

# Laboratório Ethernet Wireshark

## Alunos: Eduardo Henrique

1. Qual é o endereço Ethernet de 48 bits do seu computador?

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
2	0.000460	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
3	0.000460	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
4	0.056916	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	98	IPv6
5	0.057080	InventusPowe_68:89:a5	FiberhomeTel_89:93:e8	0x86dd	74	IPv6
6	0.057193	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6

▶ Frame 1249: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF\_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, ic

▼ Ethernet II, Src: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8), Dst: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

▼ Destination: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

Address: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0. .... = IG bit: Individual address (unicast)

▼ Source: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8)

Address: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0. .... = IG bit: Individual address (unicast)

Type: IPv6 (0x86dd)

▶ Data (1280 bytes)

2. Qual é o endereço de destino de 48 bits no quadro Ethernet? Este é o endereço de gaia.cs.umass.edu? (Dica: a resposta é não). Qual dispositivo tem isso como endereço Ethernet? [Nota: esta é uma pergunta importante, e uma que os alunos às vezes erram.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
2	0.000460	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
3	0.000460	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6
4	0.056916	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	98	IPv6
5	0.057080	InventusPowe_68:89:a5	FiberhomeTel_89:93:e8	0x86dd	74	IPv6
6	0.057193	FiberhomeTel_89:93:e8	InventusPowe_68:89:a5	0x86dd	74	IPv6

▶ Frame 1249: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF\_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, ic

▼ Ethernet II, Src: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8), Dst: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

▼ Destination: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

Address: InventusPowe\_68:89:a5 (a4:63:a1:68:89:a5)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0. .... = IG bit: Individual address (unicast)

▼ Source: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8)

Address: FiberhomeTel\_89:93:e8 (f4:6f:ed:89:93:e8)

.... ..0. .... = LG bit: Globally unique address (factory default)

.... ..0. .... = IG bit: Individual address (unicast)

Type: IPv6 (0x86dd)

▶ Data (1280 bytes)

3. Dê o valor hexadecimal para o campo Frame type de dois bytes. A qual protocolo de camada superior isso corresponde?

```

Frame 1249: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
Ethernet II, Src: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8), Dst: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
  Destination: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
    Address: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv6 (0x86dd)
  Data (1280 bytes)

```

4. Quantos bytes desde o início do quadro Ethernet até o ASCII “G” em “GET” aparece no quadro Ethernet?

```

Frame 412: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
Ethernet II, Src: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5), Dst: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
  Destination: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
    Address: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.10.100, Dst: 128.119.245.12
  Transmission Control Protocol, Src Port: 63824, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
  Hypertext Transfer Protocol
    GET /wires-lab-HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wires-lab-HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wires-lab-HTTP-ethereal-lab-file3.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:113.0) Gecko/20100101 Firefox/113.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      Priority: u=0, i\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wires-lab-HTTP-ethereal-lab-file3.html]
      [HTTP request 1/2]
      [Response in frame 417]
      [First request in frame 412]
      [Community ID: 1:AS1AQKQF0YQDQK7WY571p0QI=]
  TRAFFIC RTE Data

```

5. Qual é o endereço de origem Ethernet? Este é o endereço do seu computador, ou de gaia.cs.umass.edu (Dica: a resposta é não). Qual dispositivo tem isso como endereço Ethernet?

```

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
Ethernet II, Src: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8), Dst: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
  Destination: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
    Address: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv6 (0x86dd)
  Data (60 bytes)
    Data: 600424670014063a280003f0400100160000000000000004280436908001c327611d0040db34b3a901bbf8fc3d3e1607f76f2358501003f21d190000
    [Length: 60]

```

6. Qual é o endereço de destino no quadro Ethernet? Este é o endereço Ethernet do seu computador?

```

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
Ethernet II, Src: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8), Dst: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
  Destination: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
    Address: InventusPowe_68:89:a5 (a4:63:a1:68:89:a5)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv6 (0x86dd)
  Data (60 bytes)
    Data: 600424670014063a280003f0400108160000000000002004280436908001c327611d0040db34b3a901bbf8fc3d3e1607f76f2358501003f21d190000
    [Length: 60]

```

7. Dê o valor hexadecimal para o campo `FrameType` de dois bytes. A qual protocolo de camada superior isso corresponde?

```

Frame 34: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
Ethernet II, Src: de:07:b6:27:3f:59 (de:07:b6:27:3f:59), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....1. .... = IG bit: Group address (multicast/broadcast)
  Source: de:07:b6:27:3f:59 (de:07:b6:27:3f:59)
    Address: de:07:b6:27:3f:59 (de:07:b6:27:3f:59)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Data (68 bytes)
    Data: 4500004e4c100004011ff29c0a80a6ec0a80affe115e1150030e82253706f745564703099aafd4a817ed8ae00010000a20000da0cfb2e1cae209da9c13e1ef8e31857d8
    [Length: 68]

```

8. Quantos bytes desde o início do quadro Ethernet até o ASCII "O" em "OK" (ou seja, o código de resposta HTTP) aparece no quadro Ethernet?

9. Aonde o conteúdo do cache ARP do seu computador. Qual é o significado de cada valor de coluna?

```

PS C:\Users\erarich> arp -a

Interface: 192.168.10.108 --- 0x14
Endereço IP      Endereço físico      Tipo
192.168.10.1      f4-6f-ed-89-93-e8    dinâmico
192.168.10.255    ff-ff-ff-ff-ff-ff    estático
224.0.0.22        01-00-5e-00-00-16    estático
224.0.0.252       01-00-5e-00-00-fc    estático
255.255.255.255   ff-ff-ff-ff-ff-ff    estático

Interface: 192.168.56.1 --- 0x15
Endereço IP      Endereço físico      Tipo
192.168.56.255   ff-ff-ff-ff-ff-ff    estático
224.0.0.22       01-00-5e-00-00-16    estático
224.0.0.251      01-00-5e-00-00-fb    estático
224.0.0.252      01-00-5e-00-00-fc    estático
239.255.255.250  01-00-5e-7f-ff-fa    estático
PS C:\Users\erarich>

```

10. Quais são os valores hexadecimais para os endereços de origem e destino no Quadro Ethernet contendo a mensagem de solicitação ARP?



```

> Frame 1432: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
▼ Ethernet II, Src: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....1. .... = IG bit: Group address (multicast/broadcast)
  Source: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  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: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
  Sender IP address: 192.168.10.1
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.10.111

```

11. Dê o valor hexadecimal para o campo do tipo de quadro Ethernet de dois bytes. O que isso corresponde ao protocolo da camada superior?

```

> Frame 1432: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{BC5C697E-CDE9-476A-AD19-E1B521C8933C}, id 0
▼ Ethernet II, Src: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....1. .... = IG bit: Group address (multicast/broadcast)
  Source: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
    Address: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  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: FiberhomeTel_89:93:e8 (f4:6f:ed:89:93:e8)
  Sender IP address: 192.168.10.1
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.10.111

```

12. Baixe a especificação ARP de <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. Uma discussão legível e detalhada sobre ARP também está em <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

a) Quantos bytes desde o início do quadro Ethernet o Início do campo opcode ARP?

**Resposta:** 6 bytes.

b) Qual é o valor do campo opcode dentro da parte ARP-payload do Quadro Ethernet no qual uma solicitação ARP é feita?

**Resposta:** 0x0001

c) A mensagem ARP contém o endereço IP do remetente?

**Resposta:** Sim. O campo Sender Protocol Address no cabeçalho ARP contém o endereço IP do remetente.

d) Onde na solicitação ARP a “pergunta” aparece – a Ethernet endereço da máquina cujo endereço IP correspondente está sendo consultado?

**Resposta:** No campo Target Hardware Address.

13. Agora encontre a resposta ARP que foi enviada em resposta à solicitação ARP.

a) Quantos bytes desde o início do quadro Ethernet o Início do campo opcode ARP?

**Resposta:** 20º byte.

b) Qual é o valor do campo opcode dentro da parte ARP-payload do Quadro Ethernet no qual uma resposta ARP é feita?

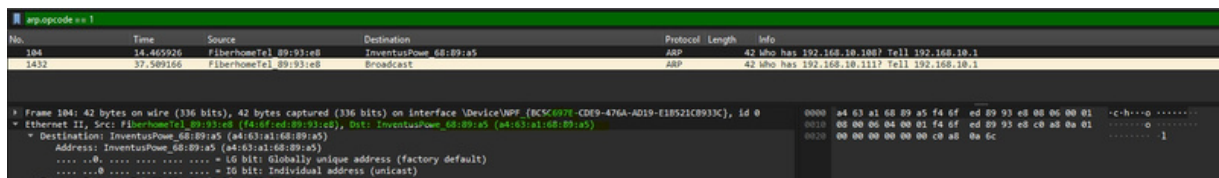
**Resposta:** 0x0002

c) Onde na mensagem ARP aparece a “resposta” à solicitação ARP anterior – o endereço IP da máquina que tem o endereço Ethernet cujo endereço IP correspondente está sendo consultado?

Sender Hardware Address: Contém o endereço Ethernet do dispositivo que respondeu.

Sender Protocol Address: Contém o endereço IP associado ao endereço Ethernet do remetente.

14. Quais são os valores hexadecimais para os endereços de origem e destino no quadro Ethernet que contém a mensagem de resposta ARP?



15. Abra o arquivo de rastreamento ethernet-ethereal-trace-1 em <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. O primeiro e o segundo pacotes ARP neste rastreamento correspondem a uma solicitação ARP enviada pelo computador que executa o Wireshark, e a resposta ARP enviada ao computador que executa o Wireshark pelo computador com o endereço Ethernet solicitado pelo ARP. Mas há ainda outro computador nesta rede, conforme indicado pelo pacote 6 – outra solicitação ARP. Por que não há resposta ARP (enviada em resposta à solicitação ARP no pacote 6) no rastreamento do pacote?

**Resposta:** O mais provável é que o endereço IP alvo no pacote 6 não corresponda a nenhum dispositivo ativo na rede.