电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302009

姓 名 陆圣珩

（实验） 课程名称 计算机网络

理论教师 刘梦娟

实验教师 刘梦娟

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学号：2017221302009 指导教师：刘梦娟**

**实验地点：信软楼西305 实验时间：2018.06.14**

**一、实验名称：数据链路层协议验证实验**

**二、实验学时：2学时**

**三、实验目的：**

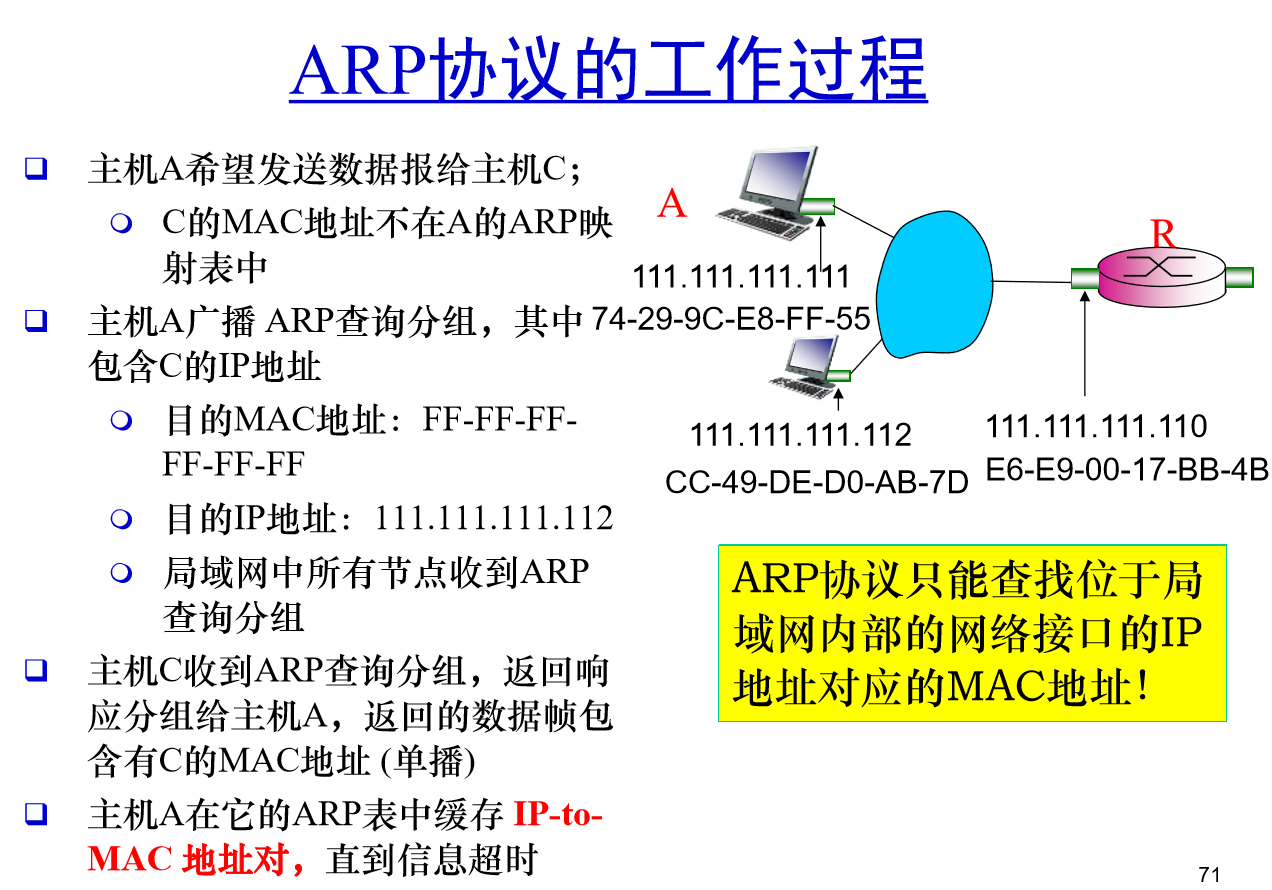
掌握以太网协议(Ethernet)的基本封装格式，掌握ARP协议的工作原理和封装格式。

**四、实验原理：**

**以太网协议的报文格式**



**ARP协议的工作过程**



**五、实验内容：**

实验内容主要包括两个部分：

第一部分是捕捉和分析以太网数据帧；

第二部分是地址解析协议(ARP)。

**六、实验器材（设备、元器件）：**

台式机，软件Wireshark

**七、实验步骤：**

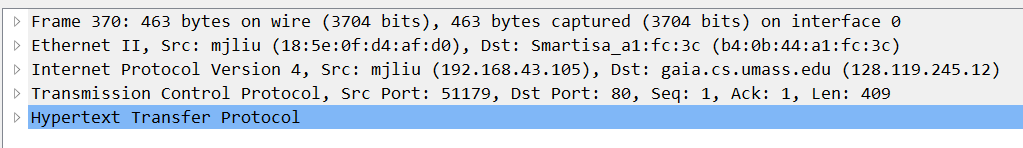
**实验1：以太网数据帧的捕获和分析**

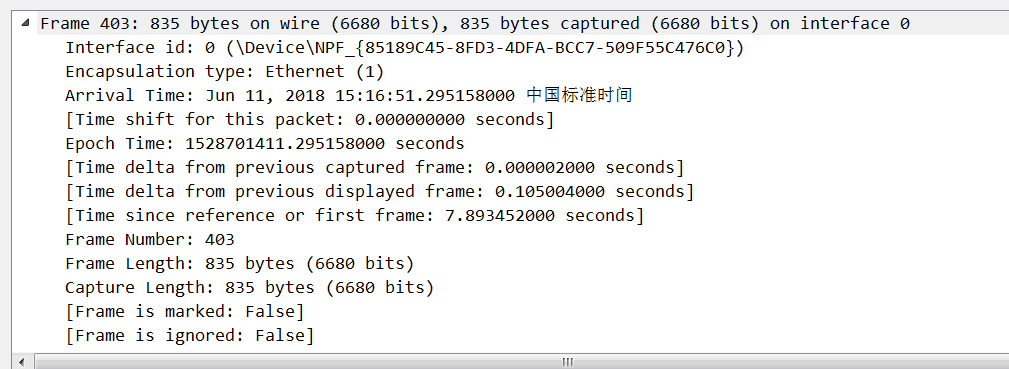
具体步骤可参考英文指南

贴截图并简单说明

这里涉及的是访问一个web网站

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>





**实验2：ARP协议分析**

在这个实验中，我们将分析观察到的ARP协议的行为。首先在控制台界面查看你本机的ARP缓存表。说明每个行的含义。



* Clear your ARP cache, as described above.（清除ARP缓存表）

C:\Users\Administrator\AppData\Roaming\Tencent\Users\4975870\QQ\WinTemp\RichOle\A9E{H~F@U(`I0ECH(7C{`ZY.png

* Next, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select Tools->Clear Recent History and check the box for Cache. For Internet Explorer, select Tools->Internet Options->Delete Files.
* Start up the Wireshark packet sniffer
* Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html Your browser should again display the rather lengthy US Bill of Rights.
* **Stop Wireshark packet capture**. Again, we’re not interested in IP or higher-layer protocols, so change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the IP box and select OK. You should now see an Wireshark window that looks like:

**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

针对捕获的以太网数据帧，回答以下问题：

* What is the 48-bit Ethernet address of your computer? （你的计算机的MAC地址是多少？）

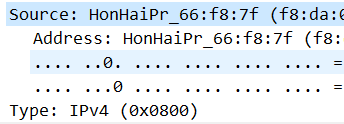
回答：

* 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.]

回答：不是请求的网站的服务器的mac，是默认网关的mac

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

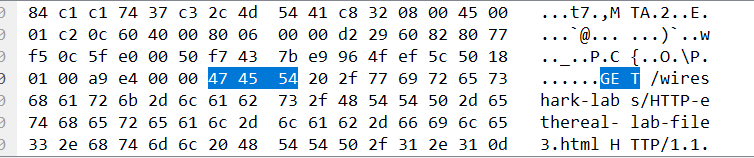
回答： 代表网络层IP协议



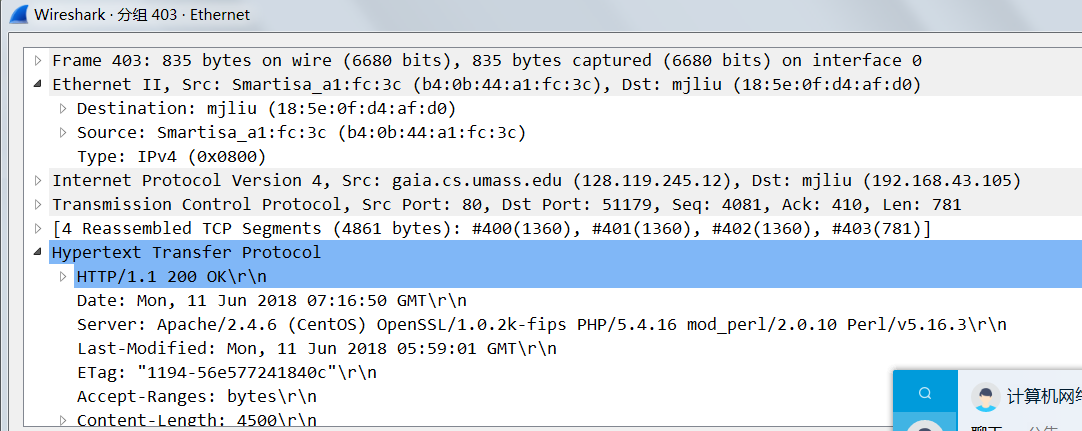
* How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

回答：

第55个字节



**基于HTTP响应消息的以太网数据帧包含的内容，回答以下问题：**



* 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?

回答：

不是，是网关的mac地址

* What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer? （在数据帧中以太网的目的地址是？这是你的计算机的以太网地址吗？）

回答：

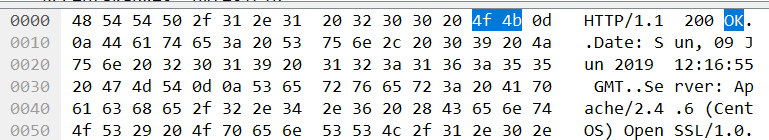
是的

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

回答：IP协议

* 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?

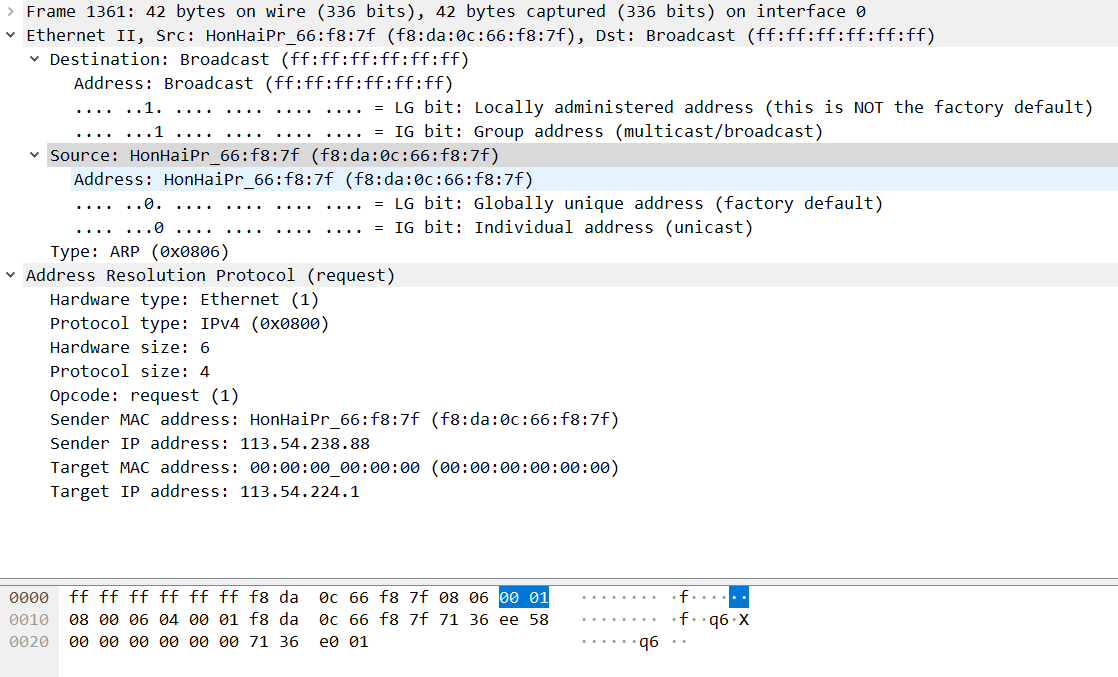
回答：



第14个字节

针对ARP协议的分析，回答以下问题：





* What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? (在包含ARP请求的以太网数据帧中，源、目的地址的16进制的值是多少？)

回答：





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

回答：  ARP

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

回答：54

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

回答： 

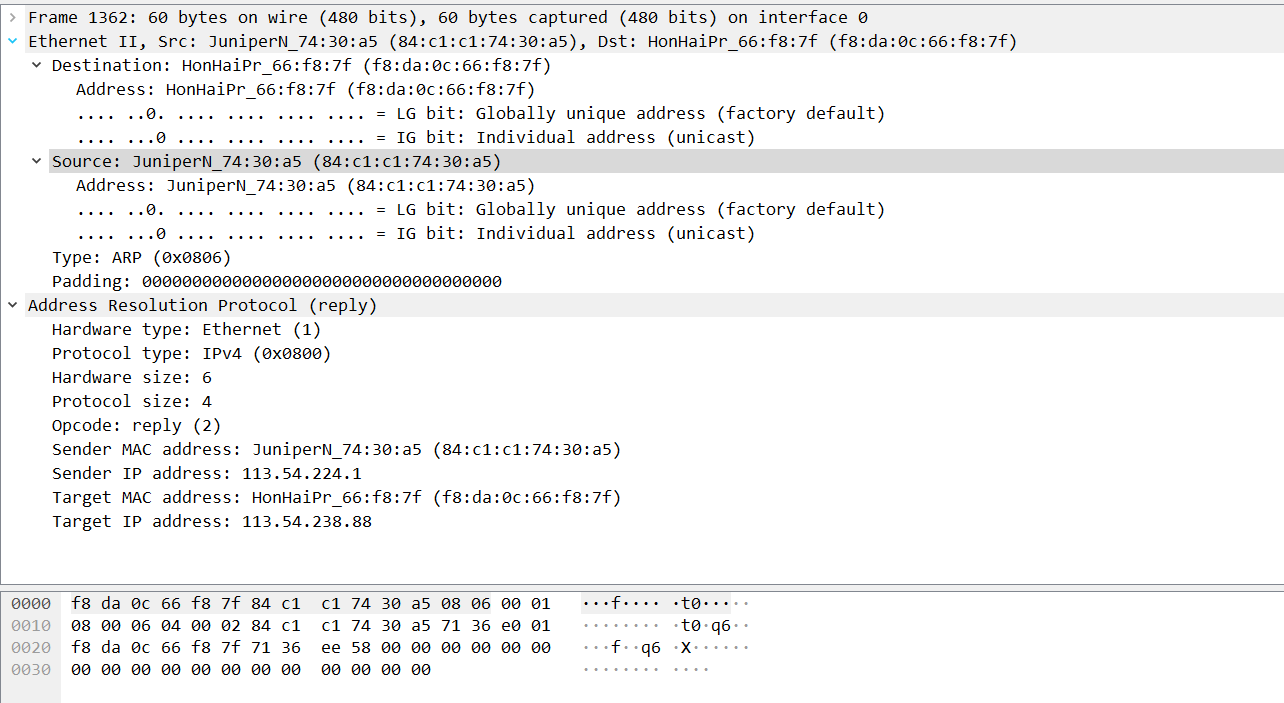
* + Does the ARP message contain the IP address of the sender?

回答：不包括

* + Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

回答：

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

* + How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

回答：54

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

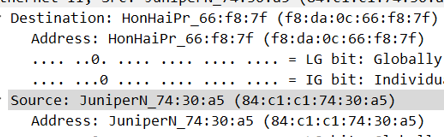
回答： 

* + 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?

回答：

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

回答：



**九、总结及心得体会：**

本次实验主要针对ARP与以太网，在实验方法上同前几次一样，经过几次是尝试已经可以熟练使用wireshark这一工具进行实验。本次实验在理解了计网关于ARP与以太网相关知识后没有太大难度，但在理解英文题目时有一些困难。

**十、对本实验过程及方法、手段的改进建议：**

**无**

**报告评分：**

**指导教师签字：**