Joshua Larkin

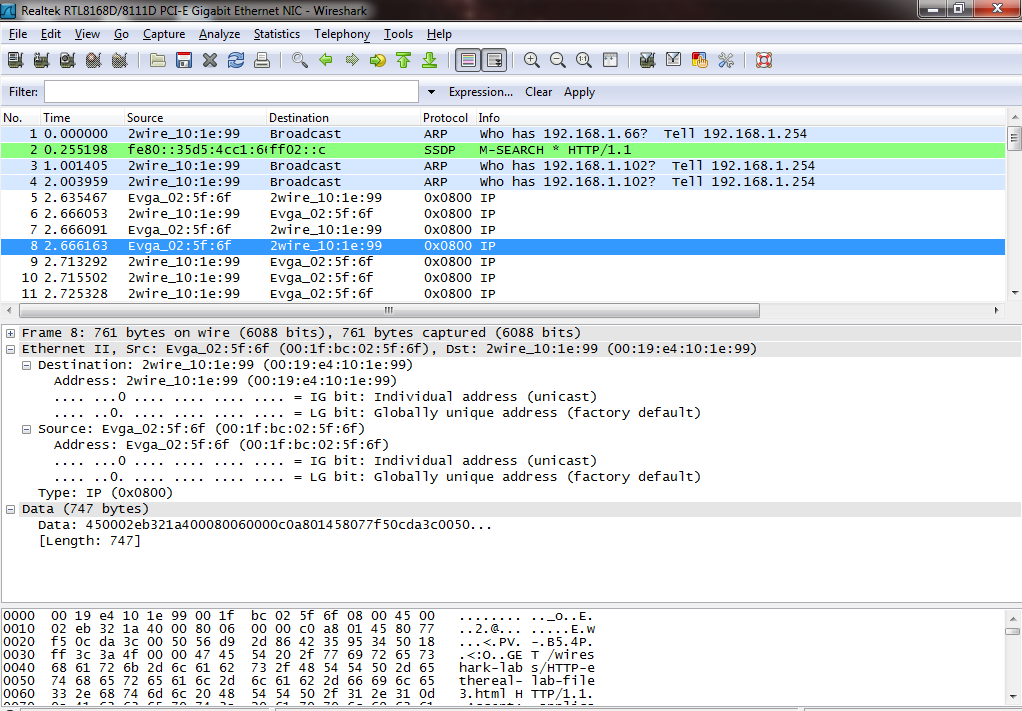
CSC 251

Net-Centric

Spring 2012

**Wireshark Lab 7: Ethernet and ARP**

**1. Capturing and analyzing Ethernet frames:**

****

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

*00:1f:bc:02:5f:6f.*

**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.]**

*00:19:e4:10:1e:99. This is the address for the home router that the host computer is connected to.*

**3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

*0800.*

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

*55 bytes.*

**5. What is the hexadecimal value of the CRC field in this Ethernet frame?**

*0d0a0d0a.*

**6. 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?**

*00:19:e4:10:1e:99. This is the address for the home router that the host computer is connected to.*

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

*00:1f:bc:02:5f:6f. This is the ethernet address of my computer.*

**8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

*0800.*

**9. 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?**

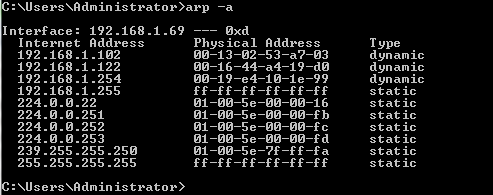
*52 bytes.*

**10. What is the hexadecimal value of the CRC field in this Ethernet frame?**

*0d0a0d0a.*

**2. The Address Resolution Protocol:**

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

****

*Each value in the left column is an IP address on my local area network. Each value in the middle column is the corresponding MAC address.*

**12. What are the hexadecimal values for the source and destination addresses in the**

**Ethernet frame containing the ARP request message?**

*Source address: 00:1f:bc:02:5f:6f.*

*Destination address: ff:ff:ff:ff:ff:ff.*

**13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

*0806. The bit flags represent a multicast (broadcast) that is sent to the subnet and not the internet.*

**14. Download the ARP specification from ftp://ftp.rfc-editor.org/innotes/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?**

*21 bytes.*

**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?**

*0001.*

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

*Yes. It is 192.168.1.69*

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

*In the Target IP address: 192.168.1.69*

**15. 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 bytes.*

**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?**

*0002.*

**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?**

*In Sender MAC address: 2wire\_10:1e:99 (00:19:e4:10:1e:99)*

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

*Source address: 00:19:e4:10:1e:99*

*Destination address: 00:1f:bc:02:5f:6f*

**17. 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 indiated 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?**

*Because this host computer is not the router that maintains the ARP table and therefore does not give the sender an answer. Only the router running the network will respond to the ARP request.*