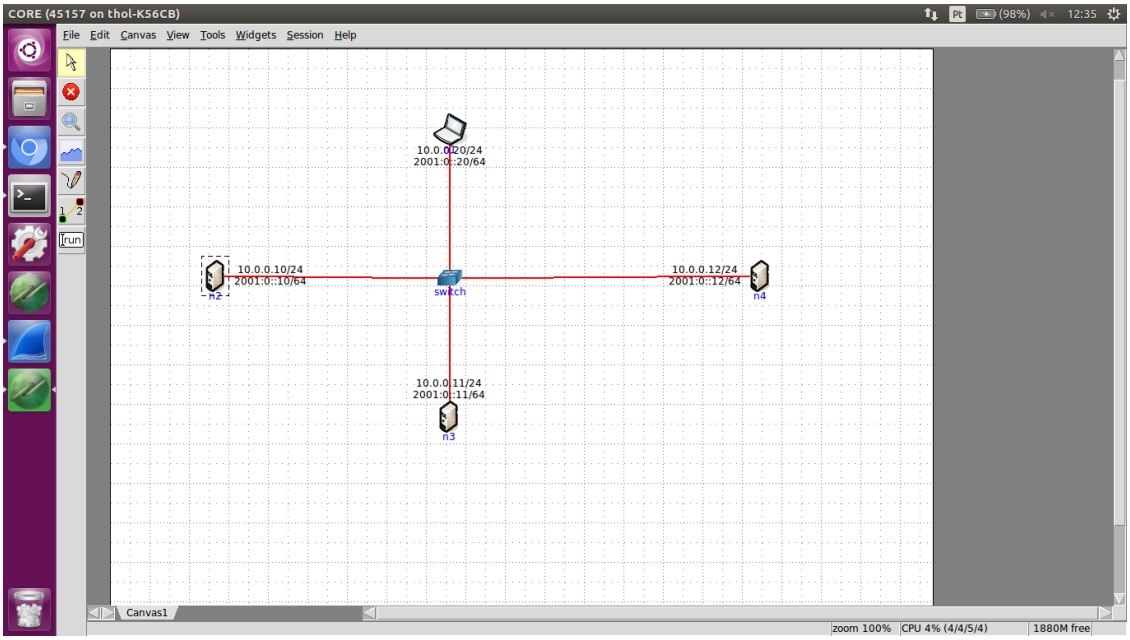

Figura 13 - Topologia com *switch*.

2 Conclusões

O desenvolvimento deste projeto permitiu um aumento no conhecimento relativamente ao protocolo *ARP*, endereçamento *MAC* em redes *Ethernet* e, ainda, contribuiu para a análise de domínios de colisão dentro de uma rede.

Sabendo que um bom conhecimento do funcionamento de uma rede à qual a nossa máquina está ligada permite conhecer as restrições e mais valias da mesma, este trabalho veio comprovar isso mesmo. Imaginando o caso da existência de um *hub* a interligar várias máquinas, o tráfego direcionado para um só dispositivo passará a ser recebido pela totalidade das máquinas, algo que nem sempre é desejado. Além disso, permitiu a perceção de como uma rede conhece os endereços *IP* dos dispositivos que necessita, associando-os aos seus endereços *MAC*.

Em suma, este projeto permitiu solidificar a matéria aprendida nas aulas teóricas, tendo sido bastante proveitoso para a possível realização de qualquer trabalho futuro relativo ao protocolo *ARP*, endereçamento *MAC* ou domínios de colisão.