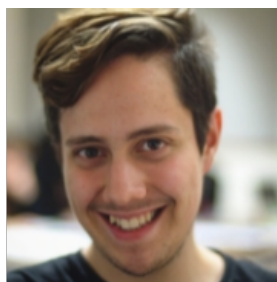




Beatriz Rocha
A84003



Filipe Guimarães
A85308



Gonçalo Ferreira
A84073

Relatório do Trabalho Prático 3 de Redes de Computadores Grupo 1

26 de Novembro de 2019



Conteúdo

1	Captura e análise de tramas Ethernet	3
1.1	Pergunta 1	3
1.2	Pergunta 2	3
1.3	Pergunta 3	4
1.4	Pergunta 4	4
1.5	Pergunta 5	4
1.6	Pergunta 6	5
1.7	Pergunta 7	5
1.8	Pergunta 8	5
2	Protocolo ARP	6
2.1	Pergunta 9	6
2.2	Pergunta 10	7
2.3	Pergunta 11	7
2.4	Pergunta 12	8
2.5	Pergunta 13	8
2.6	Pergunta 14	8
2.7	Pergunta 15	9
	2.7.1 Alínea a	9
	2.7.2 Alínea b	9
2.8	Pergunta 16	10
3	Domínios de colisão	11
3.1	Pergunta 17	11
3.2	Pergunta 18	12
4	Conclusões	13

Lista de Figuras

1.1	Captura do tráfego no Wireshark	3
1.2	Frame capturada	4
1.3	Protocolos usados	4
1.4	Trama Ethernet que contém o primeiro byte da resposta HTTP	5
2.1	Tabela arp	6
2.2	Trama Ethernet que contém a mensagem com o pedido ARP	7
2.3	Campo tipo da trama Ethernet	7
2.4	Campo ARP opcode	8
2.5	Tipo de pedido feito pelo host de origem	8
2.6	Resposta ao pedido ARP efetuado	9
2.7	ARP gratuito	10
3.1	Frame capturada	11
3.2	Frame capturada	12

Capítulo 1

Captura e análise de tramas Ethernet

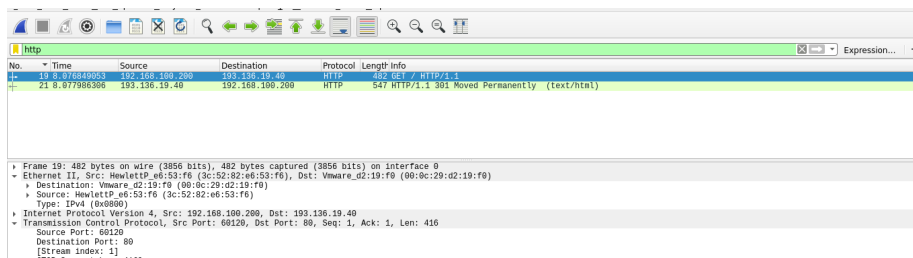


Figura 1.1: Captura do tráfego no Wireshark

1.1 Pergunta 1

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

Como podemos observar na figura acima, o endereço MAC de origem é 3c:52:82:e6:53:f6 (campo *Source*) e o de destino é 00:0c:29:d2:19:f0 (campo *Destination*).

1.2 Pergunta 2

Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem (campo *Source*) corresponde à interface da nossa placa de rede, enquanto o endereço de destino (campo *Destination*) corresponde à interface do router da rede local a que estamos conectados.

1.3 Pergunta 3

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

Como podemos ver na figura 1.1 o campo *Type* da trama Ethernet é 0x0800 que corresponde ao protocolo utilizado ao nível de rede, isto é, IPv4.

1.4 Pergunta 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.

0000	00 0c 29 d2 19 f0 3c 52 82 e6 53 f6 08 00 45 00	..)....<R . S . E .
0010	01 d4 56 5e 40 00 40 06 e8 a4 c0 a8 64 c8 c1 88	..V@.@ . . . d . .
0020	13 28 ea d8 00 50 ae 58 9f fe 1a bf 10 55 80 18	(. . P X U . .
0030	01 f6 fb e7 00 00 01 01 08 0a f8 aa bc 6f d3 b0 o
0040	15 b0 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31	..G.. / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20 6d 69 65 69 2e 64 69 2e	..Host: miei.di.
0060	75 6d 69 6e 68 6f 2e 70 74 0d 0a 43 6f 6e 6e 65	uminho.p t . . Conne
0070	63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76	ction: k eep-aliv
0080	65 0d 0a 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61	e . . DNT: 1 . . Upgra
0090	64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75	de-Insec ure-Requ
00a0	65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67	ests: 1 . . User-Ag
00b0	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00c0	20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36	(X11; L inux x86
00d0	5f 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74	_64) App leWebKit
00e0	2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20	/537.36 (KHTML,
00f0	6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f	like Gec ko) Chro
0100	6d 65 2f 37 38 2e 30 2e 33 39 30 34 2e 37 30 20	me/78.0. 3904.70
0110	53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41	Safari/5 37.36 . . A
0120	63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c	ccept: t ext/html
0130	2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74	, applica tion/xht
0140	6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69	ml+xml, a pplicati

Figura 1.2: Frame capturada

Desde o início da trama até ao caractere ASCII ”G” são usados 66 bytes. Como são usados 482 bytes no total, a sobrecarga introduzida pela pilha protocolar no envio do HTTP GET é, aproximadamente 13.69% ($66/482 \approx 0.1369$).

1.5 Pergunta 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?

Frame 19: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0
Ethernet II, Src: HewlettP-e6:53:f6 (3c:52:82:e6:53:f6), Dst: Vmware-d2:19:f0 (00:0c:29:02:19:f0)
Internet Protocol Version 4, Src: 192.168.100.200, Dst: 193.136.19.40
Transmission Control Protocol, Src Port: 80, Dst Port: 80, Seq: 1, Ack: 1, Len: 416
Hypertext Transfer Protocol

Figura 1.3: Protocolos usados

Como podemos ver na figura acima, o protocolo FCS não está a ser usado. Na nossa opinião, isto acontece porque este protocolo serve para detetar erros e, como através de uma ligação por fio é praticamente impossível estes ocorrerem, este protocolo não é usado.

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

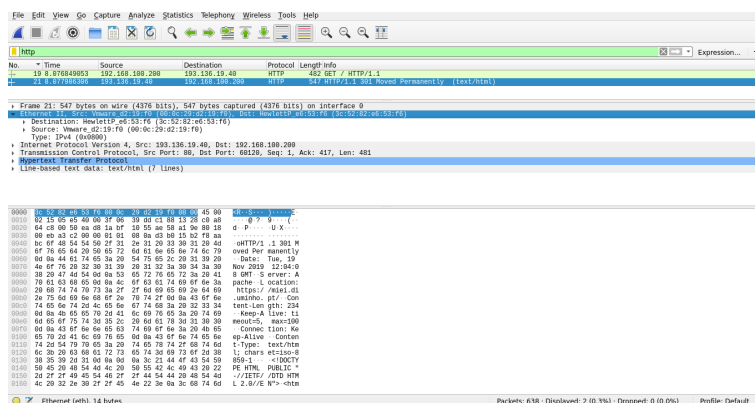


Figura 1.4: Trama Ethernet que contém o primeiro byte da resposta HTTP

1.6 Pergunta 6

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

O endereço Ethernet da fonte é 00:0c:29:d2:19:f0 (campo *Source*) e corresponde ao router da rede onde estamos ligados, já que é dele que recebemos a resposta.

1.7 Pergunta 7

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

O endereço MAC do destino é 3c:52:82:e6:53:f6 (campo *Destination*) e corresponde à interface ativa do nosso computador.

1.8 Pergunta 8

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

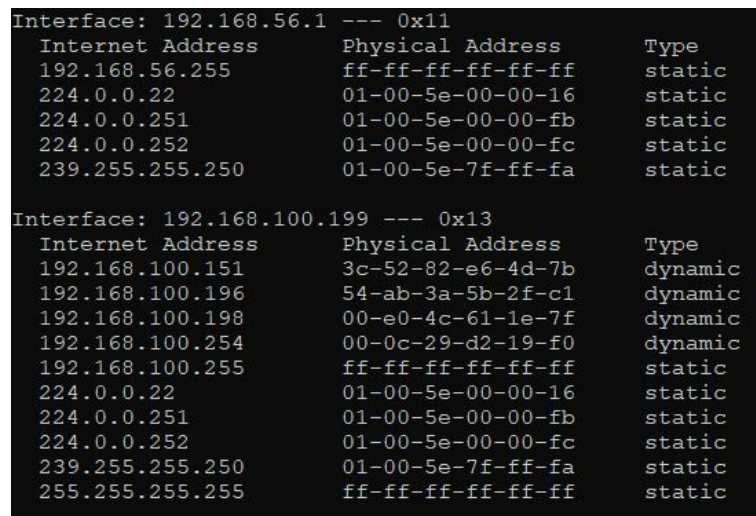
Como podemos ver na figura 2.5, os protocolos contidos na trama recebida são Ethernet II, Internet Protocol Version 4 (IPv4), Transmission Control Protocol (TCP) e Hypertext Transfer Protocol (HTTP).

Capítulo 2

Protocolo ARP

2.1 Pergunta 9

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



```
Interface: 192.168.56.1 --- 0x11
  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: 192.168.100.199 --- 0x13
  Internet Address      Physical Address      Type
  192.168.100.151       3c-52-82-e6-4d-7b    dynamic
  192.168.100.196       54-ab-3a-5b-2f-c1    dynamic
  192.168.100.198       00-e0-4c-61-1e-7f    dynamic
  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
```

Figura 2.1: Tabela arp

A função da tabela ARP é mapear o endereço IP para o endereço MAC dos sistemas que comunicaram recentemente. Assim sendo, na primeira coluna da imagem acima podemos observar o endereço IP, na segunda o endereço MAC e na terceira o tipo de endereçamento utilizado.

2.2 Pergunta 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?

```
> Frame 1073: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
  Sender IP address: 192.168.100.199
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.100.215
```

Figura 2.2: Trama Ethernet que contém a mensagem com o pedido ARP

Na figura acima, podemos observar que o endereço de origem é 3c:52:82:e6:53:f6 e o endereço de destino é ff:ff:ff:ff:ff:ff. O endereço de destino faz com que todos os endereços conectados à rede recebam a mensagem com o pedido ARP, mas apenas o endereço pretendido responde com o seu endereço MAC.

2.3 Pergunta 11

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

```
> Frame 1073: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
  Type: ARP (0x0806)
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
  Sender IP address: 192.168.100.199
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

0000  ff ff ff ff ff 3c 52 82 e6 53 f6 08 06 00 01  .....<R ..S.  ..
0010  08 00 06 04 00 01 3c 52 82 e6 53 f6 c0 a8 64 c7  .....<R ..S...d.
0020  00 00 00 00 00 00 c0 a8 64 d7  ....d.
```

Figura 2.3: Campo tipo da trama Ethernet

Na figura acima, podemos observar que o valor hexadecimal do campo tipo da trama Ethernet é 0x0806. Este indica que o campo de dados pertence ao ARP.

2.4 Pergunta 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>).

Opcode: request (1)														
0000	ff	ff	ff	ff	ff	3c	52	82	e6	53	f6	08	06 00 01<R ..S.....
0010	08	00	06	04	00 01	3c	52	82	e6	53	f6	c0	a8 64 c7<R ..S...d.
0020	00	00	00	00	00 00	c0	a8	64	d7				 d.

Figura 2.4: Campo ARP opcode

O campo opcode especifica se é um pedido ou uma resposta. Como podemos ver na figura acima, o valor do campo ARP opcode é 1 (0x0001), que é um pedido (*request*), segundo a RFC do protocolo ARP.

2.5 Pergunta 13

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

Na mensagem ARP estão contidos os endereços IP de origem e destino. Contudo, como se trata de um pedido, apenas é conhecido o endereço MAC correspondente ao endereço IP de origem.

2.6 Pergunta 14

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

1073	159.495849	HewlettP_e6:53:f6	Broadcast	ARP	42	Who has 192.168.100.215? Tell 192.168.100.199
1074	159.496678	AsustekC_89:7c:8e	HewlettP_e6:53:f6	ARP	60	192.168.100.215 is at 54:a0:50:89:7c:8e

Figura 2.5: Tipo de pedido feito pelo host de origem

Na figura acima, podemos ver que o nosso aparelho pergunta "Who has 192.168.100.215? Tell 192.168.100.199"e, portanto, iremos obter como resposta o endereço MAC do aparelho com o endereço 192.168.100.215.

2.7 Pergunta 15

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

1073	159.495849	HewlettP_e6:53:f6	Broadcast	ARP	42	Who has 192.168.100.215? Tell 192.168.100.199
1074	159.496678	AsustekC_89:7c:8e	HewlettP_e6:53:f6	ARP	60	192.168.100.215 is at 54:a0:50:89:7c:8e
1096	164.505474	AsustekC_89:7c:8e	HewlettP_e6:53:f6	ARP	60	Who has 192.168.100.199? Tell 192.168.100.215
1097	164.505487	HewlettP_e6:53:f6	AsustekC_89:7c:8e	ARP	42	192.168.100.199 is at 3c:52:82:e6:53:f6

> Frame 1074: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> Ethernet II, Src: AsustekC_89:7c:8e (54:a0:50:89:7c:8e), Dst: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)

> Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: AsustekC_89:7c:8e (54:a0:50:89:7c:8e)
Sender IP address: 192.168.100.215
Target MAC address: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
Target IP address: 192.168.100.199

0000	3c 52 82 e6 53 f6 54 a0 50 89 7c 8e 00 06 00 01	<R..S.T..P..
0010	00 00 06 04 00 02 54 a0 50 89 7c 8e c0 a8 64 d7I..P..I..d.
0020	3c 52 82 e6 53 f6 c0 a8 64 c7 00 00 00 00 00 00	<R..S...d.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figura 2.6: Resposta ao pedido ARP efetuado

2.7.1 Alínea a

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

O valor do campo ARP opcode é 2 (0x0002), que especifica uma resposta (*reply*), segundo a RFC do protocolo ARP.

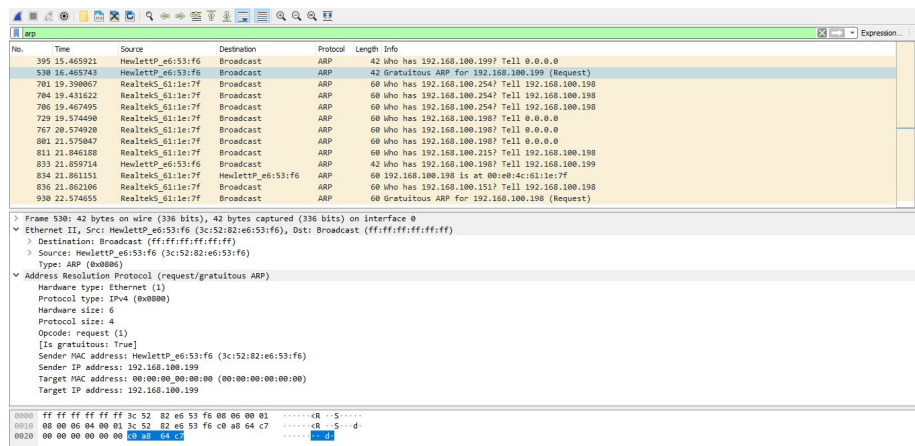
2.7.2 Alínea b

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

A resposta ao pedido ARP está entre os bytes 23 e 28 da mensagem ARP, como podemos observar na figura 2.6.

2.8 Pergunta 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?



No.	Time	Source	Destination	Protocol	Length	Info
395	15.465921	HewlettP_e6:53:f6	Broadcast	ARP	42	Who has 192.168.100.199? Tell 0.0.0.0
530	16.463743	HewlettP_e6:53:f6	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.199 (Request)
701	19.308067	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.254? Tell 192.168.100.198
784	19.431622	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.254? Tell 192.168.100.198
786	19.467495	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.254? Tell 192.168.100.198
729	19.574408	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.198? Tell 0.0.0.0
767	20.574920	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.198? Tell 0.0.0.0
801	21.575847	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.198? Tell 0.0.0.0
811	21.846188	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.215? Tell 192.168.100.198
833	21.859714	HewlettP_e6:53:f6	Broadcast	ARP	42	Who has 192.168.100.198? Tell 192.168.100.199
834	21.861151	RealtekS_61:1e:7f	HewlettP_e6:53:f6	ARP	60	192.168.100.198 is at 00:e0:4c:61:1e:7f
836	21.862106	RealtekS_61:1e:7f	Broadcast	ARP	60	Who has 192.168.100.151? Tell 192.168.100.198
930	22.574655	RealtekS_61:1e:7f	Broadcast	ARP	60	Gratuitous ARP for 192.168.100.198 (Request)

Frame 530: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
Type: ARP (0x0008)
Address Resolution Protocol (request/gratuitous ARP)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0008)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: true]
Sender MAC address: HewlettP_e6:53:f6 (3c:52:82:e6:53:f6)
Sender IP address: 192.168.100.199
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.100.199

0000 ff ff ff ff ff 3c 52 82 e6 53 f6 08 06 00 01R..S.....
0010 00 00 00 00 00 01 3c 52 82 e6 53 f6 c0 a0 04 c7R..S...d..
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figura 2.7: ARP gratuito

Como podemos observar na figura 2.7 há um campo que não existia nos restantes pedidos (*Is gratuitous: true*). Para além disso, verificamos que os endereço de origem e de destino são iguais. O resultado esperado face a este *ARP gratuito* é que não haja resposta, caso houvesse significava que existia um dispositivo com o mesmo endereço de IP, criando, assim, um conflito.

Capítulo 3

Domínios de colisão

3.1 Pergunta 17

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

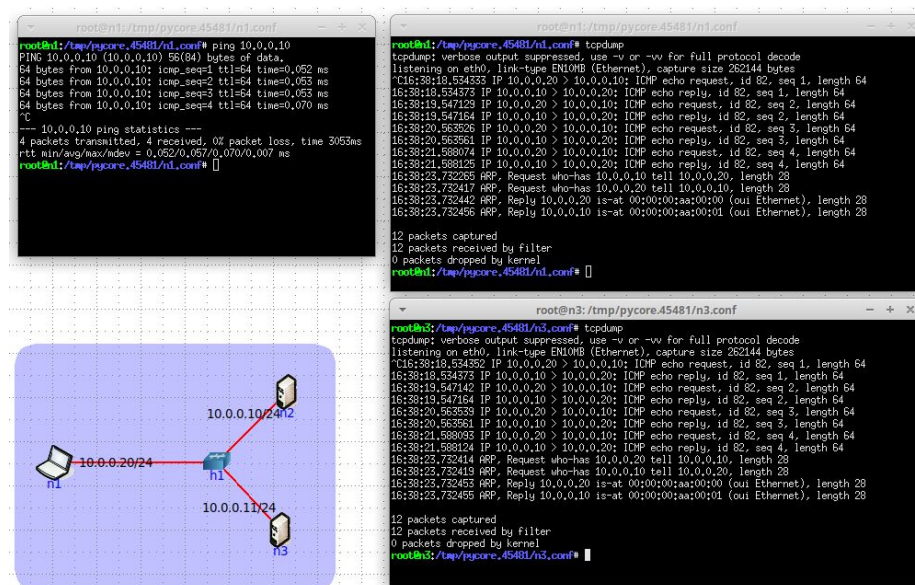


Figura 3.1: Frame capturada

Ao executar o *tcpdump* nos dois servidores e *ping* entre n1 e n2 constatamos que ambos os servidores recebem pacotes, como podemos ver na figura 3.1. Isto acontece, porque, quando o *hub* recebe os pacotes, reencaminha-os para todos os dispositivos na rede.

3.2 Pergunta 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.

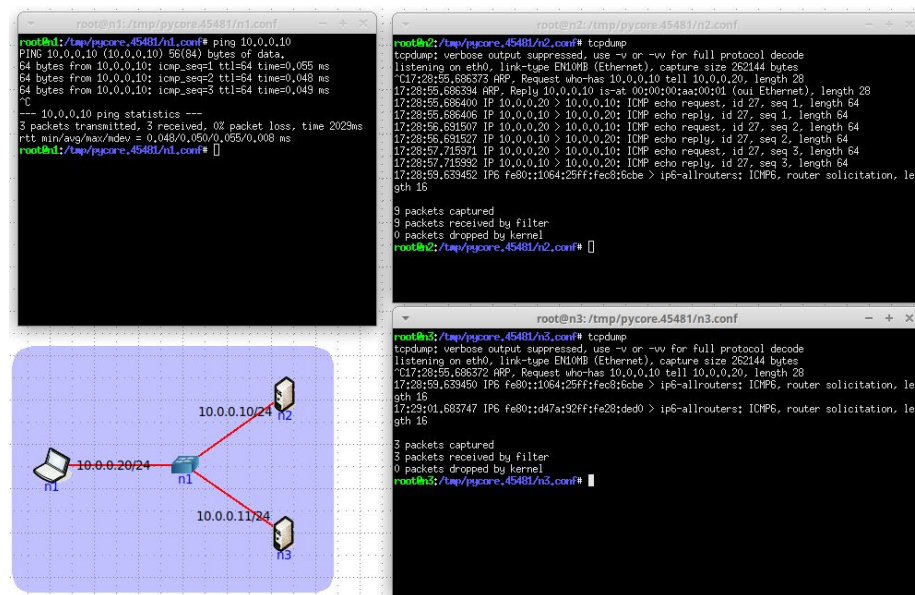


Figura 3.2: Frame capturada

Ao substituir o antigo *hub* por um *switch* e repetir o procedimento da pergunta anterior, vemos que, ao contrário da pergunta 17, o servidor n3 não recebe nenhum pacote (figura 3.2). Nesta nova topologia a mensagem é enviada ao switch e este, por sua vez, envia-a diretamente para o host. O pacote recebido pelo n3 é o *ARP request*, que é enviado para ambos os dispositivos. Tendo em conta estas informações, percebemos que os *hubs* fazem circular informação inútil na rede. Concluimos, então, que o uso de switches é mais viável que o uso de hubs.

Capítulo 4

Conclusões

Com a realização deste trabalho prático, pudemos consolidar conhecimentos acerca de rede locais, endereços *MAC* e o protocolo de rede ARP (Address Resolution Protocol).

Usamos o *Wireshark* para capturar tramas *Ethernet*, analisando, posteriormente, diversos campos e verificando se existia um controle de erros como o *FCS*.

Observamos e interpretamos o conteúdo da tabela *ARP* na nossa máquina. Verificamos também a presença deste protocolo numa captura feita a outro computador, usando o *Wireshark*. Analisamos vários campos nas diversas "perguntas" e "repostas".

Por fim, criamos uma topologia no *CORE* para analisar as diferenças entre *switches* e *hubs*.

Posto isto, ao pôr em prática aquilo que foi lecionado nas aulas teóricas, conseguimos consolidar melhor os nossos conhecimentos e acreditamos que os objetivos propostos foram alcançados.