Universidade do Minho

Departamento de Informática

TP3 - Camada de ligação lógica: Ethernet e Protocolo ARP
Redes e Computadores
Grupo 56

Bruno Martins (a80410) Filipe Monteiro (a80229)
Márcio Sousa (a82400)

10 de Dezembro de 2018

Conteúdo

1 Captura e Análise de Tramas Ethernet

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

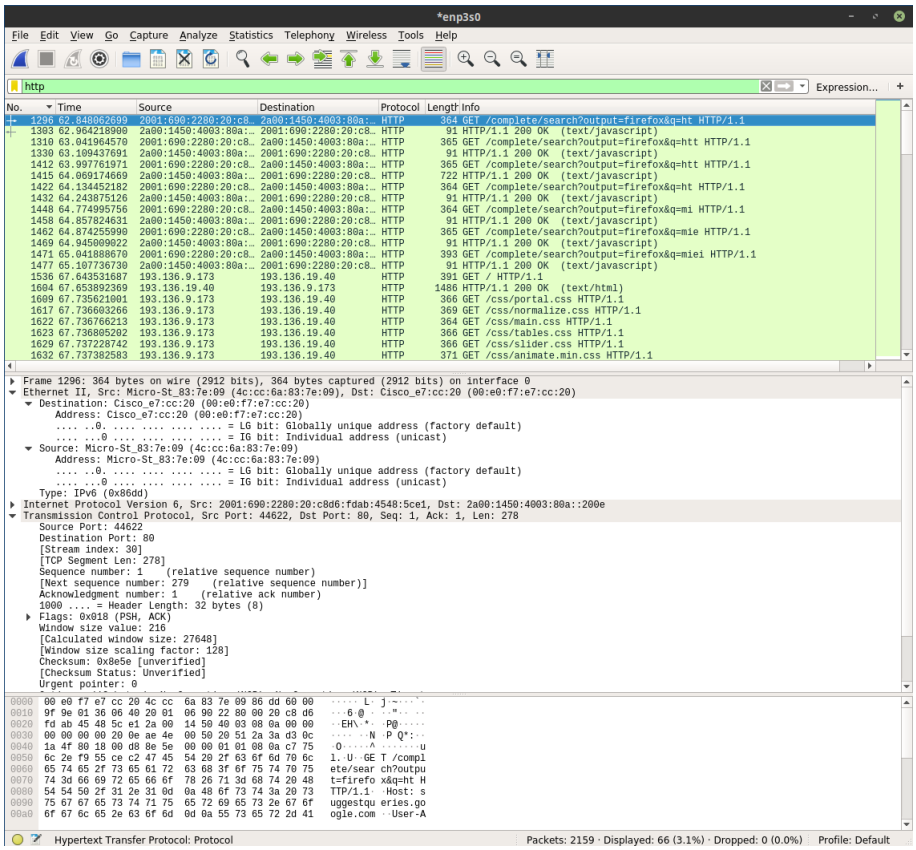

Figura 1: Primeiro trama capturada ao aceder à página miei.di.uminho.pt

O endereço MAC de origem é 4c:cc:6a:83:7e:09.
O endereço MAC do destino é 00:0a:8a:97:74:80.

1.2 Identifique a que sistemas se referem. Justifique.

```
pimonteiro@msi-fuck:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 193.136.9.173  netmask 255.255.255.0  broadcast 193.136.9.255
        inet6 fe80::cdf1:3f82:555c:55ad  prefixlen 64  scopeid 0x20<link>
        inet6 fd78:2b3:e7b0:4:c8d6:fdab:4548:5ce1  prefixlen 64  scopeid 0x0<global>
        inet6 2001:690:2280:20:c8d6:fdab:4548:5ce1  prefixlen 64  scopeid 0x0<global>
        inet6 2001:690:2280:20:6e05:f02a:225f:6979  prefixlen 64  scopeid 0x0<global>
        inet6 fd78:2b3:e7b0:4:526d:2a31:219e:a1f7  prefixlen 64  scopeid 0x0<global>
        ether 4c:cc:6a:83:7e:09  txqueuelen 1000  (Ethernet)
        RX packets 70334  bytes 60873450 (60.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34829  bytes 4076276 (4.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19

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 4401  bytes 405384 (405.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4401  bytes 405384 (405.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pimonteiro@msi-fuck:~$ host miei.di.uminho.pt
miei.di.uminho.pt is an alias for www6.di.uminho.pt.
www6.di.uminho.pt has address 193.136.19.40
```

(a) Em cima, o IP da nossa máquina (inet) assim como o endereço MAC (ether). Em baixo apresenta o IP correspondente à página da *web* em questão.

```
▼ Ethernet II, Src: Micro-St_83:7e:09 (4c:cc:6a:83:7e:09), Dst: Cisco_97:74:80 (00:0a:8a:97:74:80)
  ▼ Destination: Cisco_97:74:80 (00:0a:8a:97:74:80)
      Address: Cisco_97:74:80 (00:0a:8a:97:74:80)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: Micro-St_83:7e:09 (4c:cc:6a:83:7e:09)
      Address: Micro-St_83:7e:09 (4c:cc:6a:83:7e:09)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 193.136.9.173, Dst: 193.136.19.40
```

(b) Endereços MAC do *host* (nossa máquina) e do servidor.

Figura 2: Validação dos endereços de cada máquina.

O endereço MAC de origem corresponde à nossa máquina. O endereço MAC de destino refere-se ao servidor destino (*website*).

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

```
.... ...0 .... ....
Type: IPv4 (0x0800)
```

Figura 3: Detalhes do campo *Type* do trama *Ethernet*.

O valor hexadecimal é 0x0800 e significa que o tipo é IPv4.

1.4 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.

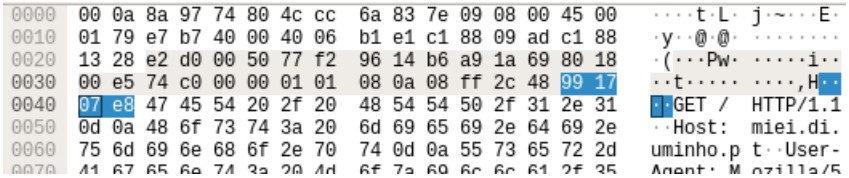

Figura 4: Frame da trama. A seguir ao selecionado começam os dados.

Existem 66 bytes de *overhead*. No total do pacote existem 391 bytes. A percentagem de overhead é aproximadamente 16,8%.

1.5 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?

O campo FCS não está a ser usado porque como o campo FCS ocupa bastante espaço no datagrama e o protocolo Ethernet já é atualmente mais fiável que no passado, não se envia este, sendo que se for preciso reenvia-se um novo pacote.

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

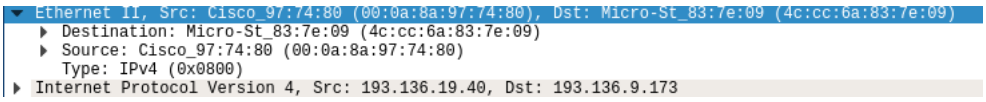

Figura 5: Trama *Ethernet* com os endereços MAC da fonte e do destino, assim como os IP's respetivos.

O endereço Ethernet da fonte é 00:0a:8a:97:74:80 e corresponde ao router que faz a ligação a uma rede exterior, pois o servidor não se encontra na nossa sub-rede, logo o MAC Address não pode pertencer ao servidor, mas sim ao aparelho de conexão à rede onde se contra o servidor.

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

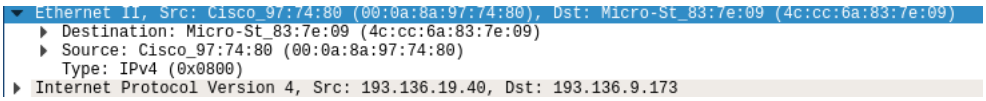

Figura 6: Trama *Ethernet* com os endereços MAC da fonte e do destino, assim como os IP's respetivos.

O enderço MAC destino é 4c:cc:6a:83:7e:09 e corresponde à nossa máquina.

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

```
No.     Time           Source                Destination           Protocol Length Info
     89 1.718876454    193.136.19.40         193.136.9.173         HTTP     1486   HTTP/1.1 200 OK  (text/html)
Frame 89: 1486 bytes on wire (11888 bits), 1486 bytes captured (11888 bits) on interface 0
Ethernet II, Src: Cisco_97:74:80 (00:0a:8a:97:74:80), Dst: Micro-St_83:7e:09 (4c:cc:6a:83:7e:09)
Internet Protocol Version 4, Src: 193.136.19.40, Dst: 193.136.9.173
Transmission Control Protocol, Src Port: 80, Dst Port: 58064, Seq: 68057, Ack: 326, Len: 1420
[34 Reassembled TCP Segments (69476 bytes): #23(1448), #25(2896), #27(1448), #29(2896), #31(1448), #33(1448), #35(1448),
#37(1448), #39(1448), #41(1448), #43(2896), #45(2896), #47(1448), #49(2896), #51(2896), #53(1448), #55(1448), #57(1448)]
Hypertext Transfer Protocol
```

Figura 7: Diferentes encapsulamentos protocolares da trama recebida.

Temos TCP, IPv4, HTTP, Ethernet II.

2 Protocolo Arp

2.9 Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas

```
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   00:d0:03:ff:94:00   C                     wlp2s0
```

Figura 8: Tabela ARP da nossa máquina.

1. *Address* - IP/endereço de uma máquina;
2. *HWtype* - tipo de ligação com essa máquina;
3. *HWaddress* - endereço MAC correspondente;
4. *Flags* - indicam o estado da entrada, ou seja, se foi deduzido, inserido manualmente ou incompleto;
5. *Iface* - indica o nome da *interface* a que o dispositivo está conectado.

2.10 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?

```
Address                  HWtype  HWaddress           Flags Mask            Iface
gw.sa.di.uminho.pt       ether   00:0c:29:d2:19:f0   C                     enp3s0
177.143.198.104.bc.goog          (incomplete)                              enp3s0
```

Figura 9: Tabela ARP da nossa máquina após conexão ao servidor.

Endereço origem: 4c:cc:6a:83:7e:09 Endereço destino: ff:ff:ff:ff:ff:ff

O endereço destino é este pois o pedido *ARP Request* usa um endereço MAC de broadcast para todas as máquinas receberem o pacote e eventualmente alguma aceitar, tratar e responder (por ser o IP destino do pacote).

Neste caso, fizemos um **ping 192.168.100.198**, não estando este guardado na tabela de ARP antes do ping.

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

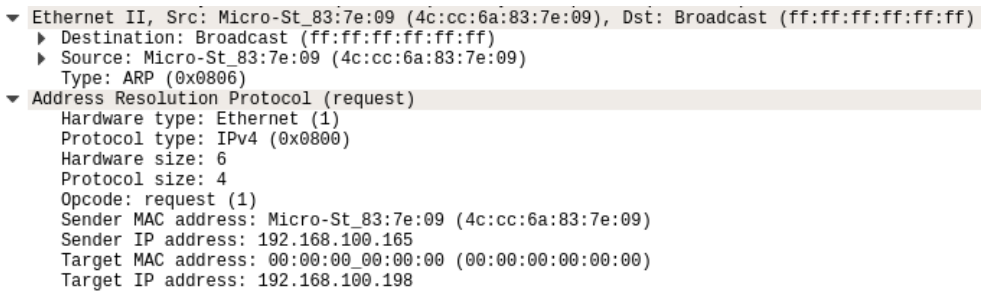

Figura 10: Trama c

O valor do campo tipo da trama é de 0x0806 que indica ser um ARP, sendo um ARP Request se analisarmos o *opcode*.

2.12 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`

O valor do campo ARP *opcode* é 1 e significa que se trata de um *Arp Request*.

2.13 Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Na mensagem ARP estão contidos dois tipos de endereços: endereços MAC e endereços IP, que serão usados para encaminhar o pacote para o destino correto e para mais tarde serem adicionados à tabela ARP.

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

O *host* de origem pede a quem tiver o IP XXX.XXX.XXX.XXX para lhe responder, ficando assim a saber o endereço MAC da máquina destino.

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

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

   O valor do campo ARP *opcode* é de 2 que significa ser uma resposta da máquina a um pedido ARP.

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

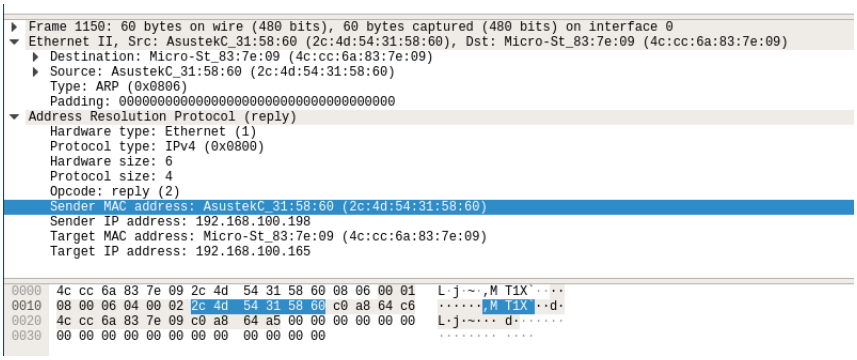

Figura 11: Ping de n1 para n2 (canto superior esquerdo), *tcpdump* de n2 (canto superior direito), *tcpdump* de n3 (canto inferior esquerdo), *tcpdump* de n4 (canto inferior direito

A resposta encontra-se não entre os *bytes* 23 e 28 (campo *MAC Address*).

3 ARP Gratuito

3.16 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?

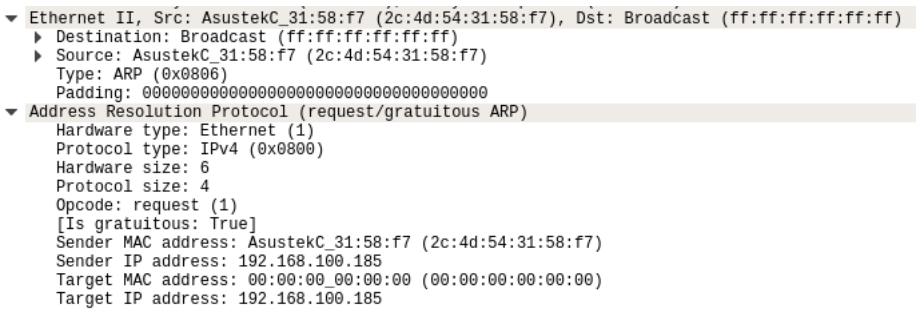

Figura 12: Pedido ARP gratuito

O pedido ARP gratuito distingue-se dos outros porque o Sender IP e o Target IP são o mesmo, o que não acontece normalmente.

4 Domínio de Colisão

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

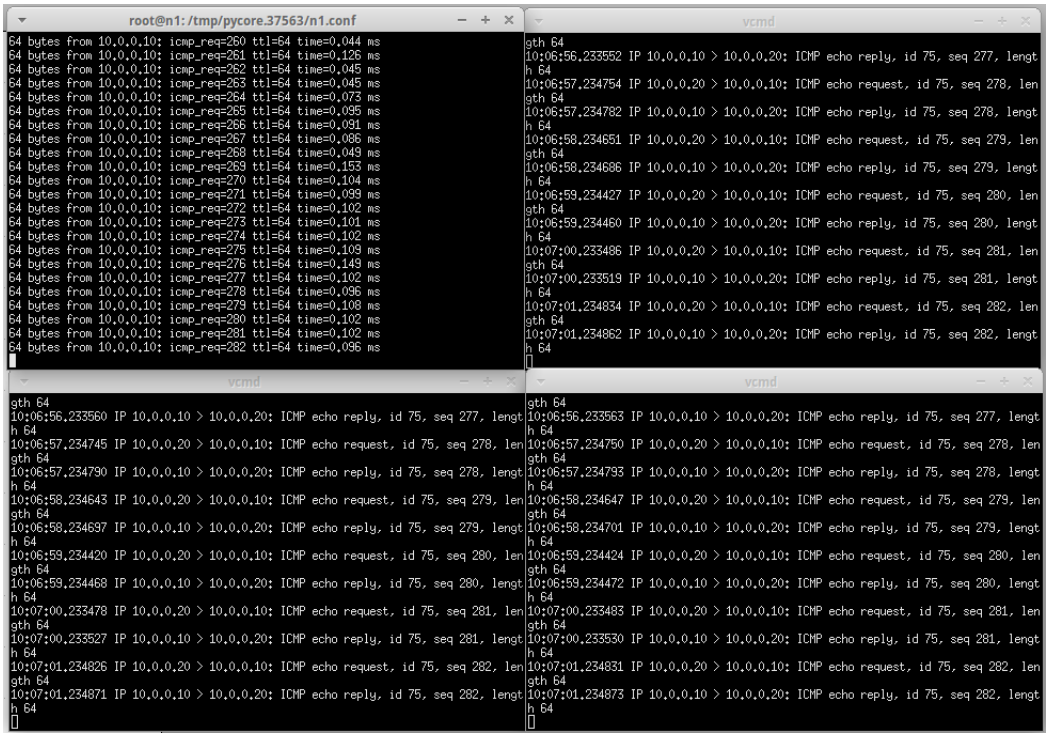

Figura 13: Ping de n1 para n2 (canto superior esquerdo), *tcpdump* de n2 (canto superior direito), *tcpdump* de n3 (canto inferior esquerdo), *tcpdump* de n4 (canto inferior direito

Analisando o tráfego, concluimos que com *hub*, apesar de estarmos a enviar tráfego de n1 para n2, os outros dispositivos conseguem ver este tráfego. Existe também a possibilidade de colisões, podendo haver a eliminação de pacotes, sendo depois necessário o seu reenvio. Para prevenir esta colisões existe o protocolo CSMA/CD que obriga dispositivos a esperar que outro acabe de comunicar antes de tentarem mandar tráfego.

4.18 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.

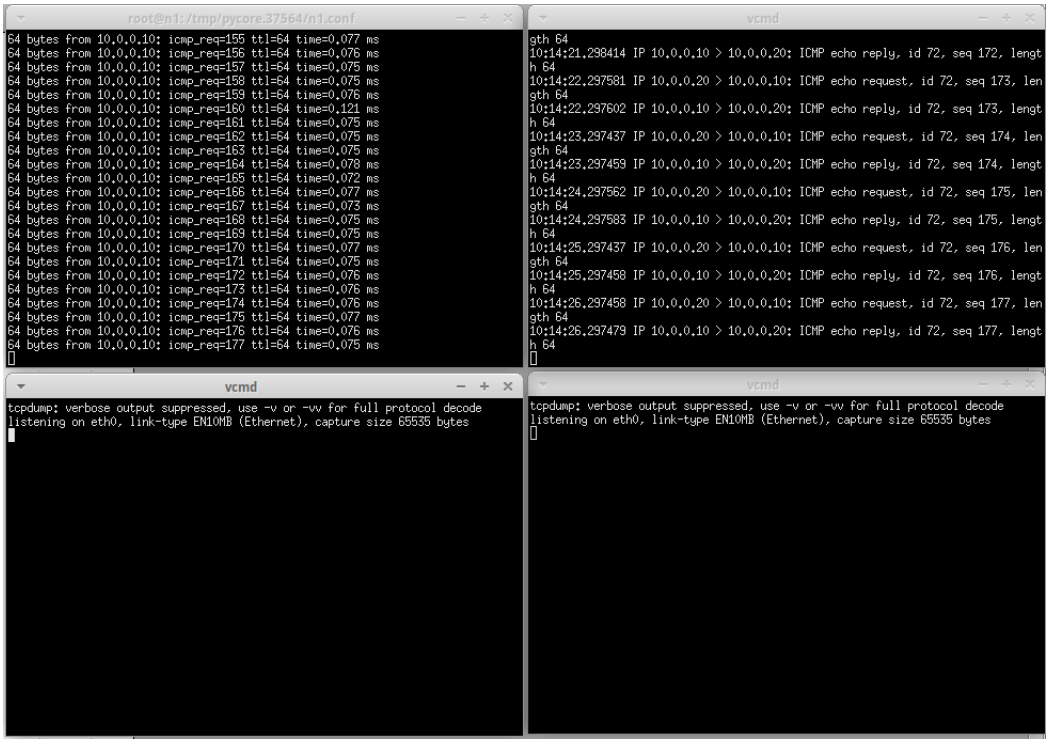

Figura 14: Ping de n1 para n2 (canto superior esquerdo), *tcpdump* de n2 (canto superior direito), *tcpdump* de n3 (canto inferior esquerdo), *tcpdump* de n4 (canto inferior direito

Utilizando um *switch* ao invés de *hub*, a rede o tráfedo de um dispositivo para outro passa a ir diretamente da origem para o destino, sendo que os outros dispositivos na rede não conseguem ver tráfego entre estes dois (o *switch* encaminha o pacote diretamente para a porta onde se encontra o destino).

5 Conclusão

Este relatório tem como objetivo appresentar as respostas à ficha apresentada nas aulas práticas. A resolução desta ficha permitiu-nos adquirir conhecimento acerca da arquitetura Ethernet fazendo com que, na prática, vissemos os endereços MAC de origem e destino das tramas que capturavamos utilizando o software *Wireshark* que nos ofereceu uma visão mais realista. Um dos grandes focos desta ficha foi também o protocolo ARP encontrado ao nível da ligação de dados, em que numa primeira fase foi analizado o conteúdo da tabela ARP, bem como os edereços lá especificados e o seu processo de encaminhamento de tramas. Já numa fase mais avançada foi forçado um pedido ARP gratuito de forma a conseguir visualizar as diferenças entre ele e os restantes pedidos. No final, através de uma topologia modelada no *CORE*, foi possível analisar as diferenças entre *hubs switches* dentro de uma rede, como funcionam e o porquê de os *switches* serem uma melhor escolha para usar.