**CS 6043/5143: Computer Networking**

**FALL 2019**

**PROJECT 4**

**Given: Nov. 27, 2019**

**Due: Dec. 06 (Friday), 2019 (NO LATER THAN 11:59PM)**

**Submission Instructions:**

1. Submit only on-line files on Blackboard before midnight. No hard copy will be accepted.

2. Wireshark files for this project can be found in the zip file “Project\_4\_Wireshark\_Traces.zip”.

**Total possible points: 10**

**Part I: Ethernet, ARP**

Load the file ‘Eth\_ARP\_project\_4.pcapng’ in Wireshark and answer the following questions. The trace was generated while a web page was accessed (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>). Include screenshots in each case.

[Hint: For some of the questions, it might be helpful to disable IP or higher layer protocols. To do this, go to *Analyze->Enabled Protocols*]

* 1. (1.0 pts) What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? Explain why you answered yes or no.
  2. (1.0 pts) Give the hexadecimal value for the two-byte ‘frame type’ field for frame number 10. What upper layer protocol does this correspond to?
  3. (1.0 pts) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
  4. (1.0 pts) Does the ARP reply message contain the IP address of the requesting host? If yes, what is it?

**Part II: 802.11**

Load the file ‘802.11\_project\_4.pcapng’ in Wireshark. This trace was collected using AirPcap and Wireshark running on a computer in a home network, consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. There are other access points in neighboring houses available as well. The wireless host activities taken in the trace file are:

* The host is already associated with the *30 Munroe St* AP when the trace begins.
* At *t = 24.82*, the host makes an HTTP request to http://gaia.cs.umass.edu/wireshark-labs/alice.txt. The IP address of gaia.cs.umass.edu is 128.119.245.12.
* At *t=32.82, t*he host makes an HTTP request to http://www.cs.umass.edu, whose IP address is 128.119.240.19.
* At *t = 49.58,* the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys\_ses\_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.
* At *t=63.0* the host gives up trying to associate with the *linksys\_ses\_24086 AP,* and associates again with the *30 Munroe St* access point.

Answer the following questions:

* 1. (1.0 pts) What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?
  2. (1.0 pts) What are the intervals of time between the transmissions of the beacon frames the *30 Munroe St* access point?
  3. (1.0 pts) The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?
  4. (1.0 pts) Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the first-hop router?
  5. (1.0 pts) What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action).
  6. (1.0 pts) Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksys\_ses\_24086* AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49?