

Universidade do Minho
Departamento de Informática
2020/2021

TP3: Nível de Ligação Lógica: Ethernet e Protocolo ARP

Redes de Computadores

3 de Dezembro de 2020

Grupo 77



Rita Gomes, A87960



Mário Real, A72720

1. Questões e Respostas

1.1. Captura e análise de Tramas Ethernet

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

Resposta:

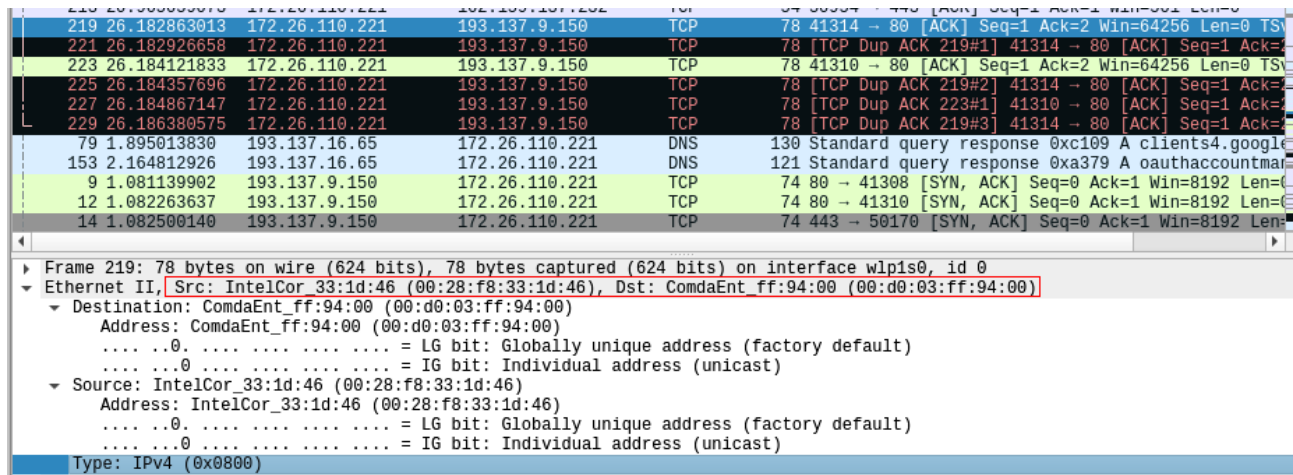


Figura 1: Endereços de origem e de destino da trama capturada.

Endereço de origem: 00:28:f8: 33:1d:46

Endereço de destino: 00:d0:03:ff:94:00

2) Identifique a que sistemas se referem. Justifique.

Resposta:

O endereço de origem corresponde à placa de rede do nosso computador (IntelCor).

O endereço de destino refere-se à interface de conexão do servidor (ComdaEnt).

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

Resposta:

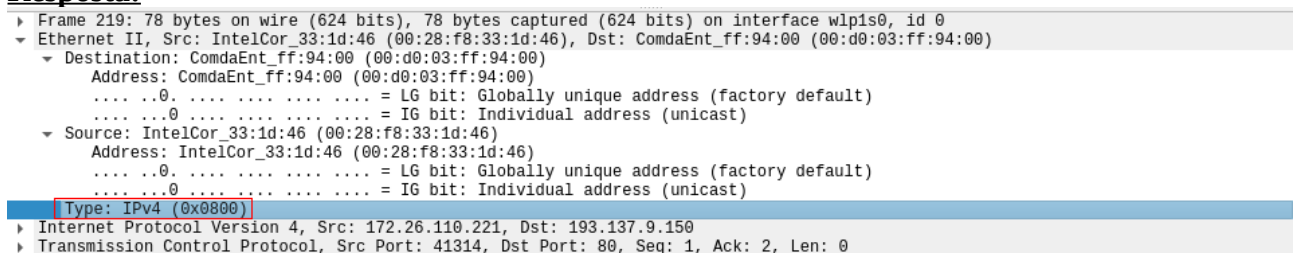


Figura 2: Trama Ethernet.

O valor hexadecimal do campo Type da trama Ethernet corresponde a 0x0800 , o que nos permite concluir que a trama possui 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.

Resposta:

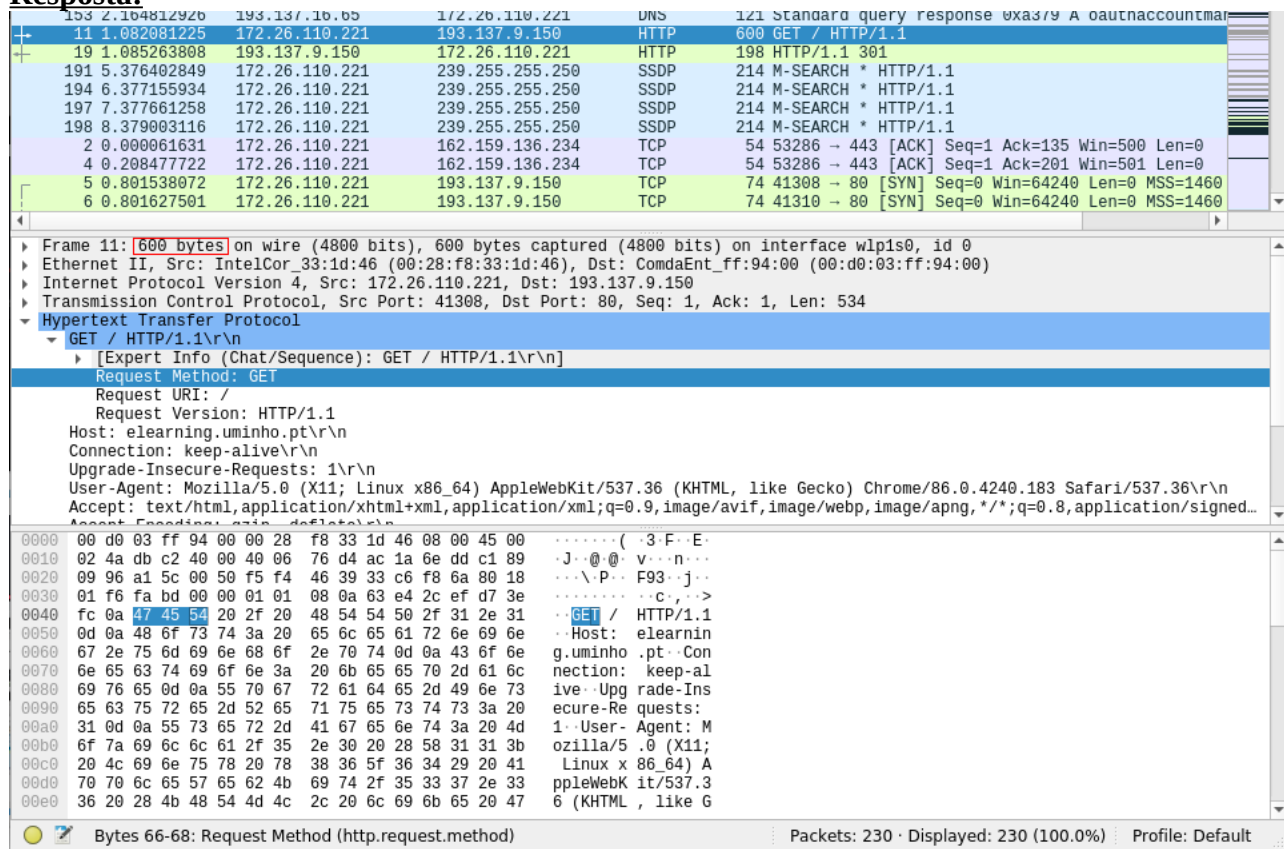


Figura 3: Caracteres ASCII do método HTTP GET.

Através da figura acima, conseguimos ver que até ao caractere ASCII “G” do método HTTP GET são usados 66 bytes. Sendo que o comprimento total da trama são 600 bytes, a sobrecarga introduzida pela pilha protocolar no envio do HTTP GET corresponde a $(66/600) \times 100 = 11$.

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)).

Resposta:

O FCS (Frame Check Sequence) é usado na camada de ligação para detetar a ocorrência de erros na transmissão do pacote. Como podemos verificar pelas imagens anteriores, o campo FCS não aparece na captura da trama, sendo assim, podemos concluir que este não está a ser utilizado. Isto acontece porque estamos a trabalhar com uma rede wired, na qual a probabilidade de existirem erros é baixa.

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

Resposta:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|-----------------|----------|--------|--|
| 79 | 1.895013830 | 193.137.16.65 | 172.26.110.221 | DNS | 130 | Standard query response 0xc109 A clients4.google |
| 152 | 2.161721895 | 172.26.110.221 | 193.137.16.65 | DNS | 105 | Standard query 0xa379 A outhaccountmanager.goo |
| 153 | 2.164812926 | 193.137.16.65 | 172.26.110.221 | DNS | 121 | Standard query response 0xa379 A outhaccountmar |
| + | 11 | 1.082081225 | 172.26.110.221 | HTTP | 600 | GET / HTTP/1.1 |
| + | 19 | 1.085263808 | 193.137.9.150 | HTTP | 198 | HTTP/1.1 301 |
| 191 | 5.376402849 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 194 | 6.377155934 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 197 | 7.377661258 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 198 | 8.379003116 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 2 | 0.000061631 | 172.26.110.221 | 162.159.136.234 | TCP | 54 | 53286 → 443 [ACK] Seq=1 Ack=135 Win=500 Len=0 |
| 4 | 0.208477722 | 172.26.110.221 | 162.159.136.234 | TCP | 54 | 53286 → 443 [ACK] Seq=1 Ack=201 Win=501 Len=0 |
| 5 | 0.801538072 | 172.26.110.221 | 193.137.9.150 | TCP | 74 | 41308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |
| 6 | 0.801627501 | 172.26.110.221 | 193.137.9.150 | TCP | 74 | 41310 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |

Frame 19: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface wlp1s0, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
Destination: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
Address: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
.....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: IPv4 (0x0800)

Figura 4: Endereço Ethernet da fonte.

O endereço da fonte é 00:d0:03:ff:94:00 e corresponde à rede Ethernet a que a máquina está ligada.

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

Resposta:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|-----------------|----------|--------|--|
| 79 | 1.895013830 | 193.137.16.65 | 172.26.110.221 | DNS | 130 | Standard query response 0xc109 A clients4.google |
| 152 | 2.161721895 | 172.26.110.221 | 193.137.16.65 | DNS | 105 | Standard query 0xa379 A outhaccountmanager.goo |
| 153 | 2.164812926 | 193.137.16.65 | 172.26.110.221 | DNS | 121 | Standard query response 0xa379 A outhaccountmar |
| + | 11 | 1.082081225 | 172.26.110.221 | HTTP | 600 | GET / HTTP/1.1 |
| + | 19 | 1.085263808 | 193.137.9.150 | HTTP | 198 | HTTP/1.1 301 |
| 191 | 5.376402849 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 194 | 6.377155934 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 197 | 7.377661258 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 198 | 8.379003116 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 | M-SEARCH * HTTP/1.1 |
| 2 | 0.000061631 | 172.26.110.221 | 162.159.136.234 | TCP | 54 | 53286 → 443 [ACK] Seq=1 Ack=135 Win=500 Len=0 |
| 4 | 0.208477722 | 172.26.110.221 | 162.159.136.234 | TCP | 54 | 53286 → 443 [ACK] Seq=1 Ack=201 Win=501 Len=0 |
| 5 | 0.801538072 | 172.26.110.221 | 193.137.9.150 | TCP | 74 | 41308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |
| 6 | 0.801627501 | 172.26.110.221 | 193.137.9.150 | TCP | 74 | 41310 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |

Frame 19: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface wlp1s0, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
Destination: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
Address: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
.....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: IPv4 (0x0800)

Figura 5: Endereço MAC do destino.

O endereço MAC do destino é 00:28:f8:33:1d:46 e corresponde ao endereço da máquina que está a ser utilizada para efetuar a ligação.

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

Resposta:

| | | | | | |
|-----|-------------|----------------|-----------------|------|--|
| 191 | 5.376402849 | 172.26.110.221 | 239.255.255.250 | SSDP | 214 M-SEARCH * HTTP/1.1 |
| 19 | 1.085263808 | 193.137.9.150 | 172.26.110.221 | HTTP | 198 HTTP/1.1 301 |
| 11 | 1.082081225 | 172.26.110.221 | 193.137.9.150 | HTTP | 600 GET / HTTP/1.1 |
| 153 | 2.164812926 | 193.137.16.65 | 172.26.110.221 | DNS | 121 Standard query response 0xa379 A oauthaccountmanager |
| 152 | 2.161721895 | 172.26.110.221 | 193.137.16.65 | DNS | 105 Standard query 0xa379 A oauthaccountmanager.google |
| 79 | 1.895013830 | 193.137.16.65 | 172.26.110.221 | DNS | 130 Standard query response 0xc109 A clients4.google |

Frame 11: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits) on interface wlp1s0, id 0
Ethernet II, Src: IntelCor_33:1d:46 (00:28:f8:33:1d:46), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.110.221, Dst: 193.137.9.150
Transmission Control Protocol, Src Port: 41308, Dst Port: 80, Seq: 1, Ack: 1, Len: 534
Hypertext Transfer Protocol

Figura 4: Protocolos contidos na trama recebida.

A trama recebidos tem os seguintes protocolos: Ethernet, IPv4, TCP e HTTP.

1.2. Protocolo ARP

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

Resposta:

```
ritagomes@RitaGomes:~$ /usr/sbin/arp
```

| Endereço | TipoHW | EndereçoHW | Opções | Máscara | Interface |
|----------|--------|------------|--------|-------------------|-----------|
| _gateway | | | ether | 00:d0:03:ff:94:00 | C |
| 0 | | | | | wlp1s |

Figura 5: Tabela ARP.

Na primeira coluna está representado o endereço da máquina na rede, que nesta situação é o 'gateway'. Na segunda coluna, o campo 'TipoHW' representa o tipo do protocolo de rede que, neste caso, é o 'ether'. Na coluna seguinte temos o 'EndereçoHW' que nos mostra o endereço MAC da máquina, que corresponde a 00:d0:03:ff:94:00. De seguida, temos a coluna 'Opções', que define o tipo de protocolo ARP, que, neste cenário, está vazio. Seguidamente, temos a coluna 'Máscara', que explicita que o endereço pertence à classe C. E, por último, temos a coluna 'Interface', que identifica qual é a interface rede que a máquina está a usar que, neste caso, é 'wlp1s0'.

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?

Resposta:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|-------------------|-------------|----------|--------|--|
| 101 | 4.497414772 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 102 | 5.522895482 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 103 | 6.546831953 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 104 | 7.571098955 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 105 | 8.594880289 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 106 | 9.618837095 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 107 | 10.6429935... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 111 | 11.6668353... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 134 | 12.6909556... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 135 | 13.7150262... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 136 | 14.7388367... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 137 | 15.7630456... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 138 | 17.7883702... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |
| 139 | 18.8029491... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.55.7? Tell 172.26.110.221 |

Frame 101: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp1s0, id 0
Ethernet II, Src: IntelCor_33:1d:46 (00:28:f8:33:1d:46), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
Type: ARP (0x0806)
Address Resolution Protocol (request)

Figura 6: Endereços de destino e de origem da trama.

O endereço de origem é 00:28:f8:33:1d:46 e o endereço de destino é ff:ff:ff:ff:ff:ff. Temos, neste caso, um endereço de broadcast (ff:ff:ff:ff:ff:ff) como destino, proveniente do facto de na tabela ARP ainda não estar registado o endereço MAC da interface de destino, pelo que é necessário fazer um request a todos os dispositivos da rede local para determinar qual o endereço MAC do destino pretendido.

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

Resposta:

Através da figura 6 no campo ‘Type’ visualizamos que o valor hexadecimal do campo do tipo da trama Ethernet é 0x0806 e indica que o protocolo utilizado foi o 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?

Resposta:

```
Frame 101: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp1s0, id 0
Ethernet II, Src: IntelCor_33:1d:46 (00:28:f8:33:1d:46), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
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_33:1d:46 (00:28:f8:33:1d:46)
Sender IP address: 172.26.110.221
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.55.7
```

Figura 7: Pedido ARP.

O valor do campo ‘Opcode’ no protocolo ARP (Adress Resolution Protocol) é 1, o que nos permite concluir que se trata de um pedido (request). Na mensagem ARP estão contidos o endereço IP e o endereço MAC da nossa máquina e o endereço IP da máquina pelo qual queremos saber o endereço MAC.

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

Resposta:

O host de origem pergunta quem tem o endereço de destino (Who has 172.26.55.77?). Assim irá, através do endereço IP de destino, descobrir o MAC address a que lhe corresponde.

14) Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

```
Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp1s0, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_33:1d:46 (00:28:f8:33:1d:46)
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_33:1d:46 (00:28:f8:33:1d:46)
Target IP address: 172.26.110.221
```

Figura 7: Resposta ao pedido ARP efetuado.

a) Qual o valor do campo ARP opcode? O que especifica?

Resposta:

O campo ARP opcode tem o valor 2 e especifica uma resposta (reply).

b) Em que posição da mensagem ARP está a resposta ao pedido ARP ?

Resposta:

A resposta ao pedido ARP está no endereço 00:d0:03:ff:94:00, correspondente ao Sender MAC address.

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?

Resposta:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|-------------------|-------------------|----------|--------|---|
| 27 | 0.168240037 | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.254.254? Tell 172.26.110.221 |
| 28 | 0.169947816 | ComdaEnt_ff:94:00 | IntelCor_33:1d:46 | ARP | 60 | 172.26.254.254 is at 00:d0:03:ff:94:00 |
| 192 | 16.0382017... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 192.168.43.213? Tell 192.168.43.182 |
| 193 | 16.0483367... | 5a:32:00:06:6c:62 | IntelCor_33:1d:46 | ARP | 42 | 192.168.43.213 is at 5a:32:00:06:6c:62 |
| 321 | 21.0277789... | 5a:32:00:06:6c:62 | IntelCor_33:1d:46 | ARP | 42 | Who has 192.168.43.182? Tell 192.168.43.213 |
| 322 | 21.0278046... | IntelCor_33:1d:46 | 5a:32:00:06:6c:62 | ARP | 42 | 192.168.43.182 is at 00:28:f8:33:1d:46 |
| 378 | 28.4333787... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.254.254? Tell 172.26.110.221 |
| 379 | 28.4349667... | ComdaEnt_ff:94:00 | IntelCor_33:1d:46 | ARP | 60 | 172.26.254.254 is at 00:d0:03:ff:94:00 |
| 577 | 50.2897430... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.254.254? Tell 172.26.110.221 |
| 578 | 50.2911643... | ComdaEnt_ff:94:00 | IntelCor_33:1d:46 | ARP | 60 | 172.26.254.254 is at 00:d0:03:ff:94:00 |
| 772 | 78.9276697... | IntelCor_33:1d:46 | Broadcast | ARP | 42 | Who has 172.26.254.254? Tell 172.26.110.221 |
| 773 | 78.9291044... | ComdaEnt_ff:94:00 | IntelCor_33:1d:46 | ARP | 60 | 172.26.254.254 is at 00:d0:03:ff:94:00 |
| 24 | 0.100982458 | 0.0.0.0 | 255.255.255.255 | DHCP | 335 | DHCP Request - Transaction ID 0xef461150 |

Figura 9: Informação referente ao pacote de pedido ARP gratuito.

Devido a uma suposta incompatibilidade e/ou um problema desconhecido, identificado na aula pelos alunos e professor, na mais recente distribuição do nosso Sistema (Linux Ubuntu), como podemos observar na imagem 9 o nosso sistema não nos permitiu a origem do pacote de pedido ARP gratuito pretendido. No entanto, caso este pacote aparecesse na nossa captura estaria identificado com 'Gratuitous ARP'.

Um pedido ARP gratuito e um não gratuito diferenciam-se no facto de que um ARP gratuito pode ser enviado a qualquer altura por um host para o endereço de Broadcast da rede, com a finalidade de verificar que o seu endereço IP não está a ser utilizado e para que outros dispositivos da rede possam atualizar a sua tabela ARP, com a finalidade de conseguirem comunicar com o host que envia o pedido. Assim, este pedido é diferente do ARP não gratuito, já que não espera uma resposta, mas sim atualiza o estado de rede.

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?

Resposta:

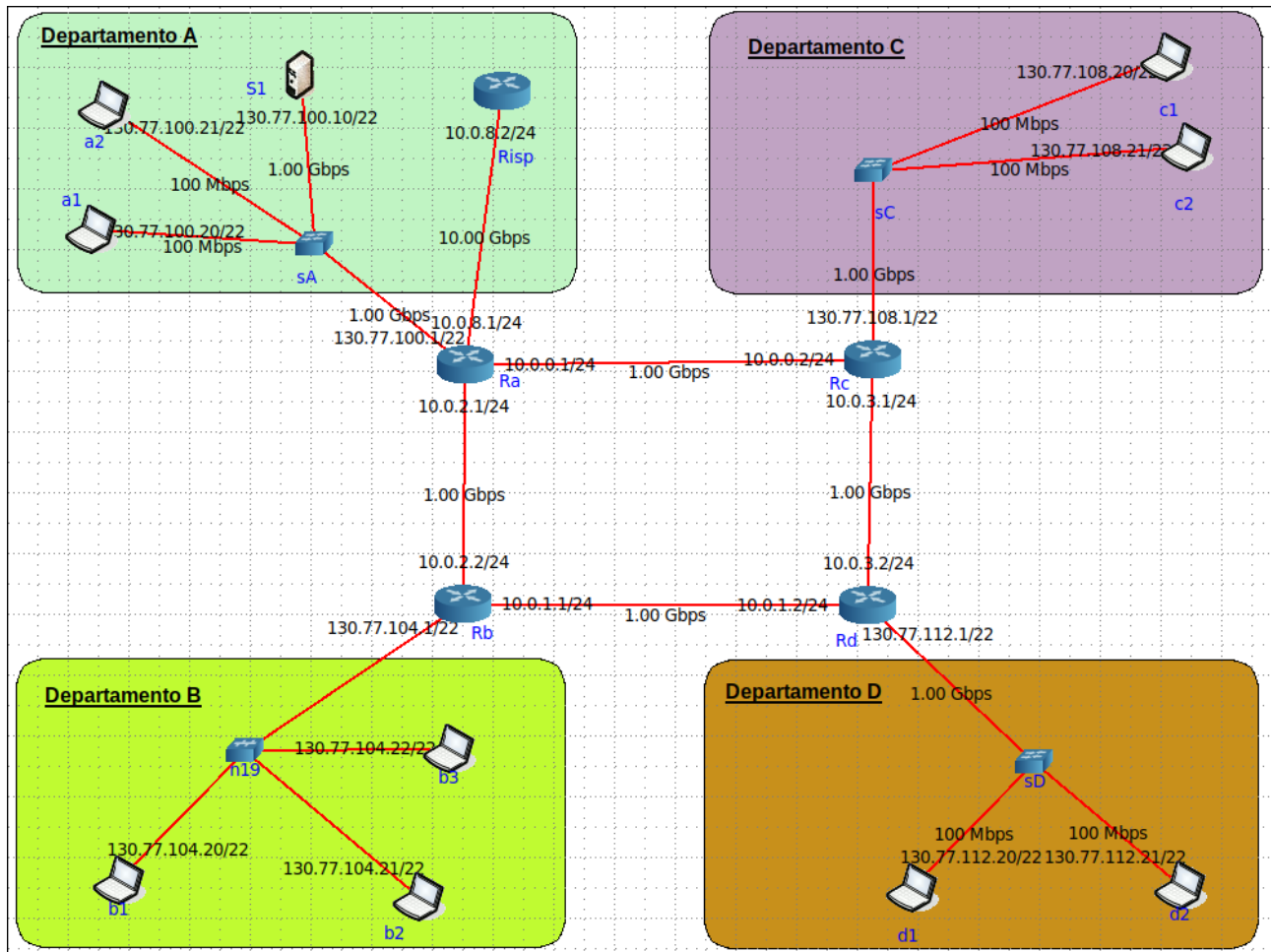


Figura 10: Solução de subnetting após substituição do Switch por um **Hub** 'n19' no Departamento B.

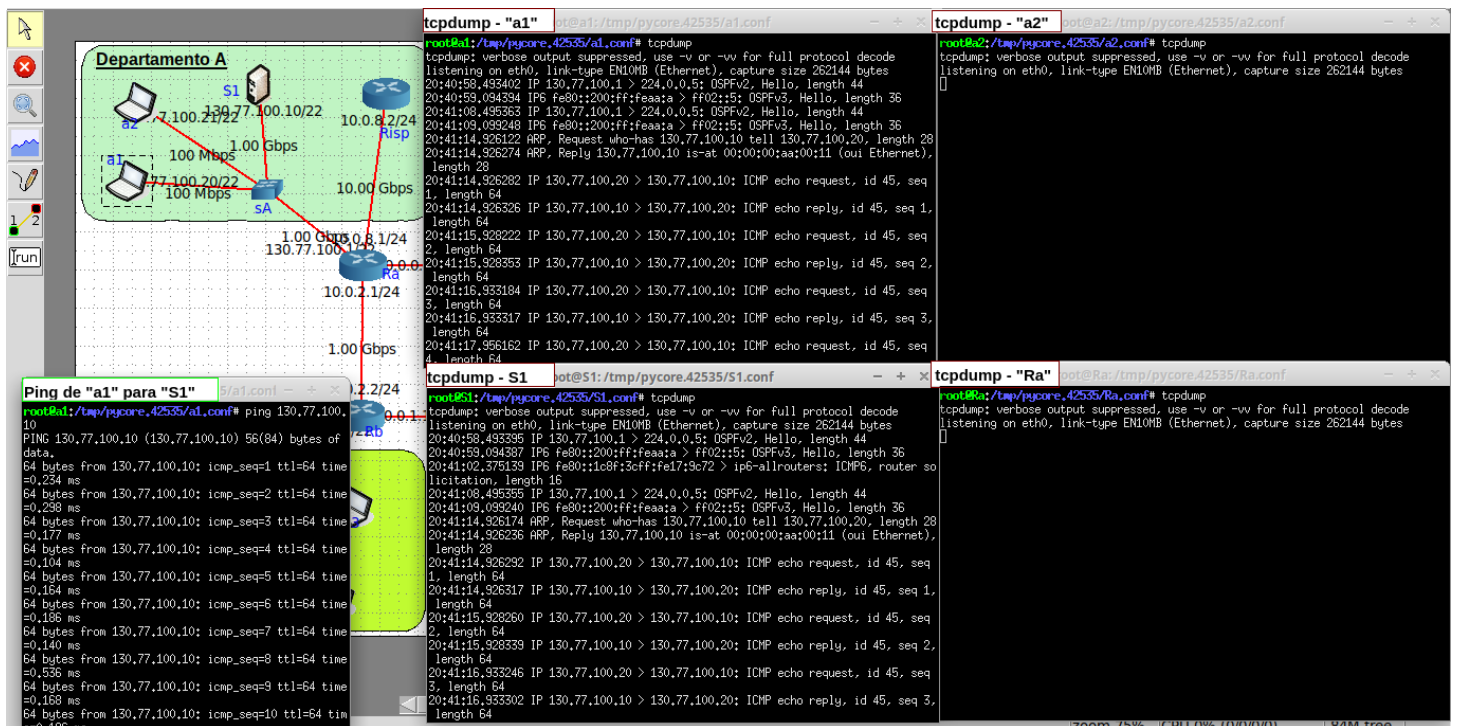


Figura 11: "Departamento A" : Análise do tráfego gerado intra-departamento.

Através da figura 11 analisámos o tráfego gerado no ‘Departamento A’, ligado por um ‘Switch’. Este resultado foi obtido usando o comando ‘ping’ do Pc ‘a1’ para o host ‘S1’. Concluimos então, pela análise do tráfego apresentado, que não há partilha de meios, e os pedidos e respostas apenas fluem pelas máquina envolvidas diretamente no nosso envio de pacotes pretendido.

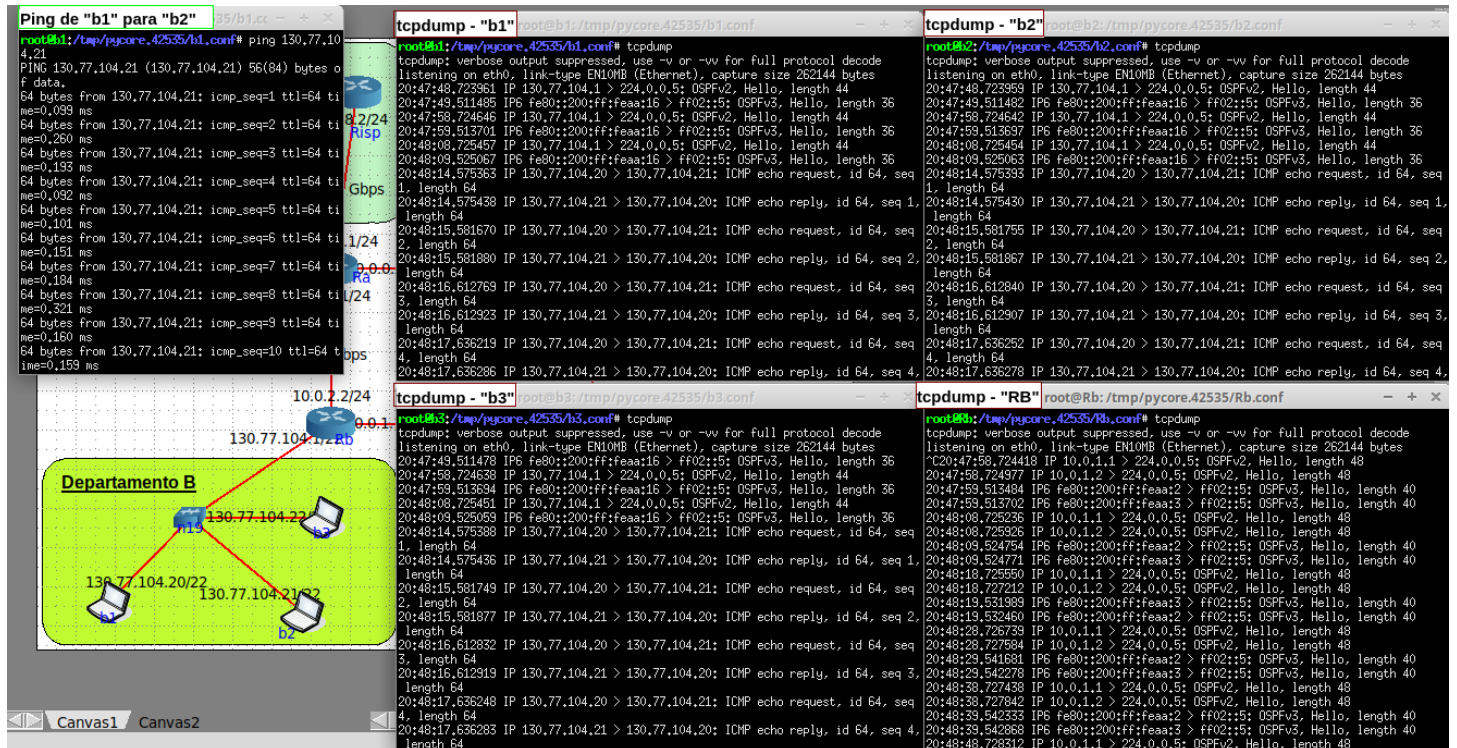


Figura 12: ‘Departamento B’: Análise do tráfego gerado intra-departamento.

Já na figura 12 analisámos o tráfego gerado no ‘Departamento B’, ligado por um ‘Hub’ (repetidor). Para isso é realizado o comando ‘ping’ do Pc ‘b1’ para o Pc ‘b2’. Concluimos então, pela análise do tráfego apresentado, que toda a informação gerada e enviada nessa rede é, primeiramente, recebida pelo hub e, posteriormente, enviada para todas as máquinas conectadas a ele dentro da rede. No entanto, sempre que há a necessidade de enviar um novo sinal é necessário aguardar que o sinal anterior seja completamente distribuído, abrindo uma janela à ocorrência de uma maior probabilidade de possíveis colisões. Para além disso, esta espera entre sinais pode tornar as redes interligadas por hubs bastante lentas. Já no caso de redes interligadas por switches, embora com funções bastantes equivalentes, mas este possui a qualidade de poder criar uma espécie de série de canais exclusivos em que os dados enviados pela máquina origem são somente recebidos pela máquina destino. Desta forma, a rede pode ficar menos congestionada, com um melhor desempenho, sendo possível estabelecer um conjunto de conexões paralelas com menor risco de colisões ou outros problemas.

2. Conclusões

Neste trabalho foram abordados temas que envolvem a camada de ligação lógica, sendo que esta abordagem é focada nos protocolos Ethernet e ARP (Address Resolution Protocol).

Ao longo da primeira parte, constatamos que o protocolo ARP é muito importante para o bom funcionamento de uma rede, pois permite mapear endereços do nível da rede com endereços

físicos, de forma a existir fluxo de dados entre os diferentes nós da rede. Só com este protocolo é possível conhecer o MAC address de destino, essencial no envio de uma trama Ethernet da camada de ligação lógica de nível 2. Este endereço MAC é obtido através do uso das primitivas ARP request e ARP reply.

Na segunda parte do trabalho, introduziu-se o protocolo ARP gratuito e abordámos diferentes formas de interligação de redes locais, com recurso a hubs e switches para o estudo de domínios de colisão. Relativamente ao ARP gratuito, percebemos que é usado, sobretudo, para determinar se um host da rede possui o mesmo endereço IP que o originador do pedido, que apesar de muitas vezes desnecessário, é importante para o correto funcionamento da rede. Foi importante abordar os diferentes tipos de ligação na rede, pois percebemos que a forma mais correta de prevenir colisões, passa pela utilização de switches.

Em suma, este trabalho permitiu solidificar a matéria aprendida nas aulas teóricas proporcionando um aumento no conhecimento relativamente ao protocolo ARP, endereçamento MAC em redes Ethernet e de domínios de colisão dentro de uma rede.