

TP2 - Camada de Ligação Lógica: Ethernet e Protocolo ARP

Universidade do Minho

Departamento de Informática, 4710-057 Braga, Portugal

Redes de Computadores

Autores:

Paulo Guedes, a74411@alunos.uminho.pt

Diogo Gomes, a73825@alunos.uminho.pt

Carlos Campos, a74745@alunos.uminho.pt

Parte I

1. Qual é o endereço MAC da interface ativa do seu computador?

The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows an HTTP GET request (No. 948) from source 172.26.20.53 to destination 193.136.19.148. The packet details pane on the right shows the Ethernet II header with the destination MAC address 00:d0:03:ff:94:00. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|----------------|
| 123 | 3.095742539 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 130 | 3.160105342 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 894 | 6.513291368 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 909 | 6.606738896 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 948 | 6.731937459 | 172.26.20.53 | 193.136.19.148 | HTTP | 446 | GET / HTTP/1.1 |

Packet Details for No. 948:

- Frame 948: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
- Ethernet II, Src: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Source: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.26.20.53, Dst: 193.136.19.148
- Transmission Control Protocol, Src Port: 56972 (56972), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 380
- Hypertext Transfer Protocol

Packet Bytes:

```

0000  00 d0 03 ff 94 00 d0 df 9a 62 3e 4e 08 00 45 00  ...b>N..E.
0010  01 b0 2d 59 40 00 40 06 76 83 ac 1a 14 35 c1 88  ...Y0..V....5..
0020  13 94 de 8c 00 50 34 f5 db 06 82 1e 9e cc 80 18  ...P4.....
0030  00 e5 94 2e 00 00 01 01 08 0a 00 00 f6 55 53 83  .....US.
0040  0c 81 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 63 65 73 69 75 6d 2e 64  ..Host: cesium.d
0060  69 2e 75 6d 69 6e 68 6f 2e 70 74 0d 0a 55 73 65  i.uminho .pt..Use
  
```

O endereço MAC da interface ativa é 00:d0:03:ff:94:00.

2. Qual é o endereço MAC destino da trama? A que sistema é destinada essa trama, será o endereço Ethernet do servidor http para cesium.di.uminho.pt? Justifique.

The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows an HTTP GET request (No. 948) from source 172.26.20.53 to destination 193.136.19.148. The packet details pane on the right shows the Ethernet II header with the destination MAC address 00:d0:03:ff:94:00. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|----------------|
| 123 | 3.095742539 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 130 | 3.160105342 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 894 | 6.513291368 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 909 | 6.606738896 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 948 | 6.731937459 | 172.26.20.53 | 193.136.19.148 | HTTP | 446 | GET / HTTP/1.1 |

Packet Details for No. 948:

- Frame 948: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
- Ethernet II, Src: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Source: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.26.20.53, Dst: 193.136.19.148
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 432
- Identification: 0x2d59 (11609)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 64

Packet Bytes:

```

0000  00 d0 03 ff 94 00 d0 df 9a 62 3e 4e 08 00 45 00  ...b>N..E.
0010  01 b0 2d 59 40 00 40 06 76 83 ac 1a 14 35 c1 88  ...Y0..V....5..
0020  13 94 de 8c 00 50 34 f5 db 06 82 1e 9e cc 80 18  ...P4.....
0030  00 e5 94 2e 00 00 01 01 08 0a 00 00 f6 55 53 83  .....US.
0040  0c 81 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 63 65 73 69 75 6d 2e 64  ..Host: cesium.d
0060  69 2e 75 6d 69 6e 68 6f 2e 70 74 0d 0a 55 73 65  i.uminho .pt..Use
  
```

O endereço MAC destino da trama é d0:df:9a:62:3e:4e, e a trama não é destinada ao servidor http para cesium.di.uminho.pt visto que os IP da origem e do destino são diferentes, quer dizer que a origem e o destino não pertencem a mesma rede, o que quer dizer que o destino da trama é um intermediário, provavelmente será um switch.

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

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list at the top shows packet 961 selected. The packet details pane shows the Ethernet II frame structure. The Type field is highlighted as 0x0800.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|-----------------|
| 123 | 3.095742539 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 130 | 3.100105342 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 894 | 6.513291368 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 909 | 6.606738896 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 948 | 6.731937459 | 172.26.20.53 | 193.136.19.148 | HTTP | 446 | GET / HTTP/1.1 |
| 950 | 6.764340723 | 193.136.19.148 | 172.26.20.53 | HTTP | 961 | HTTP/1.1 200 OK |

Frame 950: 961 bytes on wire (7688 bits), 961 bytes captured (7688 bits) on interface 0
 Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e)
 Destination: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e)
 Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 193.136.19.148, Dst: 172.26.20.53
 Transmission Control Protocol, Src Port: 80 (80), Dst Port: 56972 (56972), Seq: 1, Ack: 381, Len: 895

0000 d0 df 9a 62 3e 4e 00 00 03 ff 94 00 08 00 45 00 ...b>N.....E.
 0010 03 b3 92 49 40 00 3d 06 12 90 c1 88 13 94 ac 1a ...I@.=.....
 0020 14 35 00 50 de 8c 82 1e 9e cc 34 f5 dc 82 80 18 ...5.P.....4.....
 0030 00 eb 63 ce 00 00 01 01 08 0a 53 83 0c 89 00 00 ...C.....S.....
 0040 f6 55 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f ..UHTTP/1 .t 200 0
 0050 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a K..Conte nt-Type:
 0060 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 text/ht ml; char

O valor do campo Type da trama Ethernet é 0x0800. Este valor é referente ao protocolo IPv4.

4. Quantos bytes usados desde o início da trama até ao carácter ASCII “G” do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list at the top shows packet 948 selected. The packet details pane shows the Ethernet II frame structure. The Type field is highlighted as 0x0800.

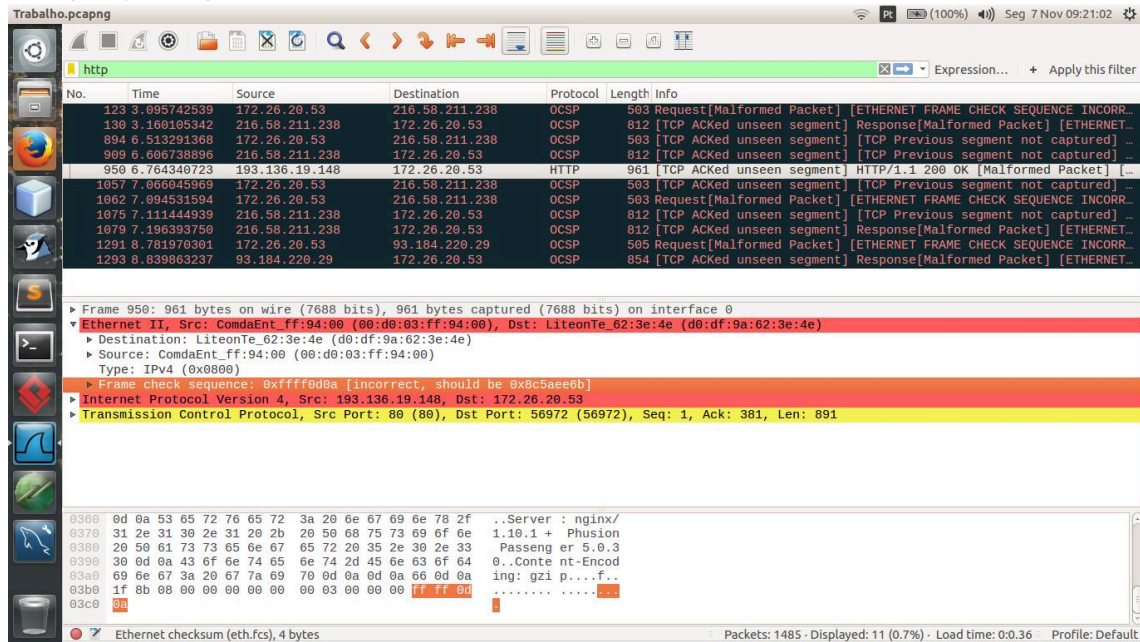
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|-----------------------------|
| 123 | 3.095742539 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 130 | 3.100105342 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 894 | 6.513291368 | 172.26.20.53 | 216.58.211.238 | OCSP | 503 | Request |
| 909 | 6.606738896 | 216.58.211.238 | 172.26.20.53 | OCSP | 812 | Response |
| 948 | 6.731937459 | 172.26.20.53 | 193.136.19.148 | HTTP | 446 | GET / HTTP/1.1 |
| 950 | 6.777164482 | 193.136.19.148 | 172.26.20.53 | HTTP | 86 | HTTP/1.1 200 OK (text/html) |

Frame 948: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
 Ethernet II, Src: LiteonTe_62:3e:4e (d0:df:9a:62:3e:4e), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 Internet Protocol Version 4, Src: 172.26.20.53, Dst: 193.136.19.148
 Transmission Control Protocol, Src Port: 56972 (56972), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 380
 Hypertext Transfer Protocol

0000 00 d0 03 ff 94 00 d0 df 9a 62 3e 4e 08 00 45 00b>N.....E.
 0010 01 b0 2d 5f 40 00 40 06 76 83 ac 1a 14 35 c1 88 ...-Y@.0. v.....
 0020 13 94 de 8c 00 50 34 f5 db 06 82 1e 9e cc 80 18P4.....
 0030 00 e5 94 2e 00 00 01 01 08 0a 00 00 f6 55 53 83US..
 0040 3c 81 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
 0050 0d 0a 48 6f 73 74 3a 20 63 65 73 69 75 6d 2e 64 ..Host: cesium.d
 0060 69 2e 75 6d 69 6e 68 6f 2e 70 74 6d 0a 55 73 65 i.uminho .pt..Use

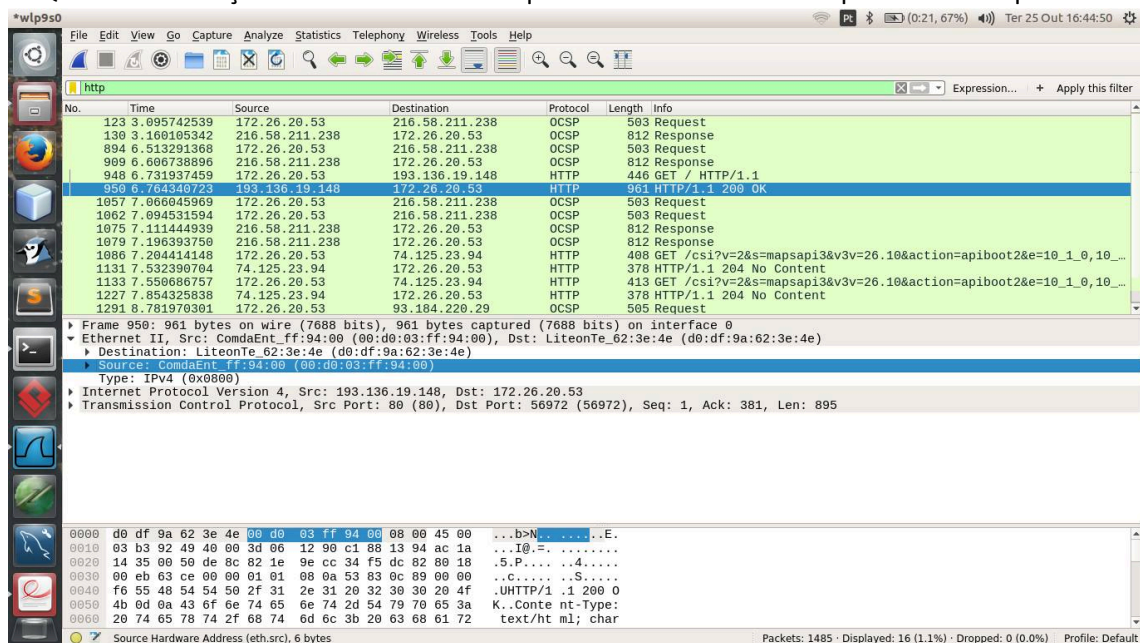
São usados desde o início da trama até ao carácter ASCII “G” do método HTTP GET são 132 bytes. O total de bytes usados é 892 e o overhead é $(132/892) \times 100 = 14\%$.

5. Em ligações com fios pouco susceptíveis a erros, nem sempre as NICs geram o código de detecção de erros. Verifique se o campo FCS está a ser utilizado. Aceda á opção Edit/Preferences/Protocols/Ethernet e indique que é assumido o uso do campo FCS. Verifique qual o valor hexadecimal desse campo na trama capturada. Que conclui? Reponha a configuração original.



Não existe valor hexadecimal desse campo na trama a analisar porque esta não foi capturada, logo no campo FCS não está a ser utilizado.

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



O endereço Ethernet da fonte é 00:d0:03:ff:94:00. O sistema de rede é o servidor do cesium, porque a trama do get tem como destino o servidor do cesium, no qual a resposta tem origem o próprio servidor.

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

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list shows frame 950 as the selected packet. The packet details pane shows the following information:

- Destination: LiteonTe 62:3e:4e (d0:df:9a:62:3e:4e)
- Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 193.136.19.148, Dst: 172.26.20.53
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 56972 (56972), Seq: 1, Ack: 381, Len: 895

The packet bytes pane shows the raw data of the packet, with the destination MAC address highlighted in blue: 00 00 00 00 00 00 03 ff 94 00 08 00 45 00.

O endereço MAC do destino é d0:df:9a:62:3e:4e. O sistema de destino é da máquina utilizada.

8. Qual é o valor hexadecimal do campo tipo (Type)?

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list shows frame 948 as the selected packet. The packet details pane shows the following information:

- Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
- Source: LiteonTe 62:3e:4e (d0:df:9a:62:3e:4e)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.26.20.53, Dst: 193.136.19.148
- Transmission Control Protocol, Src Port: 56972 (56972), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 380
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the packet, with the type field highlighted in blue: 00 00 00 00 00 00 03 ff 94 00 08 00 45 00.

O valor hexadecimal do campo tipo é 0x0800.

9. Que tipo de resposta foi enviada pelo servidor?

A resposta enviada pelo servidor foi 200 OK que é a resposta padrão para solicitações de HTTP de sucesso, em uma resposta de um GET.

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

```
oeremita@TheStaff: /usr/sbin$ arp
Endereço TipoHW EndereçoHW Opções Máscara Interface
192.168.2.1 ether c8:2a:14:58:01:60 C enp10s0
172.26.254.254 ether 08:d0:03:ff:94:00 C wlp9s0
oeremita@TheStaff: /usr/sbin$
```

A coluna da esquerda corresponde ao endereço IP, coluna da direita corresponde ao endereço MAC.

11. 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?

Trabalho2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|---|
| 31 | 3.395151307 | QuantaCo_7f:07:33 | Broadcast | ARP | 42 | Who has 192.168.2.1? Tell 192.168.2.221 |
| 32 | 3.395880763 | Apple_58:01:60 | QuantaCo_7f:07:33 | ARP | 60 | 192.168.2.1 is at c8:2a:14:58:01:60 |
| 209 | 7.103436177 | CompaIn_70:8a:f3 | Broadcast | ARP | 60 | Who has 192.168.2.1? Tell 192.168.2.246 |

Frame 31: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Sender IP address: 192.168.2.221

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.2.1

0000 ff ff ff ff ff ff e8 9a 8f 7f 07 33 08 06 00 013..

0010 08 00 06 04 00 01 e8 9a 8f 7f 07 33 c0 a8 02 dd3...

0020 00 00 00 00 00 00 c0 a8 02 01

Hardware type (arp.hw.type), 2 bytes

Packets: 358 · Displayed: 3 (0.8%) · Dropped: 0 (0.0%) · Load time: 0:0.9 · Profile: Default

O valor hexadecimal do endereço origem é e8:9a:8f:7f:07:33. O valor hexadecimal do endereço destino é ff:ff:ff:ff:ff:ff. O endereço destino corresponde a enviar a mensagem ARP a todas as máquinas.

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

Trabalho2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|---|
| 31 | 3.395151307 | QuantaCo_7f:07:33 | Broadcast | ARP | 42 | Who has 192.168.2.1? Tell 192.168.2.221 |
| 32 | 3.395880763 | Apple_58:01:60 | QuantaCo_7f:07:33 | ARP | 60 | 192.168.2.1 is at c8:2a:14:58:01:60 |
| 209 | 7.103436177 | CompalIn_70:8a:f3 | Broadcast | ARP | 60 | Who has 192.168.2.1? Tell 192.168.2.246 |

Frame 31: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Sender IP address: 192.168.2.221

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.2.1

0000 ff ff ff ff ff ff e8 9a 8f 7f 07 33 08 06 00 013..

0010 08 00 06 04 00 01 e8 9a 8f 7f 07 33 c0 a8 02 dd3...

0020 00 00 00 00 00 00 c0 a8 02 01

Type (eth.type), 2 bytes

Packets: 358 · Displayed: 3 (0.8%) · Dropped: 0 (0.0%) · Load time: 0:0.9 · Profile: Default

O valor hexadecimal é 0x0806 que corresponde a um type ARP.

13. 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>.

Trabalho2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|---|
| 31 | 3.395151307 | QuantaCo_7f:07:33 | Broadcast | ARP | 42 | Who has 192.168.2.1? Tell 192.168.2.221 |
| 32 | 3.395880763 | Apple_58:01:60 | QuantaCo_7f:07:33 | ARP | 60 | 192.168.2.1 is at c8:2a:14:58:01:60 |
| 209 | 7.103436177 | CompalIn_70:8a:f3 | Broadcast | ARP | 60 | Who has 192.168.2.1? Tell 192.168.2.246 |

Frame 31: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Sender IP address: 192.168.2.221

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.2.1

0000 ff ff ff ff ff ff e8 9a 8f 7f 07 33 08 06 00 013..

0010 08 00 06 04 00 01 e8 9a 8f 7f 07 33 c0 a8 02 dd3...

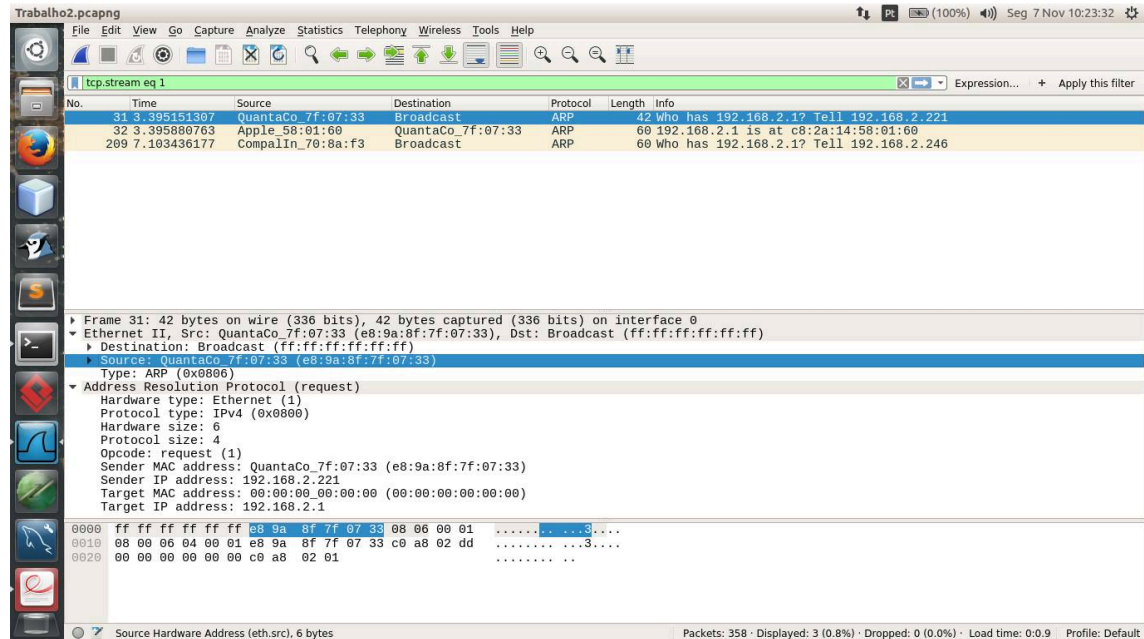
0020 00 00 00 00 00 00 c0 a8 02 01

Opcode (arp.opcode), 2 bytes

Packets: 358 · Displayed: 3 (0.8%) · Dropped: 0 (0.0%) · Load time: 0:0.9 · Profile: Default

O valor do campo ARP opcode é 1 que corresponde a um request.

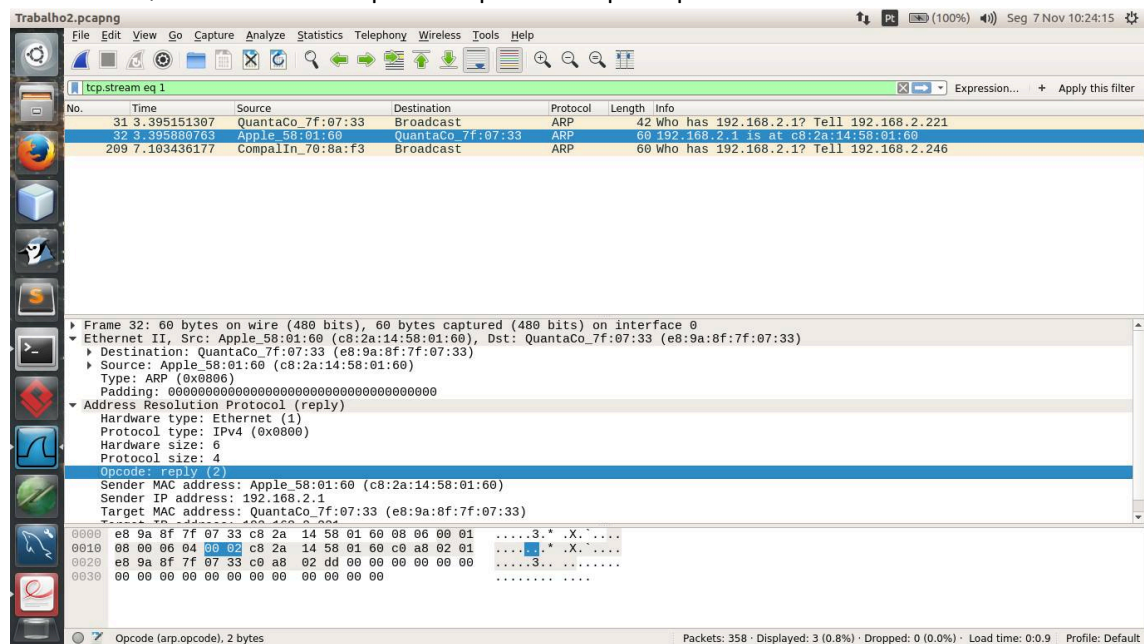
14. A mensagem ARP contém o endereço IP de origem? Que tipo de pergunta é feita?



Sim. Pergunta quem tem o endereço MAC.

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

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



O valor do campo ARP opcode é 0x0002, que corresponde a um reply.

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

Trabalho2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|---|
| 31 | 3.395151307 | QuantaCo_7f:07:33 | Broadcast | ARP | 42 | who has 192.168.2.1? Tell 192.168.2.221 |
| 32 | 3.395880763 | Apple_58:01:60 | QuantaCo_7f:07:33 | ARP | 60 | 192.168.2.1 is at c8:2a:14:58:01:60 |
| 209 | 7.103436177 | CompalIn_70:8a:f3 | Broadcast | ARP | 60 | who has 192.168.2.1? Tell 192.168.2.246 |

Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Apple_58:01:60 (c8:2a:14:58:01:60), Dst: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Apple_58:01:60 (c8:2a:14:58:01:60)

Sender IP address: 192.168.2.1

Target MAC address: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Target IP address: 192.168.2.221

0000 e8 9a 8f 7f 07 33 c8 2a 14 58 01 60 08 06 00 013.*.X.....

0010 08 00 06 04 00 02 c8 2a 14 58 01 60 c9 a8 02 01*.X.....

0020 e8 9a 8f 7f 07 33 c0 a8 02 dd 00 00 00 00 00 003.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 003.....

Sender MAC address (arp.src.hw_mac), 6 bytes

Packets: 358 · Displayed: 3 (0.8%) · Dropped: 0 (0.0%) · Load time: 0:0.9 Profile: Default

A mensagem ARP está a partir do selecionado a azul (c8 2ª 14 58 01 60) até ao selecionado a cinzento (c0 a8 02 dd).

16. Quais são os valores hexadecimais para os endereços origem e destino da trama que contém a resposta ARP? Que conclui?

Trabalho2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|-------------------|----------|--------|---|
| 31 | 3.395151307 | QuantaCo_7f:07:33 | Broadcast | ARP | 42 | who has 192.168.2.1? Tell 192.168.2.221 |
| 32 | 3.395880763 | Apple_58:01:60 | QuantaCo_7f:07:33 | ARP | 60 | 192.168.2.1 is at c8:2a:14:58:01:60 |
| 209 | 7.103436177 | CompalIn_70:8a:f3 | Broadcast | ARP | 60 | who has 192.168.2.1? Tell 192.168.2.246 |

Frame 32: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Apple_58:01:60 (c8:2a:14:58:01:60), Dst: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Apple_58:01:60 (c8:2a:14:58:01:60)

Sender IP address: 192.168.2.1

Target MAC address: QuantaCo_7f:07:33 (e8:9a:8f:7f:07:33)

Target IP address: 192.168.2.221

0000 e8 9a 8f 7f 07 33 c8 2a 14 58 01 60 08 06 00 013.*.X.....

0010 08 00 06 04 00 02 c8 2a 14 58 01 60 c9 a8 02 01*.X.....

0020 e8 9a 8f 7f 07 33 c0 a8 02 dd 00 00 00 00 00 003.....

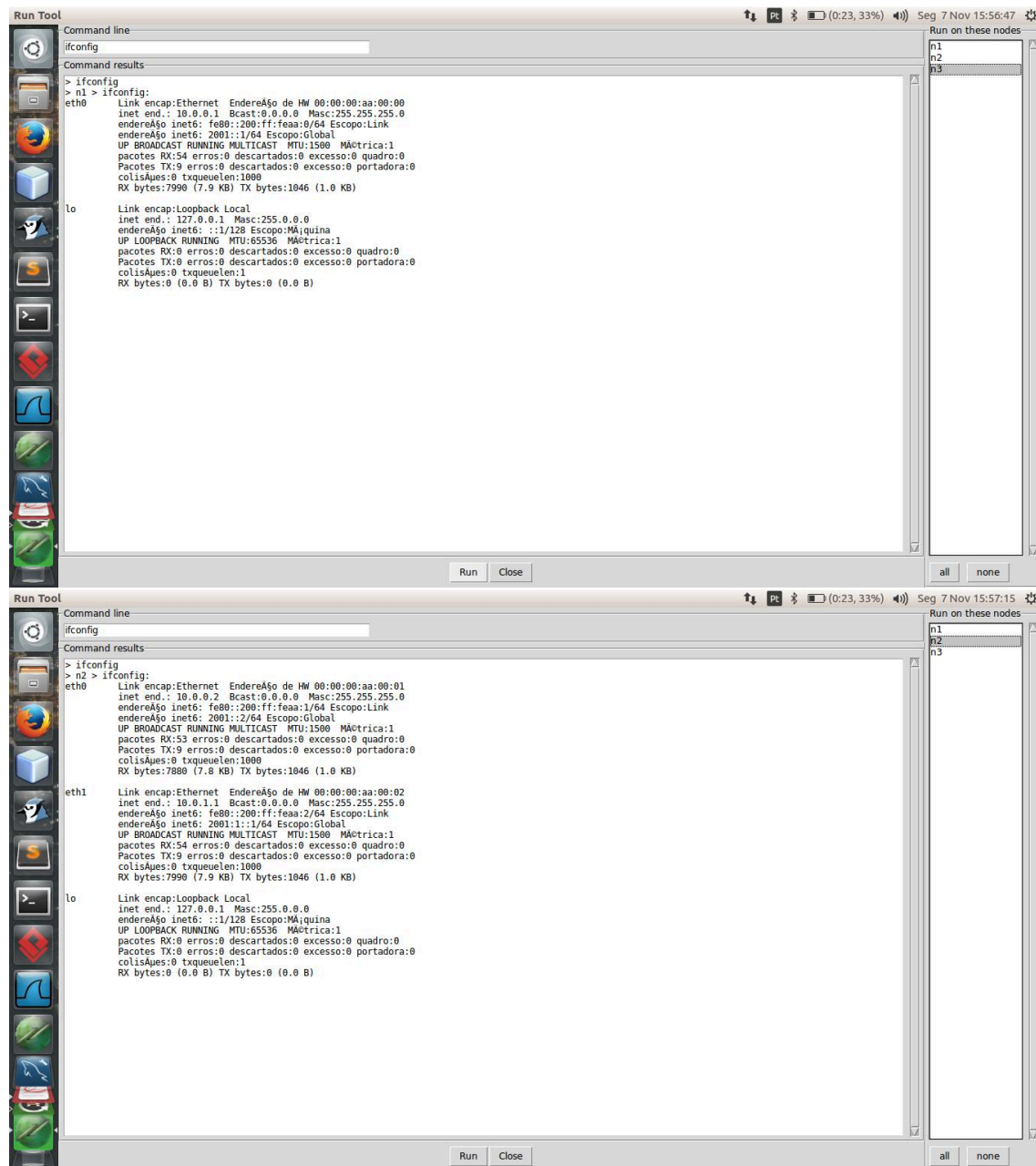
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 003.....

Sender MAC address (arp.src.hw_mac), 6 bytes

Packets: 358 · Displayed: 3 (0.8%) · Dropped: 0 (0.0%) · Load time: 0:0.9 Profile: Default

Os valores hexadecimais para os endereços origem da trama que contém a resposta ARP são c8:2ª:14:58:01:60, e os valores do destino são e8:9a:8f:7f:07:33.

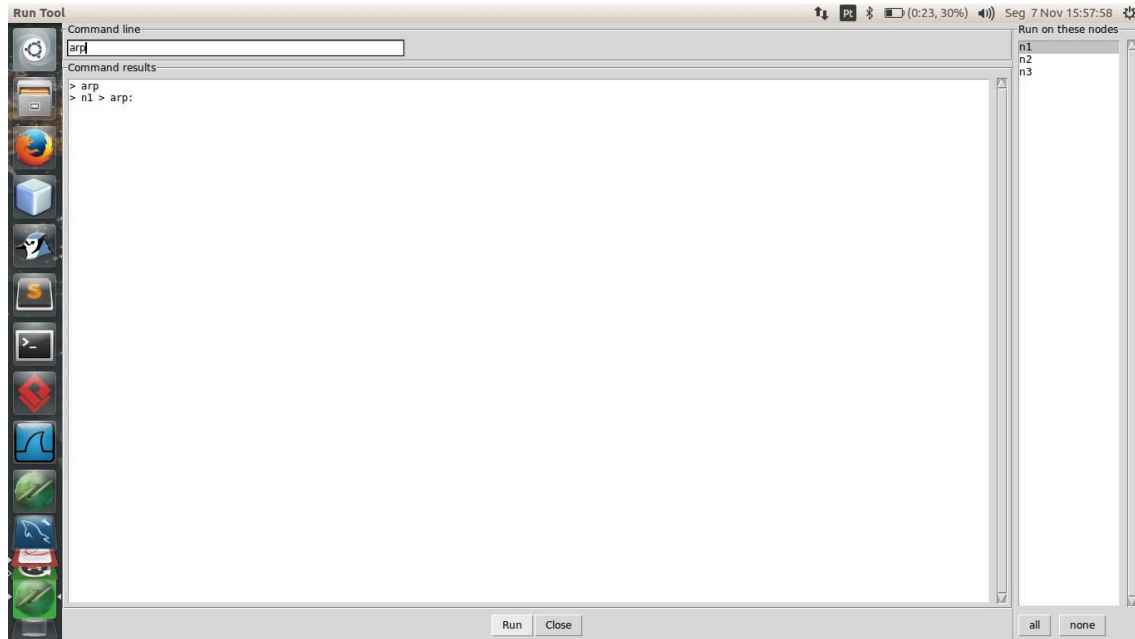
17. Com auxílio do comando `ifconfig` obtenha os endereços Ethernet das interfaces dos diversos routers.

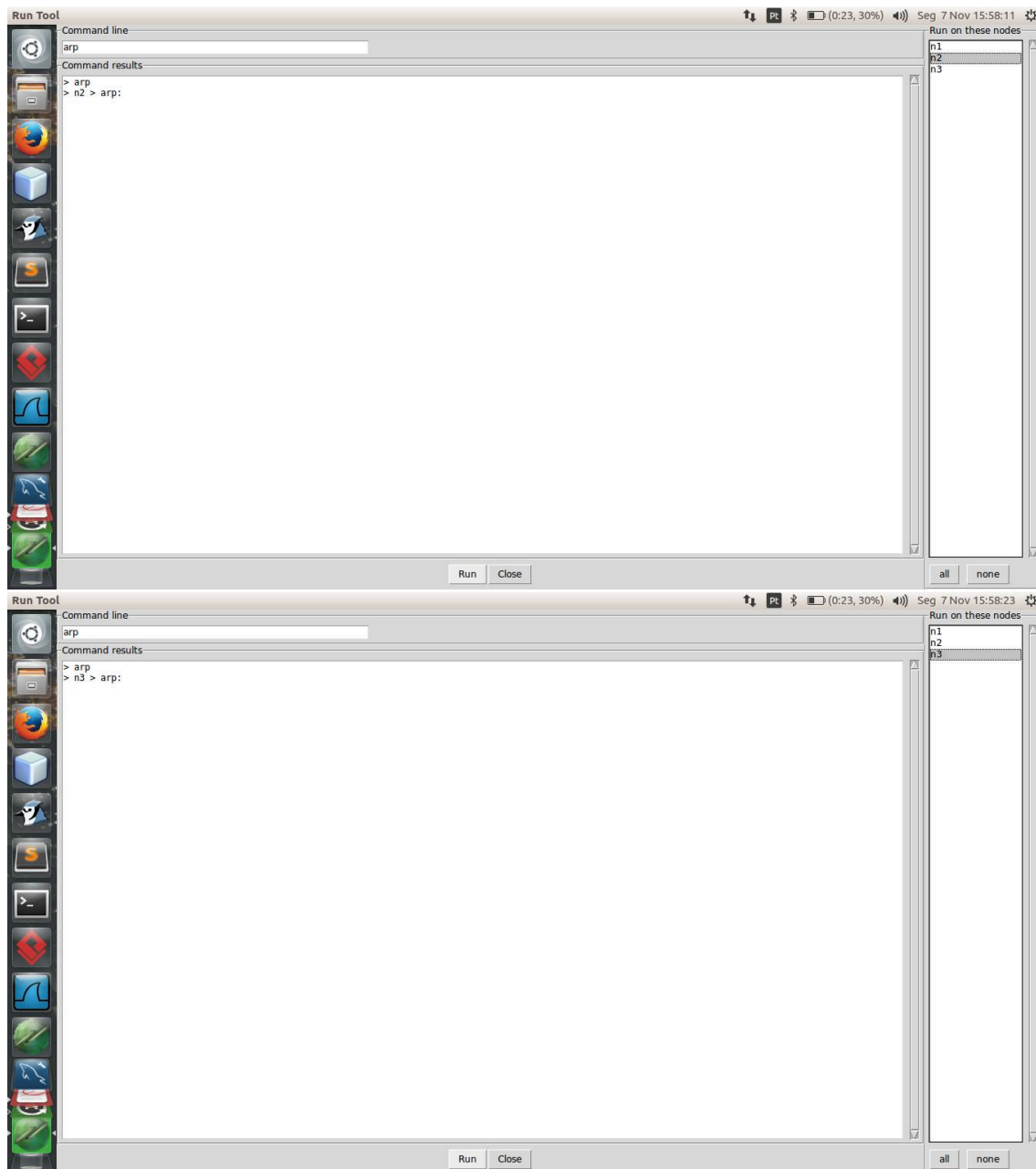




O endereço dos routers são: 00:00:00:aa:00:01 e 00:00:00:aa:00:02 e 00:00:00:aa:00:03.

18. Usando o comando arp obtenha as caches arp dos diversos sistemas.





As caches arp dos diversos sistemas estão vazias.

19. Faça ping de n1 para n2. Que modificações observa nas caches ARP desses sistemas? Faça ping de n1 para n3. Consulte as caches ARP. Que conclui?

The image shows two screenshots of the CORE network simulator interface, illustrating the state of ARP caches after network operations.

Top Screenshot (CORE 42660 on TheStaff):

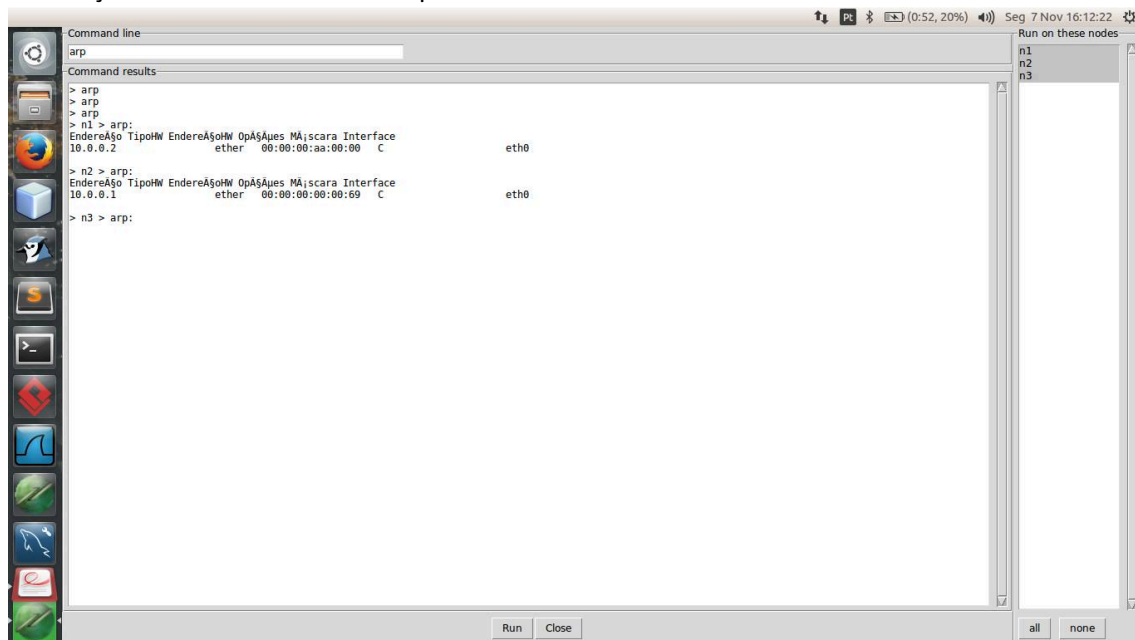
- The network diagram shows three nodes: n1 (10.0.0.1/24), n2 (10.0.0.2/24), and n3 (10.0.1.1/24). n1 and n2 are connected, and n2 and n3 are connected.
- The "Run Tool" window shows the command line with "arp" entered.
- The "Command results" window shows the output of the "arp" command for n1 and n3.
- The "Run on these nodes" list includes n1, n2, and n3.

Bottom Screenshot (CORE 39291 on TheStaff):

- The network diagram shows the same three nodes.
- The "Run Tool" window shows the command line with "arp" entered.
- The "Command results" window shows the output of the "arp" command for n1 and n2.
- The "Run on these nodes" list includes n1, n2, and n3.

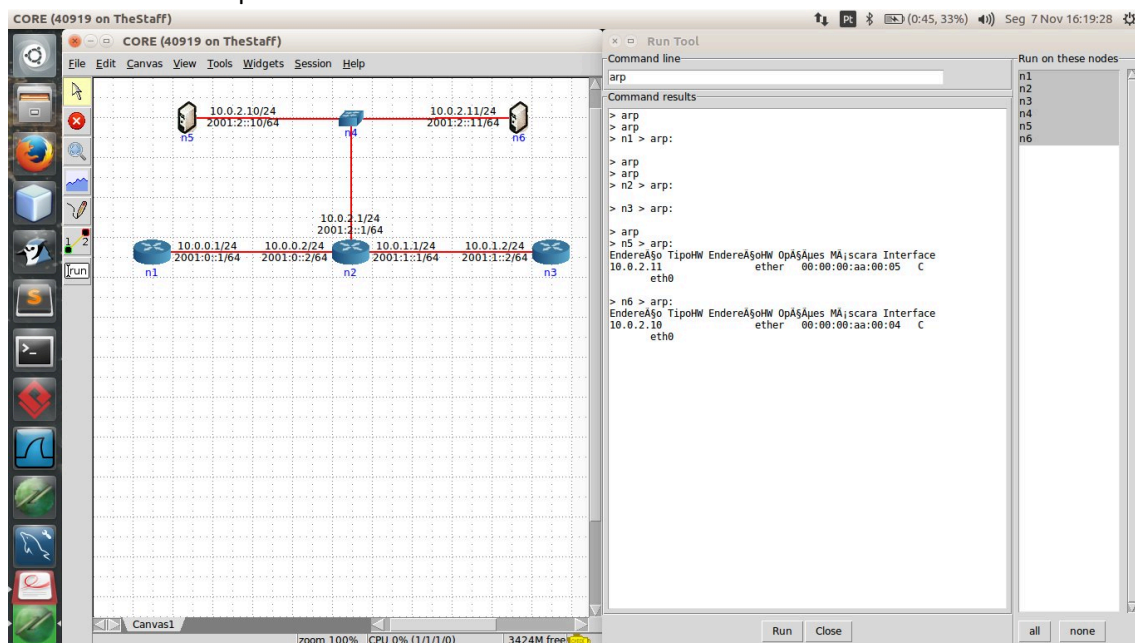
Após fazer ping de n1 para n2, a cache de n1 fica com o endereço de n2, e vice-versa. N1 não conseguiu se conectar com n3, logo a cache de n1 não modifica, e a cache de n3 fica vazia.

20. Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com endereço Ethernet inexistente. O que aconteceu?



Ap s modificarmos o endere o de n1, n2 guardou o novo endere o na cache ap s ter efetuado ping.

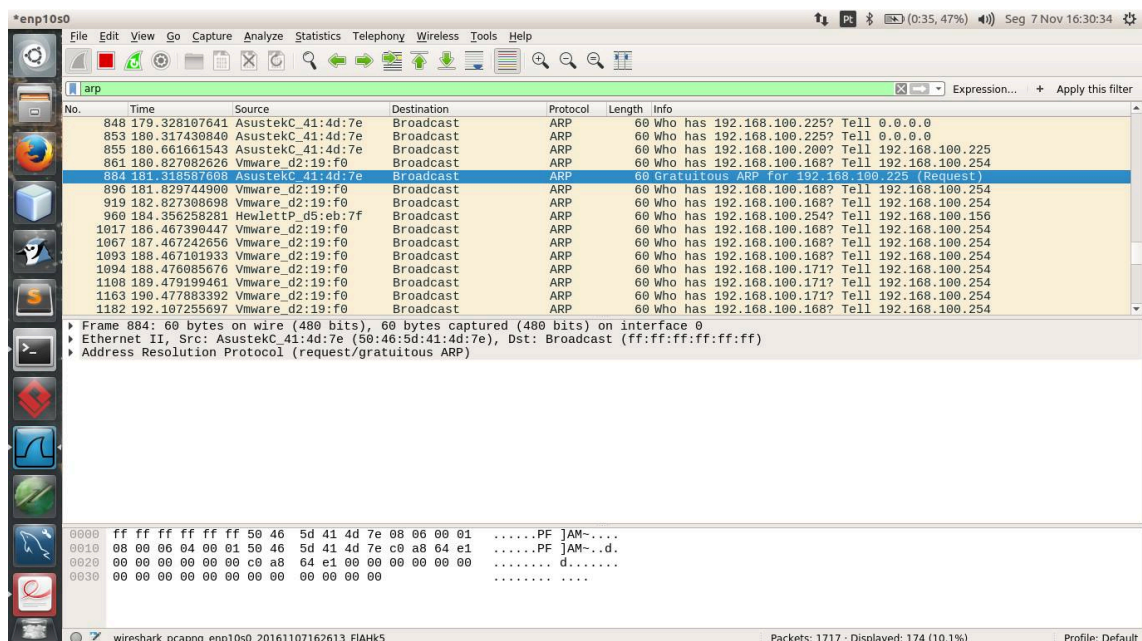
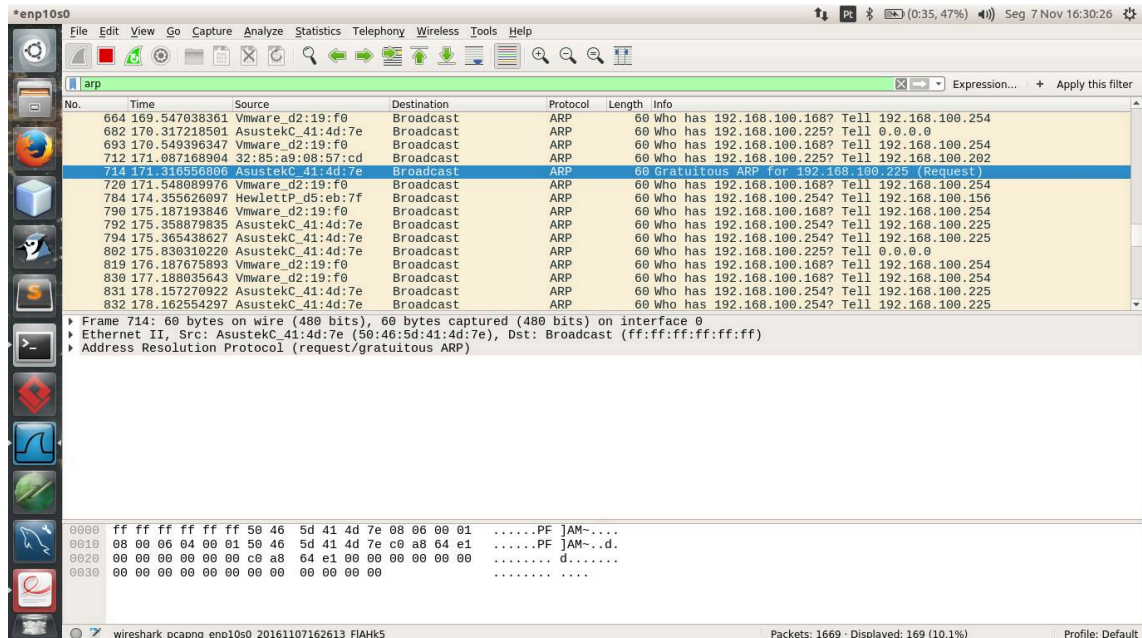
21. Fa a ping de n5 para n6. Sem consultar a tabela ARP anote a entrada que, em sua opini o,   criada na tabela ARP de n5. Verifique, justificando, se a sua interpreta  o sobre a opera  o da rede Ethernet e protocolo ARP estava correto.



Na nossa opini o, n5 vai guardar o endere o de n6 e n6 vai guardar o endere o de n5. Verificamos que a nossa opini o estava correta, visto que na cache dos sistemas, foram acrescentados os endere os do outro sistema.

Parte II

1. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Verifique quantos pacotes ARP gratuito foram enviados e com que intervalo temporal?



Como podemos verificar obtivemos este 2 pacotes ARP gratuitos, num espaço de tempo de 10 segundos, em 4 minutos.

2. 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?

Trabalho3.pcapng

Filter: arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|-------------------|-------------|----------|--------|---|
| 794 | 175.365438627 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.254? Tell 192.168.100.225 |
| 802 | 175.830310220 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 819 | 176.187675893 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 830 | 177.188035643 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 831 | 178.157270922 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.254? Tell 192.168.100.225 |
| 832 | 178.162554297 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.254? Tell 192.168.100.225 |
| 833 | 178.317132593 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 848 | 179.328107641 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 853 | 180.317430840 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 855 | 180.661661543 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.200? Tell 192.168.100.225 |
| 861 | 180.827082626 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 884 | 181.318587608 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Gratuitous ARP for 192.168.100.225 (Request) |
| 896 | 181.829744908 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |

Frame 884: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: AsustekC_41:4d:7e (50:46:5d:41:4d:7e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request/gratuitous ARP)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 [Is gratuitous: True]
 Sender MAC address: AsustekC_41:4d:7e (50:46:5d:41:4d:7e)
 Sender IP address: 192.168.100.225
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.100.225

0000 ff ff ff ff ff ff ff 5d 41 4d 7e 08 00 00 01PF |AM-...
 0010 08 00 06 04 00 01 50 46 5d 41 4d 7e c0 a8 64 e1PF |AM-...d.
 0020 00 00 00 00 00 00 c0 a8 64 e1 00 00 00 00d.....
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040 00 00 00 00 00 00 00 00 00 00 00 00 00

Packets: 4427 - Displayed: 550 (12.4%) - Load time: 0:0.57 - Profile: Default

Trabalho3.pcapng

Filter: arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|-------------------|-------------|----------|--------|---|
| 802 | 175.830310220 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 819 | 176.187675893 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 830 | 177.188035643 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 831 | 178.157270922 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.254? Tell 192.168.100.225 |
| 832 | 178.162554297 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.254? Tell 192.168.100.225 |
| 833 | 178.317132593 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 848 | 179.328107641 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 853 | 180.317430840 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.225? Tell 0.0.0.0 |
| 855 | 180.661661543 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Who has 192.168.100.200? Tell 192.168.100.225 |
| 861 | 180.827082626 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |
| 884 | 181.318587608 | AsustekC_41:4d:7e | Broadcast | ARP | 60 | Gratuitous ARP for 192.168.100.225 (Request) |
| 919 | 182.827308698 | Vmware_d2:19:f0 | Broadcast | ARP | 60 | Who has 192.168.100.168? Tell 192.168.100.254 |

Frame 919: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), 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: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
 Sender IP address: 192.168.100.254
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.100.168

0000 ff ff ff ff ff ff 00 29 d2 19 f0 08 06 00 01).
 0010 08 00 06 04 00 01 00 c0 29 d2 19 f0 c0 a8 64 fe).
 0020 00 00 00 00 00 00 c0 a8 64 a8 00 00 00 00d.....
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040 00 00 00 00 00 00 00 00 00 00 00 00 00

Packets: 4427 - Displayed: 550 (12.4%) - Load time: 0:0.57 - Profile: Default

O ARP gratuito distingue-se dos restantes pedidos ARP, pois o ARP gratuito não espera resposta, visto que este emite o próprio IP da fonte e do destino são o IP da máquina.

Conclusões

Neste trabalho expandimos o nosso conhecimento nos diversos protocolos utilizados.

Verificamos que o IP muda consoante a rede de acesso, e que ao contrario o endereço MAC continua constante, independentemente de se mudar de rede ou não, por isso considera-se o endereço MAC um endereço físico.

Podemos também descobrir o endereço Mac através do ARP. Este protocolo ARP (Address Resolution Protocol) pode ser gratuito, ou não, sendo que se for gratuito, quererá dizer que o IP da fonte e o IP do destino são o mesmo da maquina, e o endereço MAC transmitido é ff:ff:ff:ff:ff:ff, normalmente nenhuma resposta será obtida.

Para além deste conhecimentos mais teóricos, também aprendemos a implementar, tais conhecimentos, na prática.