



TRABALHO PRÁTICO 3

Redes de Computadores

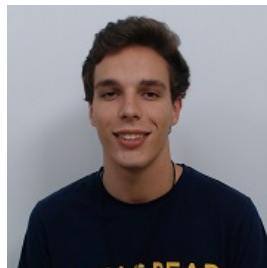
Grupo 14



Inês Bastos A89522



João Freitas A83782



João Félix A89460

Dezembro de 2020

Conteúdo

1	TP3: Nível de Ligação Lógica: Ethernet e Protocolo ARP	2
1.1	Captura e análise de Tramas Ethernet	2
1.2	Protocolo ARP	5
1.3	ARP Gratuito	7
1.4	Domínios de colisão	8
2	Conclusão	10

Capítulo 1

TP3: Nível de Ligação Lógica: Ethernet e Protocolo ARP

1.1 Captura e análise de Tramas 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.

No sentido de proceder à análise do tráfego, selecione a trama Ethernet que contém a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP está no interior de um segmento TCP que é transportado num datagrama IP que, por sua vez, está encapsulado no campo de dados de uma trama Ethernet. Expanda a informação do nível da ligação de dados e observe o conteúdo da trama Ethernet (cabeçalho e dados (payload)).

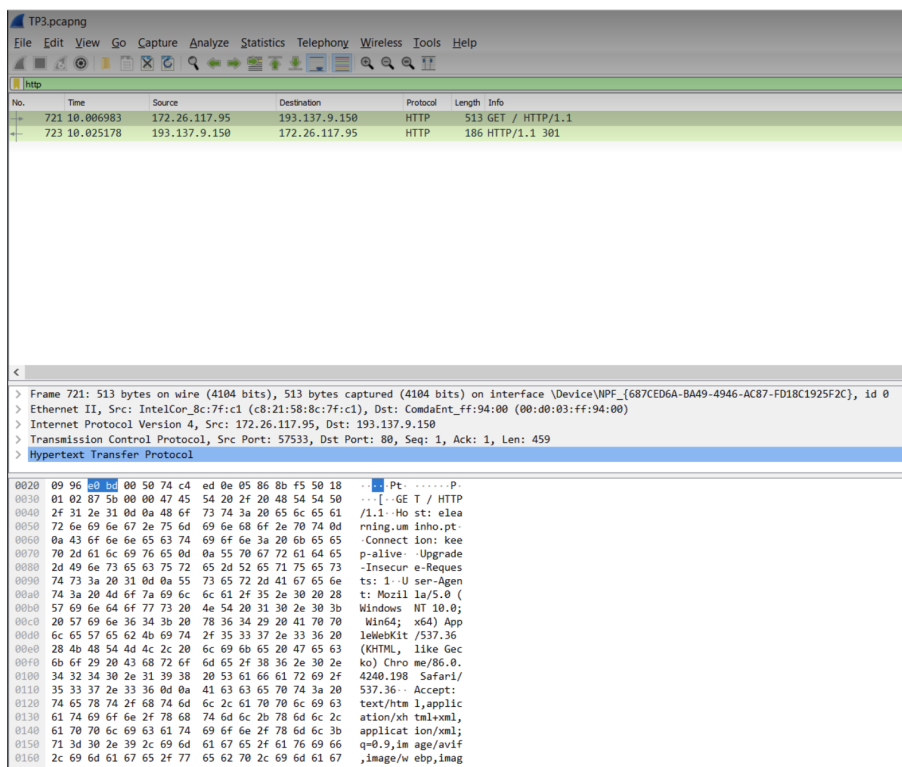


Figura 1.1

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem HTTP GET.

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

```
> Frame 721: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{687CED6A-BA49-4946-AC87-FD18C1925F2C}, id 0
Ethernet II, Src: IntelCor_8c:7f:c1 (c8:21:58:8c:7f:c1), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: IntelCor_8c:7f:c1 (c8:21:58:8c:7f:c1)
    Address: IntelCor_8c:7f:c1 (c8:21:58:8c:7f:c1)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Figura 1.2

MAC de Origem(c8:21:58:8c:7f:c1)

MAC de Destino(00:d0:03:ff:94:00)

2. Identifique a que sistemas se referem. Justifique.

O Endereço de origem refere-se à interface de Ethernet da nossa máquina.

Endereço de destino refere-se à interface de router da rede local. O Endereço de origem representa o local de onde é enviada a trama, ou seja, significa que esse endereço irá 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 , posteriormente, 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 podemos verificar na Figura 3.2. Indica que encapsula um pacote IPV4.

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.

000	00 d0 03 ff 94 00 c8 21 58 8c 7f c1 08 00 45 00! X....E.
010	01 f3 18 29 40 00 80 06 f4 42 ac 1a 75 5f c1 89	...)@...-B...u..
020	09 96 e0 bd 00 50 74 c4 ed 0e 05 86 8b f5 50 18Pt.P.
030	01 02 87 5b 00 00 47 45 54 20 2f 20 48 54 54 50	...[.]GE T / HTTP
040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 6c 65 61	/1.1..Host: elea
050	72 6e 69 6e 67 2e 75 6d 69 6e 68 6f 2e 70 74 0d	rning.um inho.pt-
060	0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65	-Connect ion: kee
070	70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65	p-alive- Upgrade
080	2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73	-Insecur e-Reques
090	74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e	ts: 1..U ser-Agen
0a0	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28	t: Mozil la/5.0 (
0b0	57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b	Windows NT 10.0;
0c0	20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70	Win64; x64) App

Figura 1.3

R: Tamanho dos cabeçalhos dos Protocolos:

IP- 20 bytes. TCP- 20 bytes. Ethernet - 14 bytes

O tamanho total são 54 bytes.

Percentagem da sobrecarga: $54/513 \times 100 = 10,53\%$

5. Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)).

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

Este campo, nas redes Wireless, já costuma ser utilizado devido à grande suscetibilidade de erros.

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

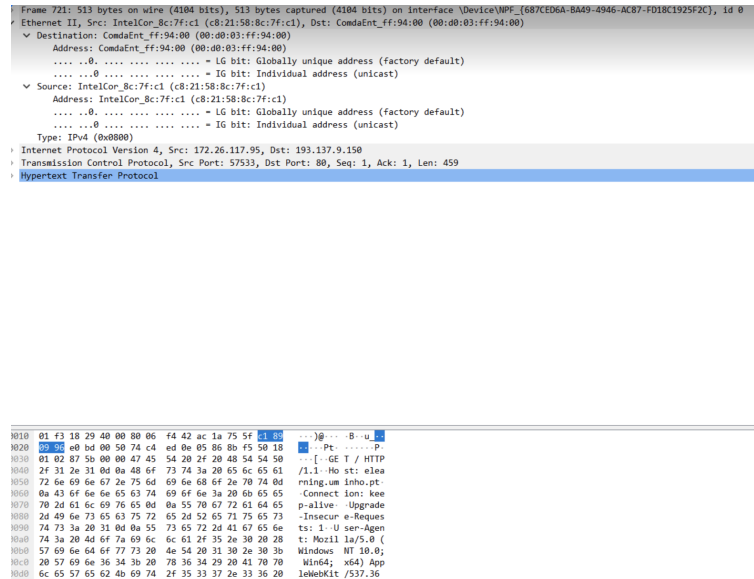


Figura 1.4

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

Source- c8:21:58:8c:7f:c1

Corresponde ao gateway da rede local, uma vez que só nós podemos ver o endereço IP das redes locais e o gateway.

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

R: Destino : 172.26.117.95.

Corresponde à interface Ethernet da nossa máquina.

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

R:TCP, IP, Ethernet.

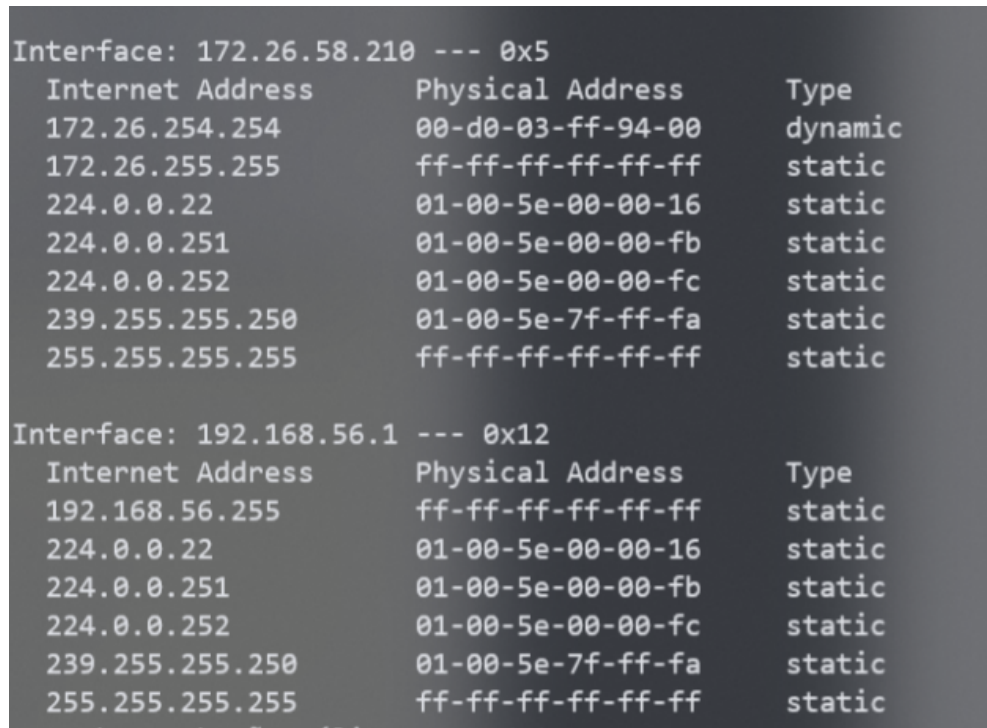
1.2 Protocolo ARP

9. Observe o conteúdo 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.

A terceira coluna representa a interface

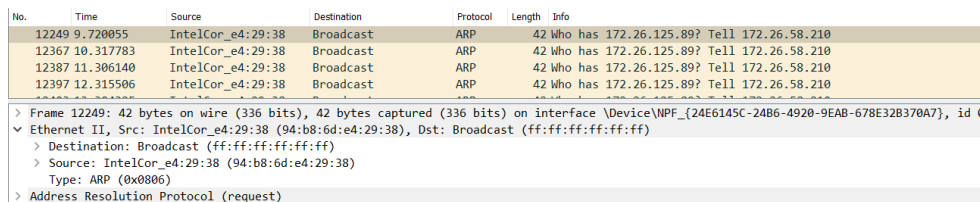


```
Interface: 172.26.58.210 --- 0x5
Internet Address      Physical Address      Type
172.26.254.254        00-d0-03-ff-94-00    dynamic
172.26.255.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          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

Interface: 192.168.56.1 --- 0x12
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
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

Figura 1.5

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?



No.	Time	Source	Destination	Protocol	Length	Info
12249	9.720055	IntelCor_e4:29:38	Broadcast	ARP	42	Who has 172.26.125.89? Tell 172.26.58.210
12367	10.317783	IntelCor_e4:29:38	Broadcast	ARP	42	Who has 172.26.125.89? Tell 172.26.58.210
12387	11.306140	IntelCor_e4:29:38	Broadcast	ARP	42	Who has 172.26.125.89? Tell 172.26.58.210
12397	12.315506	IntelCor_e4:29:38	Broadcast	ARP	42	Who has 172.26.125.89? Tell 172.26.58.210

> Frame 12249: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{24E6145C-24B6-4920-9EAB-678E32B370A7}, id 0

▼ Ethernet II, Src: IntelCor_e4:29:38 (94:b8:6d:e4:29:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: IntelCor_e4:29:38 (94:b8:6d:e4:29:38)

> Type: ARP (0x0806)

> Address Resolution Protocol (request)

Figura 1.6

O endereço de origem é 94:b8:6d:e4:29:38 e o de destino é ff:ff:ff:ff:ff:ff.
É usado o endereço do broadcast para se receber todos os hosts da rede.

11. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica? (0x0806).

Encapsula um frame ARP.

12. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? (Se necessário, consulte a RFC do protocolo ARP <http://tools.ietf.org/html/rfc826.html>).

```
type: ARP (0x0800)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_e4:29:38 (94:b8:6d:e4:29:38)
    Sender IP address: 172.26.58.210
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.125.89
```

Figura 1.7

Podemos ver que se trata de um pedido porque tem a flag request(1).

13. Explícite que tipo de pedido ou pergunta é feita pelo host de origem?

Perguntamos qual o mac do IP 172.26.125.89, e pedimos para enviar a resposta para o IP 172.26.58.210.

14. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. a. Qual o valor do campo ARP opcode? O que especifica? b. Em que posição da mensagem ARP está a resposta ao pedido ARP ?

Não obtivemos nenhuma mensagem ARP com o opcode reply (2), porque a rede que usamos, "eduroam", bloqueia este tipo de tráfego.

1.3 ARP Gratuito

15. 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?

```

  v Ethernet II, Src: IntelCor_e4:29:38 (94:b8:6d:e4:29:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: IntelCor_e4:29:38 (94:b8:6d:e4:29:38)
    Type: ARP (0x0806)
  v Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: IntelCor_e4:29:38 (94:b8:6d:e4:29:38)
    Sender IP address: 172.26.58.210
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.58.210

```

Figura 1.8

O que distingue este pedido ARP do resto é que possui uma flag que indica de que se trata de um pedido ARP Gratuito: [Is gratuitous: True] e porque a Sender e Target IP são iguais.

0000	ff ff ff ff ff ff 94 b8 6d e4 29 38 08 06 00 01 m.)8....
0010	08 00 06 04 00 01 94 b8 6d e4 29 38 ac 1a 3a d2 m.)8-:-
0020	00 00 00 00 00 00 ac 1a 3a d2 :-

Figura 1.9

Porque é uma mensagem ARP Gratuita não é suposto que não haja resposta.

1.4 Domínios de colisão

16. Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando ping). Que conclui? 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.

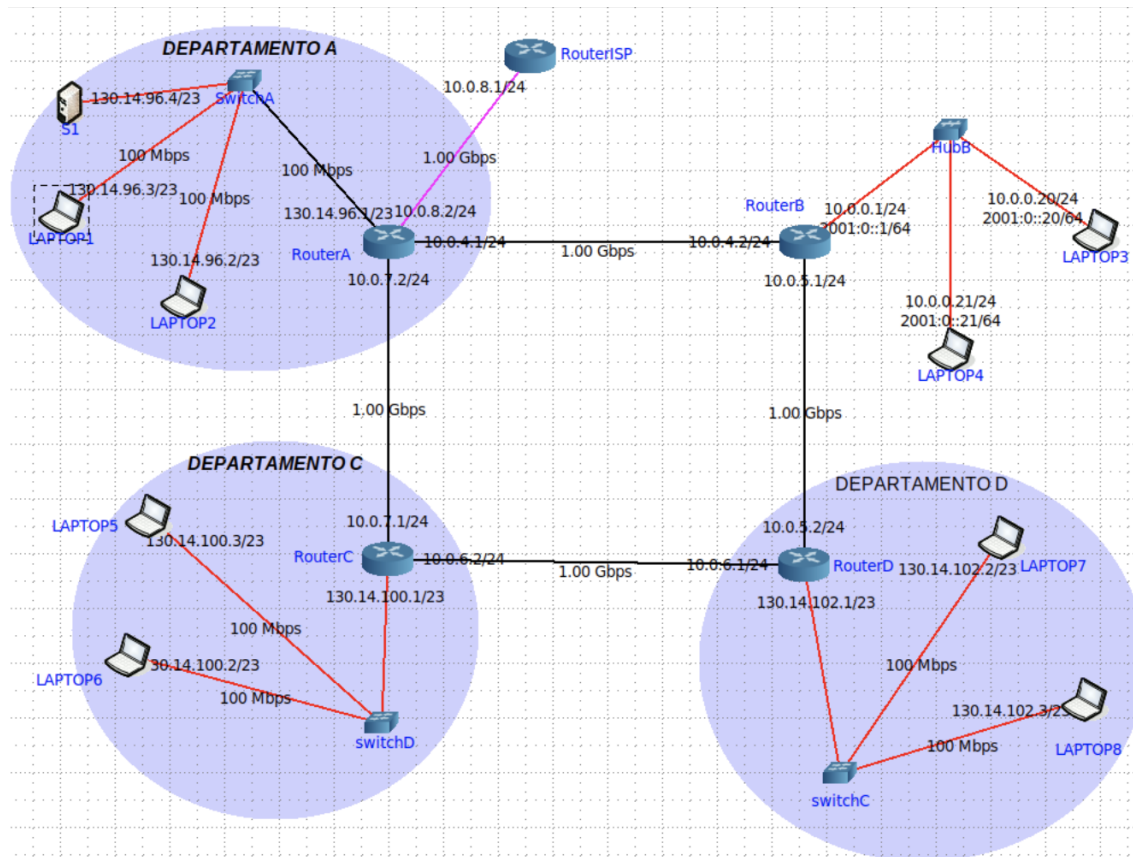


Figura 1.10

Para o departamento A, optamos por usar a opção tcpdump no Laptop1 e realizamos um ping do Laptop2 para o S1. Para o Departamento B, usamos a opção tcpdump no Laptop3 e realizamos um ping do Laptop4 para o routerB. Podemos verificar que com um switch o tráfego do host não envolvido, o LAPTOP1, não recebe qualquer tipo de pedido, enquanto que, quando temos um hub todos os hosts que a este estão ligados, recebem todos os pedidos, independentemente se lhes estava destinada a comunicação ou não.

```

root@LAPTOP4: /tmp/pycore.34897/LAPTOP4.conf
root@LAPTOP4: /tmp/pycore.34897/LAPTOP4.conf# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.117 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.256 ms
^C
[1]+  Stopped                  ping 10.0.0.1
root@LAPTOP4: /tmp/pycore.34897/LAPTOP4.conf#

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:51:02.430757 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:51:02.774059 IP6 fe80::200:ff:feaa:14 > ff02::5: OSPFv3, Hello, length 36
11:51:12.432235 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:51:12.785707 IP6 fe80::200:ff:feaa:14 > ff02::5: OSPFv3, Hello, length 36
11:51:20.497763 IP 10.0.0.21 > 10.0.0.1: ICMP echo request, id 34, seq 1, length 64
11:51:20.497765 IP 10.0.0.1 > 10.0.0.21: ICMP echo reply, id 34, seq 1, length 64
11:51:21.509104 IP 10.0.0.21 > 10.0.0.1: ICMP echo request, id 34, seq 2, length 64
11:51:21.509164 IP 10.0.0.1 > 10.0.0.21: ICMP echo reply, id 34, seq 2, length 64
11:51:22.438637 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:51:22.561112 IP 10.0.0.21 > 10.0.0.1: ICMP echo request, id 34, seq 3, length 64
11:51:22.561294 IP 10.0.0.1 > 10.0.0.21: ICMP echo reply, id 34, seq 3, length 64
11:51:22.793191 IP6 fe80::200:ff:feaa:14 > ff02::5: OSPFv3, Hello, length 36
11:51:25.671567 ARP, Request who-has 10.0.0.21 tell 10.0.0.1, length 28
11:51:25.671570 ARP, Request who-has 10.0.0.1 tell 10.0.0.21, length 28
11:51:25.671623 ARP, Reply 10.0.0.21 is-at 00:00:00:aa:00:15, length 28
11:51:25.671628 ARP, Reply 10.0.0.1 is-at 00:00:00:aa:00:14, length 28

```

Figura 1.11

```

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:52:52.655965 IP 130.14.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:52:52.848689 IP6 fe80::200:ff:feaa:6 > ff02::5: OSPFv3, Hello, length 36
11:53:02.667242 IP 130.14.96.1 > 224.0.0.5: OSPFv2, Hello, length 44
11:53:02.859061 IP6 fe80::200:ff:feaa:6 > ff02::5: OSPFv3, Hello, length 36

root@LAPTOP2: /tmp/pycore.34897/LAPTOP2.conf
root@LAPTOP2: /tmp/pycore.34897/LAPTOP2.conf# ping 130.14.96.4
PING 130.14.96.4 (130.14.96.4) 56(84) bytes of data:
64 bytes from 130.14.96.4: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 130.14.96.4: icmp_seq=2 ttl=64 time=0.088 ms
64 bytes from 130.14.96.4: icmp_seq=3 ttl=64 time=0.142 ms
^C
--- 130.14.96.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2058ms
rtt min/avg/max/mdev = 0.030/0.086/0.142/0.045 ms
root@LAPTOP2: /tmp/pycore.34897/LAPTOP2.conf#

```

Figura 1.12

Capítulo 2

Conclusão

A realização deste trabalho proporcionou-nos a oportunidade de aprofundar os nossos conhecimentos relativamente a Ethernet, Endereços MAC, Address Resolution Protocol (ARP) e Interligação de Redes Locais. Permitiu, também uma melhor compreensão dos assuntos lecionados nas aulas teóricas e a um maior enriquecimento do nosso conhecimento relativo à disciplina.

Este trabalho permitiu-nos explorar a Camada de Ligação Lógica (Ethernet e Protocolo ARP). Verificámos também a maneira com que os endereços Mac são partilhados na rede e o uso do protocolo ARP no papel de resolução de endereços na Internet Layer.

Resumindo, todo o capítulo anteriormente abordado acerca do Link Layer foi abrangido e lembrado tal como todos os conceitos inerentes ao mesmo foram consolidados.