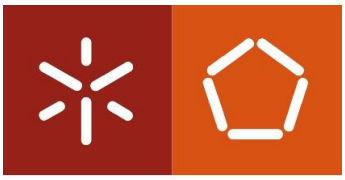

Universidade do Minho

Departamento de Informática

Trabalho 3
Redes de Computadores
Grupo 45

Catarina Machado (a81047) João Vilaça (a82339)
Ricardo Milhazes Veloso (a81919)

26 de Novembro de 2018

Conteúdo

1 TP3: Camada de Ligacao Logica: Ethernet e Protocolo ARP

3. Captura e análise de Tramas Ethernet

Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente a mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o comeco da respectiva mensagem HTTP Response proveniente do servidor.

R: Para descobrirmos o ip do website fizemos ping ao miei.di.uminho.pt e concluímos que é 193.136.19.40.

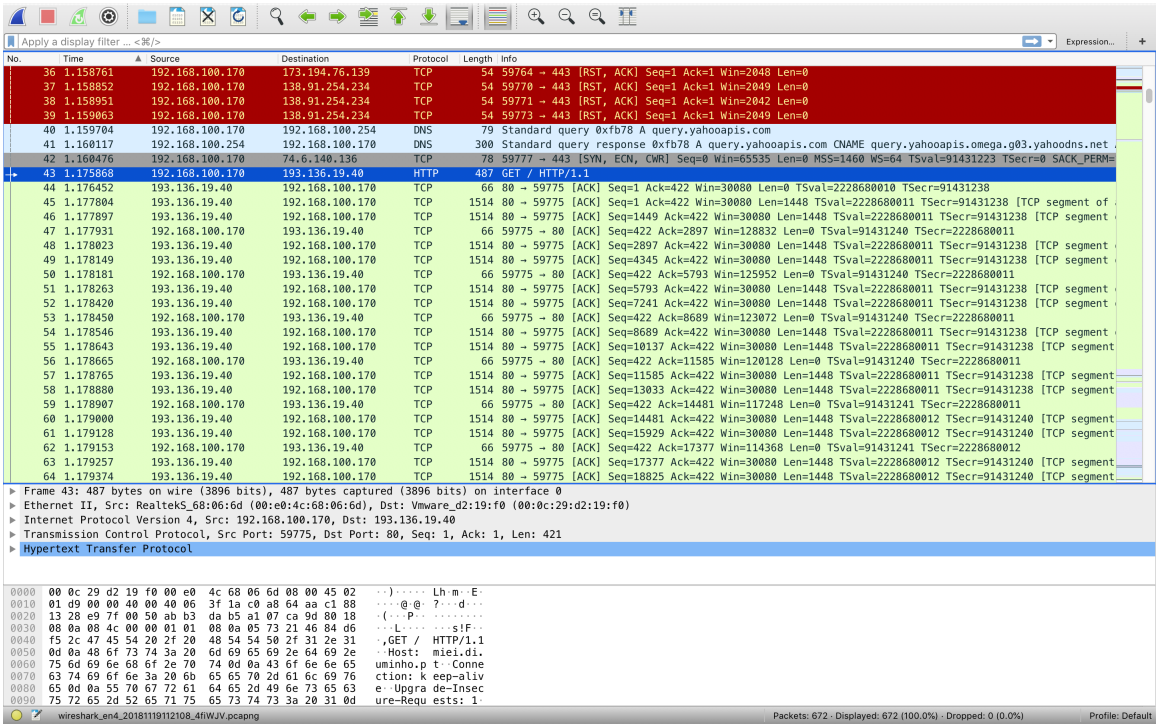

Figura 1

R1: O número de ordem de sequência de bytes capturada corresponde á mensagem HTTP GET enviada pelo computador ao servidor Web é 43.

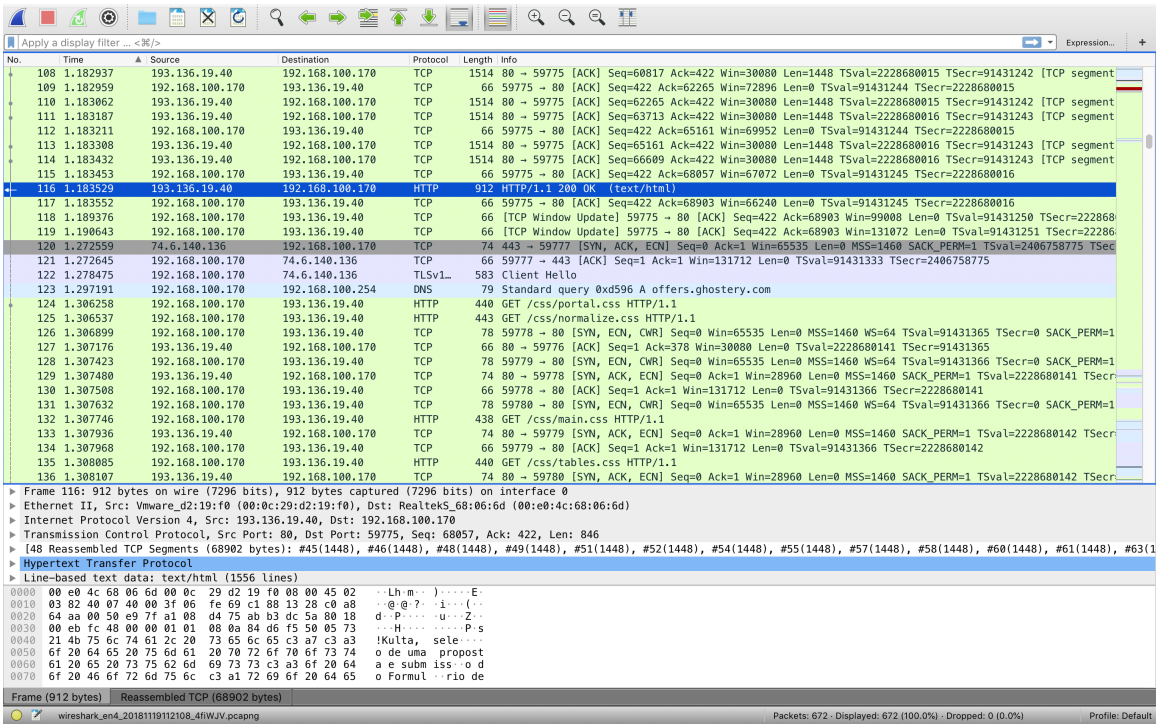

Figura 2

R2: O número de ordem de sequência de bytes capturada corresponde ao começo da mensagem HTTP Response proveniente do servidor é 116.

No sentido de proceder a analise do trafego, selecione a trama Ethernet que contem a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP esta no interior de um segmento TCP que e transportado num datagrama IP que, por sua vez, esta encapsulado no campo de dados de uma trama Ethernet. Expanda a informacao do nivel da ligacao de dados (Ethernet II) e observe o conteudo da trama Ethernet (cabecalho e dados (payload)).

Responda as perguntas seguintes com base no conteudo da trama Ethernet que contem a mensagem HTTP GET

```
No.     Time           Source                Destination           Protocol Length Info
     43 1.175868       192.168.100.170       193.136.19.40         HTTP     487    GET / HTTP/
1.1
Frame 43: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0
Ethernet II, Src: RealtekS_68:06:6d (00:e0:4c:68:06:6d), Dst: Vmware_d2:19:f0 (00:0c:
29:d2:19:f0)
Internet Protocol Version 4, Src: 192.168.100.170, Dst: 193.136.19.40
Transmission Control Protocol, Src Port: 59775, Dst Port: 80, Seq: 1, Ack: 1, Len: 421
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    116 1.183529       193.136.19.40         192.168.100.170       HTTP     912    HTTP/1.1 200
OK  (text/html)
Frame 116: 912 bytes on wire (7296 bits), 912 bytes captured (7296 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: RealtekS_68:06:6d (00:e0:4c:
68:06:6d)
Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.170
Transmission Control Protocol, Src Port: 80, Dst Port: 59775, Seq: 68057, Ack: 422, Len: 846
[48 Reassembled TCP Segments (68902 bytes): #45(1448), #46(1448), #48(1448), #49(1448),
#51(1448), #52(1448), #54(1448), #55(1448), #57(1448), #58(1448), #60(1448), #61(1448),
#63(1448), #64(1448), #66(1448), #68(1448), #69(1448), #71(1448)]
Hypertext Transfer Protocol
Line-based text data: text/html (1556 lines)
```

Figura 3

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

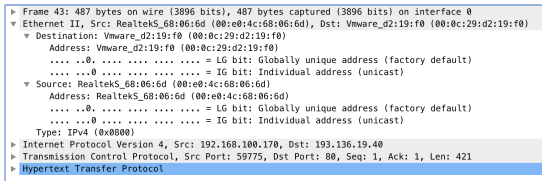

Figura 4

Endereço de Origem: 00:e0:4c:68:06:6d
Endereço de Destino: 00:0c:29:d2:19:f0

2. Identifique a que sistemas se referem. Justifique.

O endereço de origem refere-se á interface de ethernet da nossa máquina. O endereço de destino refere-se á interface do router da rede local.

O endereço de origem representa o local de onde é enviada a trama o que significa que esse endereço vai representar a interface ethernet da nossa máquina. Como a nossa máquina não reconhece endereços fora da rede local então é definido como endereço de destino a interface do router da rede local, que prosteriormente vai tratar de enviar a trama para o servidor Web.

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

R: 0x0800, como se pode ver na Figura 4. Indica que encapsula um pacote IPv4.

4. Quantos bytes sao usados desde o inicio da trama ate ao caractere ASCII "G" do metodo HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.

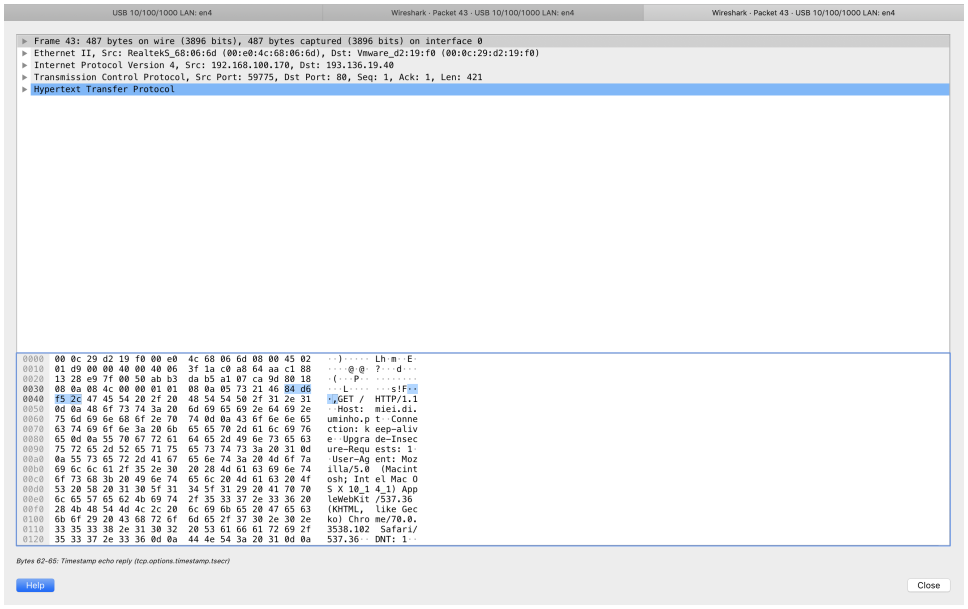

Figura 5

R: 66 bytes. 66/487 * 100 = 13.55%.

5. Atraves de visualizacao direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para detecao de erros nao esta a ser usado. Em sua opiniao, porque será?

O campo FCS (Frame Check Sequence) não aparece na trama capturada porque as redes wired (como a ethernet) são muito robustas e, automaticamente, são muito pouco suscetíveis a erros.

Nas redes Wireless estes campo já costuma ser utilizado devido á grande suscetibilidade a erros.

A seguir responda as seguintes perguntas, baseado no conteudo da trama Ethernet que contem o primeiro byte da resposta HTTP.

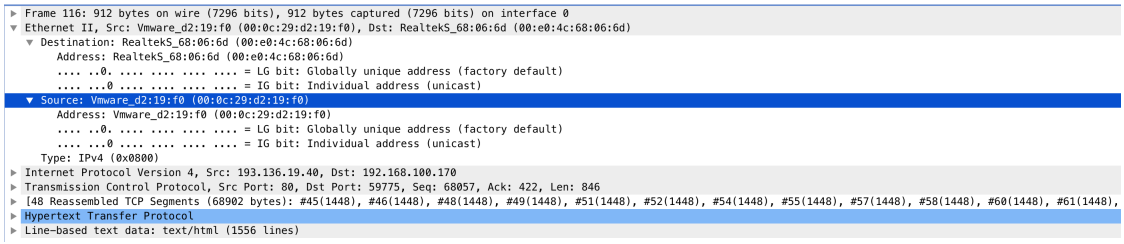

Figura 6

6. Qual e o endereco Ethernet da fonte? A que sistema de rede corresponde? Justifique

R: 00:0c:29:d2:19:f0. Corresponde ao gateway da rede local, uma vez que nós só conseguimos saber o endereço ip das redes locais e o gateway.

7. Qual e o endereco MAC do destino? A que sistema corresponde?

R: 193.136.19.40. Corresponde á interface ethernet da nossa máquina.

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

R: Ethernet, IPv4, TCP.

4. Protocolo ARP

```
▲ ~ arp -a
? (169.254.98.14) at 2c:60:c:f6:42:be on en4 [ethernet]
? (169.254.147.88) at 38:2c:4a:3f:43:30 on en4 [ethernet]
brom150.sa.di.uminho.pt (192.168.100.150) at 38:2c:4a:3f:43:30 on en4 ifscope [ethernet]
brom154.sa.di.uminho.pt (192.168.100.154) at cc:2d:8c:6:1e:27 on en4 ifscope [ethernet]
? (192.168.100.161) at e8:3:9a:17:4e:54 on en4 ifscope [ethernet]
? (192.168.100.195) at 2c:4d:54:31:59:63 on en4 ifscope [ethernet]
? (192.168.100.209) at 40:6c:8f:3b:d7:52 on en4 ifscope [ethernet]
server6.sa.di.uminho.pt (192.168.100.242) at 0:c:29:98:ac:62 on en4 ifscope [ethernet]
gw.sa.di.uminho.pt (192.168.100.254) at 0:c:29:d2:19:f0 on en4 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en4 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en4 ifscope permanent [ethernet]
```

Figura 7

9. Observe o conteudo da tabela ARP. Diga o que significa cada uma das colunas.
R: A primeira coluna representa o endereço ip do host. A segunda coluna representa o MAC address, e a terceira coluna representa o interface onde o mesmo está definido.

No sentido de observar o envio e recepcao de mensagens ARP é conveniente apagar o conteudo da cache ARP. Caso contrario, e provavel que a associacao entre enderecos IP e MAC ja exista em cache.

```
▲ ~ sudo arp -d -a
169.254.98.14 (169.254.98.14) deleted
169.254.147.88 (169.254.147.88) deleted
192.168.100.150 (192.168.100.150) deleted
192.168.100.161 (192.168.100.161) deleted
192.168.100.195 (192.168.100.195) deleted
192.168.100.209 (192.168.100.209) deleted
192.168.100.242 (192.168.100.242) deleted
192.168.100.254 (192.168.100.254) deleted
224.0.0.251 (224.0.0.251) deleted
239.255.255.250 (239.255.255.250) deleted

▲ ~ arp -a
gw.sa.di.uminho.pt (192.168.100.254) at 0:c:29:d2:19:f0 on en4 ifscope [ethernet]

▲ ~
```

Figura 8

10. Qual e o valor hexadecimal dos enderecos origem e destino na trama Ethernet que contem a mensagem com o pedido ARP (ARP Request)? Como interpreta e justifica o endereco destino usado?

```
▶ Frame 596: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: RealtekS_68:06:6d (00:e0:4c:68:06:6d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: RealtekS_68:06:6d (00:e0:4c:68:06:6d)
      Address: RealtekS_68:06:6d (00:e0:4c:68:06:6d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▶ Address Resolution Protocol (request)
```

Figura 9

Origem: 00:e0:4c:68:06:6d
Destino: ff:ff:ff:ff:ff:ff
É usada o endereço ethernet do broadcast (da camada 2) para poder ser recebido por todos os hosts da rede.

11. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?
R: 0x0806, indica que encapsula um frame ARP.

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

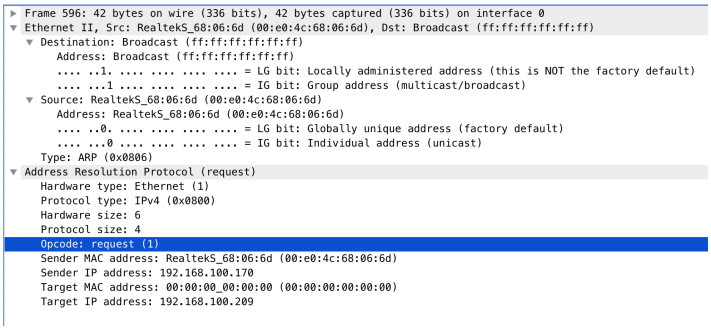

Figura 10

R: Opcode: request(1).
Especifica se é um pedido para saber um mac adress ou uma resposta a um "request"anterior.

13. Identifique que tipo de enderecos estao contidos na mensagem ARP? Que conclui?
R: Os tipos são endereços mac e endereços ip (sender mac adress, sender ip adress, target mac adress e target ip adress).
Tal como se pode ver na Figura 10, o host com ip 192.168.100.170 e MAC 00:e0:4c:68:06:6d quer saber qual é o mac do host com o ip 192.168.100.209 (target ip adress), então o target mac é o endereço de broadcast.

14. Explicite que tipo de pedido ou pergunta e feita pelo host de origem
"Who has 192.168.100.2019 Tell 192.168.100.170".
Perguntamos aos hosts da rede qual o mac de quem tem o ip 192.168.100.209, e pedimos para enviar a resposta para o 192.168.100.170.

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

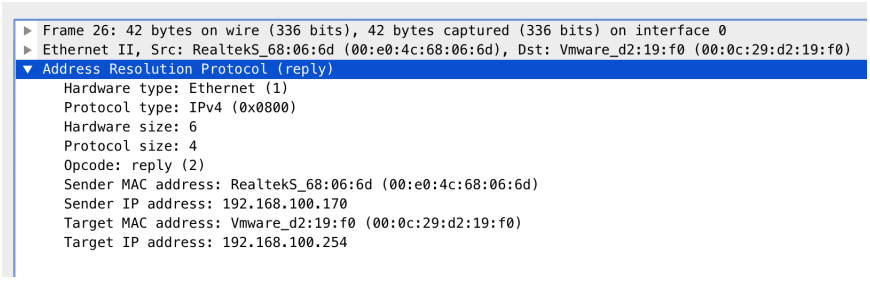

Figura 11

a. Qual o valor do campo ARP opcode? O que especifica?
R: Opcode: reply(2).
Especifica que é uma resposta a um "request"anterior.

b. Em que posicao da mensagem ARP esta a resposta ao pedido ARP?
R: A resposta ao pedido ARP encontra-se no Sender MAC address e Sender IP address.

5. ARP Gratuito

16. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteudo 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 12

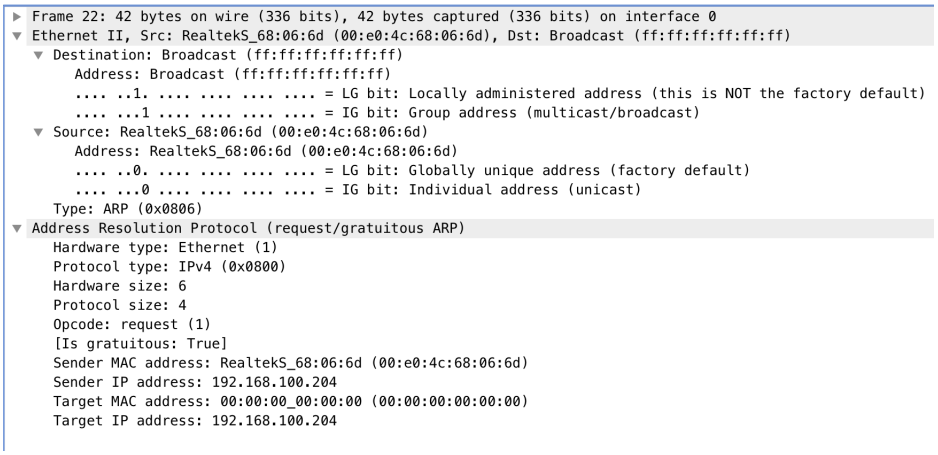

Figura 13

R: O que distingue um pedido ARP gratuito dos restantes pedido ARP é a presença de uma flag que indica que o pedido é gratuito [Is gratuitous: True].

6. Domínios de Colisão

17. Faca ping de n1 para n2. Verifique com a opcao tcpdump como flui o trafego nas diversas interfaces dos varios dispositivos. Que conclui?

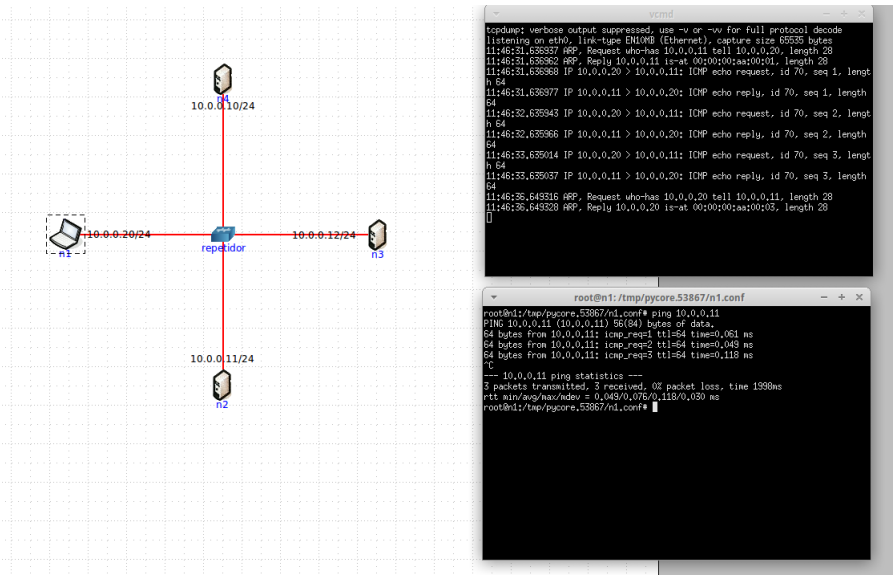

Figura 14

Depois de fazer o ping de n1 para n2, analisando o tráfego num host não envolvido na comunicação, por exemplo, n3, verificamos que apesar de o pedido não lhe ser destinado ele recebe mesmo assim essa comunicação.

18. Na topologia de rede substitua o hub por um switch. Repita os procedimentos que realizou na pergunta anterior. Comente os resultados obtidos quanto a utilizacao de hubs e switches no contexto de controlar ou dividir dominios de colisao. Documente as suas observacoes e conclusoes com base no trafego observado/capturado.

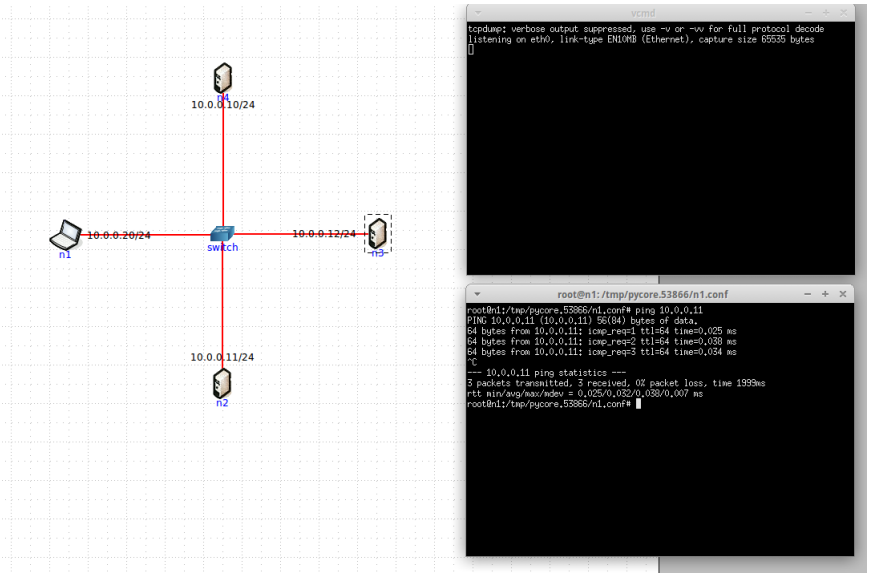

Figura 15

Com a utilização do switch o problema analisado na pergunta anterior fica resolvido, isto porque se analisarmos mais uma vez o tráfego que flui de e para n3 verificamos que com o switch ele já não recebe a ping que n1 faz para n2.

2 Conclusão

Este trabalho prático serviu de complemento às aulas teóricas e ajudou a consolidar a matéria lecionada nas mesmas.

Depois de finalizado o trabalho prático número 3, relativo à Camada de Ligação Lógica: Ethernet e Protocolo ARP, obtivemos mais conhecimentos sobre a camada de Link epercebemos como funciona a interconexão de redes locais baseado no envio de pacotes.

Estudamos ainda como são efetuadas as partilhas de endereços MAC nestas mesmas redes, com a utilização de Protocolo ARP, que é utilizado para a resolução de endereços da camada internet em endereços da camade de Link.

Simulamos ainda um ambiente da ferramenta CORE, que nos permitiu analisar como funcionam os domínios de colisão e o modo como eles são corrigidos através, por exemplo, da utilizão de um switch de rede.

Resumindo, basicamente todo o capítulo de Link Layer foi abrangido e relembrado, e os conceitos inerentes ao mesmo foram consolidados.