华东师范大学数据科学与工程学院上机实践报告

课程名称：计算机网络原理与编程　　年级：2018　　上机实践成绩:

指导教师：张召　　姓名：孙秋实　　学号：10185501402

上机实践名称：Wireshark Lab: Ethernet and ARP　　上机实践日期：2020/06/08

上机实践编号：Exp9　　组号：　　上机实践时间：

Part 1
实验目的

- 了解以太网协议
- 了解 ARP 协议

Part 2
实验任务

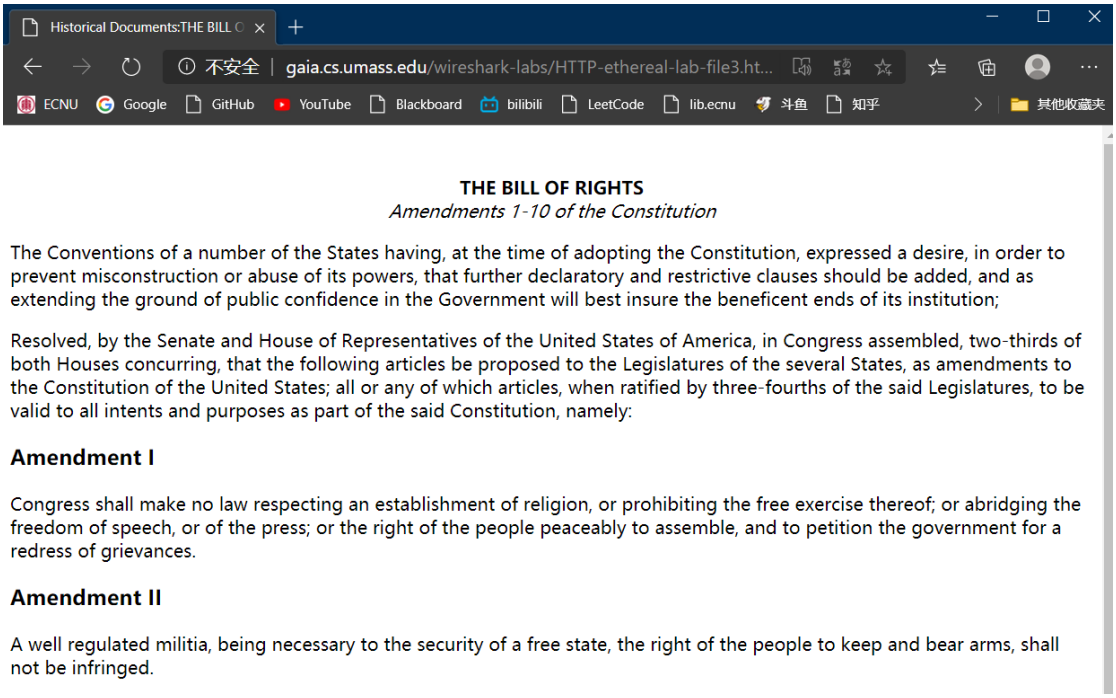
- 研究以太网协议协议
- 研究 ARP 协议

Part 3
使用环境

- Wireshark v7.0

Part 4
实验过程: 捕获和分析以太网帧

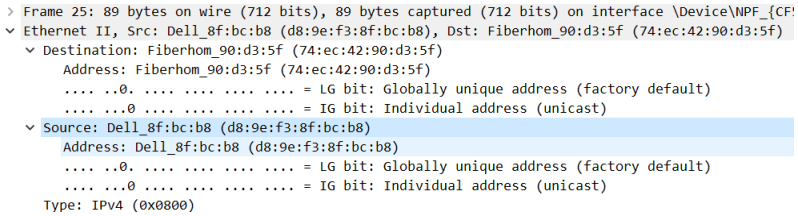
首先进行抓包，访问这个装有权利法案的实验用网页



根据包含 HTTP GET 消息的以太网帧进行分析，如果有可能建议您使用标记的方式展现您的答案。

Task 1

What is the 48-bit Ethernet address of your computer



如图所示，我的 48 位以太网地址位 d8:9e:f3:8f:bc:b8

Task 2

What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

目标地址：74:ec:42:90:d3:5f 是中继路由的地址，而不是网站 gaia.cs.umass.edu 的地址

Task 3

Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

```
> Source: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
  Type: IPv4 (0x0800)
> Data (60 bytes)
```

16 进制值：0x0800 代表上层协议是 IPV4

查询了一下常见以太网帧类型证实了这个结论

部分以太类型

部分常见的以太类型

以太类型编号	代表协议
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN[3]
0x22F0	Audio Video Transport Protocol as defined in IEEE Std 1722-2011
0x22F3	IETF TRILL Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)

Task 4

How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

```
0000  74 ec 42 90 d3 5f d8 9e  f3 8f bc b8 08 00 45 00   t·B··_·· ·····E·
0010  00 3c 79 73 40 00 40 06  00 00 c0 a8 01 02 cc 4f   ·<ys@·@· ·······O
0020  c5 db ff be 01 bb 2c ca  84 8e 00 00 00 00 a0 02   ·····,· ········
0030  fa f0 54 04 00 00 02 04  05 b4 01 03 03 08 04 02   ··T····· ········
0040  08 0a 47 88 d4 a7 00 00  00 00                     ··G····· ··
```

如上图所示，在我自己的抓包结果中直到 ASCII“G”出现在以太网帧中为止，

有 $16+16+16+16+3=67$ 字节

接下来，根据包含 HTTP 响应消息的第一个字节的以太网帧的内容，回答以下问题。

Task 5

What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

38	1.050606	Dell_8f:bc:b8	Fiberhom_90:d3:5f	0x0800	74 IPv4
39	1.074839	240e:e0:5b52:8e00:8498:dbc7:9b4:598b	240e:58:c000:1000:116:228:111:118	DNS	97 Standard query 0xc70e AAAA gaia.cs.umass.edu
40	1.077986	240e:58:c000:1000:116:228:111:118	240e:e0:5b52:8e00:8498:dbc7:9b4:598b	DNS	150 Standard query response 0xc70e AAAA gaia.cs.umass.edu SOA un
41	1.078825	Dell_8f:bc:b8	Fiberhom_90:d3:5f	0x0800	74 IPv4

查看包含 HTTP 响应消息的第一个字节的以太网帧的内容，如上图所示，74:ec:42:90:d3:5f 是中继路由的地址

```
> Frame 40: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A
v Ethernet II, Src: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f), Dst: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
  v Destination: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      Address: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
      Address: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
```

Task 6

What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

```
> Frame 40: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{CF56413B-5BE1-47
v Ethernet II, Src: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f), Dst: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
  v Destination: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      Address: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

如上图所示，目的地址是我的以太网地址

Task 7

Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

```
> Frame 40: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A
v Ethernet II, Src: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f), Dst: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
  v Destination: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      Address: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
      Address: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
```

如上图所示，16 进制值：0x86dd 代表上层协议是 IPV6，因为地址解析协议（Address Resolution Protocol）在 IPv6 中已不再适用，并被邻居发现协议（NDP）所替代，**所以接下来把自己抓到的包换为作者抓的包**，以免影响实验

Task 8

How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
```

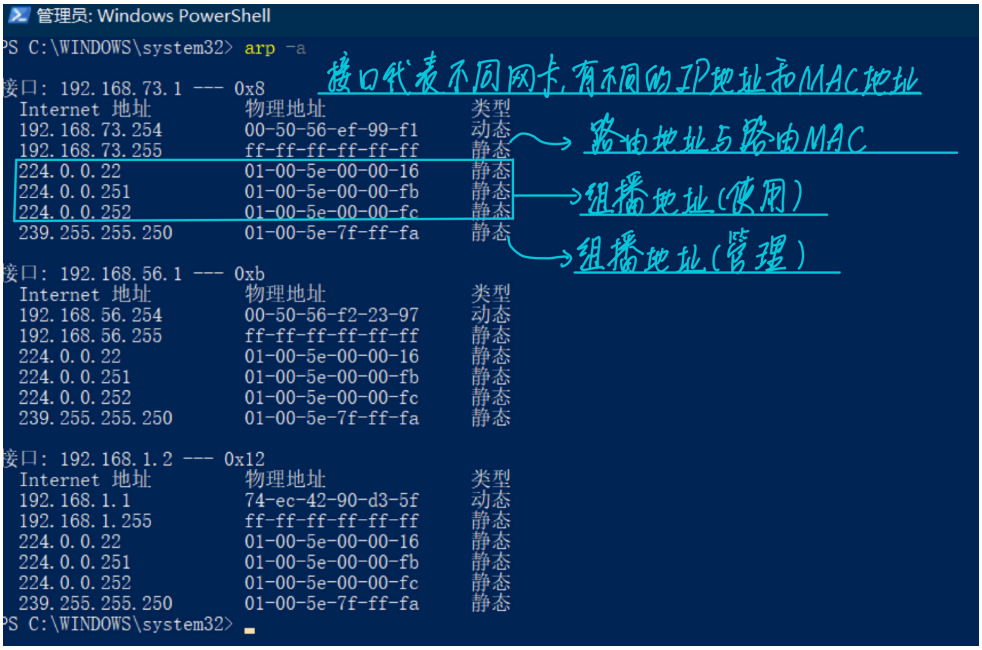
如上图所示，ASCII“O”出现为止，有 $16+16+16+4=52$ 个字节

Part 4

实验过程: 地址解析协议

Task 9

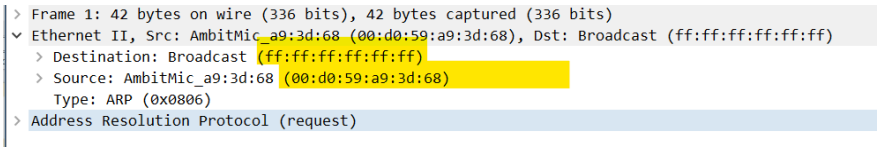
Write down the contents of your computer’s ARP cache. What is the meaning of each column value?



理论上还有一个 Internet 地址:255.255.255.255　物理地址:$ff-ff-ff-ff-ff-ff$ 的广播地址，但是不知道为什么在我的物理机上没有显示

Task 10

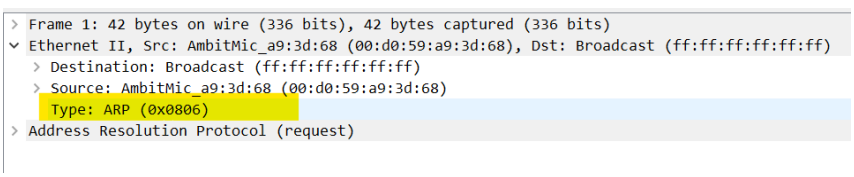
What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?



如上图所示，源：00:d0:59:a9:3d:68 目的地址：$ff-ff-ff-ff-ff-ff$

Task 11

Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



于 ARP 协议相对应，16 进制值：0x0806

Task 12

Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

(a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

(b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

(c) Does the ARP message contain the IP address of the sender?

(d) Where in the ARP request does the "question" appear -the Ethernet address of the machine whose corresponding IP address is being queried?

(a) 如下图所示，查询了 ARP 协议的数据报节构，操作码前共 20 字节

长度(位)	48	48	16	16	16	8	8	16	48	32	48	32
数据类型	目标以太网地址	源以太网地址	帧类型	硬件类型	协议类型	硬件地址长度	协议地址长度	操作码	源硬件地址	源协议地址	目标硬件地址	目标协议地址
组成	14字节 以太网首部								28字节 ARP请求/应答			

(b) 如下图所示，操作码值为 1

```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
```

(c) 包含发送者 IP 地址，地址为路由地址 192.168.1.1

```
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

(d) 这帧消息中已经显示“broadcast”，目的以太网地址为全 0

Task 13

Now find the ARP reply that was sent in response to the ARP request.

(a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

(b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

(c) Where in the ARP message does the "answer" to the earlier ARP request appear –the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

(a) 同 Task12(a)，20 字节

(b) 如下图所示，操作码值为 2

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

(c) 包含发送者 IP 地址，地址为路由地址 192.168.1.1

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

Task 14

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
```

Source：路由地址 00:d0:59:a9:3d:68 Target：PC 端地址 00:06:25:da:af:73

Task 15

Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by

the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 –another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

理由如下：因为 ARP 进行了信息广播（broadcast），所有该网段内所有的端口均可收到，但是广播的回复是单播的，只有请求者才能接收到回复信息，因此无法获取另外一台电脑的请求报文。

Part 5

附加题

Task Ex-1

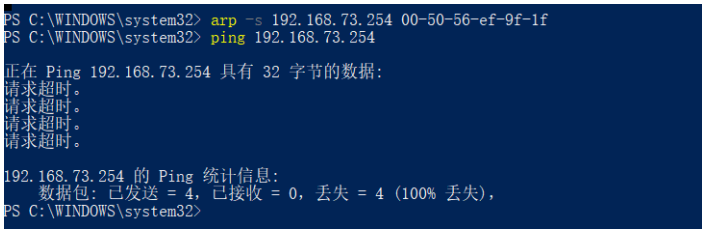
The arp command:

$$arp - sInetAddrEtherAddr$$

allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

使用我的 web 服务器地址 192.168.73.254 来测试

清除所有 arp 缓存后为其添加了一个显然错误的物理地址



如上图所示，数据报显然没有到达目标服务器而死亡了

Task Ex-2

What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

查询了一下 Microsoft 的官方文档，默认的有效时间在 15 秒（30 × 0.5 秒）和 45 秒（30 × 1.5 秒）之间

详细信息

在 Windows Vista 中，ARP 缓存行为已更改。对于 IPv4 和 IPv6 邻居发现过程，Windows Vista 中的 TCP/IP 堆栈实现均符合 RFC4861 （IP 版本 6 [Ipv6]的邻居发现协议）。

ArpCacheLife 和 ArpCacheMinReferencedLife 注册表项确定 ARP 缓存在 Windows XP 和 Windows Server 2003 中的维护方式 。这些注册表项不再适用于 Windows Vista。

在新的 Windows Vista TCP/IP 堆栈实现中，如果邻居缓存中没有匹配的项，主机会创建邻居缓存项。ARP 缓存条目为 IPv4 是邻居高速缓存项的示例。在相邻缓存中成功创建项之后，如果该项符合特定条件，则其可能更改为“Reachable”状态。如果项是以“Reachable”状态，Windows Vista TCP/IP 主机不发送 ARP 请求到网络。因此，Windows Vista TCP/IP 主机使用缓存中的信息。如果不使用某个项，并且其保持于“Reachable”状态的时间大于其“Reachable Time”值，该项将更改为“Stale”状态。如果某个项处于“Stale”状态，Windows Vista TCP/IP 主机必须发送一个 ARP 请求，才能访问该目的地。

“访问时间”值的计算公式如下：

Reachable Time = BaseReachable Time × （MIN_RANDOM_FACTOR 和 MAX_RANDOM_FACTOR 之间的随机值）

RFC 提供以下的计算的结果。

BaseReachable 次	30000 毫秒 (ms)
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

因此，“到达时间”值在某处是 15 秒 （30 × 0.5 秒） 和 45 秒 （30 × 1.5 秒） 之间。如果条目不用于之间 15 到 45 秒钟的时间，将更改为“过时”的状态。然后，主机必须发送 ARP 请求 ipv4 网络在任何 IP 数据报发送到该目标。

我自己在本地进行了检验