Relatório TP2

Feito por: João Alves (a91646), Ivo Lima (a90214), Rúben Machado (a91656)

Parte I

Captura e análise de Tramas Ethernet

1. Endereço MAC da interface ativa do meu computador é 3c:6a:a7:07:88:a2

```
Ethernet II, Src: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
```

2. O endereço do destino da trama é 00:d0:03:ff:94:00

```
Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
```

Isto não corresponde ao endereço Ethernet do servidor HTTP para http://www.portugalglobal.pt/PT/Paginas/Index.aspx . A trama é destinada ao router da rede LAN que é o link usado para sair da *subnet*.

3. Valor hexadecimal do campo *Type*

```
Ethernet II, Src: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Source: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
  Type: IPv4 (0x0800)
```

O valor Type é 0x0800 e representa o endereço IPv4.

4.

```
Hypertext Transfer Protocol
  GET /PT/inovcontacto/Paginas/InovContacto.aspx HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /PT/inovcontacto/Paginas/InovContacto.aspx HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /PT/inovcontacto/Paginas/InovContacto.aspx
    Request Version: HTTP/1.1
```

```
0000  00 d0 03 ff 94 00 3c 6a  a7 07 88 a2 08 00 45 00   ......<j ......E·
0010  02 52 f0 3e 40 00 80 06  e4 bf ac 1a 01 41 d5 3a   ·R·>@··· ·····A·:
0020  a1 11 c4 5b 00 50 85 d8  e6 53 a3 cd 54 e2 50 18   ···[·P·· ·S··T·P·
0030  02 00 3b 21 00 00 47 45  54 20 2f 50 54 2f 69 6e   ··;!··GE T /PT/in
```

Foram usados 54 bytes para o caracter ASCII “G” desde o início da trama. São encontrados 14 bytes que correspondem à trama da Ethernet, seguidos de 20 bytes do IP e mais 20 bytes do TCP que corresponde ao nivel antes do HTTP ser encontrado.

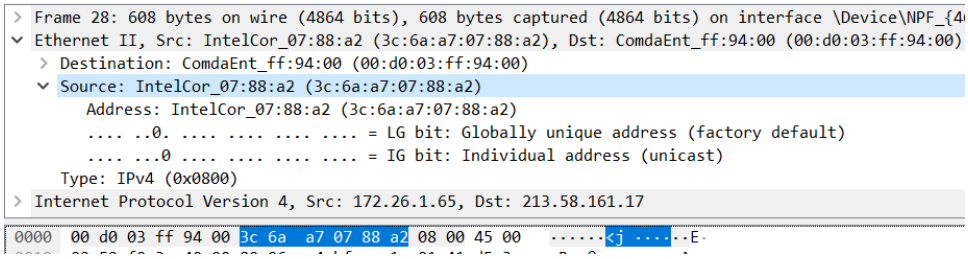
a) 54/517 = 0.10, ou seja, 10%

54 ÷ 517 =

0,10444874274661508704061895551257

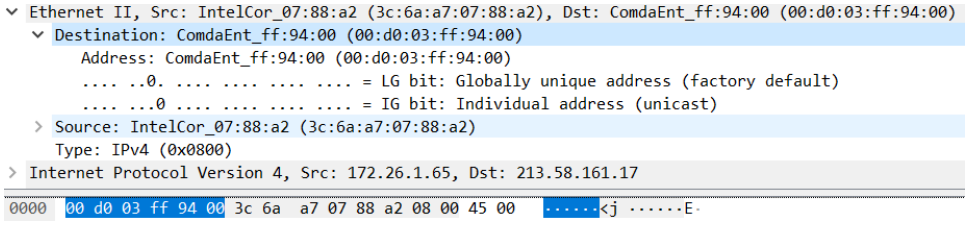
b) Este overhead é justificado pelos mesmos fatores apontados na 4.

5. Endereço Ethernet na fonte

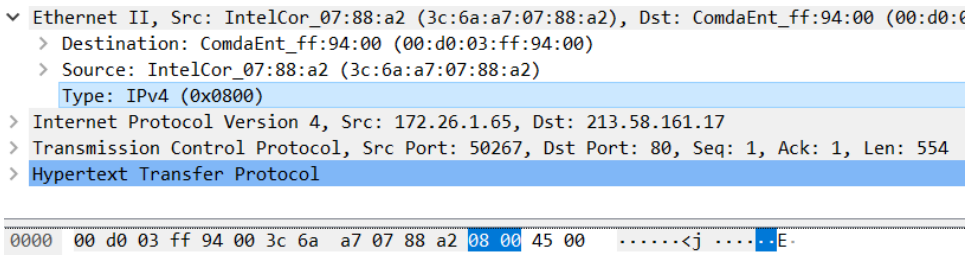


Endereço Ethernet na fonte não corresponde ao endereço Ethernet do site http://www.portugalglobal.pt/PT/Paginas/Index.aspx ou do endereço da minha máquina, mas sim ao endereço do router IntelCor, que é o *link* usado para aceder à minha subnet.

6. O endereço destino é 00:d0:03:ff:94:00 e corresponde à minha máquina.

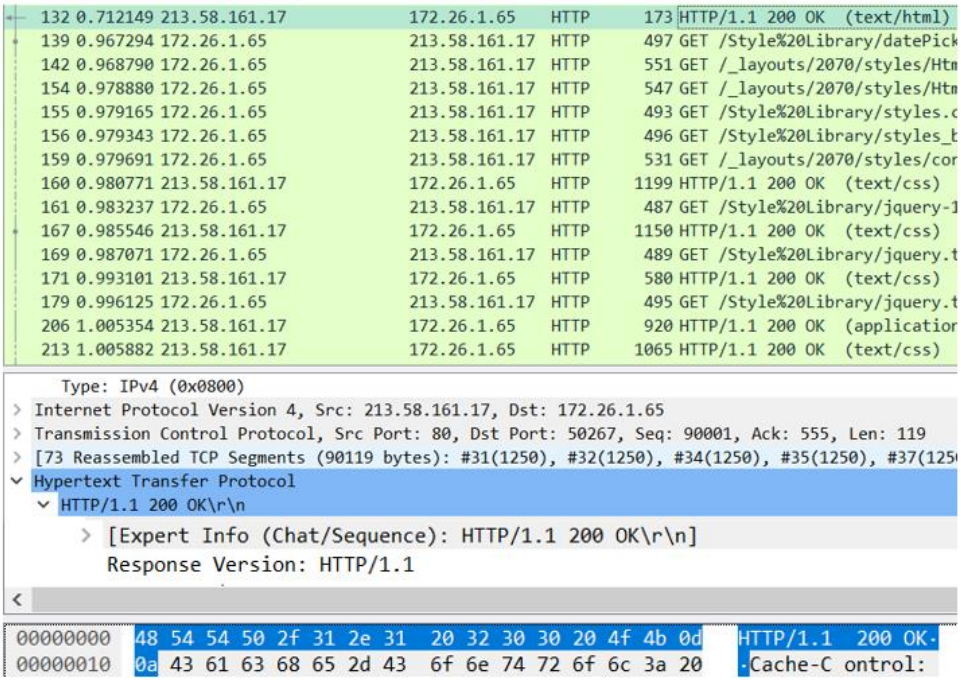


7.



O valor hexadecimal do campo *Type* é 0x0800 e este valor corresponde ao IP do protocolo que já foi mencionado na pergunta 3.

8. Resposta enviada pelo servidor foi HTTP/1.1 200 OK\r\n

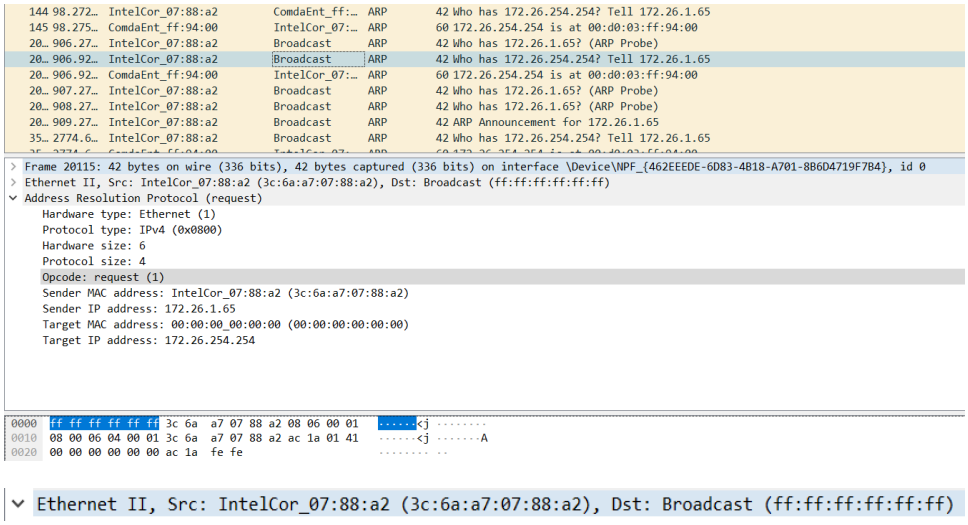


Protocolo ARP

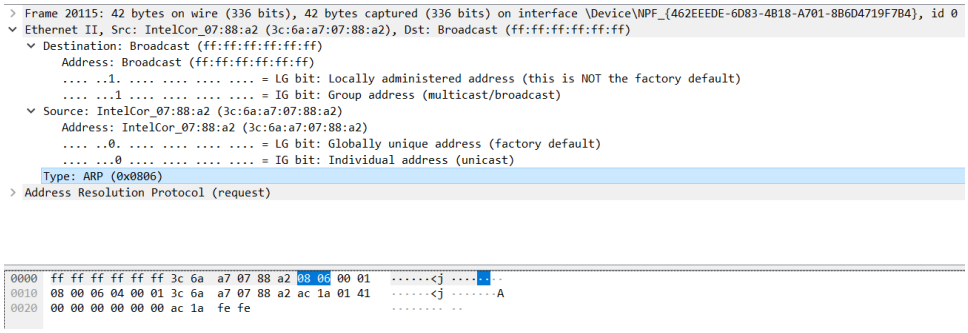
9. A coluna do endereço *Ethernet* contém o endereço IP, a coluna do endereço MAC contém o endereço físico e a coluna do endereço *type* indica o protocolo tipo, que neste caso é dinâmico.

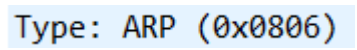
```
C:\Users\ivomi>arp -a

Interface: 172.26.1.65 --- 0x9
  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
  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 --- 0x17
  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
```

10. O valor hexadecimal do endereço da fonte é 3c:6a:a7:07:88:a2. O valor hexadecimal do endereço do destino é ff:ff:ff:ff:ff:ff. Isto pois a comunicação da minha máquina com o router que providencia a rede eduroam que a mensagem de ARP Request já estava guardada em cache.



11. O valor hexadecimal do *Type* da trama *Ethernet* corresponde a 0x0806, indicando um *ARP Request*.





12. O campo *ARP opcode* conta 20 bits desde o início da trama da Ethernet, tendo o valor igual a 1 o que significa que a minha máquina está a tentar fazer um *ARP Request*.

```
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_07:88:a2 (3c:6a:a7:07:88:a2)
    Sender IP address: 172.26.1.65
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

```
0000  ff ff ff ff ff ff 3c 6a  a7 07 88 a2 08 06 00 01   ......<j ........
0010  08 00 06 04 00 01 3c 6a  a7 07 88 a2 ac 1a 01 41   ......<j .......A
0020  00 00 00 00 00 00 ac 1a  fe fe                      ........ ..
```

13. Sim, contém o endereço de origem e a pergunta é um pedido de endereço MAC onde a resposta para o ARP address contendo o endereço Ethernet 3c:6a:a7:07:88:a2 para o remetente com o endereço de IP 172.26.1.65

```
Source: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
    Address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
```

```
Sender MAC address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
Sender IP address: 172.26.1.65
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.254.254
```

14.

No.	Time	Source	Destination	Protocol	Length	Info
144	98.272…	IntelCor_07:88:a2	ComdaEnt_ff:…	ARP	42	Who has 172.26.254.254? Tell 172.26.1.65
145	98.275…	ComdaEnt_ff:94:00	IntelCor_07:…	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
20…	906.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe)
20…	906.92…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.1.65
20…	906.92…	ComdaEnt_ff:94:00	IntelCor_07:…	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
20…	907.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe)
20…	908.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe)
20…	909.27…	IntelCor_07:88:a2	Broadcast	ARP	42	ARP Announcement for 172.26.1.65
35…	2774.6…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.1.65

```
    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)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Sender IP address: 172.26.254.254
    Target MAC address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
    Target IP address: 172.26.1.65
```

```
0000  3c 6a a7 07 88 a2 00 d0  03 ff 94 00 08 06 00 01   <j...... ........
0010  08 00 06 04 00 02 00 d0  03 ff 94 00 ac 1a fe fe   ........ ........
0020  3c 6a a7 07 88 a2 ac 1a  01 41 00 00 00 00 00 00   <j...... .A......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

a. O valor hexadecimal do campo *ARP opcode* foi 0x0002 e especifica que houveram 2 respostas ao *ARP Request*.
b. A resposta ao pedido ARP encontra-se a 20 bits desde o início da trama da Ethernet.

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Sender IP address: 172.26.254.254
    Target MAC address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
    Target IP address: 172.26.1.65
```

```
0000  3c 6a a7 07 88 a2 00 d0  03 ff 94 00 08 06 00 01   <j·····  ·······
0010  08 00 06 04 00 02 00 d0  03 ff 94 00 ac 1a fe fe   ·····  ·····
0020  3c 6a a7 07 88 a2 ac 1a  01 41 00 00 00 00 00 00   <j·····  ·A·····
0030  00 00 00 00 00 00 00 00  00 00 00 00               ·····  ····
```

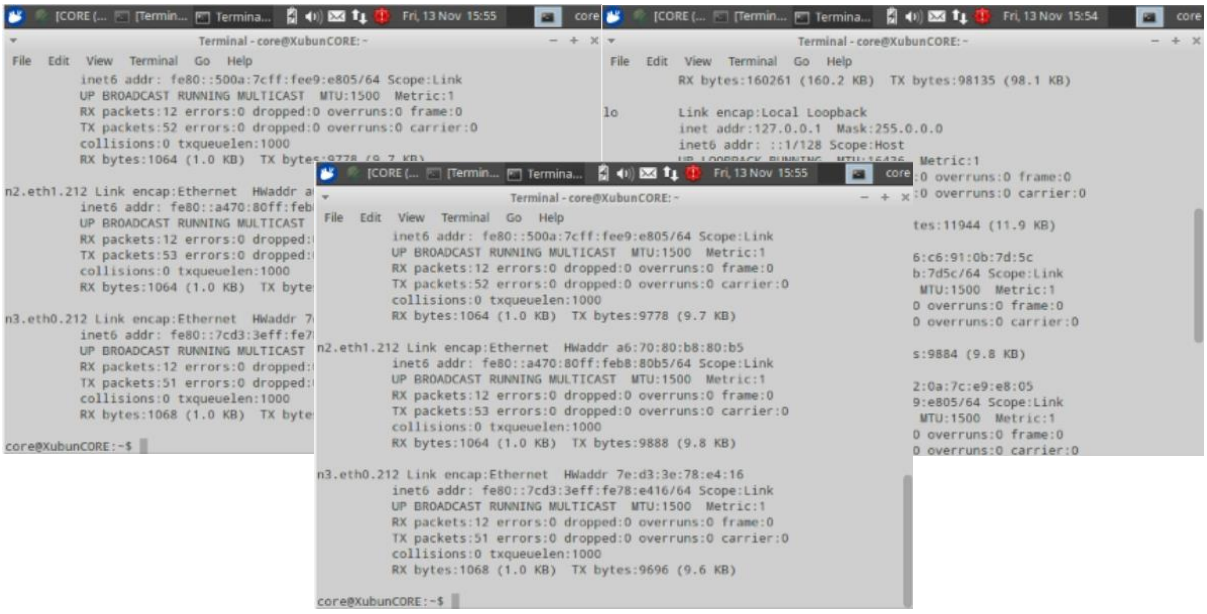
15. O valor hexadecimal para o endereço de origem é 00:d0:03:ff:94:00 e o do destino é 3c:2a:a7:07:88:a2. Com isto concluiu que o pedido de *ARP Resquest* foi respondido com sucesso pela minha máquina.

No.	Time	Source	Destination	Protocol	Length	Info
144	98.272…	IntelCor_07:88:a2	ComdaEnt_ff:…	ARP	42	Who has 172.26.254.254? Tell 17
145	98.275…	ComdaEnt_ff:94:00	IntelCor_07:…	ARP	60	172.26.254.254 is at 00:d0:03:f
20…	906.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe
20…	906.92…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.254.254? Tell 17
20…	906.92…	ComdaEnt_ff:94:00	IntelCor_07:…	ARP	60	172.26.254.254 is at 00:d0:03:f
20…	907.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe
20…	908.27…	IntelCor_07:88:a2	Broadcast	ARP	42	Who has 172.26.1.65? (ARP Probe
20…	909.27…	IntelCor_07:88:a2	Broadcast	ARP	42	ARP Announcement for 172.26.1.6

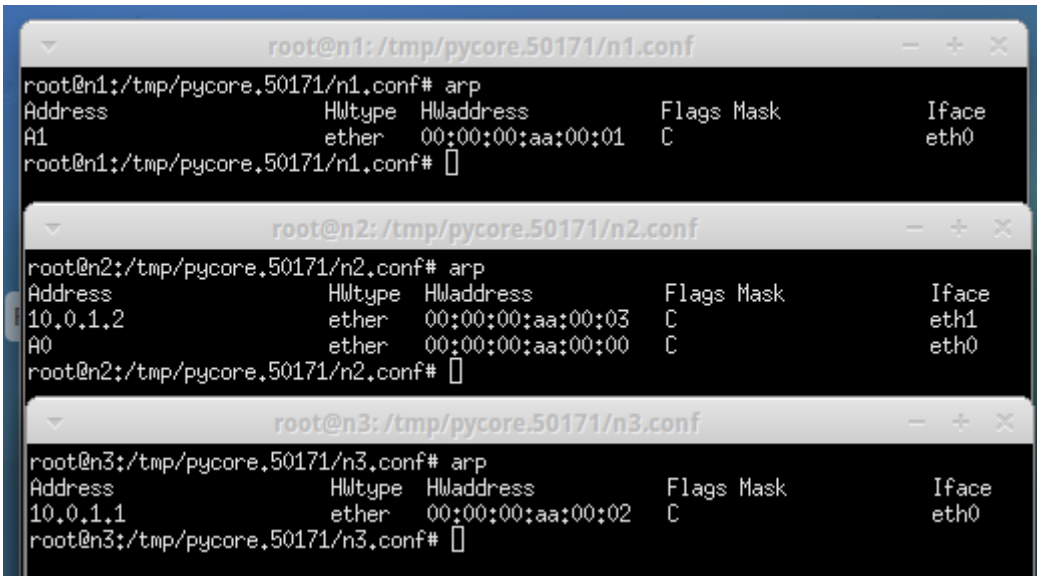
```
Frame 20116: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{462
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
    Destination: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
        Address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 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)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
```

```
0000  3c 6a a7 07 88 a2 00 d0  03 ff 94 00 08 06 00 01   <j·····  ·······
0010  08 00 06 04 00 02 00 d0  03 ff 94 00 ac 1a fe fe   ·····  ·····
0020  3c 6a a7 07 88 a2 ac 1a  01 41 00 00 00 00 00 00   <j·····  ·A·····
0030  00 00 00 00 00 00 00 00  00 00 00 00               ·····  ····
```

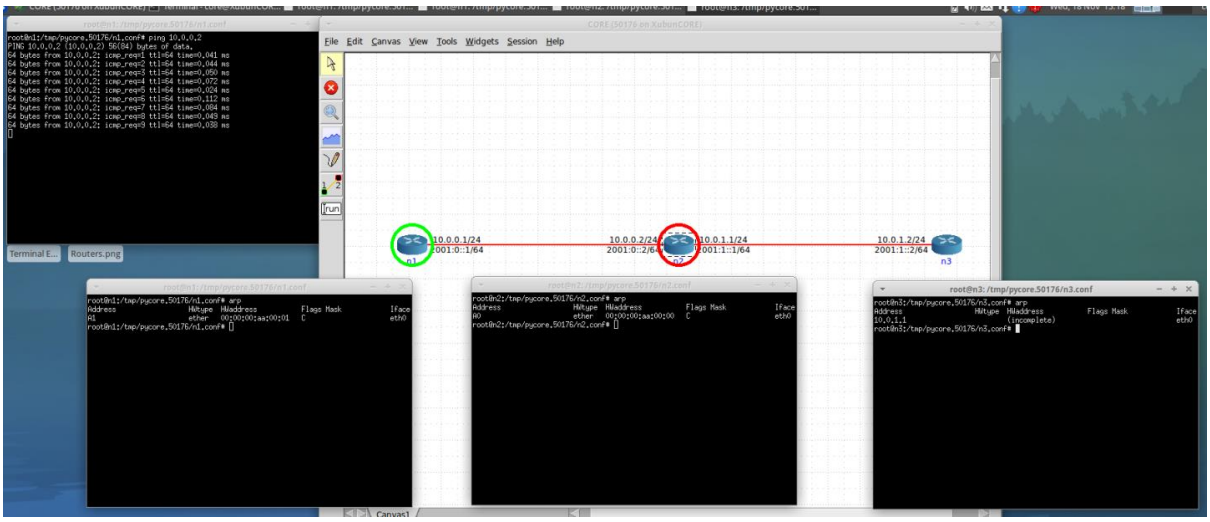
16.


Terminal - core@XubunCORE: ~
File Edit View Terminal Go Help
inet6 addr: fe80::500a:7cff:fee9:e805/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12 errors:0 dropped:0 overruns:0 frame:0
TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1064 (1.0 KB) TX bytes:9778 (9.7 KB)
n2.eth1.212 Link encap:Ethernet HWaddr a6:70:80:b8:80:b5
inet6 addr: fe80::a470:80ff:feb8:80b5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12 errors:0 dropped:0 overruns:0 frame:0
TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1064 (1.0 KB) TX bytes:9888 (9.8 KB)
n3.eth0.212 Link encap:Ethernet HWaddr 7e:d3:3e:78:e4:16
inet6 addr: fe80::7cd3:3eff:fe78:e416/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12 errors:0 dropped:0 overruns:0 frame:0
TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1068 (1.0 KB) TX bytes:9696 (9.6 KB)
core@XubunCORE:~$

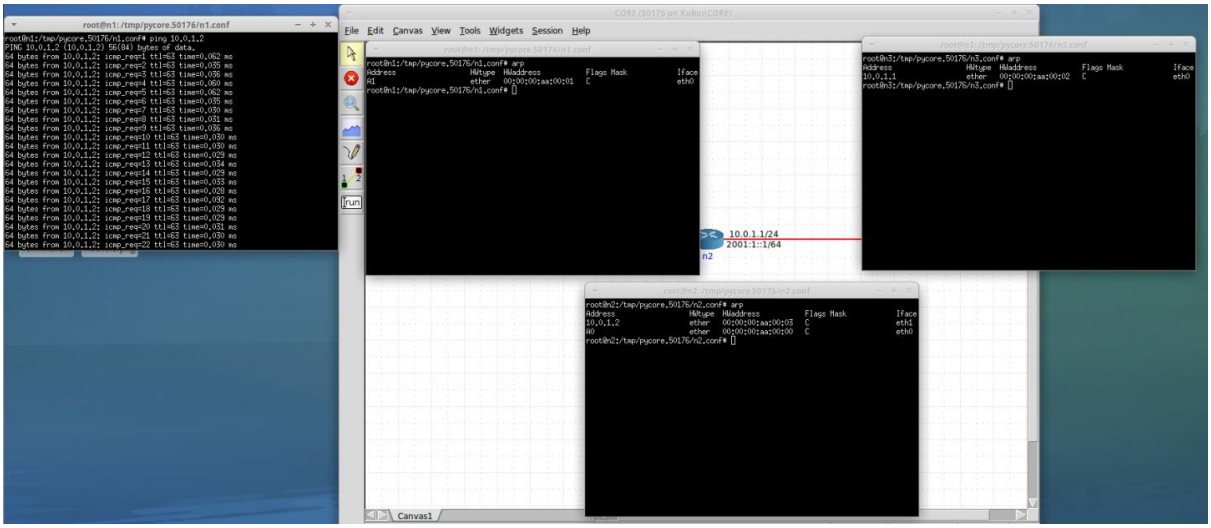
17.


root@n1:/tmp/pycore.50171/n1.conf
root@n1:/tmp/pycore.50171/n1.conf# arp
Address HWtype HWaddress Flags Mask Iface
A1 ether 00:00:00:aa:00:01 C eth0
root@n1:/tmp/pycore.50171/n1.conf#
root@n2:/tmp/pycore.50171/n2.conf
root@n2:/tmp/pycore.50171/n2.conf# arp
Address HWtype HWaddress Flags Mask Iface
10.0.1.2 ether 00:00:00:aa:00:03 C eth1
A0 ether 00:00:00:aa:00:00 C eth0
root@n2:/tmp/pycore.50171/n2.conf#
root@n3:/tmp/pycore.50171/n3.conf
root@n3:/tmp/pycore.50171/n3.conf# arp
Address HWtype HWaddress Flags Mask Iface
10.0.1.1 ether 00:00:00:aa:00:02 C eth0
root@n3:/tmp/pycore.50171/n3.conf#

18.



Após dar *ping* entre o router n1 e n2 verificamos que o router n1 guarda na sua cache o endereço do router n2, e como o router n3 não foi chamado, não possui nada na sua cache.

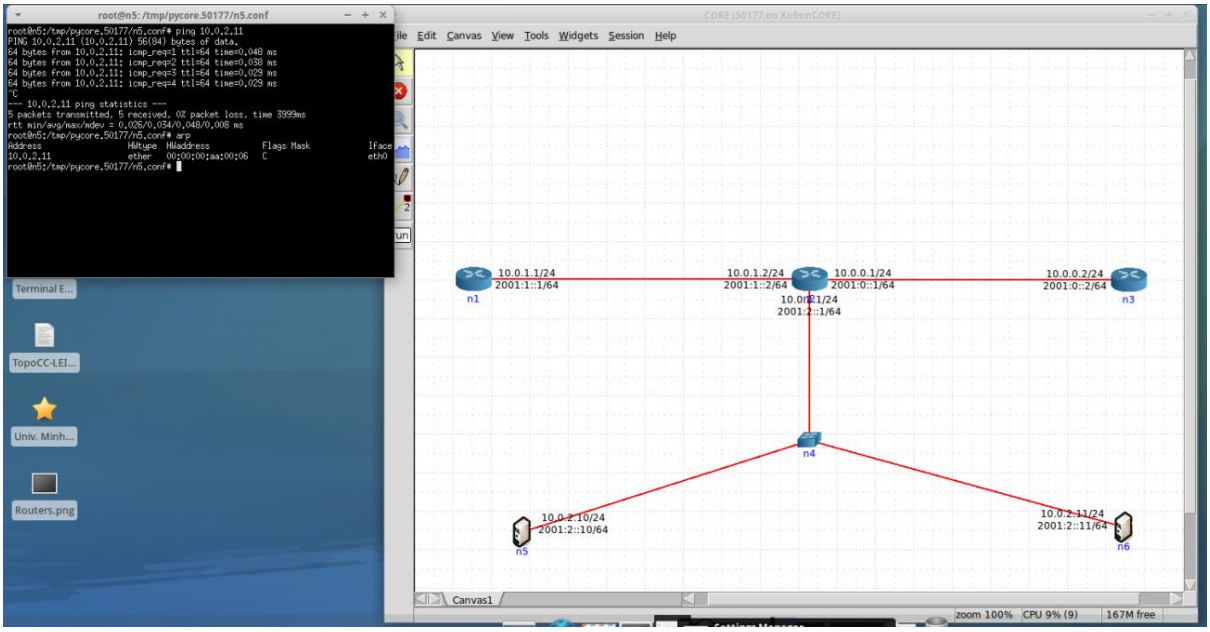


Por contrapartida no segundo *ping* de n1 para n3, o n1 continua com o endereço de n2, este (n2) contém o endereço do router n1 e n3, e este último (n3) fica com endereço do router n2.

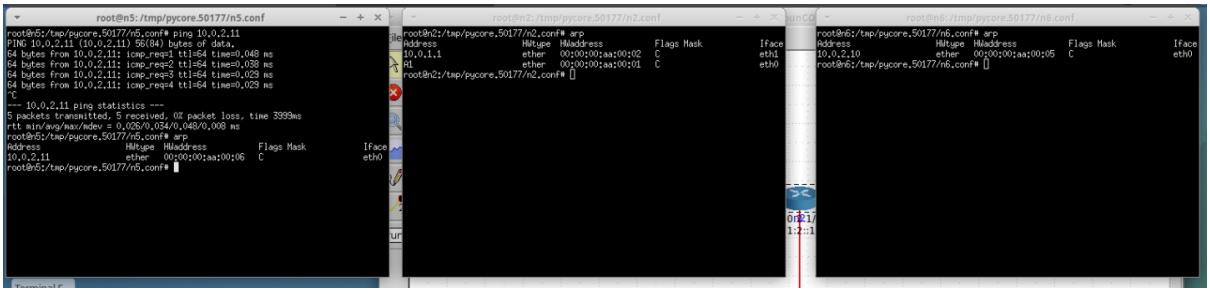
19. Ao remover-mos a ligação entre n1 e n2 e ao tentarmos fazer *ping* verificamos que não obtemos resposta, uma vez que o endereço destino é inexistente.

```
root@n1:/tmp/pycore.43195/n1.conf# arp -s 10.0.1.2 00:00:00:aa:00:12
root@n1:/tmp/pycore.43195/n1.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.1.2                 ether   00:00:00:aa:00:12   CM                    eth0
root@n1:/tmp/pycore.43195/n1.conf# ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
^C
--- 10.0.1.2 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9063ms

root@n1:/tmp/pycore.43195/n1.conf#
```

20. A nossa hipótese é que na tabela ARP de n5 apenas será adicionado o IP de n6, uma vez que ambos os *host* estão ligados ao mesmo *switch*, não há necessidade de comunicar com o mesmo router n2.

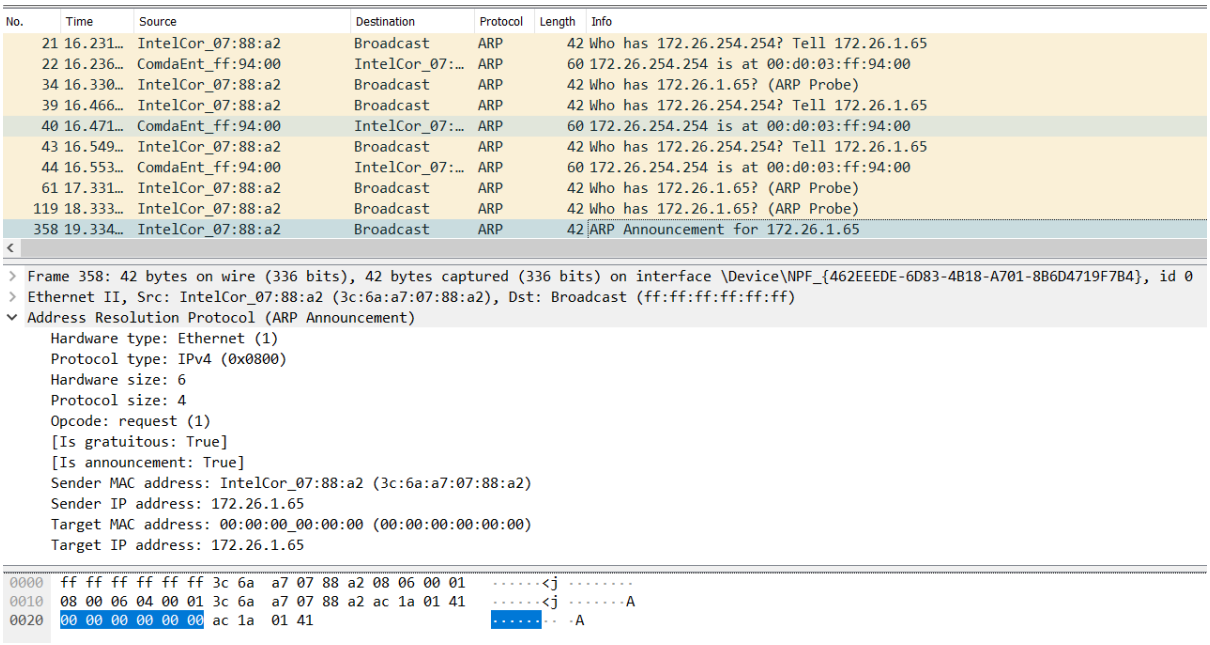


Como podemos ver pela *screenshot* em baixo, concluímos que a nossa hipótese estava correta e que apenas foram adicionados os endereços de n6 a n5 e n5 a n6, continuando n2 apenas a conter os endereços de n1 e n3.



Parte II

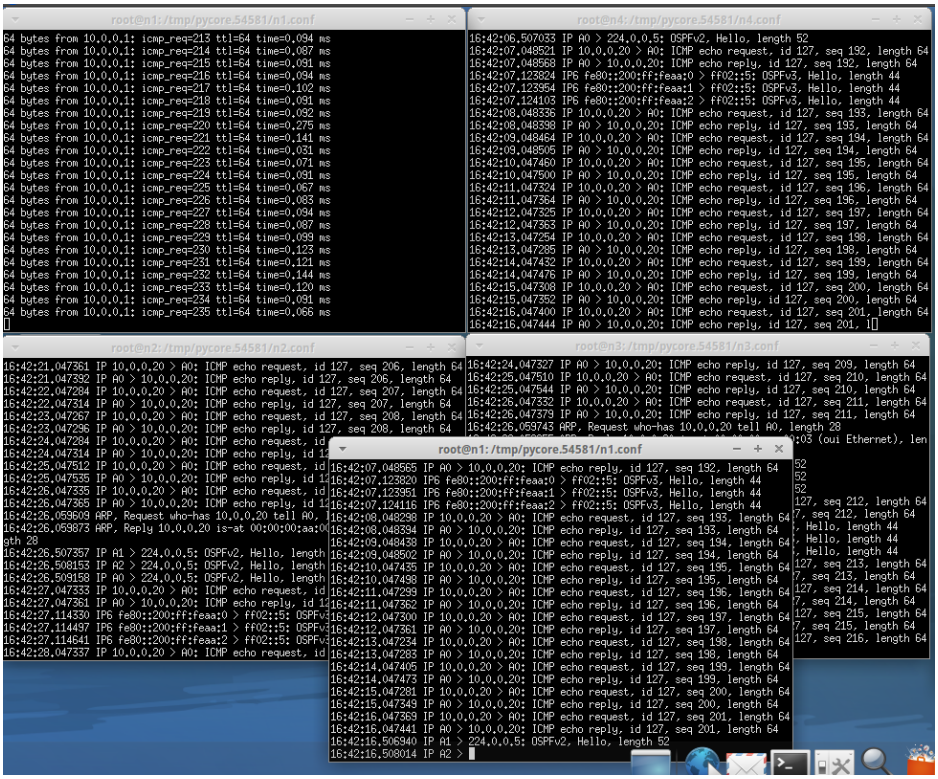
1.

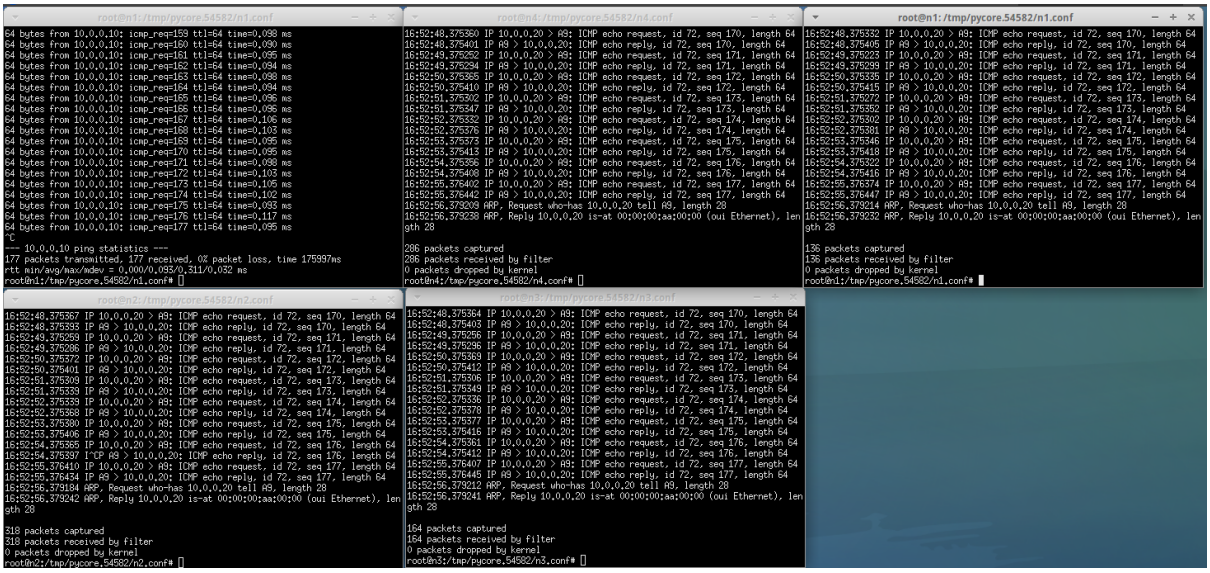


2. Neste caso, o IP do Sender coincide com o IP do Target. Ou seja, é enviado um pedido de ARP gratuito cuja função é descobrir o endereço MAC do IP da nossa máquina nativa, de forma a verificar que o endereço IP que nos foi atribuído é único.

```
Sender MAC address: IntelCor_07:88:a2 (3c:6a:a7:07:88:a2)
Sender IP address: 172.26.1.65
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.1.65
```

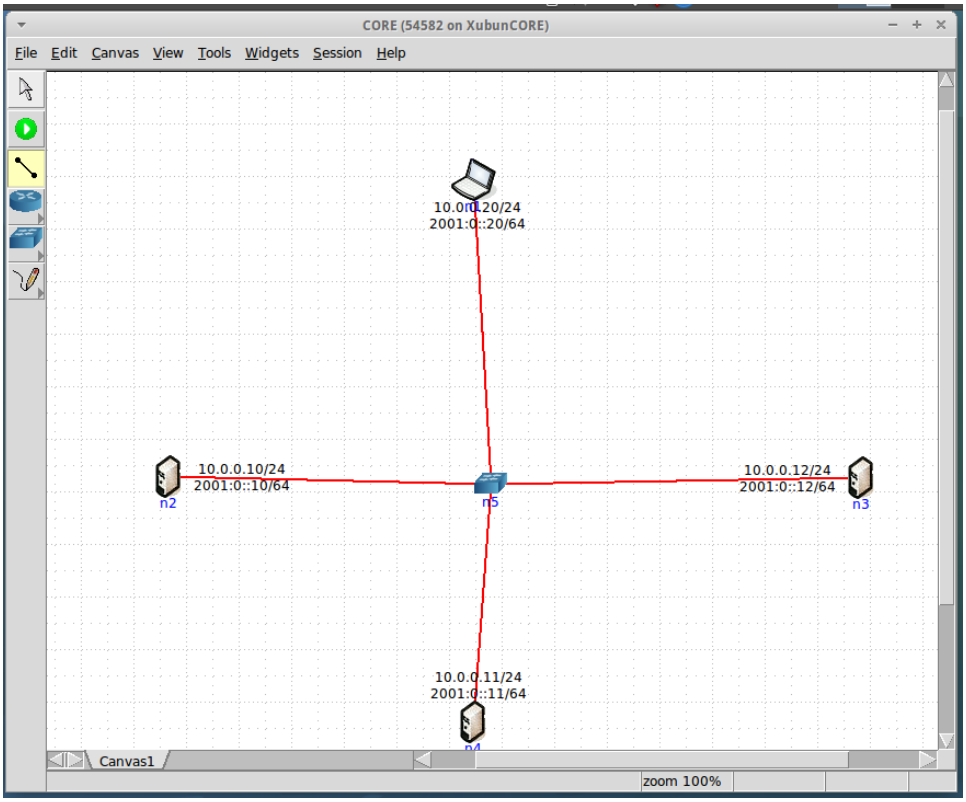
3. 1.

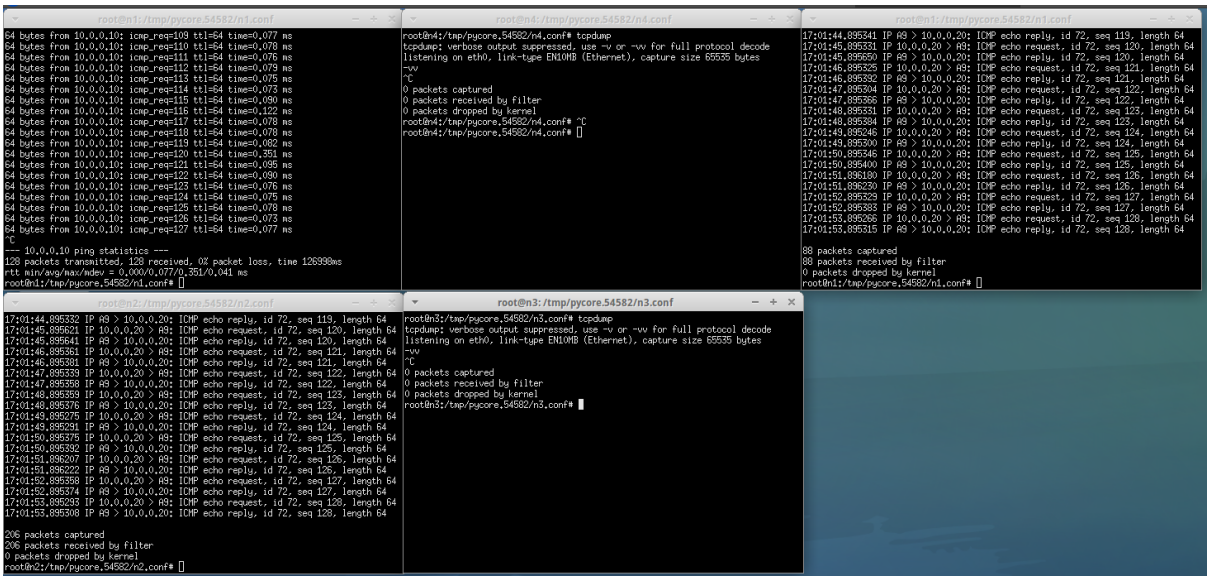




Através das *screenshots* podemos observar que através do *ping* do n1 para n2 verificamos que existe tráfego entre todos os dispositivos à exceção do n5, sendo que este *hub,* como não é do nível 2, não fará endereçamento *MAC* fazendo apenas *Broadcast*.

2.





Com o *ping* de n1 e n2 os únicos que apresentam tráfego são o n1 e n2 respetivamente, como o n4 e o n3 não apresentam nada, devido ao facto de existir uma switch que também de nível 2 que faz o endereçamento do *MAC*. Assim qualquer pedido é enviado diretamente para o endereço estipulado, uma vez que o *switch* elimina colisões e conecta cada a uma porta do comutador.

Conclusão

Este relatório teve como foco o estudo da ligação lógica, em destaque a *Ethernet* e o protocolo ARP. Precedendo a este trabalho, o nosso conhecimento sobre esta matéria era inexistente. Com o auxílio do *Wireshark* e do Core, estudámos os diferentes tipos de protocolo ARP, incluindo o *ARP Request* (pedido ARP) e o ARP gratuito. Ainda alcançamos uma maior compreensão das origens e destinos dos endereços *Ethernet* e das suas respetivas mensagens e funções. Dito isto, de forma sucinta, posteriormente ao estudo destes tópicos, adquirimos capacidade de interpretar e analisar este tema, proporcionando uma aprendizagem interativa e abrangente ao nosso grupo.