

# **Redes de computadores**

## **Nível de Ligação Lógica: Redes Ethernet e Protocolo ARP**

Pedro Calheno Pinto, Diogo do Rego Neto, and Samuel Macieira Ferreira

University of Minho, Department of Informatics, 4710-057 Braga, Portugal  
e-mail: {a87983,a98197,a100654}@alunos.uminho.pt

## 1 Captura e análise de Tramas Ethernet

|    |             |              |              |      |                             |
|----|-------------|--------------|--------------|------|-----------------------------|
| 36 | 2.121562512 | 10.0.2.15    | 91.189.91.49 | HTTP | 141 GET / HTTP/1.1          |
| 38 | 2.264299924 | 91.189.91.49 | 10.0.2.15    | HTTP | 243 HTTP/1.1 204 No Content |

Fig. 1. Endereços

```
▶ Frame 44: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits) on interface enp0s3, id 0
▼ Ethernet II, Src: PcsCompu_91:03:2d (08:00:27:91:03:2d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▶ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▶ Source: PcsCompu_91:03:2d (08:00:27:91:03:2d)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.168.164
▶ User Datagram Protocol, Src Port: 52034, Dst Port: 443
▶ QUIC IETF
```

Fig. 2. Tramas ethernet

### 1.1 Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.

Como podemos verificar na tabela, nos campos "Destination" e "Source":

Endereço MAC de origem - 52:54:00:12:35:02

Endereço MAC de destino - 08:00:27:91:03:2d

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

O valor do campo Type da trama, com o protocolo IPV4, é 0x0800.

Type: IPV4 (0x800)

### 1.3 Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (Application Data Protocol: http-over-tls, no caso de HTTPS)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

O número de bytes usados é calculado somando os bytes do Ethernet, do IP e do TCP, ou seja:  $14+20+20 = 54$ . A frame tem 125 bytes, pelo que a percentagem da sobrecarga é:  $(54/125) * 100$ , aproximadamente 43%.

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

O endereço da fonte Ethernet é 08:00:27:91:03:2d. Corresponde ao endereço físico da interface ativa do router com que estamos a comunicar.

### 1.5 Qual é o endereço MAC do destino? A que sistema (host) corresponde?

O endereço físico é 52:54:00:12:35:02 e corresponde à interface ethernet do nosso computador.

### 1.6 Atendendo ao conceito de encapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. Justifique, indicando em que campos dos cabeçalhos capturados se baseou.

Os protocolos contidos na trama recebida incluem Ethernet (no cabeçalho), IPv4 identificado pelo campo "Type" e TCP que é identificado pela porta de destino. Para confirmar que o protocolo de aplicação é HTTP-over-TLS, seria necessário analisar o conteúdo da trama após os cabeçalhos.

## 2 Protocolo ARP

### 2.1 Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp -a.

**a - Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.** Após efectuar ping para dois dispositivos localizados na outra rede e efetuarmos o comando arp -a obtivemos uma tabela ARP com uma linha.

```
root@n3:/tmp/pycore.39853/n3.conf# ping 192.168.159.22
PING 192.168.159.22 (192.168.159.22) 56(84) bytes of data.
64 bytes from 192.168.159.22: icmp_seq=1 ttl=62 time=0.066 ms
64 bytes from 192.168.159.22: icmp_seq=2 ttl=62 time=0.092 ms
64 bytes from 192.168.159.22: icmp_seq=3 ttl=62 time=0.084 ms
64 bytes from 192.168.159.22: icmp_seq=4 ttl=62 time=0.103 ms
64 bytes from 192.168.159.22: icmp_seq=5 ttl=62 time=0.118 ms
64 bytes from 192.168.159.22: icmp_seq=6 ttl=62 time=0.094 ms
^Z
[1]+  Stopped                  ping 192.168.159.22
root@n3:/tmp/pycore.39853/n3.conf# ping 192.168.159.20
PING 192.168.159.20 (192.168.159.20) 56(84) bytes of data.
64 bytes from 192.168.159.20: icmp_seq=1 ttl=62 time=0.089 ms
64 bytes from 192.168.159.20: icmp_seq=2 ttl=62 time=0.090 ms
64 bytes from 192.168.159.20: icmp_seq=3 ttl=62 time=0.357 ms
64 bytes from 192.168.159.20: icmp_seq=4 ttl=62 time=0.076 ms
64 bytes from 192.168.159.20: icmp_seq=5 ttl=62 time=0.085 ms
64 bytes from 192.168.159.20: icmp_seq=6 ttl=62 time=0.083 ms
^Z
[2]+  Stopped                  ping 192.168.159.20
root@n3:/tmp/pycore.39853/n3.conf# arp -a
? (192.168.31.1) at 00:00:00:aa:00:06 [ether] on eth0
```

**Fig. 3.** Tabela ARP depois de efetuados os pings

Esta é uma representação dos registos ARP mantidos pelo dispositivo, que mapeiam endereços IP para endereços MAC. Cada entrada tem uma função:

1. ? (192.168.31.1) - Este é o endereço IP do dispositivo na rede local. O símbolo "?" indica que o nome do host não pode ser resolvido. Neste caso, o endereço IP é 192.168.31.1, que geralmente corresponde ao gateway padrão ou ao roteador da rede local.
2. at 00:00:00:aa:00:06 - A palavra "at" indica que o endereço IP está associado ao endereço MAC especificado. Neste caso, o endereço MAC é 00:00:00:aa:00:06. O endereço MAC é um identificador exclusivo de 48 bits atribuído a cada dispositivo de rede.
3. ether - Esta parte indica o tipo de protocolo de camada física utilizado. Neste caso, "ether" é uma abreviação de Ethernet, que é o protocolo de rede amplamente utilizado em redes locais (LANs).

4. on eth0 - A palavra "on" indica a interface de rede utilizada para se comunicar com o dispositivo em questão. Neste caso, a interface de rede é "eth0". Em sistemas Linux, as interfaces Ethernet geralmente são nomeadas como "eth" seguidas por um número, enquanto as interfaces sem fio são nomeadas como "wlan" ou "wlo" seguidas por um número.

Em resumo, esta entrada da tabela ARP informa que um dispositivo com endereço IP 192.168.31.1 está associado ao endereço MAC 00:00:00:aa:00:06, usando o protocolo Ethernet na interface de rede eth0.

**b - Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.** Um equipamento que possa apresentar a maior tabela ARP em termos de número de entradas é aquele que interage com o maior número de dispositivos na rede, ou seja, um dispositivo que atue como ponto central de comunicação ou roteamento. Neste caso o equipamento que apresenta a maior tabela ARP é o router n9 pois precisa conhecer o mapeamento de endereços IP para endereços MAC para todos os dispositivos em cada uma dessas redes, neste caso são 4 e ainda tem a conexão com o outro departamento. Dado que o router normalmente está conectado a várias redes e sub-redes, este precisa de manter uma tabela ARP maior do que um dispositivo final como um PC que apenas comunica com dispositivos da mesma rede local.

## 2.2 Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).

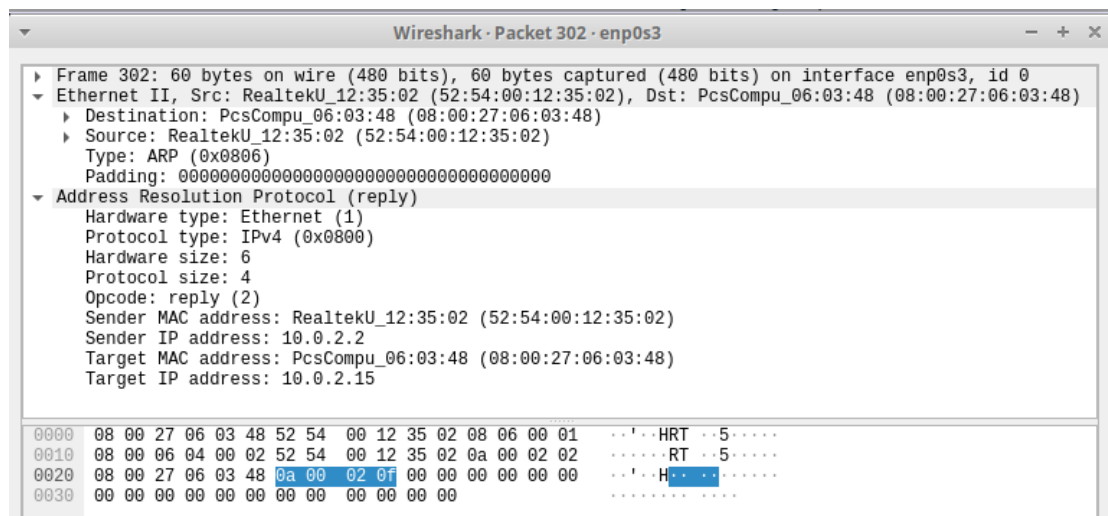


Fig. 4.

**a - Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?** endereço Source - 52:54:00:12:35:02

endereço Destination - 08:00:27:06:03:48

O endereço destino é o de broadcast, a máquina vai enviar uma mensagem para todas as interfaces e a máquina destino irá responder com o seu endereço MAC

**b - Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica? O valor 0x0806 em hexadecimal, indica que se trata de uma mensagem do protocolo ARP.**

**c - Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.** Como observamos na alínea anterior estamos perante uma mensagem de protocolo ARP em que o opcode tem valor 1, pelo que podemos verificar que é uma mensagem de request (ARP request). Os endereços contidos na mensagem ARP são endereços MAC e endereços IP. A mensagem ARP vem com estes dois tipos de endereços, para permitir a criação de linhas da tabela ARP com estes endereços, ou seja, para permitir que haja uma correspondência entre endereços IP e MAC estabelecida

**d - Explícite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?** A pergunta enviada é "Who has 10.0.2.22? Tell 10.0.2.15" e serve para saber quem tem o endereço IP 10.0.2.22, este faz essa pergunta a todos os hosts e pede para enviar a resposta, com o endereço MAC para o endereço IP 10.0.2.15.



301 313.008975098 PcsCompu 06:03:48 RealtekU 12:35:02 ARP 42 Who has 10.0.2.22? Tell 10.0.2.15

Fig. 5.

### 2.3 Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

**a - Qual o valor do campo ARP opcode? O que especifica?** O valor do ARP opcode é reply (2) que indica que se trata de uma mensagem ARP reply. Indica que a mensagem ARP capturada é uma resposta ARP enviada por um dispositivo na rede em resposta a uma solicitação ARP recebida. Quando um dispositivo recebe uma solicitação ARP perguntando "Quem possui este endereço IP?" e o endereço IP solicitado corresponde ao seu próprio endereço IP, o dispositivo responde com uma mensagem ARP de "reply". Essa resposta contém o endereço MAC do dispositivo, permitindo que o dispositivo solicitante atualize sua tabela ARP e estabeleça comunicação diretamente com o dispositivo de destino usando o endereço MAC encontrado.

**b - Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?** A resposta ao pedido ARP efetuado está no campo Sender MAC address.

**c - Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.** Os endereços MAC de origem e destino da trama em causa correspondem, respectivamente, à interface do host de origem que enviou o pedido ARP e à interface do host que respondeu ao pedido ARP. É possível identificar esses endereços executando os comandos ifconfig, netstat -rn e arp no PC selecionado. O comando ifconfig mostra as informações de configuração de interface do PC, incluindo o endereço MAC da interface. O comando netstat -rn mostra a tabela de roteamento do PC, que pode ser usada para determinar o próximo salto para o host de destino. O comando arp mostra a tabela ARP, que mapeia endereços IP para endereços MAC e pode ser usada para identificar o endereço MAC correspondente a um endereço IP.

**d - Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).** A resposta ARP é enviada em modo de comunicação unicast. Isso significa que a resposta é enviada diretamente para o host que fez o pedido ARP, em vez de ser transmitida para todos os hosts na rede (modo broadcast) de modo a minimizar o tráfego na rede e evitar que outros hosts recebam uma informação que não é relevante para eles. Além disso, o endereço MAC de destino na resposta ARP é o endereço MAC do host que fez o pedido ARP, o que permite que o host de origem associe corretamente o endereço IP ao endereço MAC do host de destino.

## 2.4 Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada.

Ao observar um ou mais pacotes ARP de "request" e, em seguida, pacotes ARP de "reply" correspondentes, isso indica que o ping originou pacotes ARP. A situação observada pode ser justificada pelo fato de que o PC n1 precisava de descobrir o endereço MAC do PC n6 antes de enviar os pacotes ICMP de solicitação de eco. O PC n1 usa o protocolo ARP para mapear o endereço IP do PC n6 para seu endereço MAC, permitindo a comunicação direta entre os dois dispositivos na rede.

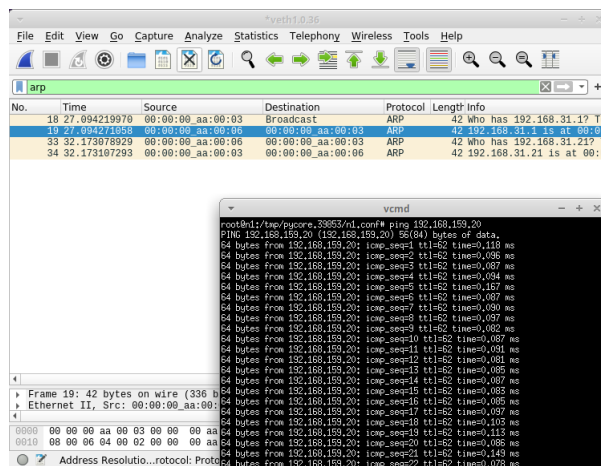


Fig. 6.

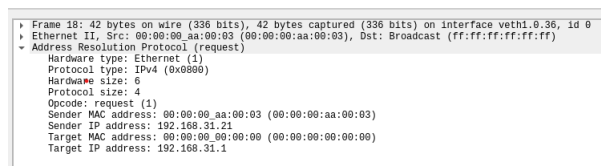


Fig. 7.

```

Frame 19: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.36, id 0
Ethernet II, Src: 00:00:00:aa:00:06 (00:00:00:aa:00:06), Dst: 00:00:00:aa:00:03 (00:00:00:aa:00:03)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 00:00:00:aa:00:06 (00:00:00:aa:00:06)
Sender IP address: 192.168.31.1
Target MAC address: 00:00:00:aa:00:03 (00:00:00:aa:00:03)
Target IP address: 192.168.31.21

```

**Fig. 8.**

**2.5 Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.**

Na mensagem ARP, os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica são:

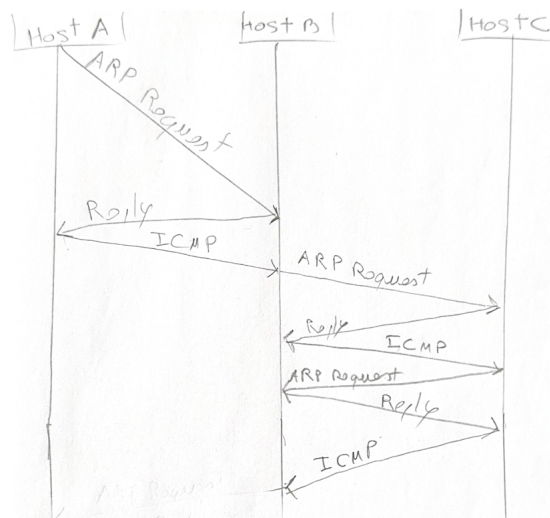
**Hardware Type:** Este campo identifica o tipo de endereço de hardware usado na rede de ligação lógica. Para Ethernet, o valor é 1.

**Protocol Type:** Este campo identifica o tipo de endereço de protocolo usado na camada de rede. Para endereços IPv4, o valor é 0x0800.

**Hardware Size:** Este campo especifica o tamanho dos endereços de hardware em bytes. Para endereços MAC Ethernet, o valor é 6, já que os endereços MAC têm 6 bytes (48 bits).

**Protocol Size:** Este campo especifica o tamanho dos endereços de protocolo em bytes. Para endereços IPv4, o valor é 4, já que os endereços IPv4 têm 4 bytes (32 bits).

**2.6 Na situação em que efetua um ping a um PC não local à sua sub-rede, esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do sistema destino (represente apenas os nós intervenientes). Assuma que todas as tabelas ARP se encontram inicialmente vazias.**



**Fig. 9.** Cronologia mensagens ARP

### 3 Domínios de colisão

a - 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 é gerado 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. As Interfaces do departamento A continuam ligas ao router através do switch enquanto que no departamento B ligam-se a partir de um hub(repetido). No departamento B, onde a rede é partilhada, ao ser realizado um pingo num dos computadores, verifica-se analisando os tráfegos dos hosts da interface que as tramas conseguem ser vistas por todos os componentes da interface. No departamento A, onde a rede é comutada, ao ser usado o comando `ping` no host, analisando o tráfego dos hosts verifica-se que o computador não captura tramas enviadas pelo host.

```
root@n10:/tmp/pucone_46423/n10.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:36:36.850449 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:36.851916 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:40.852234 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:40.935986 IP6 fe80::2001:ff:feaa:7 > ff02::5: OSPFv2, Hello, length 36
12:36:42.853256 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:44.854378 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:46.855306 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:48.856234 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:50.856478 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:50.973676 IP6 fe80::2001:ff:feaa:7 > ff02::5: OSPFv2, Hello, length 36
12:36:52.857339 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:36:54.858239 IP 192.168.31.1 > 224.0.0.5: OSPFv2, Hello, length 44

13 packets captured
13 packets received by filter
0 packets dropped by kernel
root@n10:/tmp/pucone_46423/n10.conf#
```

Fig. 10.

```
root@n11:/tmp/pucone_46423/n11.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:38:40.918339 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 36
12:38:42.920466 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:44.921823 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:46.922922 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:48.923762 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:50.923861 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:50.925549 IP6 fe80::2001:ff:feaa:8 > ff02::5: OSPFv2, Hello, length 36
12:38:52.926655 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:54.926699 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:56.926955 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:38:58.928313 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:00.929113 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:00.930594 IP6 fe80::2001:ff:feaa:8 > ff02::5: OSPFv2, Hello, length 36
12:39:02.932607 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:04.933555 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:06.934652 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:08.935900 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:10.927333 IP6 fe80::2001:ff:feaa:8 > ff02::5: OSPFv2, Hello, length 36
12:39:10.940736 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:10.941652 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44

21 packets captured
21 packets received by filter
0 packets dropped by kernel
root@n11:/tmp/pucone_46423/n11.conf#
```

Fig. 11.

b - Construa manualmente a tabela de comutação do switch do Departamento A, atribuindo números de porta à sua escolha.



```
vcmd
64 bytes from 192.168.159.20: icmp_seq=5 ttl=63 time=0.673 ms
64 bytes from 192.168.159.20: icmp_seq=4 ttl=63 time=0.538 ms
64 bytes from 192.168.159.20: icmp_seq=5 ttl=63 time=0.205 ms
64 bytes from 192.168.159.20: icmp_seq=5 ttl=63 time=0.786 ms
^C
[1]+  Stopped                  ping 192.168.159.20
root@n10:/tmp/pycore_46423/n10.conf# ping 192.168.159.20
PING 192.168.159.20 (192.168.159.20) 56(84) bytes of data:
64 bytes from 192.168.159.20: icmp_seq=1 ttl=63 time=0.553 ms
64 bytes from 192.168.159.20: icmp_seq=2 ttl=63 time=0.238 ms
64 bytes from 192.168.159.20: icmp_seq=3 ttl=63 time=0.135 ms
64 bytes from 192.168.159.20: icmp_seq=4 ttl=63 time=0.295 ms
64 bytes from 192.168.159.20: icmp_seq=5 ttl=63 time=0.147 ms
64 bytes from 192.168.159.20: icmp_seq=6 ttl=63 time=0.499 ms
64 bytes from 192.168.159.20: icmp_seq=7 ttl=63 time=0.389 ms
64 bytes from 192.168.159.20: icmp_seq=8 ttl=63 time=0.252 ms
64 bytes from 192.168.159.20: icmp_seq=9 ttl=63 time=0.378 ms
64 bytes from 192.168.159.20: icmp_seq=10 ttl=63 time=0.351 ms
64 bytes from 192.168.159.20: icmp_seq=11 ttl=63 time=0.204 ms
^C
--- 192.168.159.20 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 1024ms
rtt min/avg/max/ndev = 0.147/0.328/0.553/0.117 ms
root@n10:/tmp/pycore_46423/n10.conf#
```

Fig. 12.

```
vcmd
12:39:10.940756 IP 192.168.159.4 > 224.0.0.5: OSPFv2, Hello, length 44
12:39:12.941822 IP 192.168.159.1 > 224.0.0.5: OSPFv2, Hello, length 44
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
root@n11:/tmp/pycore_46423/n11.conf# ping 192.168.31.33
PING 192.168.31.33 (192.168.31.33) 56(84) bytes of data:
64 bytes from 192.168.31.33: icmp_seq=1 ttl=63 time=0.680 ms
64 bytes from 192.168.31.33: icmp_seq=2 ttl=63 time=0.298 ms
64 bytes from 192.168.31.33: icmp_seq=3 ttl=63 time=0.488 ms
64 bytes from 192.168.31.33: icmp_seq=4 ttl=63 time=0.467 ms
64 bytes from 192.168.31.33: icmp_seq=5 ttl=63 time=0.410 ms
64 bytes from 192.168.31.33: icmp_seq=6 ttl=63 time=0.704 ms
64 bytes from 192.168.31.33: icmp_seq=7 ttl=63 time=0.526 ms
64 bytes from 192.168.31.33: icmp_seq=8 ttl=63 time=0.691 ms
64 bytes from 192.168.31.33: icmp_seq=9 ttl=63 time=0.409 ms
^C
--- 192.168.31.33 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 810ms
rtt min/avg/max/ndev = 0.239/0.504/0.704/0.140 ms
root@n11:/tmp/pycore_46423/n11.conf#
```

Fig. 13.

| Porta | MAC Address       | Dispositivos |
|-------|-------------------|--------------|
| 1     | 00:00:00:aa:00:00 | PC n1        |
| 2     | 00:00:00:aa:00:03 | PC n2        |
| 3     | 00:00:00:aa:00:01 | PC n3        |
| 4     | 00:00:00:aa:00:02 | Host n4      |

## 4 Conclusão

Com este trabalho conseguimos consolidar os temas abordados nas aulas teóricas relativos à camada de ligação lógica, mais especificamente o uso da tecnologia Ethernet e do protocolo ARP. Desta forma é possível verificar que estas temáticas têm aplicações práticas úteis e importantes. Podemos ver também a importância destas tecnologias na nossa sociedade atual, devido à quantidade enorme de dispositivos que as utilizam para o seu correto funcionamento.