**WireShark - Packet capture experiment**

**Name: 杨烨**

**Student ID: 2022280380**

|  |
| --- |
| **The following are the questions and answers of the Ethernet protocol analysis experiment:**  Q1: What is the 48-bit Ethernet address of your computer?  Q2: 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.]  Q3. Give the hexadecimal value for the two-byte Frame type field. What upper layer  protocol does this correspond to?  Q4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?  Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.  Q5. 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?  Q6. What is the destination address in the Ethernet frame? Is this the Ethernet address  of your computer?  Q7. Give the hexadecimal value for the two-byte Frame type field. What upper layer  protocol does this correspond to?  Q8. 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?  **(1) Packet capture for file ethernet-ethereal-trace-1:**  **Answer the question:**  A1: The MAC address of my computer is 00:06:25:da:af:73;    A2: The destination MAC address of an Ethernet frame is 00:d0:59:a9:3d:68; Not gaia.cs.umass.edu's Ethernet address, which is my computer's virtual routing address;  A3: IPV4: (0x0800);  A4： From byte 14 to byte 54, total54-14=40 bytes: (G is in the 54th byte)    A5：The Ethernet source address is 00:d0:59:a9:3d:68；No, it's not the address of my computer; Is the virtual routing address of my computer；    A6：The destination address is the Ethernet address of my computer, which is 00:06:25:da:af:73；    A7：IPV4: (0x0800);  A8：489 + 13 = 501 bits.     1. **For http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html caught:**   **Answer the question:**  A1: The MAC address of my computer is 70:a8:d3:92:d4:66；    A2：The destination MAC address of an Ethernet frame is 34:58:40:35:72:16; ; Not gaia.cs.umass.edu's Ethernet address, which is my computer's virtual routing address;  A3：IPV4: (0x0800);    A4：From byte 14 to byte 54, total54-14=40 bytes: (G is in the 54th byte)  A5：The Ethernet source address is 34:58:40:35:72:16；No, it's not the address of my computer; Is the virtual routing address of my computer；  A6：The destination address is the Ethernet address of my computer, which is 70:a8:d3:92:d4:66；  A7：IPV4: (0x0800);  A8: 489 + 13 = 501 bits. |
| **The following are the questions and answers of ARP protocol analysis experiment:**  Q1：What are the hexadecimal values for the source and destination addresses in the  Ethernet frame containing the ARP request message?  Q2: Give the hexadecimal value for the two-byte Ethernet Frame type field. What  upper layer protocol does this correspond to?  Q3：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?  Q4：What are the hexadecimal values for the source and destination addresses in the  Ethernet frame containing the ARP reply message?  **(1) Packet capture for file ethernet-ethereal-trace-1:**  A1: Source: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)  Destination: Broadcast (ff:ff:ff:ff:ff:ff)    A2: Type: ARP (0x0806)    A3:  A)ARP request: 21 bytes:    B)the value of the opcode field within the ARP-payload part of the  Ethernet frame in which an ARP response is made is 1;    C)As shown in the picture box below:  1703562850260  A4: Destination: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)  Source: LinksysGroup\_da:af:73 (00:06:25:da:af:73)     1. **Packet capture for dhcp-ethereal-trace-1:**   A1: Source: LinksysGroup\_da:af:73 (00:06:25:da:af:73)  Destination: Broadcast (ff:ff:ff:ff:ff:ff)    A2:Type: ARP (0x0806)  A3:  a)ARP request: 21 bytes:    B)the value of the opcode field within the ARP-payload part of the  Ethernet frame in which an ARP response is made is 1;    C)As shown in the picture box below:    A4: Destination: LinksysGroup\_da:af:73 (00:06:25:da:af:73)  Source: Dell\_4f:36:23 (00:08:74:4f:36:23) |