**Wireshark Lab 5: Ethernet and ARP**

**Group Details:** Shayshu NR – 1005035196, Johnathan Yan - 1004745476

**Mark:**



|  |  |  |
| --- | --- | --- |
|  | **Question** | **Answer** |
| 1 | What is the 48-bit Ethernet address of your computer? | The source address is 00:d0:59:a9:3d:68 |
| Annotated Screenshot (if needed) |  | |
| 2 | What is the 48-bit destination address in the Ethernet frame?  What device has this as its  Ethernet address? | The destination address is 00:06:25:da:af:73. This is the address of a LinkSys router. |
| 3 | Give the hexadecimal value for the two-byte Frame type field.  What upper layer protocol does this correspond to? | The frame type is 0x0800, which corresponds to the IP protocol, (in particular IPv4). |
| 4 | How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? | The G appears 54 bytes into the frame. 14 bytes for Ethernet frame, 20 bytes for IP header, and 20 bytes for the TCP header. |
| Annotated Screenshot (if needed) |  | |
| 5 | What is the value of the Ethernet source address?  What device has this as its Ethernet address? | The source address is 00:06:25:da:af:73. This is the ethernet address of the LinkSys router. |
| Annotated Screenshot (if needed) |  | |
| 6 | What is the destination address in the Ethernet frame?  Is this the Ethernet address of your computer? | The destination address is 00:d0:59:a9:3d:68. This is the ethernet address of my computer. |
| 7 | Give the hexadecimal value for the two-byte Frame type field.  What upper layer protocol does this correspond to? | The frame type is 0x0800, which corresponds to the IP layer, in particular IPv4. |
| 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? | Again, the O appears 67 bytes into the frame. 14 bytes for the Ethernet header, 20 bytes for the IP header, and 20 bytes for the TCP header, then 14 bytes offset into the segment. |
| Annotated Screenshot (if needed) |  | |
| 9 | Write down the contents of your computer’s ARP cache.  What is the meaning of each column value? | The first column is the IP address, the next column is the corresponding physical address (MAC address), and the last column is the type that indicates the protocol type (Static, dynamic, etc…) |
| Annotated Screenshot (if needed) |  | |
| 10 | What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? | The source address is 00:d0:58:a9:3d:68, the destination address is the broadcast address ff:ff:ff:ff:ff:ff. |
| Annotated Screenshot (if needed) |  | |
| 11 | Give the hexadecimal value for the two-byte Ethernet Frame type field.  What upper layer protocol does this correspond to? | The code is 0x0806, which indicates that the layer protocol is ARP. |
| 12.a | How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? | The opcode fields starts 20 bytes into the ARP header. |
| Annotated Screenshot (if needed) |  | |
| 12.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? | The value is 1 |
| Annotated Screenshot (if needed) |  | |
| 12.c | Does the ARP message contain the IP address of the sender? | Yes, in this case it’s 192.168.1.105 |
| 12.d | Where in the ARP request does the “question” appear – the Ethernet  address of the machine whose corresponding IP address is being queried? | The question is the target MAC address. So, the sender is asking for the MAC address of the device with the target IP address of 192.168.1.1. |
| 13.a | How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? | Same as the request, the opcode begins at byte 20. |
| Annotated Screenshot (if needed) |  | |
| 13.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? | The value is 2 |
| 13.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? | The answer is the now filled in Sender MAC address, 00:d0:59:a9:3d:68 |
| 14 | What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? | Source (Gateway): 00:06:25:da:af:73  Destination (my computer): 00:d0:59:a9:3d:68 |
| Annotated Screenshot (if needed) |  | |
| 15 | Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace? | There is no reply because the packet has not reached the intended target yet. This packet shows up on wire shark because ARP requests are broadcasted to everyone, but the reply is sent directly to the sender. |

