School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | ARP Lab |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners | None |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019-5-28 | Lab Location | CUC #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

1. Understand the request response mechanism of ARP protocol
2. ARP cache management
3. Analysis Ethernet protocol

**Section II Methods & Materials**

A computer that connects to the campus network.

IE browser

Wireshark

**Section III Procedure & Results**

Describes ACTUAL process, especially changes from planned method.

|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form  1. First, 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 2. Enter the following URL into your browser <http://eteaching.cuc.edu.cn/computernetworks/Labs/HTTP-Wireshark-file3.html> Your browser should display the rather lengthy US Bill of Rights. 3. Stop Wireshark packet capture. First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to eteaching.cuc.edu.cn, as well as the beginning of the HTTP response message sent to your computer by eteaching.cuc.edu.cn. You should see a screen that looks something like this (where packet 4 in the screen shot below contains the HTTP GET message) 4. Clear your ARP cache, arp -d 5. 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. 6. Start up the Wireshark packet sniffer 7. Enter the following URL into your browser http://eteaching.cuc.edu.cn/computernetworks/Labs/HTTP-Wireshark-file3.html Your browser should again display the rather lengthy US Bill of Rights. 8. 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. |

**Section IV Discussion**

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout1 to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

1. What is the 48-bit Ethernet address of your computer?



0c:8b:fd:cc:a5:6a

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of

eteaching.cuc.edu.cn? (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.]

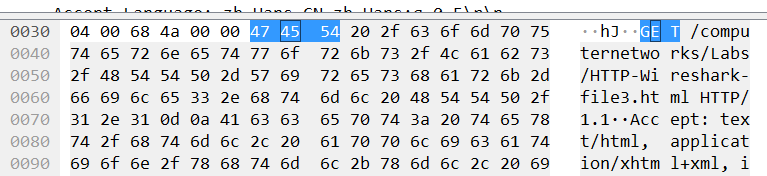


NO, it’s the MAC address of the host's default gateway

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

It’s 0x0080,on behalf of IP protocol

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



The 55th byte.

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

5. What is the value of the Ethernet source address? Is this the address of your computer, or of eteaching.cuc.edu.cn (Hint: the answer is no). What device has this as its Ethernet address?



It’s 28:8a:1c:b0:37:cc, it’s the MAC address of the host's default gateway.

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



Yes, it is.

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

It’s 0x0080,on behalf of IP protocol

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?



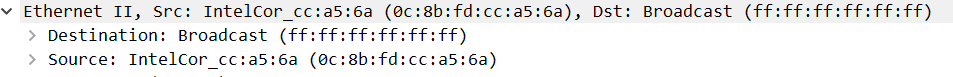
The 68th byte.

In the example above, the first two frames in the trace contain ARP messages (as does the 6th message).

The screen shot above corresponds to the trace referenced in footnote 1.

Answer the following questions:

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



Source address：0c:8b:fd:cc:a5:6a

Destination addresses：ff:ff:ff:ff:ff:ff

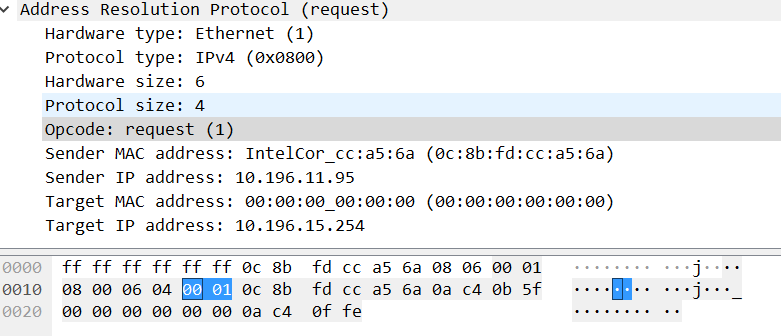
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



0x0806,on behalf of ARP protocol

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?



From 21th byte

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?

0x0002(reply)

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

Yes, it contains 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?

All of destination addresses are 00:00:00:00:00:00 when inquiring

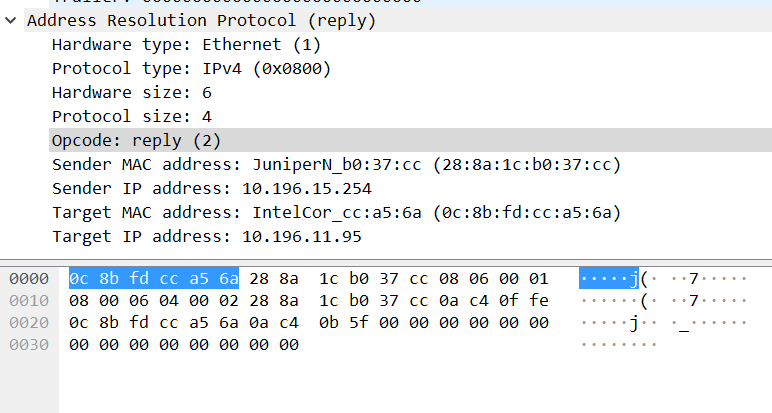
13. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode

field begin?

21 byte

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?

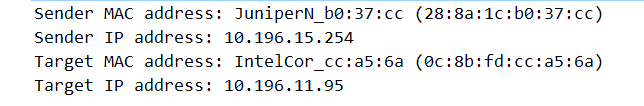


0x0002(replay)

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?

23-28 byte

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



Source address: 28:8a:1c:b0:37:cc

Destination address: 0c:8b:fd:cc:6a

15. Open the ethernet-ethereal-trace-1 trace file in http://eteaching.cuc.edu.cn/computernetworks/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?

The network device corresponding to this IP is not on or does not exist

Extra Credit

EX-1. The arp command: arp -s InetAddr EtherAddr

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?

Answer: The packet goes out and no reply comes back

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.