

Universidade do Minho

”TP3: Nível de Ligação Lógica”

Redes Ethernet

Protocolo ARP

Grupo 52

Licenciatura em Engenharia Informática

Redes de Computadores

a85646	a98286	a87978
Hugo Teles Silva	Luís Ferreira	Tiago Cunha

Braga, 27 de Abril de 2023

3 - Captura e análise de Tramas Ethernet

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

```
▼ Ethernet II, Src: Apple_55:c8:73 (f0:18:98:55:c8:73), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Source: Apple_55:c8:73 (f0:18:98:55:c8:73)
  Type: IPv4 (0x0800)
```

Figure 1: Endereços MAC origem e destino

O endereço MAC de origem da trama capturada "f0:18:98:55:c8:73" refere-se a um equipamento produzido pela Apple (<https://maclookup.app/search/result?mac=f01898>) e o endereço MAC de destino da trama capturada "00:d0:03:ff:94:00" refere-se a um equipamento produzido pela Comda Enterprises(<https://maclookup.app/macaddress/00D003>). Os 3 primeiros octetos são únicos e identificam a empresa produtora do hardware.

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

O valor do campo Type da trama Ethernet é 0x0800, este valor indica que a trama que está contida é IPv4.

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

```
▼ Internet Protocol Version 4, Src: 172.26.54.37, Dst: 193.137.9.171
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
```

Figure 2: Tamanho do cabeçalho IP

```
▼ Transmission Control Protocol, Src Port: 50418, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 50418
  Destination Port: 443
  [Stream index: 7]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 4003976431
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 560072513
  1000 .... = Header Length: 32 bytes (8)
```

Figure 3: Tamanho do cabeçalho TCP

O tamanho de um cabeçalho Ethernet é de 14 bytes (<https://library.netapp.com/ecmdocs/ECMP1155586/html/GUID-E29F791E-4AD5-4EB1-AC22-78A7B25783AC.html>)

Assim, o nº de bytes utilizados no encapsulamento protocolar pode ser obtido da seguinte maneira:
 $20+32+14 = 66$ bytes

```

Transmission Control Protocol, Src Port: 50418, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 50418
Destination Port: 443
[Stream index: 7]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 4003976431
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 560072513
1000 .... = Header Length: 32 bytes (8)

```

Figure 4: Tamanho total da trama

O tamanho total do pacote é de 143. Subtraímos o tamanho total do pacote ao valor anteriormente calculado, $143 - 66 = 77$. Deste modo, é possível calcular a sobrecarga introduzida pela pilha protocolar que é $77/143 * 100 = 53.8$

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

O endereço MAC da fonte é 00:d0:03:ff:94:00 e corresponde ao router ao qual a máquina nativa está conectada.

```

Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_55:c8:73 (f0:18:98:55:c8:73)
  Destination: Apple_55:c8:73 (f0:18:98:55:c8:73)
  Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Type: IPv4 (0x0800)

```

Figure 5: Endereço Ethernet fonte

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

O endereço MAC de destino é f0:18:98:55:c8:73 e corresponde à máquina nativa.

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.

```

Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_55:c8:73 (f0:18:98:55:c8:73)
Internet Protocol Version 4, Src: 35.214.255.218, Dst: 172.26.54.37
Transmission Control Protocol, Src Port: 443, Dst Port: 50255, Seq: 7410, Ack: 78, Len: 535
Transport Layer Security

```

Figure 6: Trama

Como se pode verificar na figura, os protocolos contidos na trama recebida são: Ethernet, IPv4, TCP e TLS.

4 - Protocolo ARP

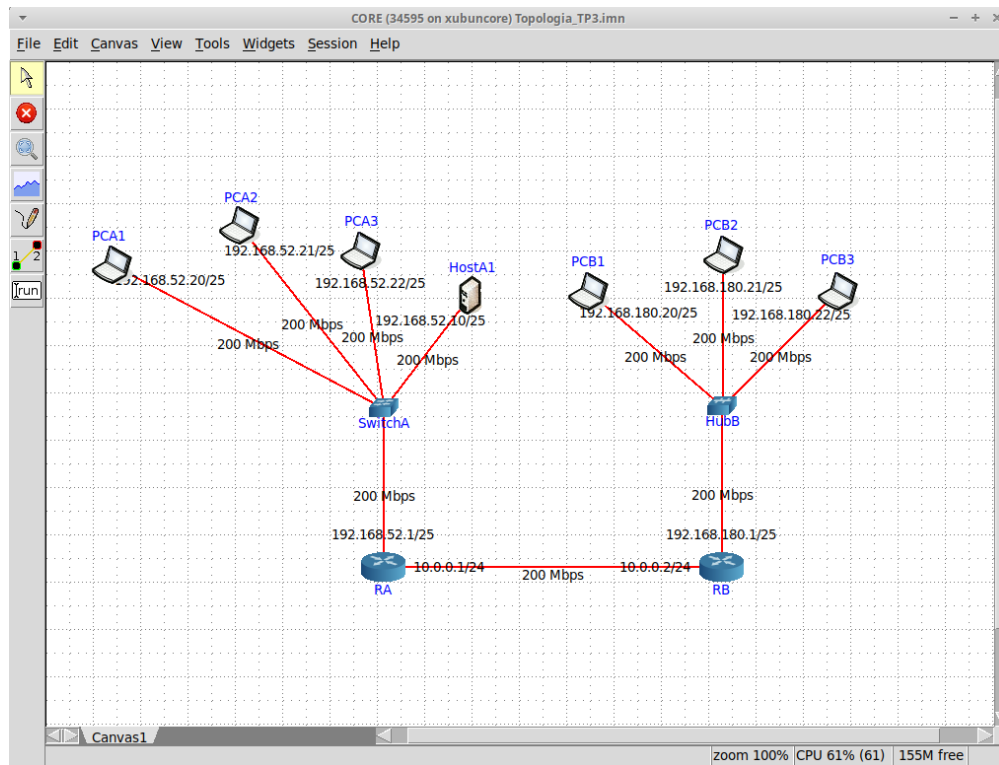


Figure 7: Topologia

- 1 Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando `arp -a`.
- 1.a Com a ajuda do manual ARP (`man arp`), interprete o significado de cada uma das colunas da tabela.

```
root@PCA1:/tmp/pycore.37473/PCA1.conf# arp -a
? (192.168.52.1) at 00:00:00:aa:00:02 [ether] on eth0
```

Figure 8: Terminal do PCA1 - Comando `arp -a`

```
root@PCA1:/tmp/pycore.37473/PCA1.conf# arp
Address      Hwtype      Hwaddress    Flags Mask    Iface
192.168.52.1 ether       00:00:00:aa:00:02 C            eth0
```

Figure 9: Terminal do PCA1 - Comando `arp`

Com o auxílio do manual ARP, temos que para este caso em particular router e PC, a tabela Address diz-nos o endereço IP do router com o qual o PC se comunicou, o HwType diz-nos o tipo de endereço MAC do router com o qual o PC se comunicou, o HwAddress diz-nos o endereço MAC do router com o qual o PC se comunicou, a Flag Mask diz-nos o tipo de endereço, se é dinâmico ou estático, neste caso a Flag 'C' refere-se a um tipo de endereço dinâmico, por fim a Iface refere-se ao nome da interface de rede (neste caso eth0) por meio da qual o PC se comunicou com o router.

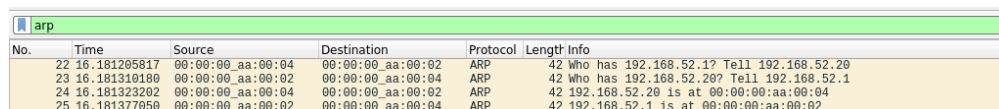
1.b Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.

O equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas são os routers RA e RB, uma vez que possuem duas interfaces que são um ponto de passagem para receber informação e reencaminhar ao destino.

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

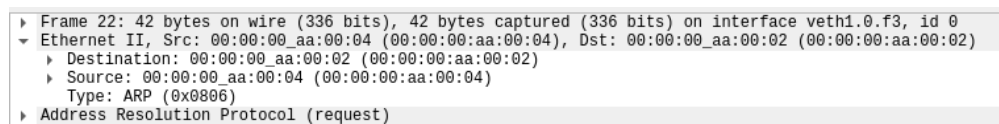
2.a a. Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

O valor hexadecimal do endereço MAC origem é 00:00:00:aa:00:04 e o endereço MAC destino é 00:00:00:aa:00:02. No ARP Request em questão, o endereço MAC destino é de broadcast, uma vez que o objetivo do envio deste pacote é o host de origem saber qual é o endereço MAC de um certo host. Como a cache havia sido limpa antes da captura no Wireshark, o PC de origem tem de enviar um ARP Request a todos os dispositivos da subrede para obter essa informação.



No.	Time	Source	Destination	Protocol	Length	Info
22	16.181295817	00:00:00:aa:00:04	00:00:00:aa:00:02	ARP	42	Who has 192.168.52.1? Tell 192.168.52.20
23	16.181310180	00:00:00:aa:00:02	00:00:00:aa:00:04	ARP	42	Who has 192.168.52.20? Tell 192.168.52.1
24	16.181323202	00:00:00:aa:00:04	00:00:00:aa:00:02	ARP	42	192.168.52.20 is at 00:00:00:aa:00:04
25	16.181377050	00:00:00:aa:00:02	00:00:00:aa:00:04	ARP	42	192.168.52.1 is at 00:00:00:aa:00:02

Figure 10: Wireshark - Captura com o filtro arp



▶ Frame 22: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.f3, id 0
▼ Ethernet II, Src: 00:00:00:aa:00:04 (00:00:00:aa:00:04), Dst: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
▶ Destination: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
▶ Source: 00:00:00:aa:00:04 (00:00:00:aa:00:04)
▶ Type: ARP (0x0806)
▶ Address Resolution Protocol (request)

Figure 11: Trama Ethernet - ARP Request

2.b Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?

O valor hexadecimal do campo Tipo da trama ethernet é 0x0806, que indica o protocolo da camada superior que está a ser utilizada na trama, neste caso, o valor "0x0806" indica que a trama Ethernet contém um protocolo ARP.

- 2.c Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
  Sender IP address: 192.168.52.20
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.52.1
```

Figure 12: Trama Ethernet - Cabeçalho do ARP Request

Através da figura podemos verificar que se trata efetivamente de um pedido ARP pelas seguintes razões:

De acordo com o valor do campo "opcode" da mensagem ARP que é 1 e pelos tipos de endereços presentes no pedido ARP que são IP e MAC, tanto de origem como destino.

- 2.d Explícite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?

Neste pedido ARP, o host de origem envia uma mensagem para todos os hosts na subrede, a questionar qual deles possui um endereço IP específico mencionado no pedido. O dispositivo com o endereço IP em questão responde com um pacote ARP que contém o endereço MAC desejado.

3 Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

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

O valor do campo ARP "opcode" é 2 o que indica que a mensagem refere-se a uma resposta (reply).

```
▶ Frame 24: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.f3, id 0
▼ Ethernet II, Src: 00:00:00_aa:00:04 (00:00:00:aa:00:04), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  ▶ Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  ▶ Source: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
  Type: ARP (0x0806)
▼ 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:00:04 (00:00:00:aa:00:04)
  Sender IP address: 192.168.52.20
  Target MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  Target IP address: 192.168.52.1
```

Figure 13: Trama Ethernet - ARP Reply

- 3.b Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?

A resposta ao pedido ARP efetuado (endereço MAC) está no campo Sender MAC address

- 3.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.

```
root@PCA1:/tmp/pycore.37473/PCA1.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.52.20 netmask 255.255.255.128 broadcast 0.0.0.0
    inet6 2001:1::20 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:4 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:04 txqueuelen 1000 (Ethernet)
    RX packets 2175 bytes 175961 (175.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 3440 (3.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28 bytes 2380 (2.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2380 (2.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 14: Terminal PCA1 - ifconfig

```
root@PCA1:/tmp/pycore.37473/PCA1.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.52.1 0.0.0.0 UG 0 0 0 eth0
192.168.52.0 0.0.0.0 255.255.255.128 U 0 0 0 eth0
```

Figure 15: Terminal PCA1 - netstat -rn

```
root@PCA1:/tmp/pycore.37473/PCA1.conf# arp
Address HWtype HWaddress Flags Mask Iface
192.168.52.1 ether 00:00:00:aa:00:02 C eth0
```

Figure 16: Terminal PCA1 - arp

Recorrendo ao comando `ifconfig` temos que o seu output apresenta duas interfaces de rede, a interface `eth0` que possui o endereço IP 192.168.52.20, com máscara de rede 255.255.255.128 e o seu endereço MAC 00:00:00:aa:00:04, a interface `lo`, que possui o endereço IP 127.0.0.1, com máscara de rede 255.0.0.0 e que não possui endereço MAC. Sendo o sistema com o IP 192.168.52.20 o PCA1 (pertencente ao Departamento A)

Recorrendo ao comando `arp` temos que o endereço IP 192.168.52.1 está associado ao endereço MAC 00:00:00:aa:00:02. A informação adicional "[ether] on eth0" indica que esta entrada foi obtida através da interface de rede `eth0`, que é a interface de rede do sistema que está associada a esta entrada na tabela ARP.

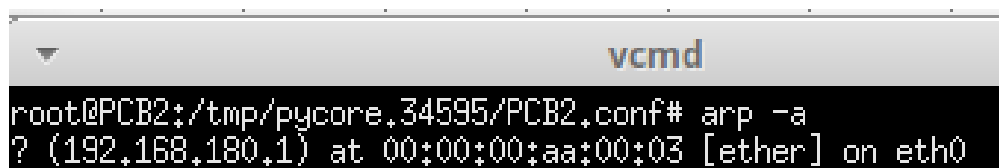
Em suma os endereços MAC origem e destino da trama, referem-se ao PCA1 pertencente ao Departamento A e o Router RA, respetivamente.

3.d Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

O modo de comunicação usado no envio da resposta ARP (ARP Reply) é unicast. Isto acontece pois, ao contrário do ARP Request, que é enviado um broadcast para toda a rede, a resposta ARP é direcionada especificamente ao dispositivo que fez o pedido, utilizando o endereço MAC conhecido do dispositivo que efetuou o pedido.

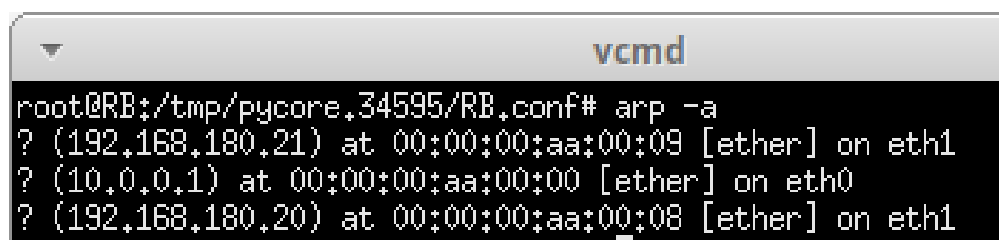
4 Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada.

O ping efetuado ao segundo PC (PCB2) originou pacotes ARP no router RB, uma vez que, há um novo caminho descoberto, neste caso para o PCB2. Tendo sido originado também no PCB2.



```
vcmd
root@PCB2:/tmp/pycore.34595/PCB2.conf# arp -a
? (192.168.180.1) at 00:00:00:aa:00:03 [ether] on eth0
```

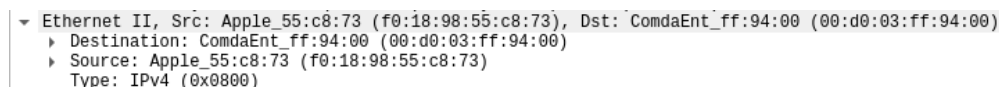
Figure 17: Terminal PCB2 - arp



```
vcmd
root@RB:/tmp/pycore.34595/RB.conf# arp -a
? (192.168.180.21) at 00:00:00:aa:00:09 [ether] on eth1
? (10.0.0.1) at 00:00:00:aa:00:00 [ether] on eth0
? (192.168.180.20) at 00:00:00:aa:00:08 [ether] on eth1
```

Figure 18: Terminal RB - arp

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.



```
▼ Ethernet II, Src: Apple_55:c8:73 (f0:18:98:55:c8:73), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Source: Apple_55:c8:73 (f0:18:98:55:c8:73)
  Type: IPv4 (0x0800)
```

Figure 19: Cabeçalho Ethernet

Os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear, são o tipo de hardware e o tipo do protocolo, o valor para o tipo de hardware é Ethernet (1), que representa o valor padrão para o endereço MAC que é 0x0001, o valor para o tipo do protocolo é IPv4 (0x0800), que é o tipo de protocolo mais comum em redes IP.

No que toca ao valor 1 no campo "tipo de hardware", este valor corresponde ao valor atribuído pela Internet Assigned Numbers Authority (IANA) para o tipo Ethernet (<https://www.iana.org/assignments/arp-parameters/arp-parameters.xhtml>), o valor 0x0800 no campo "tipo do protocolo" corresponde ao protocolo IPv4 (<https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>).

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.

Na situação em que efetua um ping a um PC não local à sua sub-rede, o PC Origem que efetuou o ping precisa de conhecer o endereço MAC desse PC não local à sub-rede do dispositivo em causa.

Supondo que existem duas sub-redes, sendo a sub-rede 1 referente ao PC origem e a sub-rede 2 referente ao PC destino, é possível esboçar o seguinte diagrama, com a respetiva ordem:

Origem	Destino	Protocolo	Informação
MAC PC Origem	Broadcast	ARP (Request)	MAC Origem: MAC PC Origem IP Origem: IP PC Origem MAC Destino: ??:??:??:??:??:?? (Desconhecido) IP Destino: IP Router Sub-rede1
MAC Router Sub-rede1	MAC PC Origem	ARP (Reply)	MAC Origem: MAC Router Sub-rede1 IP Origem: IP Router Sub-rede1 MAC Destino: MAC PC Origem IP Destino: IP PC Origem
IP PC Origem	IP PC Destino	ICMP	MAC Origem: MAC PC Origem IP Origem: IP PC Origem MAC Destino: MAC Router Sub-rede1 IP Destino: IP Router Sub-rede1
MAC Router Sub-rede2	Broadcast	ARP (Request)	MAC Origem: MAC Router Sub-rede2 IP Origem: IP Router Sub-rede2 MAC Destino: ??:??:??:??:??:?? (Desconhecido) IP Destino: IP PC Destino
MAC PC Destino	MAC Router Sub-rede2	ARP (Reply)	MAC Origem: MAC PC Destino IP Origem: IP PC Destino MAC Destino: MAC Router Sub-rede2 IP Destino: IP Router Sub-rede2
IP PC Destino	IP PC Origem	ICMP	MAC Origem: MAC PC Destino IP Origem: IP PC Destino MAC Destino: MAC PC Origem IP Destino: IP PC Origem

5. Domínios de colisão

- 1 **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.**

No departamento A os pacotes passam por um switch, que encaminha os pacotes para o destino pretendido. O switch permite uma organização mais estruturada das comunicações e também separa os domínios de colisão em função da conexão de cada dispositivo.

```

root@PCA1:/tmp/pycore.38425/PCA1.conf# ping 192.168.52.22
PING 192.168.52.22 (192.168.52.22) 56(84) bytes of data.
64 bytes from 192.168.52.22: icmp_seq=1 ttl=64 time=0.223 ms
64 bytes from 192.168.52.22: icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from 192.168.52.22: icmp_seq=3 ttl=64 time=0.109 ms
^C
--- 192.168.52.22 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.109/0.164/0.223/0.046 ms
root@PCA1:/tmp/pycore.38425/PCA1.conf#

```

Figure 20: Ping em PCA1 para PCA3

```

root@PCA2:/tmp/pycore.38425/PCA2.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
^C17:45:31.186960 IP 192.168.52.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:45:33.185705 IP6 fe80::200:ff:feaa:2 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
17:45:33.187006 IP 192.168.52.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:45:33.189031 IP6 fe80::200:ff:feaa:2 > ff02::5: OSPFv3, Hello, length 36
17:45:33.489779 IP6 fe80::200:ff:feaa:2 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
17:45:35.187265 IP 192.168.52.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:45:36.597037 ARP, Request who-has 192.168.52.22 tell 192.168.52.20, length 28
17:45:37.188260 IP 192.168.52.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:45:39.189475 IP 192.168.52.1 > 224.0.0.5: OSPFv2, Hello, length 44

0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@PCA2:/tmp/pycore.38425/PCA2.conf#

```

Figure 21: tcpdump em PCA2

Já no departamento B os pacotes passam por um hub, que direciona em broadcast, fazendo com que todos os dispositivos ligados recebam os pacotes, mesmo não sendo estes o destino pretendido. O hub permite então que haja apenas um domínio de colisão.

```

root@PCB1:/tmp/pycore.38425/PCB1.conf# ping 192.168.180.22
PING 192.168.180.22 (192.168.180.22) 56(84) bytes of data.
64 bytes from 192.168.180.22: icmp_seq=1 ttl=64 time=0.212 ms
64 bytes from 192.168.180.22: icmp_seq=2 ttl=64 time=0.151 ms
64 bytes from 192.168.180.22: icmp_seq=3 ttl=64 time=0.150 ms
^C
--- 192.168.180.22 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.150/0.171/0.212/0.029 ms
root@PCB1:/tmp/pycore.38425/PCB1.conf#

```

Figure 22: Ping em PCB1 para PCB3

```

root@PCB2:/tmp/pycore.38425/PCB2.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
^C17:46:39.210273 IP 192.168.180.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:46:41.211433 IP 192.168.180.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:46:41.276808 ARP, Request who-has 192.168.180.22 tell 192.168.180.20, length 28
17:46:41.276845 ARP, Reply 192.168.180.22 is-at 00:00:00:aa:00:0a (oui Ethernet), length 28
17:46:41.276893 IP 192.168.180.20 > 192.168.180.22: ICMP echo request, id 29, seq 1, length 64
17:46:41.276907 IP 192.168.180.22 > 192.168.180.20: ICMP echo reply, id 29, seq 1, length 64
17:46:42.289704 IP 192.168.180.20 > 192.168.180.22: ICMP echo request, id 29, seq 2, length 64
17:46:42.289763 IP 192.168.180.22 > 192.168.180.20: ICMP echo reply, id 29, seq 2, length 64
17:46:43.085364 IP6 fe80::200:ff:feaa:3 > ff02::5: OSPFv3, Hello, length 36
17:46:43.211620 IP 192.168.180.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:46:43.313687 IP 192.168.180.20 > 192.168.180.22: ICMP echo request, id 29, seq 3, length 64
17:46:43.313750 IP 192.168.180.22 > 192.168.180.20: ICMP echo reply, id 29, seq 3, length 64
17:46:45.211522 IP 192.168.180.1 > 224.0.0.5: OSPFv2, Hello, length 44

13 packets captured
13 packets received by filter
0 packets dropped by kernel
root@PCB2:/tmp/pycore.38425/PCB2.conf# █

```

Figure 23: tcpdump em PCB2

Em conclusão, hubs e switches diferem na maneira de controlar e dividir domínios de colisão. Hubs dão broadcast a todos os dispositivos na rede, criando um único domínio de colisão, e os switches apenas enviam os dados ao destino pretendido, criando domínios de colisões para cada conexão da rede, o que leva a um switch ser mais eficiente a controlar ou dividir os domínios de colisão do que um hub.

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

Dispositivo	Endereço MAC	Nº Porta
PCA1	00:00:00:aa:00:04	1
PCA2	00:00:00:aa:00:05	2
PCA3	00:00:00:aa:00:06	3
HostA1	00:00:00:aa:00:07	4
RA	00:00:00:aa:00:02	5

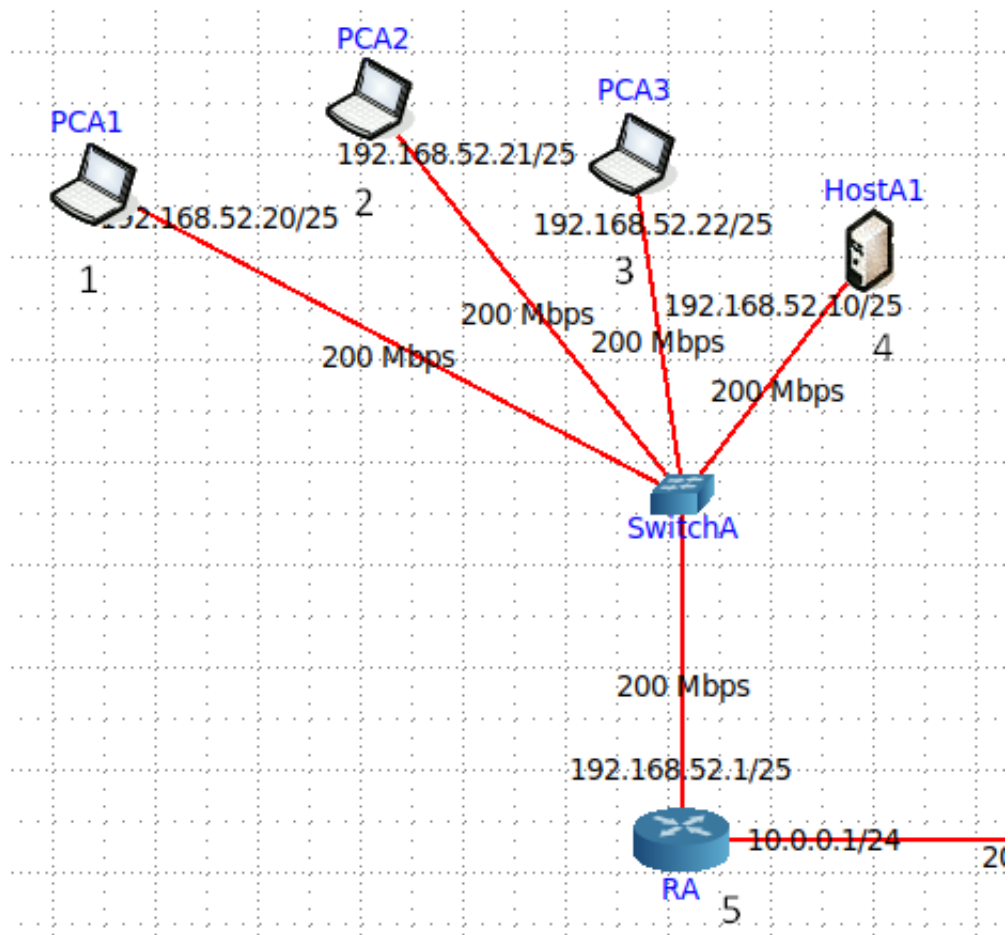


Figure 24: Departamento A

Conclusões

Este trabalho permitiu abringir os conhecimentos sobre o funcionamento de redes ethernet, permitindo ter noção da carga que um encapsulamento protocolar tem no tamanho de um pacote, e sobre o protocolo ARP, entendendo o funcionamento do mesmo. Serviu também para estudarmos as maneiras de lidar com os dominios de colisão que podem existir numa rede, através de switches e hubs.