Networks Wireshark Lab 3

Ethan Fison and Zan Montieth

A)

1. (a0:99:9b:19:ff:91)
2. (00:00:0c:9f:f2:54). This is not the router for the umass website, but rather the first-hop router on the path, quite possibly the router we are currently connected to at MSU.
3. IP: (0x0800)
4. The asccii representation of the word GET is 47:46:54 the first character of the command is 52 bytes from the start of the internet frame.

B) ARP queries are sent in broadcast frames because the host does not know which adapter is linked to the IP address needed. When responding, the sender does not need to do this, as the adapter address for the recipient will be known.

C)

1. from the wireshark lab a. The opcode field begines 20 bytes from the start of the ethernet frame. b) the opcode field is the hax value 0x0001 when an ARP request is made c) yes the message contains the IP of the sender d) The "question" appears when the target mac address is set to 00:00:00:00:00:00

2. a) The opcode field begines 20 bytes from the start of the ethernet frame.

   b) the opcode field is the hax value 0x0002 when an ARP reply is made

   c) the "answer" to the "question" shows up in the Sender MAC Address field

3. The source is 00:de:d4:f2:d7:88 and the destination is 00:95:f0:2a:f8:2a

4. There is no reply in the trace, because we are requesting data from an invalid sender.

D) For macOS, a dynamically-created ARP table is used to create routes on demand. For the entries in this table, the BSD caching behaviour is used. From the BSD ARP manpage: "These routes time out periodically (normally 20 minutes after validated; entries are not validated when not in use)"