

Universidade do Minho

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

26/11/2019

Redes de Computadores

TP3: Camada de Ligação Lógica

PL4 Grupo 9:

António Gonçalves (A85516)

João Araújo (A84306)

João Silva (A81761)

Contents

1	Captura e análise de tramas Ethernet.	2
1.1	Questão 1 - Anote os endereços MAC de origem e de destino da trama capturada.	2
1.2	Questão 2 - Identifique a que sistemas se referem. Justifique.	2
1.3	Questão 3 - Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?	2
1.4	Questão 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.	3
1.5	Questão 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?	4
1.6	Questão 6 - Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.	4
1.7	Questão 7 - Qual é o endereço MAC do destino? A que sistema corresponde?	4
1.8	Questão 8 - Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.	5
2	Protocolo ARP	5
2.1	Questão 9 - Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas	5
2.2	Questão 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?	6
2.3	Questão 11 - Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?	6
2.4	Questão 12 - Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP.	6
2.5	Questão 13 - Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?	7
2.6	Questão 14 - Explícite que tipo de pedido ou pergunta é feito pelo host de origem?	7
2.7	Questão 15 - Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.	7
2.7.1	a. Qual o valor do campo ARP opcode? O que especifica?	7
2.7.2	b. Em que posição da mensagem ARP está a resposta ao pedido ARP?	8

2.8	Questão 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?	8
3	Domínios de colisão	9
3.1	Questão 17 - Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?	9
3.2	Questão 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. .	10
4	Conclusão	11

1 Captura e análise de tramas Ethernet.

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

16	2.010439	192.168.100.187	193.136.19.40	HTTP	609 GET / HTTP/1.1
17	2.011055	193.136.19.40	192.168.100.187	TCP	60 80 → 57133 [ACK] Seq=1 Ack=556 Win=30336 Len=0
18	2.012140	193.136.19.40	192.168.100.187	HTTP	535 HTTP/1.1 301 Moved Permanently (text/html)
19	2.017219	192.168.100.187	193.136.19.40	TCP	66 57135 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

> Frame 16: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits) on interface 0
▼ Ethernet II, Src: HewlettP_3b:00:68 (e4:e7:49:3b:00:68), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
 > Destination: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
 > Source: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
 Type: IPv4 (0x0800)

Figure 1: Endereços de origem e de destino da trama.

Endereço origem: **e4:e7:49:3b:00:68**

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

1.2 Questão 2 - Identifique a que sistemas se referem. Justifique.

O endereço de origem corresponde ao endereço MAC da máquina nativa, registrado como HewlettP. O endereço de destino refere-se ao endereço MAC do destino, registrado como Vmware, fazendo a ligação entre a rede em que estamos e a rede exterior.

1.3 Questão 3 - Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

O valor hexadecimal do campo Type da trama Ethernet corresponde a 0x0800, o que nos permite concluir que a trama possui um pacote IPv4.

1.4 Questão 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.

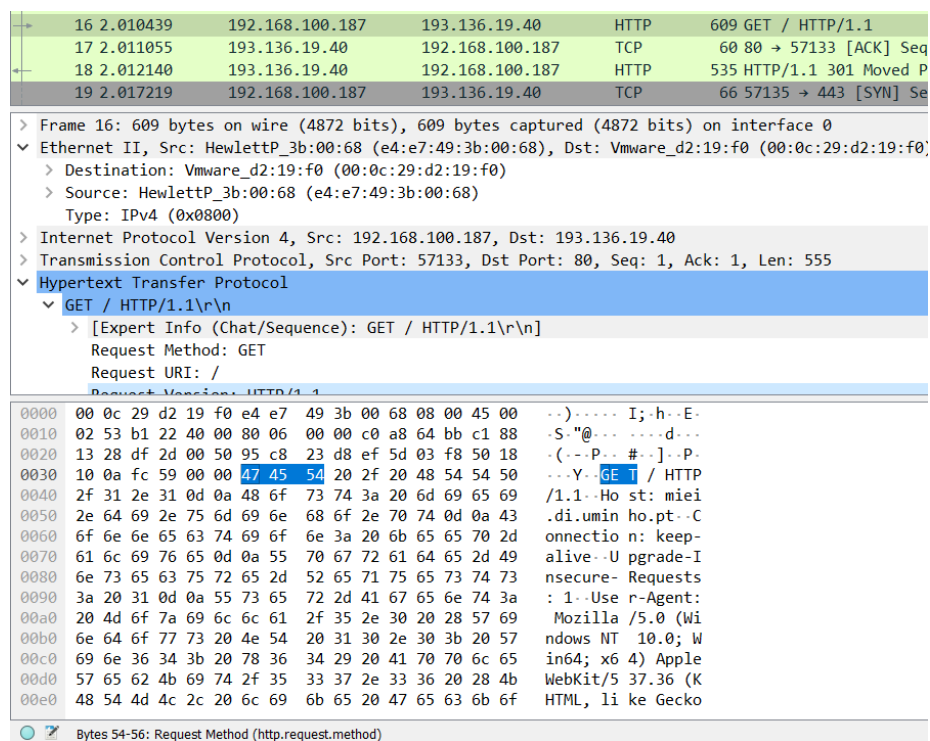


Figure 2: Caracteres ASCII do método HTTP GET.

Através do print apresentado, sabemos que até ao caractere 'G' vão 54 bytes. Sendo o comprimento total da trama correspondente a 609 bytes, a sobrecarga introduzido pela pilha protocolar corresponde a $\frac{54 \times 100}{609} = 8.867\%$

1.5 Questão 5 - Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para detecção de erros não está a ser usado. Em sua opinião, porque será?

Como podemos verificar, o campo FCS não aparece na captura da trama, e deduz-se então que não está a ser utilizado. Como estamos a trabalhar com uma rede wired, a probabilidade de existirem erros é baixa, o que faz com que o custo do cálculo destes não compense.

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

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

33	1.576530	193.136.19.40	192.168.100.187	HTTP	535 HTTP/1.1 301 Moved Permanently (text/html)
34	1.579925	192.168.100.187	193.136.19.40	TCP	66 57326 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
35	1.580623	193.136.19.40	192.168.100.187	TCP	66 443 → 57326 [SYN, ACK] Seq=0 Ack=1 Win=29200

> Frame 33: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
v Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
 > Destination: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
 > Source: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
 Type: IPv4 (0x0800)

Figure 3: Endereço Ethernet da fonte e do destino.

O endereço da fonte é 00:0c:29:d2:19:f0, e corresponde à rede Ethernet a que a máquina está ligada.

1.7 Questão 7 - Qual é o endereço MAC do destino? A que sistema corresponde?

O endereço do destino é e4:e7:49:3b:19:f0, e corresponde à máquina que está a ser utilizada para efetuar a ligação.

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

33	1.576530	193.136.19.40	192.168.100.187	HTTP	535 HTTP/1.1 301 Moved Permanently (text/html)
> Frame 33: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0					
> Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)					
> Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.187					
> Transmission Control Protocol, Src Port: 80, Dst Port: 57324, Seq: 1, Ack: 556, Len: 481					
> Hypertext Transfer Protocol					
> Line-based text data: text/html (7 lines)					

Figure 4: Protocolos contidos na trama.

A trama recebida tem os seguintes protocolos: Ethernet, IPv4, TCP e HTTP.

2 Protocolo ARP

2.1 Questão 9 - Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas

Interface: 192.168.56.1 --- 0x10		
Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
Interface: 192.168.100.187 --- 0x12		
Internet Address	Physical Address	Type
192.168.100.254	00-0c-29-d2-19-f0	dynamic
192.168.100.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Figure 5: Tabela ARP.

A primeira coluna representa os endereços IP, a segunda os MAC address e a terceira os diferentes tipos de endereçamento.

2.2 Questão 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 endereço de origem é 00:0c:29:d2:19:f0 e o endereço de destino ff:ff:ff:ff:ff:ff. Isto acontece uma vez que o endereço de destino tem que ser identificável por todas as máquinas da rede. Assim, o pedido será enviado para todos os hosts da rede uma vez que, mesmo sabendo o endereço IP, não sabemos o endereço físico (MAC address).

Time	Source	Destination	Protocol	Length	Info
629	7.182361	Vmware_d2:19:f0	Broadcast	ARP	60 Who has 192.168.100.199? Tell 192.168.100.254
> Frame 629: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0					
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)					
> Source: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)					
Type: ARP (0x0806)					
Padding: 00					
> Address Resolution Protocol (request)					

Figure 6: Endereços de destino e de origem da trama.

2.3 Questão 11 - Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?

O valor do campo tipo da trama é 0x0806, o que significa que se trata de uma trama ARP.

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

```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Sender IP address: 192.168.100.254
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.100.199
```

Figure 7: Valor do campo ARP opcode.

Como podemos observar na imagem anterior, o valor do campo ARP opcode é 1, o que identifica um ARP request.

2.5 Questão 13 - Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

```
Sender MAC address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Sender IP address: 192.168.100.254
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.100.199
```

Figure 8: Endereços contidos na mensagem ARP.

Estão contidos na mensagem ARP o IP e MAC address da nossa máquina e o IP do destino. Para além disso, uma vez que ainda não conhecemos o MAC address do destino, este é identificado por 00:00:00:00:00:00.

2.6 Questão 14 - Explícite que tipo de pedido ou pergunta é feito pelo host de origem?

O host de origem pergunta quem tem o endereço de destino (Who has 192.168.100.199?). Assim irá, através do endereço IP, descobrir o MAC address a que lhe corresponde.

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

634 7.563926	HewlettP_3b:00:68	Vmware_d2:19:f0	ARP	42 192.168.100.187 is at e4:e7:49:3b:00:68
635 7.611091	Cisco_4b:19:09	Cisco_4b:19:09	LOOP	60 Reply
636 7.817033	Cisco_4b:19:09	Spanning-tree-(for-- STP	60 Conf.	Root = 4096/720/00:0a:8a:97:74:80

Frame 634: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HewlettP_3b:00:68 (e4:e7:49:3b:00:68), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
Sender IP address: 192.168.100.187
Target MAC address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Target IP address: 192.168.100.254

Figure 9: Resposta ao pedido ARP.

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

O campo ARP opcode tem o valor de 2 e identifica um ARP reply.

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

Sender MAC address: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)	
Sender IP address: 192.168.100.187	
Target MAC address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)	
Target IP address: 192.168.100.254	

0000	00	0c	29	d2	19	f0	e4	e7	49	3b	00	68	08	06	00	01	..)	Ij;h...
0010	08	00	06	04	00	02	e4	e7	49	3b	00	68	c0	a8	64	bbIj;h...	-d-
0020	00	0c	29	d2	19	f0	c0	a8	64	fe							..)	d.

Figure 10: Posição da resposta ao pedido ARP.

A resposta ao pedido ARP está na posição 22-27, correspondente ao Sender MAC address.

2.8 Questão 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?

108 6.836832	HewlettP_3b:00:68	Broadcast	ARP	42 Gratuitous ARP for 192.168.100.187 (Request)
109 6.836862	HewlettP_3b:00:68	Broadcast	ARP	42 Who has 172.26.254.254? Tell 192.168.100.187
79 5.781782	Cisco_4b:19:09	CDP/VTP/DTP/PAGP/UD...	CDP	416 Device ID: Bastidor0_SW3 Port ID: FastEther
80 5.782989	Cisco_4b:19:09	CDP/VTP/DTP/PAGP/UD...	CDP	416 Device ID: Bastidor0_SW3 Port ID: FastEther
81 5.784514	Cisco_4b:19:09	CDP/VTP/DTP/PAGP/UD...	CDP	416 Device ID: Bastidor0_SW3 Port ID: FastEther
16 4.073006	Cisco_4b:19:09	Cisco_4b:19:09	LOOP	60 Reply
1 0.000000	Cisco_4b:19:09	Spanning-tree-(for-...	STP	60 Conf. Root = 4096/720/00:0a:8a:97:74:80 Cos
15 4.005767	Cisco_4b:19:09	Spanning-tree-(for-...	STP	60 Conf. Root = 4096/720/00:0a:8a:97:74:80 Cos


```

> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: HewlettP_3b:00:68 (e4:e7:49:3b:00:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
    Type: ARP (0x0806)
v Address Resolution Protocol (request/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is gratuitous: True]
  Sender MAC address: HewlettP_3b:00:68 (e4:e7:49:3b:00:68)
  Sender IP address: 192.168.100.187
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.100.187

```

Figure 11: Informação referente ao pacote de pedido ARP gratuito.

Como podemos observar, o pedido ARP gratuito tem o Sender IP address e o Target IP address iguais. Isto acontece para ter a certeza que não existe outro equipamento na rede com o IP da máquina igual, uma vez que, se houvesse outra com o mesmo, este iria responder ao pedido. Uma vez que não obteve resposta, podemos concluir que não existe nenhum equipamento ligado à rede com o IP igual a este.

3 Domínios de colisão

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

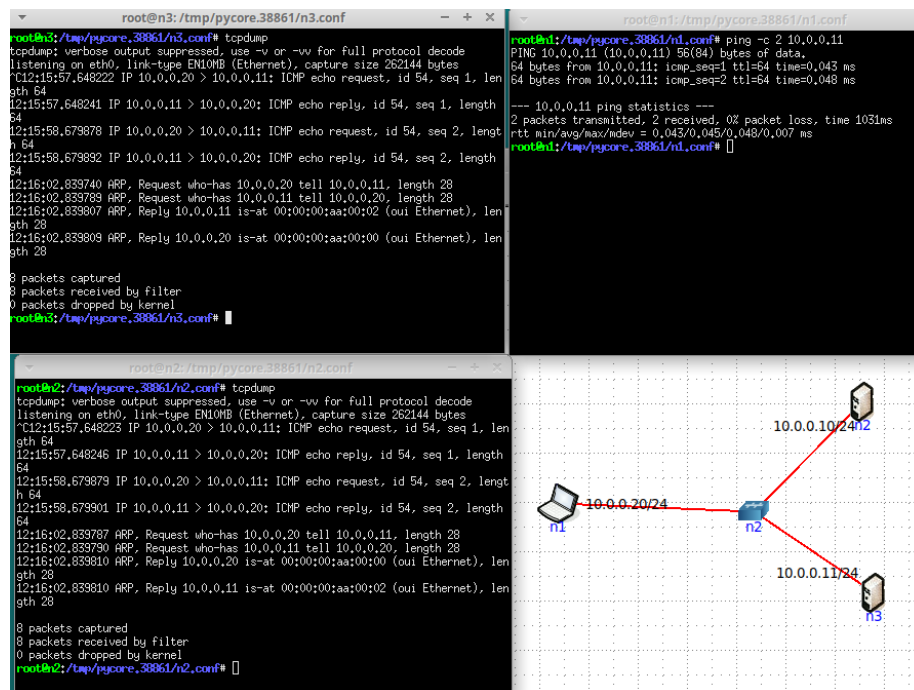


Figure 12: Tráfego na Topologia do CORE.

Podemos observar que a mensagem enviada de n1 para n2 foi também recebida por n3. Isto acontece porque o hub repete a mensagem a todos os equipamentos a ele ligados. Assim, qualquer mensagem que seja enviada através do hub será posteriormente repetida para por todos os equipamentos a ele ligados.

3.2 Questão 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.

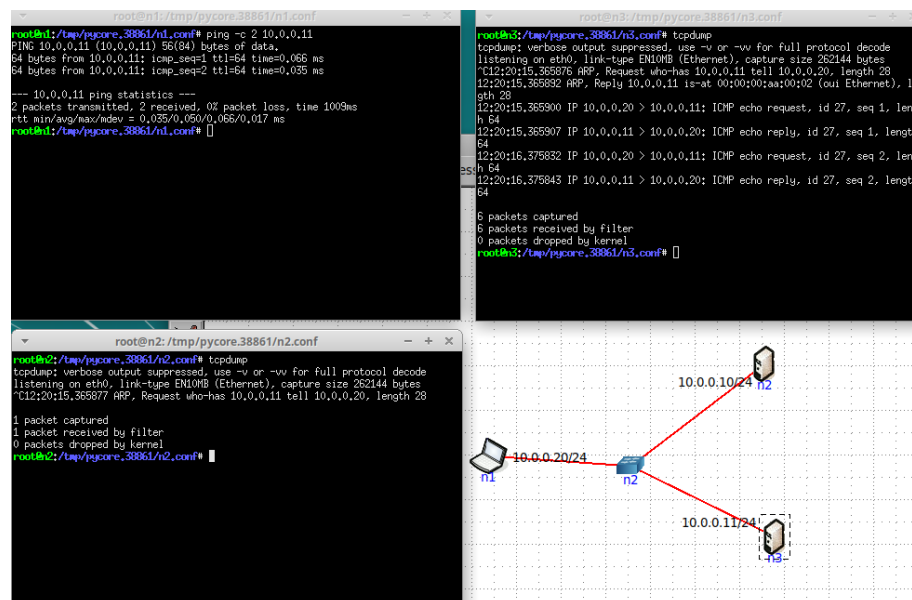


Figure 13: Tráfego na Topologia do CORE com um Switch.

Após substituir o hub por um switch, podemos observar que não ocorre o mesmo. A mensagem enviada de n1 para n3 não é repetida para todos os equipamentos. Ao usar um switch são criados canais utilizados unicamente para transmitir as mensagens da origem para o destino, sem ter de transmitir às máquinas restantes.

4 Conclusão

Através da resolução deste trabalho, cuja primeira parte se baseia no estudo das ligações Ethernet, foi-nos possível compreender melhor o funcionamento da camada de ligação lógica. Analisámos tramas e estudamos o seu funcionamento, aprendemos sobre o protocolo ARP que nos facilitou e ajudou na compreensão dos mecanismos de mapeamento entre os diversos endereços de rede.

Com o último exercício, aprendemos a estudar as diferenças entre a utilização de diferentes dispositivos físicos, como um hub e um switch. Analisámos os diferentes funcionamentos e as características associadas a estes, fatores chave para escolher aquele que melhor se adequa consoante a situação. Neste trabalho, concluímos que o switch era a melhor opção.